Healthcare Data Under Siege: Ransomware and the Cyber Threat Landscape

Introduction

The healthcare industry was the target of the highest number of reported cyberattacks in 2015[1]. That same year, one out of every three Americans was the victim of a healthcare data breach.

Three factors make the healthcare industry both attractive and vulnerable to cyber criminals.

1

Protected health information (PHI) is worth considerably more on the black market than other types of personal information such as credit card accounts. In fact, it's worth an estimated 10x more.

2

Industry-specific risk is incurred by employees with little cybersecurity training, such as doctors and nurses, who are able to access highly sensitive data.

3

Many medical systems and devices cannot be updated or scanned on a regular basis due to the nature of their functions, leaving them open to attack.

The combination of these factors has encouraged cyber criminals to continue to attack the healthcare industry, and many have been successful.

Ransomware

Some of the recent well-publicized attacks on the healthcare industry were in the form of ransomware. Ransomware is malware that prevents the victim from accessing information on the infected system. The victim is then required to pay a ransom to the operators of the ransomware campaign to remove the restriction and regain full access to their data.

Many of these victims–desperate to avoid losing their sensitive data–decided to pay the ransom, as was the case with the Hollywood Presbyterian Medical Center when they were attacked with Locky[2] ransomware in February of 2016[3]. The medical center paid 40 BTC (Bitcoin), equivalent to approximately $17,000.

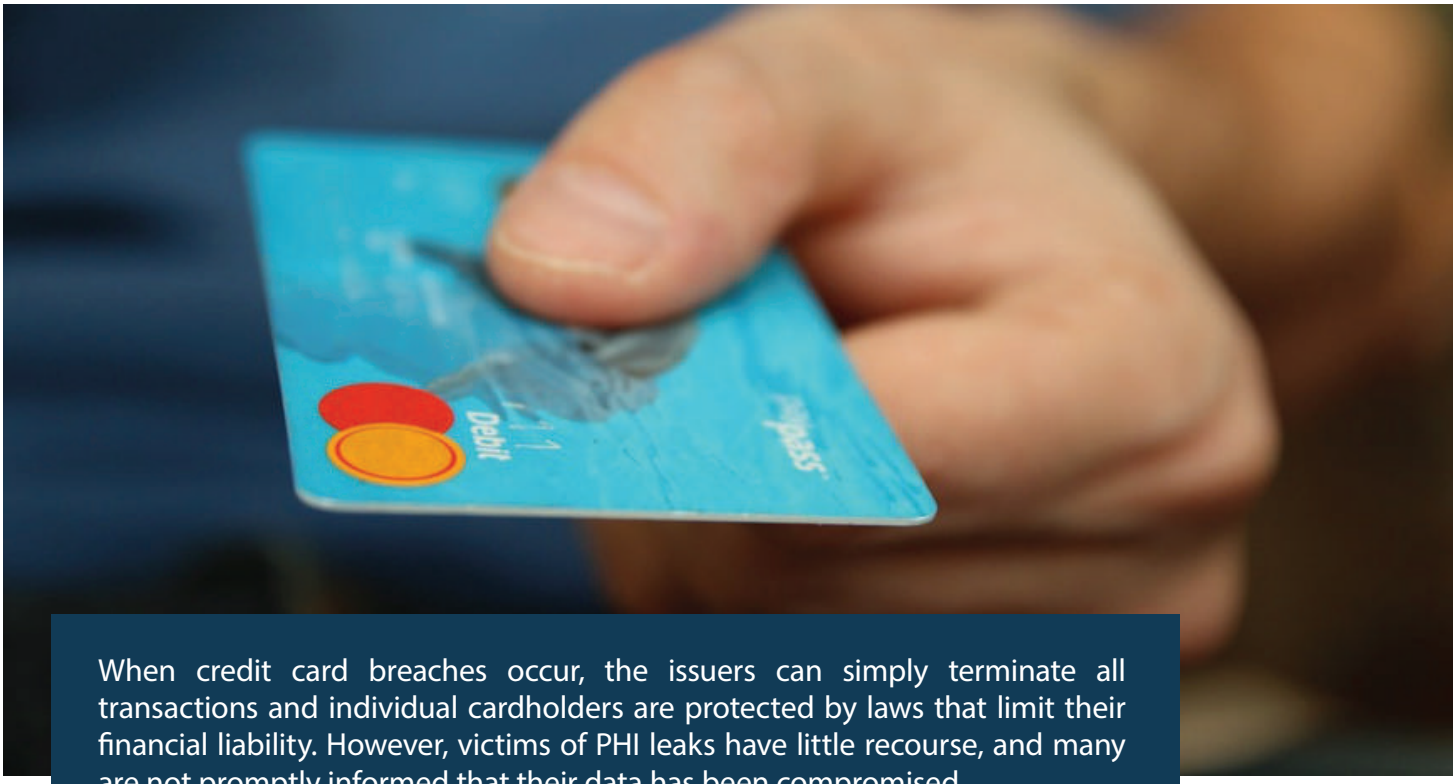
Another example is the hospital chain MedStar, which was attacked with the Samsam ransomware in March of 2016. Reports suggest the attack may have infected their systems through web servers running JBoss, which forced them to deactivate their entire computer system. This affected more than ten hospitals, obligating them to send patients to other facilities and delay minor treatments. Eventually they were able to recover their systems using backups[4].

