Zettaset

WHITE PAPER

Healthcare Cybersecurity

What Data Thieves Are After

A Growing Threat

Data breaches within the healthcare industry have been growing at an alarming rate since 2013. That was the first year the healthcare industry topped the list of data breaches by industry; 44% of all data breaches in 2013 targeted the healthcare industry.[1] Since then, the data security crisis has grown more dire as cybercriminals expand their reach. Healthcare is at the center of the concern.

In 2015, 98% of all record leaks were attributed to healthcare data breaches.[2] The damage equaled over 113 million stolen healthcare records.[3]

Only six months into the year, 2017 is set to break 2016's record of one healthcare breach per day with 233 reported healthcare breaches between January 1 and August 4.[4]

The threat continues to evolve, as cybercriminals become more sophisticated and specific in their attacks. This white paper will examine how attacks are carried out, the goal of cyber criminals, the impact of breaches, why healthcare is a target, and the measures healthcare security professionals can take to mitigate these attacks.

> *Only six months into the year, 2017 is set to break 2016's record of one healthcare breach per day with 233 reported healthcare breaches between January 1 and August 4*

How Cybercriminals Carry Out Attacks

Cybercriminal attacks are never the same twice in a row. The techniques vary from attacker to attacker, and the methodology is constantly evolving.

Before administering their attacks, cybercriminals gain access to computer networks a multitude of ways:

- **Keylogging** — This method refers to recording an individual's keyboard strokes. The main goal here is to record username and passwords that individuals use to access the information cybercriminals are after. Keylogging can be done both in software and hardware. This means an attacker could inject code on a website to record usernames and passwords for a specific site, or a keylog could be API-based. It is also possible for an attacker to alter and place a physical piece of hardware on a computer to record keystrokes. For instance, the USB dongle for a wireless mouse.[5]
- **Phishing** — Probably the type of infiltration most people are aware of, phishing refers to tricking the end user into thinking they are a trusted entity. This type of attack is usually carried out via email or social media and is sometimes referred to as spoofing. The goal of the attacker is to get the victim to click on a link that will forward them to landing page with a

[1] https://www.theatlantic.com/technology/archive/2015/03/the-next-cybersecurity-target-medical-data/388180/

[2] https://www.helpnetsecurity.com/2016/01/28/why-cybercriminals-target-healthcare-data/

[3] https://hbr.org/2017/06/11-things-the-health-care-sector-must-do-to-improve-cybersecurity

[4] http://www.healthcareitnews.com/news/insiders-hackers-causing-bulk-2017-healthcare-data-breaches

[5] https://en.wikipedia.org/wiki/Keystroke_logging

form where they may be asked to enter personal or login information.[6] If an attacker wished to gain access to a certain portal, they might recreate the login page for that portal and send a phishing email to anyone who might have access. All they need is one person with administrative access to fall for their fake email in order to infiltrate these files.

- Trojan horses — Similar to the idea of phishing, a trojan horse is a malicious web program that poses as a benign one. This is usually placed on a website or an email, and the target of the attack must download the trojan horse. The trojan horse usually contains code that allows the attacker remote access of the computer. Often, a person will not know if they have downloaded a trojan horse. While cybercriminals are able to access personal files by using trojan horses, this method is mostly associated with ransomware attacks.[7]
- Vulnerability scanners — As a security professional, vulnerability scanning is a tool that you can use to make sure you don't have any weaknesses in your infrastructure. However, black hat hackers are also able to use these tools to find points of entry.[8]

At the time of this publication, these are the most common methods that cybercriminals employ.

Ransomware

Ransomware is one of the most common forms of cyberattacks, no matter the industry. A form of malware, a ransomware attack occurs when the victim's data is encrypted by an outsider, rendering the data inaccessible and unusable. The attacker then demands a ransom fee in exchange for the safe return of the data. If a victim chooses not to pay the ransom, the threat is that they will permanently lose access to all of their data and it may later be resold on the "dark web."

Because of the anonymity provided by bitcoin, ethereum, or other cryptocurrencies, ransomware attacks can be carried out more easily than ever. The exchange of currency can be made without the intervention of a third party (usually a bank) and does not include traditional routing numbers that signal the location or identity of the cybercriminal.

