Zettaset

WHITE PAPER

The Biggest Healthcare Data Breaches and Their Impacts

The healthcare industry has the greatest risk of being targeted by a data breach, and is the No. 1 target of ransomware attacks. Cyber attackers have been targeting the healthcare industry with greater frequency since 2013. Just in 2016, 88% of all ransomware victims were in the healthcare industry.[1]

The average healthcare organization pays $380 for every record affected—that's more than any other industry.[2] Of course, that cost varies depending on the severity of the data breach. Let's take a look at the worst data breaches in the healthcare industry to date and the impact they had on the target organization and the industry:

5. CareFirst Insurance

In May 2015, CareFirst Insurance discovered that they were the victims of a cyber attack.[3] The assailants gained access to member IDs, names, birthdays, and email addresses. After the attacks, CareFirst spent money not only hiring a large security firm, but two years of free credit monitoring for all CareFirst members impacted by the attack. They requested that all members create new usernames and passwords in their account portals. As of August 2, 2017, a class-action lawsuit against CareFirst was in progress.[4]

4. Britain NHS (National Health Services) Database

In May 2017, London hospitals suffered a major WannaCry ransomware attack that took down their computer systems rendering them unable to administer new patients.[5] While the number of patient records directly affected was low compared to other high-profile data breaches with 1,200,000 compromised patient records, the NHS (National Health Service) database attack might be the worst on this list. The data breach took down 40 hospitals and 24 trusts.[6] Surgeries were canceled and ambulances were sent to other hospitals further away from London.

This attack brought to light the outdated computer systems used by NHS trusts in the UK; as many as 90 percent of trusts were using the operating system Microsoft XP when attacked.[7] That operating system first debuted in 2001 and has not been supported since 2014, the year of its last security update.[8]

3. Community Health Systems

Community Health Systems is a U.S.-based organization that operates 206 hospitals with a strong presence in Alabama, Florida, Mississippi, Oklahoma, Pennsylvania, Tennessee, and Texas.[9] In 2014, they detected a data breach that compromised 4,500,000 patient records. This not only affected patients treated at their hospitals between 2009 and 2014, but any individuals who were referred to a physician at the hospital without even receiving treatment there.

The information captured by hackers included Social Security numbers, addresses, birthdates, and phone numbers—putting patients at high risk for identity theft. Luckily for the patients,[10]

---

[1] http://www.healthcaredive.com/news/must-know-healthcare-cybersecurity-statistics/435983/
[2] https://www.ibm.com/security/data-breach/
[3] http://carefirstanswers.com/
[4] http://www.fiercehealthcare.com/privacy-security/d-c-appeals-court-overturns-dismissal-carefirst-breach-class-action-lawsuit
[5] https://www.nytimes.com/2017/05/12/world/europe/nhs-cyberattack-warnings.html
[6] http://www.wired.co.uk/article/nhs-trusts-affected-by-cyber-attack
[7] http://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/
[8] https://en.wikipedia.org/wiki/Windows_XP
[9] http://money.cnn.com/2014/08/18/technology/security/hospital-chs-hack/
[10] https://en.wikipedia.org/wiki/Community_Health_Systems

hackers could not access credit card information or medical history, making the likelihood of being affected by health insurance fraud low.

The attackers accessed the Community Health Systems' database between April and June of 2014, going undetected until August of that same year. After the attacks, Community Health Systems paid for credit monitoring for those affected by the breach.

2. Premera Health Insurance

In January 2015, Premera Health Insurance detected a data breach that affected over 11,000,000 patient records.[11] The breach was not announced until March 2015, though the breach occurred between May 2014 and February 2015.[12] The attack was carried out via email phishing; an email was sent to an employee telling them to click a link to install a software update. The information targeted was bank account and Social Security information.[13]

In just days after the announcement of the breach, there were five class-action lawsuits filed against Premera.[14]

1. Anthem Health Insurance

Announced in February 2015, the Anthem Health Insurance data breach is the worst data breach the healthcare industry has suffered to date.[15] When you consider that Anthem Health Insurance was the second-largest health insurance company at the time, it's not surprising that over 37,500,000 patient records and 80,000,000 company records were compromised.

This breach was carried out through a phishing attack that began as early as December 10, 2014 and continued until January 27, 2015.[16] This gave intruders more than one full month of access to valuable organizational and personal data. Compromised information included Social Security numbers, email addresses, physical addresses, medical IDs, employment information, and more.

Anthem continues to feel the aftershocks of this data breach. In June 2017, Anthem agreed to pay a $115 million settlement, with a majority of the payout going towards two years of credit monitoring for those affected by the data breach.[17]

What the Healthcare Industry Can Learn

If the industry does not make cybersecurity a higher priority, healthcare organizations will continue to be a target of data breaches. The best way to prevent unauthorized access to PHI and other sensitive information is for healthcare organizations to re-examine their cybersecurity policies and implement a powerful data encryption solution. By encrypting their stored data, they can prevent malicious attacks from resulting in data theft.

Try XCrypt™ Full Disk Today

[11] http://www.healthcareitnews.com/news/premera-blue-cross-hack-exposes-data-11m
[12] https://www.law360.com/articles/890649/premera-blue-cross-can-t-escape-data-breach-suit
[13] https://www.bloomberg.com/graphics/2014-data-breaches/
[14] https://www.hipaajournal.com/5-class-action-lawsuits-filed-against-premera-for-hipaa-breach-812/
[15] https://en.wikipedia.org/wiki/Anthem_medical_data_breach
[16] https://www.bankinfosecurity.com/anthem-breach-phishing-attack-cited-a-7895
[17] https://threatpost.com/anthem-agrees-to-settle-2015-data-breach-for-115-million/126527/

465 Fairchild Drive, Suite 234, Mountain View, CA 94043
www.zettaset.com // +1.650.314.7920 // Fax: +1.650.314.7950 // sales@zettaset.com

About Zettaset

A leader in data protection, Zettaset's XCrypt™ line of encryption products are optimized for unmatched performance and infinite scalability to address the demanding data protection requirements of today's high-volume compute, storage, and cloud environments.