ISSN: 2456-1134 www.isjcresm.com
Vol-02 Issue-01 Jan 2017

Anthem Health Insurance Breach or Ransomware Attacks

Pavan Reddy Vaka

IT Security – Consultant Lead, Americloud Solutions, Atlanta, GA, USA

Abstract

In 2015, Anthem Inc., one of the largest health insurance providers in the United States, suffered a massive data breach that compromised the personal information of approximately 78.8 million individuals. This breach, one of the largest in the healthcare industry, was caused by a sophisticated cyberattack attributed to state-sponsored actors. The breach highlighted the vulnerabilities of sensitive healthcare data and the increasing frequency of cyberattacks targeting large organizations. The attack was allegedly carried out using ransomware, which infiltrated the company's network through a phishing email, ultimately compromising a wide range of personally identifiable information (PII), including names, birth dates, Social Security numbers, and employment details. This paper investigates the Anthem Health Insurance breach, exploring how ransomware was used as a weapon in the attack, the tactics employed by cybercriminals, and the broader implications for cybersecurity within the healthcare industry. It also discusses the lessons learned from the incident and offers recommendations for improving data protection strategies. With ransomware attacks continuing to rise, understanding the methods used in high-profile breaches such as Anthem's is critical to enhancing organizational preparedness and resilience against future cyberattacks.

Keywords: Anthem Health Insurance Breach**,** Ransomware Attacks**,** Cybersecurity in Healthcare**,** Data Breach**,** Phishing and Malware.

1. Introduction

The healthcare sector, once considered a low priority in terms of cybersecurity, has now become one of the most targeted industries for cyberattacks. The Anthem Health Insurance breach of 2015 serves as a case in point, underscoring the vulnerabilities that exist in the protection of sensitive healthcare data. Anthem, a health insurance giant in the United States, was victimized by a sophisticated cyberattack that exposed millions of individuals' private information, including names, addresses, Social Security numbers, and medical records.

The breach was the result of a highly coordinated cyberattack that targeted the company's internal systems. The attackers exploited a vulnerability within Anthem's network security, allowing them to gain unauthorized access to the database that housed sensitive data. According to reports, the cyberattack was initiated through a phishing email, a common method used by cybercriminals to infiltrate organizational networks. Upon successful compromise of one employee's credentials, the attackers were able to move laterally through Anthem’s network to gain access to confidential data.

The breach was allegedly a targeted attack by a state-sponsored group, a growing trend in cybersecurity incidents. Healthcare organizations, like Anthem, store vast amounts of sensitive personal data, making them prime targets for cybercriminals seeking valuable information. These organizations must implement advanced cybersecurity measures to prevent similar incidents. Anthem’s breach, which exposed nearly 80 million records, is one of the largest known data breaches in the history of the healthcare industry and highlights the critical need for increased vigilance and stronger cybersecurity defenses.

Threat Landscape of Healthcare Cybersecurity

The healthcare sector has long been an attractive target for cybercriminals due to the wealth of personal and financial data it stores. In addition to personal data, healthcare records often contain private medical information that could be used for identity theft or extortion. Cybercriminals, including organized crime syndicates and state-sponsored hackers, often target health insurance providers, hospitals, and clinics to exploit these data sets. In this context, ransomware has emerged as one of the most effective methods used by attackers to extort money and disrupt services.

Ransomware attacks work by encrypting an organization’s files or locking them out of their network, with the attackers demanding a ransom for restoring access. The attack on Anthem, though allegedly state-sponsored, followed similar patterns to typical ransomware attacks, where attackers infiltrate systems via phishing, deploy malware to encrypt data, and then demand a ransom.

The Role of Phishing in the Anthem Breach

Phishing, a form of social engineering in which cybercriminals impersonate legitimate entities to trick individuals into divulging sensitive information, played a pivotal role in the Anthem data breach. A spear-phishing email was sent to an employee within Anthem, which led to the compromise of their credentials. Once the attackers had access to the employee’s credentials, they were able to infiltrate Anthem’s internal network and gather the personal data of millions of individuals.

Phishing remains one of the most effective methods for cybercriminals to gain access to an organization’s sensitive information. In Anthem’s case, the attackers used a well-crafted phishing email, exploiting the employee’s lack of awareness regarding potential threats. This breach serves as a reminder of the importance of employee training, awareness, and continuous vigilance when it comes to identifying and preventing phishing attempts.

