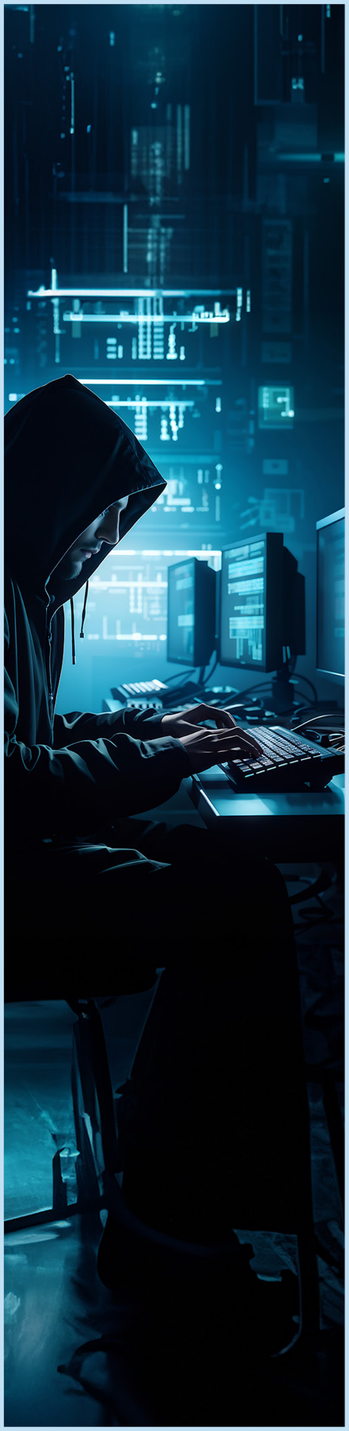
VIEW POINT



BREACHED RECORDS, BROKEN TRUST:

CYBERSECURITY THREATS IN HEALTHCARE

Infosys®
Navigate your next

Introduction

The healthcare industry, heavily reliant on technology, has become an increasingly attractive target for cybercriminals. The confluence of sensitive patient data, complex IT (Information Technology) infrastructures, and often outdated security measures create a perfect storm for cyberattacks. These attacks not only compromise patient privacy but can also disrupt critical healthcare services, leading to severe consequences.

One of the most prevalent cyber threats to healthcare is ransomware. This malicious software encrypts a victim's data, rendering it inaccessible unless a ransom is paid. In 2021, a ransomware attack on Colonial Pipeline caused widespread fuel shortages, highlighting the potential impact of such attacks on critical infrastructure.[1] Healthcare organizations are particularly vulnerable because they rely on uninterrupted operations.

Another significant threat is data breaches. Hackers often target healthcare organizations to steal patient records, which contain valuable personal information like Social Security numbers, birth dates, and medical histories. These breaches can lead to identity theft, pecuniary loss, and reputational damage for healthcare providers. A high-profile example is the 2015 Anthem data breach, which affected millions of individuals.[2]

Common Cyber Threats

Ransomware Attacks

Ransomware attacks pose an extreme danger to healthcare insurance corporations. Attackers install malicious software to encrypt statistics, annoying a ransom for its launch. This type of attack now not only disrupts operations but also can lead to a lack of vital information. A distinguished example is the 2021 assault on the Illinois-based total coverage company, CNA Monetary. The attack encrypted files and disrupted operations across the enterprise,[3] highlighting the vulnerabilities faced by coverage providers who deal with good-sized quantities of private and monetary information supply.

Phishing and Social Engineering Attacks

Phishing and social engineering attacks target employees with misleading communications designed to steal credentials Business Enterprise (AMCA), which manages medical collections for numerous fitness insurers, experienced a primary breach. Attackers used the phishing processes to gain unauthorized access to the right of entry to touchy records, inclusive of non-public and insurance information of over twenty million individuals (about the population of New York).[4] This breach illustrates the efficacy of phishing assaults in breaching coverage facts protection supply.

Insider Threats

Insider threats involve present-day or former employees misusing their access to data. There have been cases of former employees of health insurance organizations stealing patient data and selling it on the dark web. This breach exposed many private and health facts, emphasizing the need for stringent admission to control and tracking structures inside insurance corporation's source.

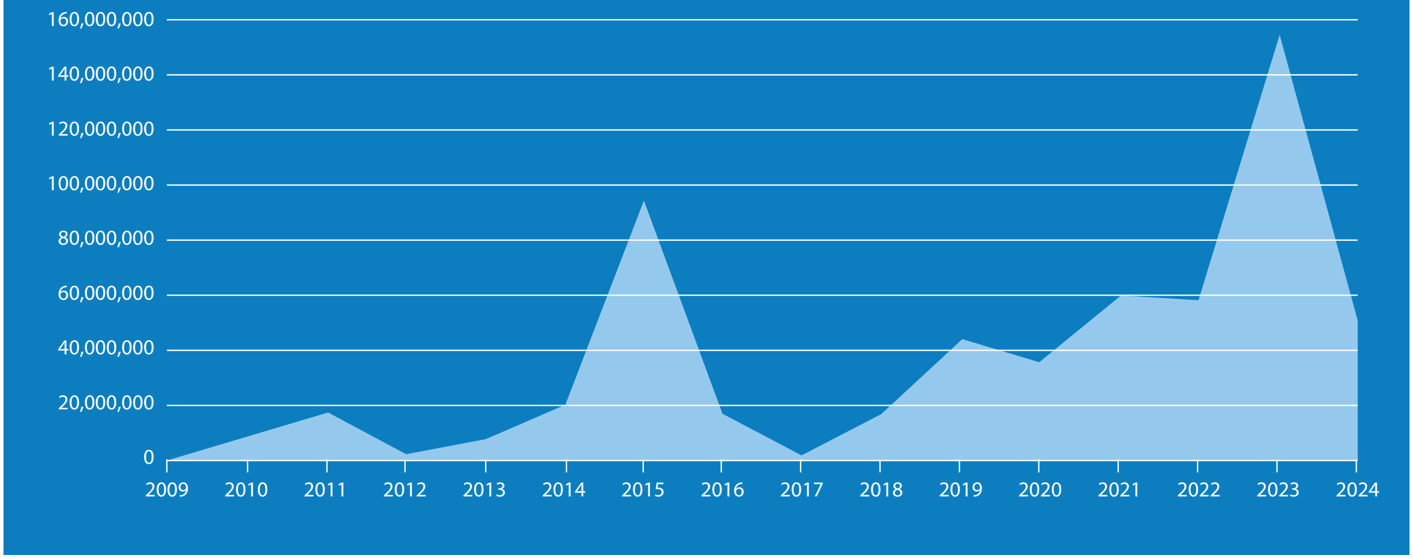
Types of Cyber Security Attacks in Healthcare

- Phishing attacks
- Malware attacks
- Ransomware attacks
- DDoS attacks
- Insider threats
- Social engineering attacks
- Password attacks
- IoT attacks
- Man-in-the-middle attacks
- Supply chain attacks

Annual Overview: Healthcare Data Breaches

Data breaches can occur due to hacking, unauthorized disclosure from website tracking tools, ransomware attacks, theft of devices or data, and impermissible disclosure from improper use of tracking codes. These incidents often involve cybercriminals exploiting vulnerabilities or unintentionally exposed information. The graph shows the number of individuals affected by healthcare security breaches from 2009 to 2024. There are notable spikes in 2015, with 78.8 million affected due to the Anthem Inc. breach,[5] in 2023, with over 140 million affected. A recent ransomware attack on Change Healthcare in February 2024 potentially exposed the health information of nearly 100 million Americans.[6] The overall trend indicates a general increase in the number of affected individuals, highlighting persistent challenges in healthcare data security.

Individuals Affected by Healthcare Security Breaches (2009 - 2024)

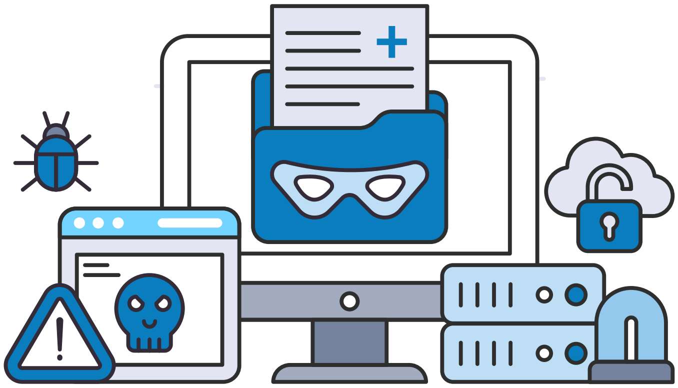


High-profile Data Breaches

Premera Blue Go (2015). One of the maximum massive data breaches in the healthcare insurance industry came about in 2015 while Premera Blue Cross experienced a cyberattack that compromised the private and scientific records of eleven million individuals.[7] The breach, attributed to an advanced hacking institution, exposed sensitive facts such as social security numbers and medical data. The incident underscores the massive effect that cybersecurity breaches will have on medical insurance groups' supply.

Excellus **BlueCross BlueShield** Data Breach (2015). The personal information of approximately 10.5 million individuals (about half the population of New York) was compromised.[8] This included names, Social Security numbers, birth dates, addresses, email addresses, and medical information. The breach led to increased cybersecurity spending for Excellus and caused significant reputational damage. Affected individuals were at risk of identity theft and financial fraud. The incident underscored the ongoing challenge of protecting sensitive healthcare data.

Ransomware Payment and Data Leak Threat



UnitedHealth Group, the parent company of Change Healthcare, paid a $22 million ransom to regain access to its systems.[9] However, the ransomware group, now identified as Blackcat ransomware gang,[9] threatened to leak stolen data unless an additional payment was made. This incident underscores the complex nature of ransomware attacks and the potential for ongoing risks even after paying the ransom.

Lessons Learned

The Change Healthcare attack offers critical lessons for the healthcare industry:

Supply Chain Vulnerability

The attack highlighted the vulnerability of healthcare organizations to cyberattacks through their supply chain partners.

The High Cost of Ransomware

Paying a ransom does not guarantee the return of data or prevent further attacks.

The Importance of Data Backup and Recovery

Robust backup and recovery plans are essential for mitigating the impact of ransomware attacks.

Need for Enhanced Cybersecurity Measures

Healthcare organizations must invest in advanced cybersecurity solutions to protect against evolving threats.

Patient Privacy and Trust

Protecting patient data is paramount. Data breaches can erode patient trust in healthcare providers.

The Change Healthcare ransomware attack serves as a stark reminder of the challenges faced by the healthcare industry in protecting sensitive patient data. By learning from this incident, healthcare organizations can strengthen their cybersecurity defenses and mitigate the risk of future attacks.

Recommendations

To prevent similar incidents, healthcare organizations should:

Conduct regular cybersecurity risk assessments.

Build strong relationships with cybersecurity experts and law enforcement.

Implement robust data protection measures, including encryption and access controls.

Prioritize employee cybersecurity training to prevent human error.

Develop and test incident response plans.

Maintaining HIPAA (Health Insurance Portability and Accountability Act) compliance is essential to protect patient data and avoid penalties.

Cyber Resilience in Healthcare: Essential Strategies

AI & Machine Learning
These technologies help healthcare insurance companies detect and respond to cyber threats by analyzing large data sets, identifying patterns of attacks, and automating responses. This leads to quicker and more accurate threat detection and prevention.

Endpoint Detection and Response (EDR)
In healthcare insurance, EDR enhances cybersecurity by detecting and responding to threats on devices in real-time. It analyzes endpoint data, isolates affected devices, and blocks malicious activity, protecting sensitive patient and insurance data.

Blockchain
Blockchain architecture enhances healthcare security by decentralizing data storage, eliminating single points of failure, employing cryptographic algorithms for tamper-proof records, ensuring verifiability, traceability, and immutability. This guarantees data integrity and reduces the risk of tampering and unauthorized modifications, making it difficult for unauthorized parties to alter information.

Security Information and Event Management (SIEM)
SIEM tools help healthcare insurance companies by consolidating and analyzing security data for a comprehensive view of network activities, providing real-time threat detection and actionable insights. They support compliance through detailed logs, aid in understanding attack patterns, and enhance security by integrating with other tools.

Identity and Access Management (IAM)
IAM in healthcare controls access to EMRs and critical systems, ensuring only authorized personnel can access sensitive patient information. It enhances security with strong authentication, improves regulatory compliance, and streamlines user identity and permission management.

Conclusion

The specter of data security breaches in healthcare looms large, casting a long shadow over patient trust, organizational reputation, and the broader healthcare ecosystem. The convergence of sensitive patient data, complex IT infrastructures, and an increasingly sophisticated threat landscape has created a perfect storm, demanding urgent and comprehensive countermeasures. This white paper has illuminated the multifaceted nature of this challenge, exploring the root causes, consequences, and potential mitigation strategies.

A multi-faceted approach is indispensable for successfully addressing this critical issue. Robust cybersecurity infrastructure, coupled with stringent data governance and employee training, forms the bedrock of a resilient healthcare organization. Proactive threat intelligence, incident response planning, and continuous risk assessment are essential to staying ahead of the evolving threat landscape. Moreover, fostering a culture of security awareness among healthcare providers, patients, and the public is vital for building a shared responsibility in safeguarding sensitive health information.

Ultimately, the protection of patient data is a cornerstone of ethical and moral responsibility, transcending mere compliance requirements. By investing in robust data security measures, healthcare organizations can not only mitigate financial losses and reputational damage but also reinforce patient trust, fostering a culture of care and confidence. As technology continues to advance, so too must our commitment to safeguarding the privacy and security of the most sensitive information entrusted to our care. Creating a truly secure healthcare system is a formidable challenge, but one we must confront it with resolute purpose.

References

1. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
2. https://www.infosecinstitute.com/resources/healthcare-information-security/the-breach-of-anthem-health-the-largest-healthcare-breach-in-history/
3. https://saltcommunications.com/news/a-look-back-on-2021-the-years-top-cyber-attacks/
4. https://www.zdnet.com/article/amca-data-breach-has-now-gone-over-the-20-million-mark/
5. https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/
6. https://krebsonsecurity.com/2024/10/change-healthcare-breach-hits-100m-americans/
7. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/premera/index.html
8. https://www.twingate.com/blog/tips/Excellus%20BlueCross%20BlueShield-data-breach
9. https://www.healthcarefinancenews.com/news/unitedhealth-reportedly-pays-22m-ransomware

Authors

Jatinder Chohan
jatinder.chohan@infosys.com

Jatinder Chohan is a results-oriented Business/Technical Analyst/Developer with 9 years of hands-on experience in healthcare IT. she excels in analyzing complex business requirements and translating them into effective technical solutions, particularly in the areas of claims, payment integrity, and enrollment for Medicaid, Medicare, and marketplace programs.

Avani Joshi
avani.jigar@infosys.com

Avani Joshi is a skilled Business Analyst with 10 years of experience in Healthcare domain, specializing in Quality, HEDIS, Risk Adjustment, Compliance, Network, Appeals & Grievances, Value-Based Services, and Claims across Medicaid, Medicare, and Marketplace lines of business.

Srishti Gangwar
srishti.gangwar@infosys.com

Srishti Gangwar is a seasoned Business/Technical Analyst with almost 14 years of IT experience in Healthcare and various other domains. She has worked in Enrollment, Contact Center, Omni Channel, UM/CM and Encounters in Medicaid LOB.

For more information, contact askus@infosys.com

Infosys® Navigate your next