Hackers performing ransomware attacks can receive a huge return. In 2014, the FBI reported that the hackers behind CryptoLocker turned a profit of at least $27 million.[9]

> *The healthcare industry is the largest target of ransomware attacks. In 2016 alone, 88% of all ransomware victims were in the healthcare industry.*

The healthcare industry is the largest target of ransomware attacks. In 2016 alone, 88% of all ransomware victims were in the healthcare industry.[10] This is precisely because they are more willing to pay in exchange for the health records, as it is a matter of safety more than a matter of security. Without access to patient records when necessary, patients *will* die.

[6] https://en.wikipedia.org/wiki/Phishing

[7] https://en.wikipedia.org/wiki/Trojan_horse_(computing)

[8] https://en.wikipedia.org/wiki/Vulnerability_scanner

[9] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[10] http://www.healthcaredive.com/news/must-know-healthcare-cybersecurity-statistics/435983/

Information theft

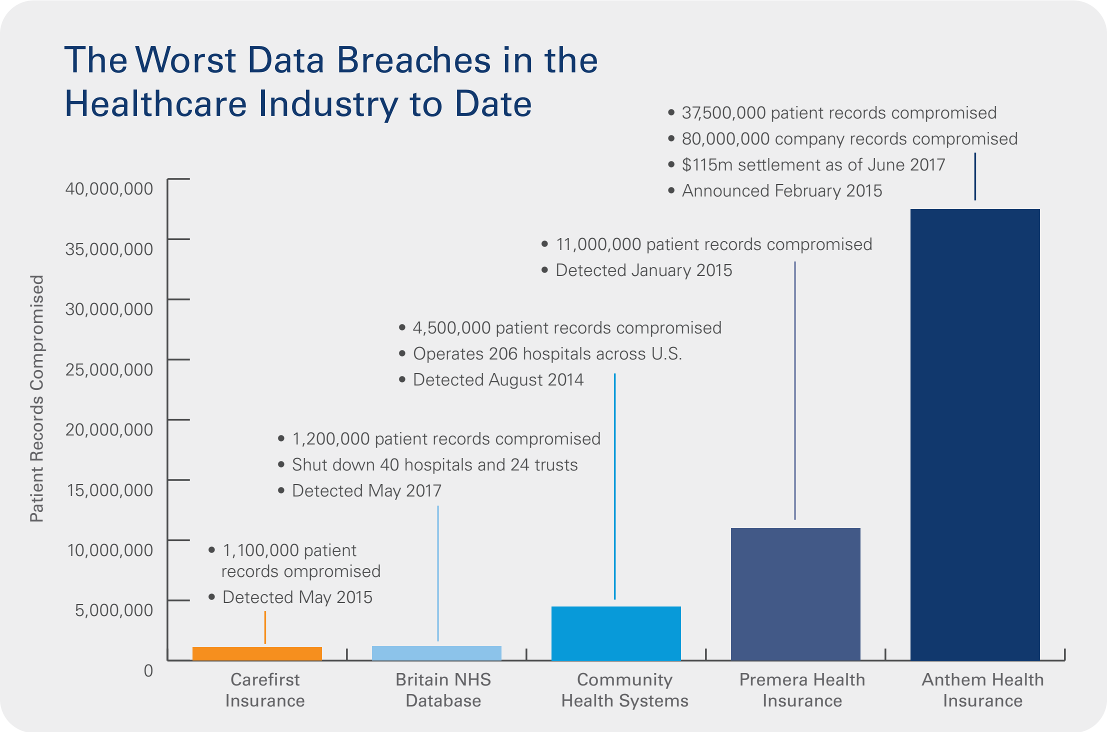
Electronic healthcare records (EHR) are more than just a list of doctors' visits and personal allergy information. They are highly personalized records that can include your social security number, credit card details, insurance information, bank data, and more. Hackers will often seek vulnerabilities in computer systems in order to access and sell this private information.

Cybercriminals infiltrate computers and retrieve information without detection. Unlike ransomware attacks, hackers who steal and re-sell files won't necessarily leave a trace. In fact, the average time to detect a data breach is 205 days.[11] That means 205 days have passed since the initial breach, during which time information might be continuously compromised.