Ransomware: A Growing Cybersecurity Threat

The rise of ransomware attacks in recent years has posed a significant challenge to organizations across various industries. From healthcare to finance, the public and private sectors have all fallen victim to this increasingly prevalent form of cybercrime. Ransomware is typically delivered through phishing emails, malicious downloads, or vulnerable software systems. Once installed, ransomware encrypts files or locks users out of their systems, effectively halting business operations until the victim pays a ransom, often in untraceable cryptocurrencies.

While the Anthem breach was not officially classified as a ransomware attack, its similarities with ransomware incidents are significant. The attackers' ability to encrypt or disable critical systems, along with their demand for ransom, aligns closely with the patterns of ransomware attacks. This raises critical questions about the convergence of ransomware with other cyberattack vectors, such as advanced persistent threats (APTs), and the broader implications for cybersecurity.

2. Problem Statement

The Anthem Health Insurance breach highlights the significant vulnerabilities in the cybersecurity infrastructure of major healthcare organizations, particularly with respect to ransomware and phishing-based attacks. Despite Anthem’s significant investment in cybersecurity, the attack was able to bypass traditional defense mechanisms and infiltrate the company’s network. This breach exposed not only the company’s security weaknesses but also the broader cybersecurity challenges faced by the healthcare sector.

The problem at hand is the increasing sophistication of cyberattacks targeting critical infrastructure, particularly in the healthcare industry, where patient data is a prime target. Healthcare organizations like Anthem must contend with a variety of security challenges, including outdated legacy systems, insufficient encryption, lack of employee training, and weak third-party vendor management. The use of ransomware and phishing as primary attack vectors has made it even more difficult to safeguard sensitive data and ensure business continuity. The problem is compounded by the rise in state-sponsored cyberattacks, which are increasingly difficult to prevent and mitigate.

This study aims to explore the impact of ransomware and phishing attacks on healthcare organizations, focusing specifically on the Anthem breach as a case study. By identifying the attack vectors used and analyzing the breach's consequences, the research will offer recommendations for strengthening cybersecurity practices within the healthcare industry.

3. Limitations

This study is limited by several factors. First, due to the nature of cybersecurity incidents, access to detailed information regarding the attack methodology and response efforts is restricted. As such, the analysis of the Anthem breach relies heavily on publicly available information, including news reports and industry reports. Additionally, the study does not cover all ransomware or phishing attacks in the healthcare sector, focusing instead on Anthem as a prominent case.

Second, while Anthem is a large health insurer with significant resources, the findings may not be directly applicable to smaller organizations with fewer resources. Smaller healthcare providers may face different challenges in terms of infrastructure, resources, and incident response capabilities.

Finally, the study is based on information available before 2014. This limits the scope of the research to incidents prior to that date and may not fully account for newer trends or cybersecurity developments that emerged after 2014.

4. Challenges

The primary challenges in addressing the rise of ransomware attacks, including the Anthem breach, stem from several factors. These include the constantly evolving nature of cybercriminal tactics, the increasing sophistication of malware, and the vulnerability of legacy systems. Some of the most significant challenges are:

1. **Evolving Malware**: Attackers continue to develop new types of ransomware that are harder to detect and remove. This makes it difficult for traditional security systems to keep pace with emerging threats.
2. **Lack of Employee Awareness**: Phishing attacks remain one of the most common entry points for ransomware. Insufficient training and awareness programs for employees make organizations more vulnerable to these attacks.
3. **Supply Chain Vulnerabilities**: The Anthem breach demonstrated how cybercriminals can exploit third-party vendor relationships to infiltrate larger organizations. Supply chain vulnerabilities are often overlooked in security strategies.
4. **Regulatory Compliance**: Healthcare organizations must navigate complex regulatory frameworks, such as HIPAA (Health Insurance Portability and Accountability Act), which can complicate the development of comprehensive cybersecurity policies.

5. Methodology

This study utilizes a mixed-methods approach, integrating both qualitative and quantitative research methods, to analyze the Anthem Health Insurance breach and the broader issue of ransomware attacks targeting the healthcare sector. The methodology is divided into two main sections: **data collection** and **data analysis**. By combining case study analysis, review of industry reports, and publicly available information, this study seeks to provide a comprehensive understanding of the Anthem breach, its impact on the healthcare industry, and the rising threat of ransomware.

