Optimizing Cybersecurity Program - Evidence from Data Breaches in Healthcare

Anantha Narayana Vasishta  
Management Information Systems  
State University at Buffalo  
Buffalo, USA  
avasisht@buffalo.edu

Manish Gupta  
Management Information Systems  
State University at Buffalo  
Buffalo, USA  
mgupta3@buffalo.edu

Sameer Kumar Misra  
Management Information Systems  
State University at Buffalo  
Buffalo, USA  
smisra5@buffalo.edu

Pavankumar Mulgund  
Management Information Systems  
State University at Buffalo  
Buffalo, USA  
pmulgund@buffalo.edu

Raj Sharman  
Management Information Systems  
State University at Buffalo  
Buffalo, USA  
rsharman@buffalo.edu

Abstract—The problem of security is on the rise over the years in healthcare domain. One of the main challenges that senior management of a healthcare company faces today is to optimize the security spending and to derive the maximum value from it. With limited security budget for security programs, organizations strive to optimize their security program. There are new threats evolving around us, even as companies continue to invest in various controls. This research studied healthcare data breaches of 2016, to analyze and understand which controls could have been prevented or mitigated the impact of the breach. Based on some breached data records being breached, the controls identified are prioritized. The companies can compare their security program with our prioritized list of controls and optimize their security program. In case the company has already invested in a specific control identified by us, they can invest in other controls from the identified prioritized list. By doing so, security managers can benchmark and optimize their security program. This paper aims to present a list of critical controls that can be used by CISO or security managers to channel the security investments to receive the most risk reduction from each dollar spent on controls.

Keywords—Enterprise Cyber Risk Management, Information Security Investments, Healthcare Data breaches, Security controls, security program

I. INTRODUCTION

Over the years, the problem of risks associated with IT security and breaches have caused sleepless nights to CISOs of large organizations. As more and more incidents of breaches are being reported, there has been some serious focus on security programs within the organizations. Organizations have dedicated teams to look at the vulnerabilities, controls, and threats to safeguard their IT systems from attacks. According to the Gartner, current threat and vulnerability management have proven to be ineffective [1]. Old vulnerabilities continue to be exploited, as shown in recent breaches. With all disclosed vulnerabilities open in public for the exploit, there are few who are currently being exploited. These exploited vulnerabilities might be available within our organization’s environment. So, the organization must prioritize and address these vulnerabilities through controls first. With limited budget allocated for security and controls, the main challenge of the CISO is to decide where he needs to allocate his funds so that he can get maximum value out of his investment. According to IBM X-Force/Analysis by Gartner research, even though organizations invest in security controls every year, there has been an increasing trend in some breaches and threats. As companies keep working on controls to address these vulnerabilities new incidents and breaches occur. According to the Gartner report, an average number of days between a vulnerability being announced and it being exploited has reduced from 45 days to 15 days between 2006 and 2015 [2][7]. In the recent times, there has been a steady increase in the number of data breaches reported in the healthcare sector; second to the financial sector and exposure to PHI and PHI contribute to 28.7% and 27.5% of the data breaches. Due to HIPAA regulations, Healthcare companies are obligated to report incidents, and authentic breach data are published in OCR for the public to access. Moreover, healthcare data is quite sensitive, and there is a need for enhanced measures to secure patients’ PHI [3]. For these reasons, we focus to restrict our study to healthcare domain as we have full real-world access to all the healthcare data breaches. In this paper, we analyze all the 226 investigated and closed data breaches published by OCR for the year 2016. Based on...
data report, we collected various parameters like covered entity type, number of data records breached, type and location of the breach, internal or external attacker, involvement of Business associate in the breach, type of data breached, Motive of the attack, control category which could have prevented the data breach incident, line of defense category (Preventive, detective or corrective) related to each data breach incident. This will help the CISO to get an idea of designing a cyber-security framework based on recent data breach evidence. This framework gives a complete picture of the various controls which needs to be in place in the organization. This way, companies can identify various vulnerabilities which were unidentified earlier. CISO can compare this prioritized list of controls with the existing controls in place within the organization and decide where they should invest next. As this data is based on evidence from recent healthcare company data breaches, companies can optimally focus their resources on security program and reap out maximum value out of security investment.