IoT

The internet of things (IoT) and the associated connected devices are the latest target for cybercriminals. After all, there are now between 10 and 15 Wi-Fi connected devices per patient bed in a hospital.[12] In a survey conducted by Deloitte, 36% of 370 of healthcare organizations surveyed said they suffered security incidents related to their IoT medical devices.[13] One of the major issues for healthcare organizations is that IoT devices each have their own unique security requirements.

The decision to attack healthcare devices as opposed to stealing or holding data for ransom is a genuinely malicious attack. It signals that the attacker is willing to cause physical harm to the victims as opposed to seeking a payout. As time goes on, and IoT is engrained throughout the healthcare industry, attacks on IoT devices are expected to increase.



The Worst Data Breaches in the Healthcare Industry to Date

- 37,500,000 patient records compromised
- 80,000,000 company records compromised
- $115m settlement as of June 2017
- Announced February 2015

- 11,000,000 patient records compromised
- Detected January 2015

- 4,500,000 patient records compromised
- Operates 206 hospitals across U.S.
- Detected August 2014

- 1,200,000 patient records compromised
- Shut down 40 hospitals and 24 trusts
- Detected May 2017

- 1,100,000 patient records ompromised
- Detected May 2015

[11] http://www.institutionalinvestor.com/blogarticle/3569785/blog/the-ongoing-battle-of-cybersecurity.html#/.V4Ytn5MrLIE

[12] https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

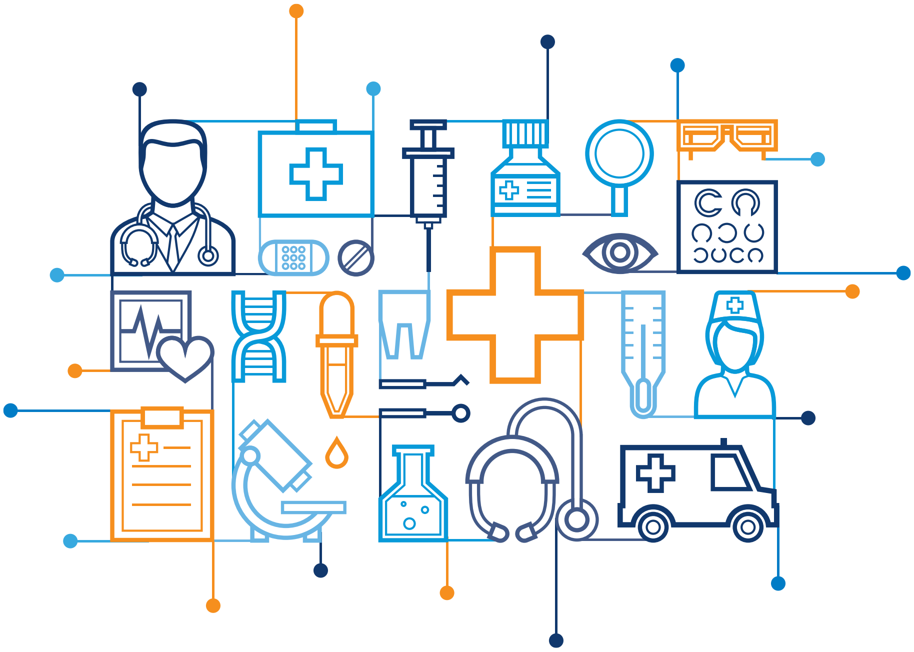
[13] http://www.hipaajournal.com/security-incidents-experienced-third-organizations-iot-medical-device-sphere-8929/

The Impact

There are many reasons for concern over the cybersecurity vulnerabilities in the healthcare industry. Both the patient whose data is at risk and the healthcare provider or insurer that was a target of an attack are impacted negatively by a breach.

The Patient

First and foremost, the safety of patients may be compromised during a breach depending on the type of attack. If files are encrypted by a cybercriminal, healthcare professionals will lose access to health records. This breach can delay care and result in potential harm to the patient. Without information on allergies, records of last shots, previous surgeries, family history, and health insurance providers, many treatments and medications cannot be administered.



In addition to the threat against safety, the breach can affect patients on another personal level. Patients whose health records are stolen are at a higher risk of identity theft and health insurance fraud. Unlike credit card fraud, victims of health insurance fraud are still responsible for the costs accrued by the fraudulent party.[14] Some victims paid out as much as $13,500 after finding themselves the victim of medical identity theft.[15]

Health insurance fraud can also impact future care of a patient. When fraudulent activity affects a health record, it creates a permanent change to that health record. This can mean unknown changes to existing conditions, allergy information, family history, or more. These fraudulent episodes can also saddle patients with undeserved healthcare debt.

Healthcare Organizations

Hospitals, private practices, and health insurance agencies must also think about themselves and how a loss of data might impact them financially. As an industry, healthcare spends the most to recover from a data breach: The average healthcare organization pays a staggering $380 per record affected.[16] The financial services industry ranks No. 2, paying out $336 on average for every compromised record.

[14] http://www.modernhealthcare.com/article/20150304/NEWS/150309960

[15] https://blog.vasco.com/application-security/impact-data-breaches-within-healthcare-industry/

[16] https://www.ibm.com/security/data-breach/

Whenever a data breach occurs in the healthcare industry, the HIPAA Breach Notification Rule requires covered entities to notify affected individuals, HHS, and in some cases, the media of a breach of unsecured PHI (protected health information). Most notifications must be provided without unreasonable delay and no later than 60 days following the discovery of a breach.

Notifications of smaller breaches affecting fewer than 500 individuals may be submitted to HHS annually. The Breach Notification Rule also requires business associates of covered entities to notify the covered entity of breaches at or by the business associate.

The minimum cost to a HIPAA-covered entity is a fine. This varies based on the severity of the data breach, but fines can extend into the millions. The largest fine paid to date was $5.5 million by Advocate Health Care Network after being found responsible for three separate breaches that compromised 4 million individuals[17] between July and November of 2013[18]. In this instance, the data was compromised by stolen equipment and improper data access.

HIPAA fines are not the only monetary burden on a healthcare facility after a data breach. Additional costs include the investigation of the attack to discover the source, legal expenses if patients or employees bring forth a lawsuit, offering identity protection services to those affected, and lowering rates to limit abandonment.

While it is hard to attach a number to it, the decrease in trust that results from a data breach can impact a healthcare facility well into the future. According to a Forbes report, 46% of organizations (not specific to healthcare) affected by a data breach experienced damage to their reputation.[19] Ironically, 80% of consumers claimed they trusted that their information is safe in the hands of a healthcare organization compared to other industries despite the evidence to the contrary.[20]

If a data breach affects those trusting patients, there is a chance that hospital attendance or healthcare enrollment (depending on the target of the breach) will decrease. Healthcare organizations must consider the affected patients, the likelihood local and national media will pick up the story, and the word of mouth both locally and online. Patients are more inclined to switch providers in metropolitan areas, or places where there are numerous alternatives close to the affected organization.

Government

With the increase of healthcare cyberattacks, the government may step in to create new regulations. After the WannaCry ransomware attacks in June 2017[21], the U.S. Health and Humanities Services sought public-private collaboration to assist with the prevention of these attacks[22].

The only current regulations affecting healthcare cybersecurity are the Health Information Technology for Economic and Clinical Health (HITECH) and Health Insurance Portability and Accountability Act (HIPAA).

[17] http://www.hipaajournal.com/ocr-hipaa-enforcement-summary-2016-hipaa-settlements-8646/

[18] https://www.cnbc.com/2016/08/04/huge-data-breach-at-health-system-leads-to-biggest-ever-settlement.html

[19] http://www-935.ibm.com/services/multimedia/RLL12363USEN_2014_Forbes_Insights.pdf

[20] http://www.hipaajournal.com/ponemon-study-reveals-impact-data-breaches-organizations-reputation-8846/

[21] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[22] http://www.modernhealthcare.com/article/20170608/NEWS/170609910

Why Healthcare is a Target

There's no doubt that healthcare is the industry most vulnerable to cyber security attacks. Here's why cybercriminals continue to hit healthcare the hardest.