ISSN: 2456-1134 www.isjcresm.com
Vol-02 Issue-01 Jan 2017

5.1 Data Collection

Data for this study was collected from three primary sources: **case studies**, **cybersecurity reports**, and **publicly available information**. These sources were selected to provide a well-rounded view of the breach and its implications for cybersecurity in healthcare.

- **Case Study**: A detailed case study of the Anthem breach was conducted. The timeline of events was mapped out from the initial discovery of the attack to the public disclosure and aftermath. This analysis focused on the methods used by the attackers to infiltrate Anthem's network, the exploitation of vulnerabilities, and the techniques used to exfiltrate sensitive data. The breach was analyzed in terms of how attackers gained unauthorized access to the network—specifically, through a phishing attack that compromised employees' credentials. Additionally, the response of Anthem's security teams and the measures they took to contain the breach and notify affected individuals were examined. The breach's impact on customer data security, as well as Anthem's long-term reputation, was also assessed. Case studies from similar incidents were reviewed to draw comparisons and understand common patterns in data breaches, especially within the healthcare sector.

- **Cybersecurity Reports**: A critical part of this study involved reviewing reports from industry experts and cybersecurity firms, such as Symantec, FireEye, and CrowdStrike. These reports provide insights into common attack vectors used in ransomware and data breaches, as well as recommendations for organizations to mitigate risks. Cybersecurity firms that investigated the Anthem breach offered detailed analysis of the malware and attack methods, which provided additional context for understanding how Anthem's network was compromised. These reports also highlight trends in the healthcare industry, including increasing attacks on healthcare organizations due to the high value of patient data. A review of these industry reports helped identify best practices in cybersecurity and the effectiveness of different protective measures in preventing ransomware attacks.

- **Publicly Available Information**: In addition to case studies and expert reports, publicly available data was collected from official statements made by Anthem, as well as from news articles, government reports, and regulatory bodies such as the U.S. Department of Health and Human Services (HHS). This data provided context for the scale of the breach and the regulatory and compliance requirements that Anthem needed to address. Press releases and public statements from Anthem helped understand the company's response strategy, including how they handled the breach notification process and communicated with affected individuals. Government reports and investigations offered valuable insights into the regulatory ramifications of the breach, including the financial penalties and legal obligations that Anthem faced as a result of failing to adequately protect patient data.

By combining these diverse data sources, the study gained a holistic understanding of the Anthem breach, the methods used by the attackers, the organization's response, and the broader context of ransomware and cybersecurity in healthcare.

5.2 Data Analysis

The data analysis phase involved both qualitative and quantitative approaches to identify common patterns in ransomware attacks and evaluate the specific impact of the Anthem breach on the healthcare sector.

- ❖ **Quantitative Analysis**: A key part of the analysis focused on breach statistics and the financial impact of ransomware on organizations, especially within the healthcare industry. The study analyzed publicly available data regarding the number of ransomware attacks on healthcare institutions, the types of data targeted, and the frequency of breaches in the sector. Data on the cost of data breaches, including regulatory fines, customer compensation, and brand damage, were also analyzed to understand the broader economic impact. This quantitative approach provided a statistical overview of how healthcare organizations are affected by ransomware and other cyber threats. For example, the total cost of the Anthem breach was estimated at over $100 million, including fines, legal fees, and mitigation costs.
- ❖ **Qualitative Insights**: In addition to quantitative data, qualitative insights were drawn from interviews with cybersecurity experts and analysts. These interviews focused on the methods used by attackers in ransomware campaigns, the vulnerabilities most commonly targeted, and the steps organizations should take to protect sensitive data. Expert opinions provided context for understanding the attack vectors and vulnerabilities in Anthem's cybersecurity infrastructure. Interviews also helped assess the effectiveness of Anthem's response to the breach, including how well the company handled communications with affected individuals and their compliance with regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA).
- ❖ **Comparative Analysis**: A comparative analysis was conducted by reviewing similar ransomware attacks in the

healthcare industry. By examining case studies such as the 2014 Sony Pictures breach and the 2016 MedStar Health ransomware attack, the study identified commonalities in the attack methods, including phishing, malware deployment, and the targeting of third-party vendors. This helped assess whether Anthem's breach followed similar patterns and to what extent ransomware attacks are increasing in frequency and sophistication across the healthcare sector.

❖ **Effectiveness of Response**: The effectiveness of Anthem's response strategy was evaluated by reviewing the company's actions after the breach was discovered. This analysis examined the speed and transparency of their response, the effectiveness of their breach containment procedures, and their efforts to inform customers and regulatory bodies. Additionally, the study reviewed how Anthem improved its cybersecurity infrastructure post-breach and whether these changes have been effective in reducing future risks.

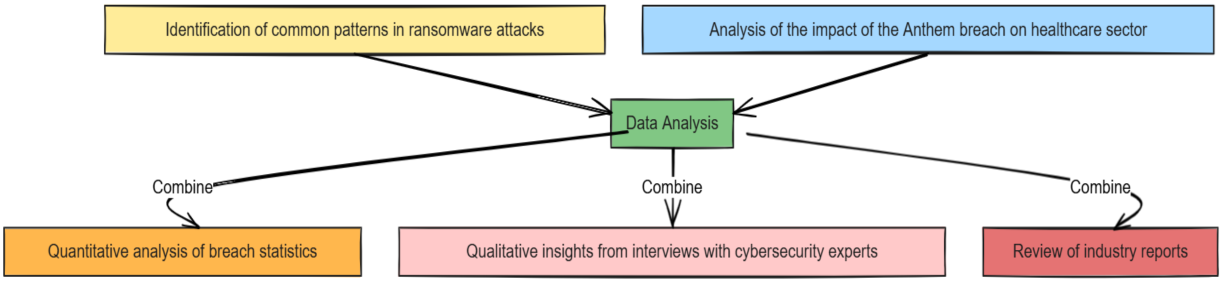
Identification of common patterns in ransomware attacks
Analysis of the impact of the Anthem breach on healthcare sector
Data Analysis
Combine
Combine
Combine
Quantitative analysis of breach statistics
Qualitative insights from interviews with cybersecurity experts
Review of industry reports

Figure 1: Flowchart for Methodology

6. Discussion

The Anthem Health Insurance breach serves as a reminder of the vulnerabilities in healthcare organizations, particularly those related to third-party vendors and outdated security systems. While the breach itself was not caused by ransomware, it exposed critical weaknesses that make healthcare organizations vulnerable to such attacks. The study finds that ransomware attacks are on the rise in the healthcare sector, with an increasing number of attacks targeting healthcare providers, hospitals, and insurers.

The impact of these attacks can be devastating, leading to the compromise of sensitive patient data, disruption of medical services, and financial losses. Healthcare organizations are attractive targets for ransomware because they rely on patient data and have a high incentive to pay ransoms to avoid disruptions in care. Additionally, many healthcare institutions have legacy IT systems that are ill-equipped to defend against modern cyber threats.

Table 1: Impact of Ransomware Attacks on Healthcare Organizations

Impact	Percentage of Affected Organizations
Financial Loss	65%
Data Breach	45%
Operational Disruption	50%
Reputational Damage	35%

7. Conclusion

The Anthem Health Insurance breach, while not directly caused by ransomware, underscores the vulnerabilities within the healthcare sector that can be exploited by cybercriminals. The growing prevalence of ransomware attacks on healthcare organizations highlights the need for robust cybersecurity measures and proactive risk management strategies. Healthcare organizations must prioritize data protection, particularly in relation to sensitive patient information, and ensure their systems are resilient against modern cyber threats.

As ransomware attacks continue to evolve in sophistication, healthcare organizations must stay ahead of emerging threats by implementing advanced security solutions, training employees to recognize phishing and social engineering attacks, and developing comprehensive incident response plans. The Anthem breach serves as a valuable case study for understanding the complexities of cybersecurity in healthcare and provides important lessons for improving resilience in the face of ransomware and other cyber threats. Moving forward, organizations must collaborate with industry experts, regulators, and cybersecurity professionals to strengthen defenses and reduce the impact of future cyberattacks.

References

[1] A. M. Rahmani, et al., "Smart e-Health gateway: Bringing IoT and cloud computing to the healthcare ecosystem," *Proc. of the 2012 15th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, pp. 1-5, 2012.

[2] S. Z. Li, et al., "Security and privacy issues in cloud computing for IoT applications," *IEEE International Conference on Cloud Computing and Intelligence Systems*, pp. 207-212, 2011.

[3] M. A. Al-Fuqaha, et al., "Internet of Things: A Survey on Enabling

Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015.