This paper is organized into seven sections. Section II provides working definitions of cybersecurity framework, social engineering in the context of security controls. Section III presents the background of the study. Section IV presents the research methodology of the study. Section V contains information of data source and data collection. Section VI is data analysis section where we present the ways data was analysed for developing the framework. Section VII provides the results, conclusions, and recommendations.

II. CYBERSECURITY FRAMEWORK

Cybersecurity Framework is used by companies to apply the principles and best practices of risk management to reduce cyber risk while enhancing its resilience to cyber threats. The security program may call this framework differently. The Cybersecurity framework broadly falls under the four categories. IT Security, Employee awareness, Risk Audit, and Internal policies. These broad categories cover almost all aspect of cybersecurity. IT security mainly deals with the first line of defense using security controls. All the technology controls in place to protect the workstations, networks, and servers play a key role in this. OS patching and critical network security is one of the key components of IT security and are handled by the security staff.

With the increase in breaches via Phishing or social engineering, employee awareness is also an important aspect of cyber security. As people are holding sensitive information about the organization, they are also equally vulnerable to unintentional disclosure of information through malware, phishing or other kinds of social engineering attacks. With a well-designed training awareness and IT security training program to all the employees, companies can reduce the likelihood of data breaches. Employees will be aware of the Do’s and Don’ts. This will drastically reduce the breaches as we see a number of breaches happening in healthcare due to unintentional disclosure of information. IT policies is the 3rd component of the overall Cybersecurity framework in an organization. IT security policies is important because it dictates employees the Do’s and Doesn’t on IT security. When all the IT programs within the organization are in alignment with IT policies, risk and security are embedded within the business processes. This way it ensures the organizations are well secure. IS audit being the third layer of defense. With internal and external IS audit in place, organizations can ensure that all the controls in place are working and serving the control objective.

III. BACKGROUND

The healthcare industry in general has seen a surge in the number of data breaches since 2015. Thousands of PHIs and PIIs of patients have been breached over time. Over the last five years, over 140 million American health information has been reported to have breached. Even though the motivation of the attack can vary depending on the attacker and covered entity control framework; there has been an increase in the PHI and PII theft over the years. Health records are proving out to be more valuable than simple credit card details for various reasons. The healthcare records are not subjected to change easily. PHIs are the basis for credit and insurance fraud. Since the healthcare data is deeply personal and of very high quality, there has been an increased interest among hackers. Healthcare information can also be more valuable to people involved in illegal activities for getting access to illicit drugs or even mere blackmailing. Criminal attacks are up by 125% in healthcare ever since 2010 and now one of the leading cause of the data breach. According to FBI, the increase in the cyber threats in healthcare is because all the sensitive information like PII, PHI and credit card information are all located in one single place, which makes it more attractive to the attacker to monetize it. This trend is common for organizations of all size and scale. No company is spared by cybercriminals. The threat is not just limited to Covered Entities. Business associates are also not spared. Most of the Small and medium businesses have limited processes, personnel, budget, and technology capabilities. Due to this, they are more susceptible to attacks. The only way companies can respond to these threats is by investing in controls to protect the organizations from external threats without ignoring the internal threats. Even though companies have invested heavily in controls, there are still reports of data breaches on a daily basis. It is impossible to have full proof technical control to protect the entire organization from threats. Companies need to figure of a way to protect their data by optimizing their spending by investing on right controls and improving their security program.

IV. RESEARCH METHODOLOGY

The research is based on 226 data breaches in healthcare in the year 2016. This includes all resolved breach reports in the year 2016. Fig 1 shows the research procedure for the paper; how we analyzed the data. The inferences derived in this paper are from the breach data report from Notice to the Secretary of HHS Breach of Unsecured Protected Health Information by U.S. Department of Health and Human Services Office for
Civil Rights (OCR) for the year 2016. The year 2017 was not considered because many of the data breaches reported during this time are still under investigation by US Department of Health and Human Services office for civil rights. Hence, we restricted the study to 2016. As the first step, the healthcare data breach data was obtained from OCR website. All the data breaches were identified, and we read about the details of all 226 data breaches. The OCR website, Privacy rights website and HIPAA journals along with other online newspaper articles were read to understand the nature of the breach [16]. The data read from various sources were coded under various categories as mention in the fig.1. As this study is restricted to the healthcare industry, the nature of data compromised is mainly PHI, and this data is highly sensitive and valuable. [17] [18]

