SECURING THE HEALTHCARE INDUSTRY

Kady Bird

Matthew Miller

George Mason University

ABSTRACT

Increased digitization of health records and patient data has made the healthcare industry a prime target for hackers and data thieves alike. In an ongoing effort to protect patient and consumer data, the U.S. Department of Health and Human Services created the *Online Breach Portal Reporting Tool* (2009). Meant to increase public trust through transparency in reporting, critics have nicknamed this tool “The Wall of Shame” since it publicly lists organizations who are guilty of data breaches in which 500 or more patient records were compromised. Technology evolves so quickly that companies are often forced to take a reactive approach to security breaches instead of allocating resources toward prevention, resulting in entire industries that are susceptible to data theft. Analysis of the breach portal data helps to reveal information regarding trends, statistics, and general components of security systems that are most susceptible to attack that can be used by healthcare organizations as they develop a more resilient cybersecurity framework.   
 INTRODUCTION

The frequency and scale of data breaches continues to increase across the healthcare sector, revealing patterns and key areas of concern worthy of analysis.  This project aims to produce insights that will assist organizations in establishing a preventative procedural framework to minimize losses and take steps that will more adequately protect their data.  It will also analyze breach data from the Department of Health and Human Services Wall of Shame Breach Portal tool to reveal weak areas that are more susceptible to intrusion. By doing so, we hope to gain insights surrounding these and other similar questions as we seek more adequate solutions for cybersecurity systems in the healthcare industry:

* Discover technologies most susceptible to breaches (laptops, servers, paper records).
* Identify the most common breach attack methods (theft, loss, hacking).
* Identify and discuss notable trends and insights discovered throughout the analysis.

This report will contain several sections, including a discussion the problems faced by the healthcare industry that makes it so attractive to cybercriminals. The report will go on to discuss the problems in more detail and acknowledge potential technical challenges faced during the project. Additional notable research on this topic will be discussed in the related works section, followed by a series of proposed solutions and recommendations.

HIGH LEVEL PROBLEM DEFINITION

As health organizations continue to digitize their operations to meet regulatory requirements and patient demands, the digital landscape continues to expand. Each hospital network around the nation has its own cybersecurity systems in place for protecting patient data, but they are often antiquated in comparison to today’s sophisticated cyber threats. The existence of so many exploitable access points on a broadening attack surface makes successful defense almost impossible. Due to its sensitive nature, data from health organizations is of particular interest to cyber-criminals, making the healthcare sector the leading recipient of hacks and data theft.

DETAILED PROBLEM DEFINITION AND TECHNICAL CHALLENGES

In recent years, large-scale cyber-crime has grown in frequency and sophistication, with each attack compromising a larger number of records than the attack preceding it. It is clear that the complexity and breadth of today’s networks, coupled with growing threat sophistication, have surpassed the ability of most traditional security networks to keep up (Lakahani, 2017).

Cyber-criminals have proven to be adept at staying ahead of traditional protections by constantly evolving their attack methods. Such nefarious technologies are proving to be devastatingly effective, largely because they utilize cutting-edge data science tools capable of evading and exploiting outmoded security infrastructures with ease. Healthcare organizations are often dealing with layered, legacy security systems that are little more than a series of patches that were put into place whenever a prior vulnerability was found. Such systems are easy for even an inexperienced hacker to exploit.

In the area of data protection, the problems faced by the healthcare industry are clear, but the solutions are easier said than done. Today, there are only two methods of successfully defending against data theft. Organizations must either use defense methods that are just as sophisticated as the attacks, or render the data useless from inception by encrypting it.

Without question, encryption is the most desirable method of data protection, but it can be extremely expensive to deploy and quite slow when it comes to decryption (depending on the computer hardware). The issue of speed and efficiency is the primary reason for the lack of use in industries such as healthcare, where time is of the essence on a regular basis.

As time goes on, the amount of data will only continue to grow, but so will the need for enhanced cybersecurity measures meant to protect it. In the absence of encryption, it is critical that health organizations become aware of current threats, constantly update their systems, and deploy defenses that are equipped to protect against these attacks are continuing to grow in scale and sophistication.

RELATED WORKS

The prevalence of data theft and misuse will continue to increase as the globe becomes more connected. This subject has garnered an extraordinary amount of attention from the academic community and cybersecurity firms alike. Much research exists to explore security issues relating to less complicated topics, such as websites or cellular applications, however an often overlooked area of cybersecurity is that of the threats to database storage systems and their servers. This topic is of particular relevance to healthcare, as it is one of the larger underlying problems that contributes to the industry’s increasing attack frequency. Otherwise known as “Big Data,” massive amounts of patient data are stored in cloud platforms becoming targets for thieves who manage to break into the database and skim sensitive information unnoticed. One of the biggest issues facing data security today is the detection of such intrusions or theft to begin with.

        An in-depth look at the purposes of data leak prevention and detection (DLPD) systems is given by Cheng and Lui (2017) in their article *Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions.* The article discusses how such systems are used to identify, monitor and prevent unintentional or deliberate exposure of sensitive information and explains how typical user query profiles are created to help identify database intrusions by alerting the system to atypical query activity (2017). In many cases, this is the only hope of discovering a data breach at all, making it a crucial component of cybersecurity software packages that health organizations could benefit from using today, as opposed to the traditional systems currently in operation.