[1] http://www.computerweekly.com/news/4500254005/Healthcare-sector-340-more-prone-to-IT-security-threats
[2] https://blog.threatstop.com/2016/02/24/locky-not-to-be-confused-with-lucky/
[3] http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf
[4] http://arstechnica.com/security/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware/

Data Breaches

While ransomware can prevent access to data, or in some cases loss of data altogether, having that personal health data stolen then sold on the black market can be far more harmful.

As mentioned previously, the healthcare industry is a highly profitable and insufficiently protected sector that attracts hackers. Facilities store sensitive PHI including Social Security numbers, medical records, and date of birth. Just one of these pieces of information can be sold for around $363 on the black market in 2015. Comparatively, individual credit card records were selling for just $1.



When credit card breaches occur, the issuers can simply terminate all transactions and individual cardholders are protected by laws that limit their financial liability. However, victims of PHI leaks have little recourse, and many are not promptly informed that their data has been compromised.

While criminals often leverage healthcare data for the purposes of identity theft, it can also be used to access medical care in the victim's name or to conduct corporate extortion. In some cases, this data has been used for political purposes or business espionage. For example, in early 2015 hackers were able to access health insurer Anthem's database. This breach, which remains one of the largest hacks to date, contained the names, Social Security numbers and birth dates of over 78 million people who had been enrolled in its insurance plans dating back to 2004. Amongst those whose information was breached were several high-ranking government officials such as Michael Daniel, the chief adviser on cybersecurity for President Obama[5]. An investigation determined that the hackers originated from China. The Chinese government has denied any involvement in the attack; however, American investigators believe hackers in China targeted insurers in the United States as part of a broader effort to obtain healthcare records and other personal information for millions of U.S. government employees and contractors.

[5] http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack

Additionally, it is speculated that these hackers were attempting to discover how U.S. medical coverage and databases are structured in response to China's current healthcare challenges as the country is faced with an aging and affluent population that is demanding better care[6].

> The damage from such a data breach can be severe for the organization, not only from the breach itself, but also the ensuing negative press and legal fallout. In the case against Anthem following the breach, it was determined that the theft of personally identifiable information (PII) is a harm to consumers in itself; separate from any subsequent misuse of it[7].

Due to the legal and financial implications, many healthcare organizations have been hesitant to report breaches. In reaction to this, the U.S. Department of Health and Human Services has instituted the Breach Notification Rule, which states that organizations with a breach of 500 or more HIPPA-protected entities must notify the affected parties following the breach. Similar regulations have been implemented and enforced by the Federal Trade Commission (FTC) which are applicable to both vendors of personal healthcare records and third party service providers.

In order for these safeguards to be effective, organizations must first be aware that a breach occurred, and unfortunately, many are not. For example, 21st Century Oncology did not know that they had been breached until the FBI notified them that PHI linked to their organization was found. The organization then hired a forensic firm to conduct an investigation coordinated with the FBI, the results of which determined that the attackers accessed their database on October 3, 2015 and affected 2,213,597 individuals. These findings were not reported to the public until March of 2016[8].