Fig 1. Research Procedure steps

If the number of records breached is high corresponding to each classification mentioned above, it is inferred that the controls which protect such kind of data are of higher priority in the control framework proposed. The number of data records affected by each breach is used to quantify the severity and impact of the breach. The classification under healthcare entity type is important to understand the which healthcare entity the type is most targeted by cyber criminals and to see how important is 3rd party cybersecurity programs based on evidence from past breaches. If a business associate is a place where data breach occurs, it means there is lack of administrative control or poor 3rd party risk management by the organization. With the available information from various sources, the 226 breaches the e also classified based on the type of the breach. Type of breach includes Hacking/IT incident, Loss, Theft, Improper disposal of data and unauthorized disclosure of data. The above classification of the data breach incidents is important to come up with the controls needed to prevent the breach. Based on the report submitted to the OCR and conclusion of our investigation, the controls which could have prevented the breach is identified in hindsight. Fig 2 shows the various broader classification of controls. They are mainly classified as technical controls and non-technical the controls in a broader sense. Under each of these, there are various controls identified. For example, non-technical controls include education and awareness, policy compliance, administrative control, competence, organization culture, etc. To understand the layer of defense, these controls are further classified under preventive, detective and corrective Controls. This classification is very important to relate it to the cost of implementing the control and defining a portfolio of preventive, detective and corrective controls for technical and non-technical controls. To come up with an optimized security investment program, these classifications are important.

Fig 2. Control classification and security investments

V. ABOUT DATA

The 226 data breach records were coded as per various categories mentioned above for analysis. The details of the data breaches [19] were collected from Notice to the Secretary of HHS Breach of Unsecured Protected Health Information by U.S. Department of Health and Human Services Office for Civil Rights (OCR). All the data breaches affecting over 500 individuals or more have been reported here as required by section 13402(e)(4) of the HITECH Act. [20] Out of them, we had very little information available in the public forum to analyze. So we excluded 22 reported breaches by OCR in our analysis. We have used only the breaches which have been completely investigated and cases which are closed by HHS. The raw data from the downloaded from the breach report published by the Office for Civil Rights was extracted and categorized under various parameters to analyze the data more precisely. The description of the breach and the action taken as a response were analyzed in detail to classify under various categories. The company which reported the breach along with various other details like State, covered entity type, number of individuals affected, type of the breach, the location of the breach, the presence of business associate in
the breach incident were extracted from OCR breach report. Form the web description and other published sources, various data was inferred. Based on the type of data being compromised, they were classified under PHI, PHI or PII, and PHI. This helps us understand what type of data is most likely being targeted by the attackers. Along with this, the motive of the attacker is also identified. Motive of the attacker was either of these: Data and identity theft. Device theft, data loss, ransomware, data exposed to public or unauthorized disclosure. By analyzing the data, we have listed which type of control lapse had led to the breach. Is it the absence/lapse of a technical control or a non-technical control that led to the data breach? The list of controls which could have prevented or mitigated the impact of the incident is collected based on remedial measures taken by the covered entity and suggestions from investigating the agency. These controls are categorized whether they are preventive, detective or corrective control. By doing this, we get an idea of the nature of the data breach, its impact and the controls which could have avoided the breach. Based on this, the senior management or the CISO will have a clear understanding of various data breaches which have happened within healthcare companies, controls which needs to be in place and also get an idea of how much to invest on controls and on what priority. This result will be like a guide for CISO to understand and prioritize company’s cybersecurity [21] investments on controls. This will eventually reduce the chances of data breach occurrence and thereby adding value [22] to the business.

VI. DATA ANALYSIS

The data related to the breaches within the healthcare industry extracted from the OCR breach report provides many insights about the nature of the breach, impact, type of the breach, location of the data breach, involvement of a business associate, motive of the attacker, etc. Based on the evidence of the past breaches, we can get insights on key findings which can help the CISO optimize the cybersecurity program within the organization. The CISO can compare the findings based on the evidence from the past breaches with their internal cybersecurity program and take actions to optimize it.

Out of 226 breach incidents which have their investigations completed, we could find information of 204 cases, and 22 cases did not have complete information to analyze. Based on these 204 cases, CA tops the list with 30 data breach incidents. It is followed by Florida and Texas with 18 and 15 cases reported. Fig 3. Shows the state wise count of the number of data breach incidents across all the states within the united states.

In the healthcare industry, the companies are mainly classified into three main categories. Covered Entity, health plan, and business associate. Fig 4 shows the number of breach incidents based upon the covered entity types. From the figure, it is clear that healthcare providers are the ones who are getting targeted the most followed by health plan and business associate. Out of the 204 cases analyzed, 160 data breach incidents have been targeted towards the healthcare provider. It is followed by 31 cases reported by health plan and 13 from a business associate. 81.3 % of healthcare records compromised were from a healthcare provider, making it one of the prime targets for cyber attackers compared to a business associate and health plan. This concludes that the cyber attackers mainly target the healthcare providers. The reasons could be anything ranging from poor cybersecurity program, lack of competent IT Security resources or nontechnical [23] aspects of basic awareness towards data security.

Fig 3. Shows the Number of breach incidents in the US.

Out of 226 breach incidents which have their investigations completed, we could find information of 204 cases, and 22 cases did not have complete information to analyze. Based on these 204 cases, CA tops the list with 30 data breach incidents. It is followed by Florida and Texas with 18 and 15 cases reported. Fig 3. Shows the state wise count of the number of data breach incidents across all the states within the united states.

In the healthcare industry, the companies are mainly classified into three main categories. Covered Entity, health plan, and business associate. Fig 4 shows the number of breach incidents based upon the covered entity types. From the figure, it is clear that healthcare providers are the ones who are getting targeted the most followed by health plan and business associate. Out of the 204 cases analyzed, 160 data breach incidents have been targeted towards the healthcare provider. It is followed by 31 cases reported by health plan and 13 from a business associate. 81.3 % of healthcare records compromised were from a healthcare provider, making it one of the prime targets for cyber attackers compared to a business associate and health plan. This concludes that the cyber attackers mainly target the healthcare providers. The reasons could be anything ranging from poor cybersecurity program, lack of competent IT Security resources or nontechnical [23] aspects of basic awareness towards data security.

Fig 4. Number of data breach records based on Entity Type

From the evidence from the data breaches in the healthcare industry for the year 2016, we have classified the number type of attacks mainly under four categories Hacking/IT Incident, Improper Disposal, Loss, Theft and Unauthorized Access/Disclosure. This covers all the categories of the types of a data breach. From the data available, we observe that out of 204 breach incidents, 82 cases are due to Unauthorized Access/Disclosure of data. This constitutes to nearly 40% of the incidents followed by Hacking/IT incidents which constitute 31% of the cases. Both together constitutes nearly 71% of the breach incidents. 69.8 % of healthcare records were compromised using external hacking or an IT incident. The Unauthorized access can be either from an external attacker or internal employee who has access to data which he is not supposed to have access to. This type of data breach type can be addressed by having good technical controls to protect the databases and IT infrastructure and having proper segregation of duties and role-based access control. Such data
Breaches can be addressed using both technical and non-technical controls. IT/Hacking incidents are mainly from external sources who have to get access to the internal network by exploiting vulnerabilities. Technical controls which are preventive can prevent unauthorized access from an external source and hacking of IT systems of an organization. Fig 5. Provides a view of the type of attacks which the healthcare organizations were prone to in the year 2016.

![Fig 5. Type of Data Breach](image)

The location of a data breach is important to analyze because it shows at what point the data is being compromised. Looking at the data evidence, we can see that 118 cases of the data breaches have an external involvement. Predominantly, data compromises have happened at covered entity site, nearly 33% of the breaches have happened at the business associate site. CISO must ensure that 3rd party cyber risk management must be strengthened as it contributes to nearly 1/3rd of the data breaches incidents. This can be done by incorporating non-technical controls like ensuring the presence of an exhausting business contract covering all the security aspects. Periodic audits and imposing of covered entity security policies to the team involved with the business operations can substantially reduce or detect the occurrence of data compromise at the business associate site. Importance of involving a 3rd party or business associate in the organization’s cybersecurity program can be justified from the results of the study. 1/3rd of the 4073872 healthcare data records being compromised in the year 2016 had security control lapse at the business associate site. Based on the nature of the business, CISO must optimize his security program accordingly to prevent data compromise at the business associate site. Figure 7 shows the number of.