Government Regulations Promoting Technology Usage

HITECH passed in 2009 with a goal of promoting "the adoption and meaningful use of health information technology"[23]. This essentially made the use of Electronic Healthcare Records (EHR) mandatory, as healthcare facilities are now subject to fines if they choose not to use EHRs. This increased adoption of technology has opened up hospitals and private practices to internet-born attack vectors they were previously unaffected (or seldom affected) by. This is not only limited to patient data, but also affects connected medical devices that are part of the IoT[24].

More Likely to Cooperate With Hackers

Being in a hospital often means involvement in a life-threatening situation. Without access to records, patient care is in jeopardy. This makes the healthcare industry less reluctant than others to hand over funds in exchange for regaining access to their patient data[25]. Without access to backup files (or if the backup files are also affected by the attacker), hospitals will often have no choice but to pay the ransom.

However, paying a ransom is likely to lead to subsequent attacks as the healthcare organization has made an implicit statement that they are willing to pay what is necessary to recover their data[26].

Out-of-Date Systems

The most vulnerable systems are the ones that are out-of-date. These systems lack the security sophistication of their newer counterparts, creating an easier target for attackers. In May 2017, London hospitals suffered a major WannaCry ransomware attack that took down their computer systems rendering them unable to administer new patients[27]. Surgeries were canceled and ambulances were sent to other hospitals further away.

This attack was made possible by vulnerabilities in an outdated Windows computer system. The hospitals had ignored warnings that their systems were out-of-date and vulnerable to attack. However, hospitals are more likely to have out-of-date computer and networking equipment because of cost restrictions. This exposes them to the greater possibility of attack.

Underinvesting in IT Security

Healthcare has historically underinvested in IT security due to lack of budget and resources[28]. It is challenging to find senior-level security professionals, and thus more difficult to initiate proper security procedures.

[23] https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

[24] https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

[25] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[26] http://www.fiercehealthcare.com/privacy-security/should-hospitals-pay-up-following-a-ransomware-attack-answer-far-from-simple

[27] https://www.nytimes.com/2017/05/12/world/europe/nhs-cyberattack-warnings.html

[28] http://www.npr.org/sections/health-shots/2017/07/26/539290596/hospitals-face-growing-cybersecurity-threats

In 2016, 52% of healthcare IT professionals polled said they spent between 0 and 3% of their overall IT budget on security[29]. Out of that same group, only 28% said they spent as much as 6% of their IT budget on security.

While unlikely that healthcare organizations lack security altogether, hospital administrators and IT personnel may also overlook vital software updates on security resources they do have in place[30]. Mistakes like this are a product of lack of resources, usually due to time or staffing constraints.

The Value of Health Records

While health records are considered less valuable to hackers than they used to be, they still fetch a good profit on the black market. Individual EHRs can fetch as much as $100[31].

This information is resold to individuals who want to commit identity theft or health insurance fraud. EHRs are more valuable than credit card information since it is harder to detect fraudulent information related to health records[32]. Fraudulent activity on a credit card is obvious, and victims recognize the charges immediately and cancel their cards. The same cannot be said for the theft of healthcare records and how it affects the individual. If the breach goes undetected for a year, plenty of damage can be done in that time period.

What Can Be Done?

Healthcare providers, including hospitals and clinics, and healthcare payers including HMOs and other insurers must protect themselves by taking the right security measures to secure their sensitive information.

Zettaset's XCrypt™ Data Encryption Platform delivers proven protection for sensitive data at-rest and in-motion in Relational/SQL, Object, NoSQL, and Hadoop data environments. XCrypt solutions are designed and optimized for effortless scalability and unmatched performance in today's complex and demanding distributed, virtualized and cloud environments. Enterprise customers and cloud service providers can rely on Zettaset for advanced solutions that easily fit into existing IT security and policy frameworks.

Try XCrypt Full Disk Today

[29] http://hitconsultant.net/2016/03/31/newsflash-healthcare-not-spend-enough-data-security/

[30] https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/why-hackers-are-going-after-health-care-providers/?utm_term=.61a885912a8e

[31] http://www.itproportal.com/features/what-is-the-value-of-stolen-digital-data/

[32] http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/

Zettaset

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$^{\text{TM}}$ 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.