Similarly, The Alliance Health Networks, LLC was notified by independent investigators of a possible data breach that could have affected all of their communities which serve more than 1.5 million registered users. The leak was traced to a configuration error in their MongoDB database installation. It was found that some of the IP addresses that had accessed the database via this method were unaccounted for, leading to the possibility of a data breach.

In March of 2016, data storage contractor Bizmatics was hacked through unauthorized access to their servers. This attack exposed data on 26,588 patients of The Illinois Valley Podiatry Group[9] and 5,883 patients from Complete Family Foot Care.

[6] http://www.bloomberg.com/news/articles/2015-06-05/u-s-government-data-breach-tied-to-theft-of-health-care-records
[7] http://www.therecorder.com/id=1202749865875/Judge-Rejects-Key-Defense-in-Anthem-DataBreach-Suits?slreturn=20160311083239
[8] http://www.esecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html
[9] http://www.databreaches.net/illinois-valley-podiatry-group-warned-26588-patients-after-contractor-hacked/

Phishing Attacks

Given the amount of non-security trained professionals with access to highly sensitive information, it should come as no surprise that the healthcare industry has been the target of several successful phishing attacks in recent years.

During March of 2016, Mercy Iowa City, reported that up to 15,625 patients' personal information may have been compromised by a targeted phishing attempt when a request for information–that appeared to be from an authorized source–was successful. At this time, the extent of the attack remains unknown. There is still an ongoing investigation of this breach[10].

Another example of a phishing attempt was reported at the beginning of April 2016 from The Metropolitan Jewish Health System, Inc. This particular attempt affected up to 2,483 patients. According to reports, only one single target was solicited, which resulted in this breach[11].

Hacking

Another area where the healthcare industry remains vulnerable is hacking. In March of 2016, tax-filing company GreenShades' database was accessed by hackers using stolen credentials. This exposed the data of many of their clients, including a number of healthcare providers who used their services[12].

In January, home care agency JASACare was hacked through a compromised email account, leaving the personal healthcare data of their customers exposed[13], and in early 2016, hackers were able to access Norfolk General Hospital's website due to out of date hosting software. The hackers then were able to use the compromised website to serve the ransomware TeslaCrypt[14].

[10] http://www.databreaches.net/co-mercy-regional-medical-center-patient-records-breaches/
[11] http://www.databreaches.net/metropolitan-jewish-health-system-notifies-members-and-patients-of-phishing-incident/
[12] http://www.databreaches.net/dozens-of-nextcare-employees-report-fraudulent-activity-following-greenshades-hack/
[13] http://www.hipaajournal.com/jasacare-email-system-breach-impacts-1154-patients-3370/
[14] https://blog.malwarebytes.org/security-world/2016/03/canadian-hospital-serves-ransomware-via-hacked-website/

Hacktivism and DDoS

Healthcare is not immune to the repercussions of Hacktivism either. Hacktivist group Anonymous targeted Michigan Governor Rick Snyder during the Flint water crisis. This attack inadvertently led to a disruption in the Hurley Medical Center's food service resulting in the loss of information regarding patient dietary needs and causing major delays in delivering food[15].

Distributed Denial of Service or DDoS attacks have also had major implications for the healthcare industry. Thirty-seven percent of healthcare IT departments report that their organization has experienced a DDoS attack that caused a disruption to operations and/or system downtime as often as every four months. The resulting fallout of these attacks cost an average of $1.32 million each[16].

The United States is Not Alone

Although most of the attacks and breaches we have described occurred in the U.S., the United States is not alone in this fight. Systems at the Lincolnshire County Council in England were hit by ransomware, which affected employee health records. The hackers demanded over £1,000,000. Fortunately, they were able to restore their systems from backups[17].

Another example is the Royal Melbourne Hospital in Australia. Due to vulnerabilities in Windows XP, which is no-longer-supported, they were attacked with Qbot, a self-replicating malware that can steal data and harvest credentials[18].

Additional attacks were reported at Lukas Hospital in Germany, and the Whanganui District Health Board in New Zealand[19].