![Fig 6. Involvement of Internal Employees in the Data Breach](image)

Most of the data breaches, hacking incidents are carried out using attackers who are external to the organization with a motive of data theft or gaining unauthorized access to data. From the data breach evidence, we see that 86 cases of the data compromises have an external involvement. Having said that remaining 64 cases of data breaches had had some sort of internal employee involvement. Employee sabotage, the disclosure of data due to security threat unawareness and the accidental disclosure are few of the compromises which involves internal employees. 26% of the 4073872 healthcare records compromised were due to people involved in the organization. This is an important finding because it reinstates the importance of non-technical and behavioral controls like security policies and security awareness training within the organization. Form the data evidence; organizations can reduce the probability of data breaches occurrence which involves internal employees using a right balance of technical controls like data encryption and non-technical controls like security awareness training and also well-implemented policies. Fig 6 shows some data breach incident where internal employees were involved in disclosure of sensitive data and number of incidents involving people external to the organization. The CISO could use this evidences obtained from past healthcare breaches to optimize his security spendings to balance between both technical and behavioral controls.
security breach incidents which have occurred with and without business associate involvement.

![Image](image_url)

**PRESENCE OF BUSINESS ASSOCIATE IN THE DATA BREACH**

- **Yes**: 34%
- **No**: 66%

**Fig 7:** Business associate involvement in Data breach incident

Generally, most of the cyber attackers have some kind of motive behind the attack they are involved in. The most common motive behind healthcare breach incidents is data and identity theft constituting 110 of the 204 breach incidents being analysed. Data loss by some kind of intentional or unintentional exposure of data by employees within the organization constituted to 46 cases of data breaches in 2016.

**Fig 8:** Control classification which could have prevented the breach incident

Based on the detailed analysis of the investigative description from OCR data breach report, we studied each of this 204 data breach incidents in the year and classified them based on controls which would have prevented the breach. We broadly classified them into three categories, technical controls, non-technical controls and technical/ Nontechnical controls. By doing this, we can get a better insight what controls could have avoided this incident from occurring, had the control be in place. 2371504 of 4073872 healthcare data records which amount to nearly 58% of data records compromised in 2016 could have been prevented using non-technical controls such as security awareness training, well-implemented security policies and internal audits. Among the three different layers of controls, 82% of the healthcare data compromise in 2016 could have been addressed using some sort of preventive control measures. This classification gives better clarity to the CISO to focus on behavioral and nontechnical controls which is one of the major control deficiency which has led to 122 data breach incidents. The nontechnical controls include mainly Security awareness training, security policies and procedures, data handling and destruction policies, etc. Based on this data evidence, CISO can strengthen cybersecurity program of the organization by focusing on nontechnical controls. Within the 122 nontechnical breach, 78 falls under preventive controls, and 44 falls under detective control. If these nontechnical controls were effectively in place, these breach incidents could have been avoided. Therefore the CISO can plan his security program budget according to these aspects if they are not currently in place in his/her organization. This way the security program within the organization can be strengthened and security budget spending can be optimized. These evidence from breach incidents Fig 9 gives a detailed list classification of the count of technical and nontechnical control deficiencies in each of the 204 cases.

The table below shows the controls which need to be in place to prevent the data breach incidents.

<table>
<thead>
<tr>
<th>Breach Motive</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accident</strong></td>
<td>1. Data Encryption and password protection</td>
</tr>
<tr>
<td></td>
<td>2. Security awareness training</td>
</tr>
<tr>
<td></td>
<td>3. Audit logs and trails to track activities on the database or the IT systems</td>
</tr>
<tr>
<td><strong>Data and Identity theft</strong></td>
<td>1. Intrusion Prevention Systems IPS</td>
</tr>
<tr>
<td></td>
<td>2. Strengthening its network firewalls</td>
</tr>
<tr>
<td></td>
<td>3. Processes to manage admin accounts</td>
</tr>
<tr>
<td></td>
<td>4. Effective Risk management/mitigation plans</td>
</tr>
<tr>
<td></td>
<td>5. Security awareness trainings</td>
</tr>
<tr>
<td></td>
<td>6. Securing the web server, the web applications using HTTPS, SPAM</td>
</tr>
<tr>
<td></td>
<td>7. Two-factor Authentication, Certificate-based Login, Role based Access Control</td>
</tr>
<tr>
<td><strong>Data exposed to public</strong></td>
<td>1. Policies of handling PHI</td>
</tr>
<tr>
<td></td>
<td>2. Security awareness training</td>
</tr>
<tr>
<td></td>
<td>3. Role based Access controls</td>
</tr>
<tr>
<td><strong>Device Theft</strong></td>
<td>1. Policies and Procedures</td>
</tr>
<tr>
<td></td>
<td>2. Encryption of data to prevent data misuse</td>
</tr>
<tr>
<td></td>
<td>3. Role of access and reset of passwords</td>
</tr>
<tr>
<td><strong>Ransomware</strong></td>
<td>1. Enhanced firewall update</td>
</tr>
<tr>
<td></td>
<td>2. Up to date antivirus and software update</td>
</tr>
<tr>
<td></td>
<td>3. Enhanced access management practice</td>
</tr>
<tr>
<td></td>
<td>4. Data backup and recovery</td>
</tr>
<tr>
<td><strong>Unauthorized Disclosure</strong></td>
<td>1. Security policy on email and encryption to send secure emails</td>
</tr>
<tr>
<td></td>
<td>2. Security awareness Training programs</td>
</tr>
</tbody>
</table>

**Fig 9**

**CONTROL CLASSIFICATION WHICH COULD HAVE PREVENTED THE BREACH INCIDENT**

<table>
<thead>
<tr>
<th>Security</th>
<th>Technical</th>
<th>Non Technical</th>
<th>Nontechnical</th>
<th>Technical/ Nontechnical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>No</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

VII. RESULTS

Based on the study and evidence collected after analyzing the 204 data breaches [24] within the healthcare industry for the year 2016, CISO of any organization can get a fair amount of idea to optimize the organization’s cybersecurity program. This research would give CISO an understanding of what are the recent trends in the healthcare data breaches along with the motive, place of data compromise. Importance of having a
robust 3rd party security program plan, the importance of having a good portfolio of right technical and non-technical controls and adopting the right type of controls (Preventive, detective and corrective). As these findings are based on the recent 205 data breach incident from an authentic source, the findings are quite relevant and useful. Nearly 75% of the data records breached out of total 4073872 healthcare records compromised in the US in 2016 were with the motive of data and identity theft. 81.3% of healthcare records compromised were from a healthcare provider, making it one of the prime target for cyber attackers compared to a business associate and health plan. 69.8% of healthcare records were compromised using external hacking or an IT incident. This calls for a robust preventive technical control to be in place to safeguard external threats. 26% of the 4073872 healthcare records compromised were due to people involved within the organization. This is an important finding because it reinstates the importance of non-technical and behavioral controls like security policies and security awareness training within the organization. Importance of involving a 3rd party or business associate in the organizations' cybersecurity program can be justified from the results of the study. 1/3rd of the 4073872 healthcare data records being compromised in the year 2016 had security control lapse at the business associate site. 2371504 of 4073872 healthcare data records which amounts to nearly 58% of data records compromised in 2016 could have been prevented using non-technical controls such as security awareness training, well implemented security policies and internal audits. Among the 3 different layers of controls, 82% of the healthcare data compromise in 2016 could have been addressed using some sort of preventive control measures. This gives a clear picture to the CISO while designing the cybersecurity program for the organization as to where he needs to focus and invest the yearly security budget so that he can make the best use of limited budget allocated for the cybersecurity program. This study gives the CISO a checklist [25] kind of resource where he can compare the findings of this study against organization’s cybersecurity program and prioritize the actions within. As these evidences are from authentic data published by HHS and relatively recent, the findings are very valuable. This study reiterates the importance of security awareness programs and user education in reducing the data breach incidents within the healthcare industry, Training and education is key in managing risk and preventing data breaches.

REFERENCES