        If organizations are still not convinced of the severity of data security threats by now, then perhaps some exploration of the financial ramifications is necessary. According to the IBM (2017) *Ponemon Institute Cost of Data Breach Study*, the average cost for each lost or stolen record containing sensitive and confidential information is $141, resulting in an average data breach cost of around $3.4 million dollars. These figures are representative of several industries, including healthcare, and give the reader a better sense of the seriousness of the threat landscape. The study goes on to mention that there has been a decline in overall cost due to increased preventative efforts being made by entities, but notes that it is being offset by the increase in the sheer size of data breaches. The study mentions that the average size of the data breaches in this research increased 1.8 percent to more than 24,000 records (2017). This is of particular relevance to the healthcare sector, which sustained some of the largest data breaches on record leading up to this report, such as the Anthem hack in 2015 where nearly 80 million patient records were stolen (Edwards, 2016). It is disturbing to think that larger and larger breaches continue to occur despite increased prevention efforts.

        Due to the accessibility of large databases by so many people, it seems as if risk can never be completely eradicated. This phenomenon is known as “The Anderson Rule,” which was named after Ross J. Anderson, a Professor of Security Engineering at Cambridge University. In the article *Nine Sacked for Breaching Core ID Card Database* by Porter (2009) Anderson is quoted as saying that “if a large system is designed for ease of access, it becomes insecure; if made watertight, it becomes impossible to use.” Though this statement was made in 2009, it remains just as true today as it did back then and provides the logical basis for today’s security monitoring systems. This is of particular significance to the healthcare industry, since one of the main reasons for the increase in data breaches is that too many people are able to access the data, setting the stage for any number of breaches to occur.

The ultimate struggle of cybersecurity teams everywhere involves making sure that the people who need access to the data can easily get it, while also keeping the data safe. It sounds simple, but as discussed throughout Ullah and Babar’s (2018) article *Architectural Tactics for Big Data Cybersecurity Analytic Systems,* it is anything but. The article mentions that it is crucial for security analytic systems to achieve the required balance between performance, accuracy, and reliability, but acknowledges that this may be particularly difficult in certain industries, such as healthcare. The inherent need for data to be accessible by a large number of users creates persistent opportunities for data to be harvested by any number of nefarious persons or entities. The article provides a broad discussion about how various analytic methods can be put into place that would ultimately allow for data to be accessed easily, but also monitored for intrusion at the same time.

TENTATIVE PROPOSED SOLUTION

To implement a successful cybersecurity program, companies must be willing to invest in time, technology and human capital. Organizations must take a proactive, risk-based approach to their information protection systems by going the extra mile to understand the data that they hold and generate, as well as the risks associated with it. Once this has been accomplished, then the most appropriate data protection methods can be chosen.

Companies must first create a structured environment for new and existing data in their platform, hiring qualified talent who can begin the task of auditing, categorizing, and cataloguing it; all crucial steps of any security plan. Once a company truly understands their data, they will be better equipped to recognize malicious data, or data that requires different security measures due to its sensitive nature. At this point, the organization will be in a better position to make choices on monitoring systems or software products.

Monitoring for intrusion is one of the most fundamental components of a modern security system. Responsible teams and management will need a one-stop, easy-to-use access point where they can monitor for threats and malicious activity in real-time. An essential tool for accomplishing this is a cybersecurity dashboard. Certain dashboards are better suited for certain organizations depending upon the type of data that is collected or generated, and how it is stored. A cybersecurity dashboard will focus on a few general areas that pertain to the organization and their current risk profile. Organizations may wish to see information pertaining to current threats and risks, live intrusion monitoring, incident statistics, compliance with any adopted frameworks (such as the NIST framework) and general housekeeping items, such as training opportunities for personnel.

Finally, companies must realize that data protection is an ongoing process that requires constant upkeep and attention. Companies who will win today’s cyber battles are those who choose to take a more holistic approach to their security by dedicating the time and resources toward developing a robust and comprehensive security platform capable of sustaining a diverse range of attacks.

REFERENCES

Cheng, L., Lui, Y.. (2017). Enterprise Data Breach: Causes, Challenges, Prevention, and Future

Directions. *Wiley Online Library*. www.doi.org/10.1002/widm.1211.

Edwards, B.. (2016). Hype and Heavy Tails: A Closer Look At Data Breaches. *Journal of*

*Cybersecurity, 2(1), 3-14.* doi.org/10.1093/cybsec/tyw003

IBM, Inc. (2017). *Ponemon Institute* *2017 Cost of Data Breach Study: United States.* Retrieved

from https://www.ibm.com/security/data-breach

Lakhani, A.. (2017). The Future of Cybersecurity Part II: The Need for Automation. *CSO:*

*Interconnecting Business & Cybersecurity.* Retrieved from https://www.csoonline.com/article/3235945/

Porter, H.. (2009). Nine Sacked for Breaching Core ID Card Database. *The Guardian.*

Retrieved from https://www.theguardian.com/commentisfree/henryporter/2009/aug/10/id-card-database-breach

Ullah, F., Babar, M. A.. (2018). *Architectural Tactics for Big Data Cybersecurity Analytic*

*Systems: A Review, 1-48.*

Various. (2009). Department of Health and Human Services. HHS Breach Portal. *Office for Civil*

*Rights.* Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach\_report.jsf