[15] http://www.mlive.com/news/flint/index.ssf/2016/02/anonymous_claims_responsibilit.html
[16] https://blog.eset.ie/2016/03/01/new-ponemon-study-cyber-onslaught-threatens-to-overwhelm-healthcare-survey/
[17] http://www.lincolnshireecho.co.uk/Cyber-hack-Lincolnshire-council-refute-claims/story-28641205-detail/story.html
[18] http://www.lifehacker.com.au/2016/01/hack-attack-on-a-hospital-it-system-highlights-risk-of-sticking-with-windows-xp/
[19] http://www.databreaches.net/nz-health-board-hit-with-ransomware/

Medical Devices

While computers and mobile devices remain the most obvious targets, medical devices provide an often-overlooked gateway for security breaches. Take CareFusion's Pyxis SupplyStation system for example. Security researchers were able to discover over 1,418 vulnerabilities in the device alone[20].

There is a wide variety of clinical devices employing a range of configurations. Additionally, many clinical devices that report findings over the network do so in a non-encrypted format[21].

Medical devices are particularly vulnerable due to the nature of their services. Equipment used to provide life support or administer medicine, for example, cannot be taken offline due to the risk of service disruption during a scan. This often leaves those devices as "unknown variables," and as this particular case study found, what you don't know can hurt you. In the reported study, a member of the hospital staff clicked on a link in an email, which installed a worm. The worm spread through the hospital's network and then hid inside a clinical device, in this case a portable x-ray machine. The IT team thought it had remediated devices infected with the worm network wide, but it missed the infection inside the device, where the worm had created a back door into the hospital's systems[22].

To add to an already critically vulnerable security environment, there are currently thousands of hospital devices that can be found online by using the Shodan search engine–self-described as "the search engine for the Internet of Things." This includes radiology applications, MRI devices and of course, webservers[23]. If these publically searchable devices are installed and used with their default permissions, or outdated software, they can be accessed with little effort to not only steal patient records and other data, but potentially to control the devices for malicious purposes.

One example from researchers at TrapX found that an attack had compromised three different blood gas analyzers (BGAs) in the hospital's lab via backdoors that allowed the attacker to enter and pivot through to the network. Each BGA was several years old, and ran on an older version of Windows. In another attack they found that a picture archive and communications system (PACS), which is used to store and access images originating from CT and MRI scanners, X-ray, and ultrasound equipment was being used as an access point to the network while the attacker was hunting for other targets. The infection was the byproduct of a previous attack, which occurred as the result of a user visiting a malicious website. The infection was discovered and removed, but not before spreading to the PACS. As none of the hospital's defense mechanisms were able to scan the PACS properly, the infection went undetected giving the China-based hackers, a backdoor into the system[24].

Recently, the U.S. Food and Drug Administration issued a safety warning to healthcare facilities using the Hospira Symbiq Infusion System, a computerized pump made for delivering medication. The device was found to have several critical security vulnerabilities, which could potentially be accessed remotely allowing an unauthorized user to control the device and change the dosage that the pump delivered.

[20] https://www.helpnetsecurity.com/2016/03/30/1400-flaws-automated-medical-supply-system/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29

[21] https://securityevaluators.com/hospitalhack/

[22] http://trapx.com/resources/case-studies/

Conclusion

The healthcare sector has many points of weakness and highly desirable data. Factors such as multiple types of systems in hospital networks, clinical devices that are not or cannot be updated, and the lack of cybersecurity knowledge of users with access to highly sensitive data, all create high levels of risk in the industry. Hacks can cost medical organizations millions and leave unwitting patients open to damages or even injury.

To ensure your organization's compliance, visit the HIPAA checklist at: http://www.hipaajournal.com/hipaa-compliance-checklist/

About ThreatSTOP

ThreatSTOP is a network security company offering a cloud-based threat protection service that protects every device and workload on a network from cyberattacks and data theft. It can protect any network, from virtual cloud networks to branch LANs to the largest carrier networks. The service leverages market-leading threat intelligence to deflect inbound and outbound threats, including botnet, phishing and ransomware attacks, and prevents data exfiltration. For more information visit www.threatstop.com.

[23] https://www.shodan.io/search?query=ct+scan+
[24] http://www.csoonline.com/article/2931474/data-breach/attackers-targeting-medical-devices-to-bypass-hospital-security.html
[25] http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm