Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **February 2020**
Sponsored by **Yubico**

Cyber Security in Healthcare

Executive Summary

Healthcare is one of the most highly targeted industries by cyber criminals, with attacks including ransomware, data theft, and business email compromise (BEC), among others. New ransomware attacks against healthcare organizations across the world are disclosed almost daily, such as Great Plains Health in the United States[i] (November 2019), Rouen University Hospital in France[ii] (also in November), and two health alliances in Australia[iii] (September 2019). Hospitals account for one-third of data breaches in the United States,[iv] and the industry has faced increasing threats during 2019. BEC attacks, initiated through successful phishing and other attacks, lead to data theft, snooping, and unauthorized access to patient data. Attacks result in numerous negative outcomes:

- Disruption in health care delivery and lost business, e.g., when hospitals must refer patients to other health care providers or cancel surgeries.
- High recovery costs, including, but not limited to, paying staff working around the clock to recover data, funding independent security and forensics experts to determine the scope of a data breach, notifying affected patients through postal mail services, paying for victims' credit monitoring services, and implementing mitigations under urgency.
- Business termination or seeking bankruptcy protection, as seen during 2019 at both small medical providers after ransomware attacks, and at a large medical billing entity after a massive data breach that led to many of its health care customers cancelling their service agreements and going to a new provider.
- Reputational damage to healthcare institutions when the details of their security problems are made public. For example, breaches in the United States of more than 500 individuals' personal information must be posted to the US Department of Health and Human Services (HHS), Office for Civil Rights (OCR) "wall of shame".[v]

Healthcare is one of the most highly targeted industries by cyber criminals.

KEY TAKEAWAYS

Without significant improvements in cyber security readiness, healthcare providers will continue to suffer at the hands of cyber criminals.

- Healthcare presents a potent mixture of threat factors that together make the industry a prime target for cyber criminals. It is no wonder that healthcare is relentlessly targeted for financial gain through extortion and cybertheft.
- Ransomware attacks against healthcare providers and their supply chain partners dominated the news during 2019. Every ransom payment amplifies the attractiveness of healthcare organizations to cyber criminals.
- Email continues to be a primary threat vector for healthcare organizations because it so widely used, and because the vast majority of phishing attempts are delivered through the email channel.
- While ransomware attacks capture the headlines, data breaches at healthcare providers are not far behind. For the 2019 calendar year, approximately 45 million healthcare records in the United States were breached or accessed by unauthorized individuals.[vi] Two mega-breaches in 2015 compromised a combined 90 million medical records,[vii] but the pattern of more recent years is for more breaches at more healthcare providers.
- We expect cyber criminals to tighten the screws on ransomware to increase the likelihood of ransom demands being paid by healthcare providers, target supply chain firms to quickly amplify the pain of an attack across healthcare

ecosystems, and compromise increasingly vulnerable medical devices (including wearable or implantable medical devices).

- Every healthcare provider needs to urgently undertake – or update – its enterprise-wide risk assessment for cyber security. Effective mitigations can be planned only in light of real data.

- Cyber security solutions that cover the triad of people, process and technology offer effective approaches for mitigating risks, reducing threats, and hardening security defenses.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Yubico; information about the company is provided at the end of this paper.

Anatomy: Cyber Security in Healthcare

Healthcare providers, systems and practices face a plethora of cyber security threats. In this section we consider recent and enduring threats.

RANSOMWARE

While commodity ransomware attacks hope to snag any possible victim, targeted attacks aim to compromise specific targets. Healthcare providers subject to a successful ransomware attack face urgent life-or-death situations for patients which can be enough to force the paying of the ransom demand. The global WannaCry ransomware attack in 2017 was devastating to health care providers. For example, affected providers in the National Health Service in the United Kingdom collectively had to cancel 19,000 appointments and operations, refuse acceptance of new patients, and pay a clean-up bill of more than €90 million.[viii] It's important to note that while ransomware is the direct threat vector discussed here, most ransomware is delivered through email, and so this is largely an email security problem as opposed to security other communication, collaboration and information channels.

Healthcare providers subject to a successful ransomware attack face urgent life-or-death situations.

Several research studies list healthcare as high on the list of targeted industries, such as:

- In 2017, NTT Security ranked healthcare and retail as third equal on the list of industries targeted by ransomware, behind business and professional services in first place and government in second.[ix]

- In 2019, Recorded Future catalogued more than 140 targeted ransomware attacks against healthcare providers and the government sector.[x]

- For the first nine months of 2019, Emsisoft put the number even higher, saying that of 621 tracked ransomware attacks against government agencies, healthcare providers and school districts, the vast majority were perpetuated against healthcare (491 attacks out of 621 total).[xi]

But these summary numbers are not the only evidence of ransomware attacks in healthcare during 2019; both disclosure notices from affected providers and widespread angst on social media offer many individual examples. While none have yet approached the devastation of WannaCry, the pattern is disturbing:

- An attack against the Brooklyn Hospital Center in New York in July 2019 resulted in some patient data being irretrievably lost due to an ineffective backup system.[xii]

- An attack against the DCH Health System in Alabama in early October 2019 affected three of its medical centers.[xiii] Patients were referred to other providers, emergency manual procedures with paper-based record keeping were put in place, and external experts were hired to assist with resolving the incident. Some local residents received phone calls reportedly from DCH requesting personal information, but whether these calls were purely opportunistic fraud attempts or the consequence of breached patient data is unclear; DCH says no patient data was accessed. Recovery relied on both backup systems and paying the ransom demand.

- Normal operations at all five sites of the Rouen University Hospital-Charles Nicolle in France were disrupted by a ransomware attack in mid-November 2019.[xiv] The attack affected 6,000 of the hospital's computers, and to prevent further infection, all IT systems were shut down. No ransom demand was forthcoming, meaning that the hospital had to recover from backup.

- Great Plains Health was compromised by an attack in late November 2019 that encrypted patient records, the phone system, and email.[xv] Officials expected recovery to take "weeks or months."

The above are but four examples; hundreds of others were been reported during 2019 with similar effects and flow-on consequences.

DATA BREACHES FROM POOR INTERNAL PROCESSES

Poorly designed internal processes and ineffective training practices can result in breaches of Protected Health Information (PHI). Incidents during 2019 included:

Poorly designed internal processes and ineffective training practices can result in breaches of Protected Health Information.

- The creation of mailing labels at Sentara Hospitals in April 2019 breached patient data due to 577 patient records being incorrectly merged into mailing labels for guarantors.[xvi] Although patient diagnosis, treatment information and medical data was not disclosed on the labels, the hospital was fined more than US$2 million for breaching the privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA), and was required to take other corrective actions, as well.

- A patient was incorrectly admitted to an unnamed hospital in Germany.[xvii] The patient mix-up resulted in the wrong patient receiving the invoice for health care services, and the hospital received a €150,000 fine under the European Union's General Data Protection Regulation (GDPR) for its ineffective in-take process.

- A photo of an operating room display at a health provider in the United States was publicly released.[xviii] The display showed PHI of two individuals, one of whom was a well-known sports star. The health provider was fined US$2 million under HIPAA for this privacy breach.

- A food services employee at the Zuckerberg San Francisco General Hospital disposed of meal tray tickets incorrectly, discarding the tickets into regular rubbish bins rather than the confidential shredder bin.[xix] More than 1,100 tickets with sensitive health data on patients were incorrectly discarded over a six-month timeframe, including PHI including full name, birth month and day, bed/unit information at the hospital, and food selections.

- An incident from 2016 is also worth noting: in January 2016, the Village of Oak Park, IL, city officials discovered that one of their employees had emailed a spreadsheet containing PHI on 688 people to a personal email account. The information contained in the spreadsheet included information on these individuals' healthcare benefits, Social Security numbers, and other sensitive information.[xx]

While the specific actions in each incident were quite minor, each resulted in a breach of PHI. It doesn't take much for a breach to happen, with costly fallout.

DATA BREACHES FROM MALICIOUS INSIDER ACTIONS

Not all data breaches in healthcare result from careless or accidental mistakes: some are deliberately undertaken, usually for financial gain. Three examples from 2019 were:

- Email continues to be a primary threat vector in the healthcare space. As of January 2020, for example, about 40 percent of the cases currently under investigation by the US Department of Health and Human Services Office for Civil Rights are the result of a breach through email. Twelve percent of the email-related cases are the result of "Unauthorized Access/Disclosure".[xxi]

- The New South Wales Ambulance service in Australia paid AUD$275,000 to settle a class action brought as a result of a data breach in 2013-2014.[xxii] At the time, a contractor inappropriately accessed personal and sensitive health information on 130 paramedics at the service, and sold the data to a group of injury lawyers.

- An employee was selling personal health information to law firms and health clinics that specialized in patients involved in motor vehicle accidents.[xxiii] The data was stolen from NYC Health and Hospitals Corp. over three years starting in 2016. The hospital became aware of the theft only in November 2019.

- The United States Secret Service contacted the Aegis Medical Group to notify them of an employee attempting to sell patient health records.[xxiv] Since most of the health reports at Aegis were in physical form, the employee potentially had access to 9,800 records over several months.

Malicious insider actions cause reputational damage to a healthcare provider, and can result in class actions or other fines for privacy breaches.

DATA BREACHES FROM MALICIOUS EXTERNAL ACTORS

The Office of Civil Rights at the United States HHS department reported that more than 38 million health records were breached during the first 10 months of 2019 (39.8 million records for all of 2019).[xxv] Of the 52 individual data breaches in October, 18 were from hacking or other IT incidents. Assuming the same rate of breach during November and December, the total number of records breached approached 45 million for 2019, a high number indeed, but only half of the records breached during 2015 due to the mega-breaches at Anthem[xxvi] (78.8 million records) and Premera Blue Cross[xxvii] (11 million records). Fines for breaches are expensive; for example, the breach at Banner Health of financial and health data on 2.9 million people in 2016 was recently settled with an overall cap of US$6 million to reimburse patients for costs incurred as a result of the breach.[xxviii]

Many healthcare providers were compromised by successful phishing attacks in 2019.

PHISHING ATTACKS AND ACCOUNT COMPROMISE

Many healthcare providers were compromised by successful phishing attacks in 2019, leading to account credentials being used by unauthorized individuals to gain access to email accounts that contain PHI. While the number of email accounts compromised at each provider is generally small, each email account usually contains data on thousands of patients. For example:

- Several email accounts at the Central Valley Regional Center in California were breached between July 25 and August 2, 2019.[xxix] The email accounts contained health data on almost 16,000 patients with intellectual and developmental disabilities, as well as financial data on some of these patients.

- A phishing attack at Kalispell Regional Healthcare in Montana in November 2019 resulted in a data breach on up to 130,000 patients.[xxx] One patient has filed a civil complaint of negligence in Montana against the provider, alleging that insufficient protections were implemented before the breach.

- A widespread phishing attack against the Monash IVF clinic in Australia during November 2019 came to light when patients received phishing emails using Monash IVF email accounts.[xxxi]

- A phishing attack at the Atria Senior Living provider enabled an unauthorized individual to access several email accounts.[xxxii] Atria's forensic specialists were unable to determine which email messages and attachments had been accessed within the email accounts, which in principle, should force Atria to notify every patient of the breach. This is an expensive process for any healthcare provider.

Given the widespread use of email to discuss patient matters, arrange appointments, and coordinate care, any compromise of an email account at a healthcare provider is almost certain to lead to a breach of PHI. Specialists in forensic analysis are usually able to determine the types of data that exist within a compromised email account, and depending on the email system used, which messages or attachments were inappropriately accessed by the attacker. Of course, as organizations embrace cloud services like Office 365, compromising account details for email gives a wide remit to access other services in Office 365, such as OneDrive for Business, SharePoint document libraries, and Microsoft Teams, thus magnifying the breach surface.

MFA-RESISTANT PHISHING

Cyber criminals have designed phishing attacks that can circumvent some types of multi-factor authentication (MFA) protections. Carefully created phishing campaigns linking to fake-but-realistic destination login sites have been able to bypass both short message service (SMS)-based and authenticator-app based second factor approaches, enabling successful account credential compromise. For example, Amnesty International noted the use of MFA-resistant phishing attacks on journalists and activists in the Middle East and North Africa. Several security experts have demonstrated similar attack methods.

Cyber criminals have designed phishing attacks that can circumvent some types of multi-factor authentication protections.

SUPPLY CHAIN THREATS: RANSOMWARE

Several variants of ransomware (e.g., Ryuk and Zeppelin) have been designed to inflict maximum damage on an ecosystem by targeting supply chain businesses, including those that supply cyber solutions to healthcare organizations. Compromising the hub through ransomware is devastatingly effective at amplifying the pain of an attack across hundreds or thousands of dependent organizations that, through no deficit of their own direct security infrastructure, have introduced a weak link in the chain. Several significant supply chain incidents happened during 2019 in healthcare:

- About 400 dental practices in the United States were locked out of their patient data in August 2019 after a ransomware attack against DDS Safe, a medical records retention and backup solution offered by The Digital Dental Record and PerCSoft.[xxxiii] While the intent of the service was to minimize the disruption caused by ransomware, it actually amplified it across a larger number of providers. The suppliers paid the ransom for the decryptor key, and shared this with affected parties, although some dental offices claimed some data remained unrecoverable.

- A Ryuk ransomware attack in November 2019 against Virtual Care Provider – a supplier of internet services, email, electronic patient records, billing and phone systems for 110 nursing homes in the United States – compromised all of its core offerings, as well as its own internal systems.[xxxiv] The attackers demanded a US$14 million ransom, which Virtual Care said it could not afford. Nurses at some nursing homes were unable to order new drugs for patients, and one nursing home was close to going out of business because of the ransomware attack. The attackers appear to have compromised Virtual Care in September 2018 through phishing attacks dropping Trickbot or Emotet (or both) onto the network.

- A ransomware attack against Complete Technology Solutions in December 2019, also a provider of IT services to the dental industry in the United States, resulted

in encryption affecting more than 100 dental offices.[xxxv] Complete Technology Solutions did not pay the ransom demand of US$700,000, but individual dental offices negotiated with the attackers to clean their own systems. The attackers used multiple encryption keys in the attack to complicate recovery attempts, with one dental office having to pay 20 different ransom notes to restore its 50 devices to operational status.

- Ryuk disrupted operations for 400 clinics aligned with National Veterinary Associates (NVA) in October 2019, compromising access to patient records, payment systems, and the day-to-day practice management software used across all clinics.[xxxvi] This was the second successful Ryuk ransomware attack against NVA during 2019.

These incidents followed a major breach in December 2017, in which Nuance suffered a NotPetya ransomware attack. While remediating that incident, hackers were able to access 45,000 individuals' healthcare records. The net loss from the incidents totaled $98 million[xxxvii].

SUPPLY CHAIN THREATS: DATA BREACHES

Data breaches at other firms in the supply chain create cyber threats for healthcare providers. A data breach of PHI at a supply chain firm responsible for billing, for example, creates an active data breach for the originating healthcare provider, as well, which incurs breach notification requirements and expenses. Incidents during 2019 included:

- A successful phishing attack at Magellan Health compromised patient data sourced from several health plans.[xxxviii] In October 2019, Geisinger Health Plan notified more than 5,800 of their patients that their data had been breached at Magellan. The following month, TeamCare did the same to almost 44,000 patients and the McLaren Health Plan notified an undisclosed number of their patients. All firms had a HIPAA Business Associate Agreement with Magellan Health, and yet all were still affected by the breach.

- More than 20 million patient records were breached in June 2019 at the American Medical Collection Agency (AMCA), a billing collections vendor for healthcare organizations.[xxxix] One affected client was Quest Diagnostics, although its relationship with AMCA was through an intermediary. Nonetheless, Quest notified patients about 11.9 million breached records, and quickly had almost 20 class actions filed in federal courts against itself. LabCorp, another client, notified patients about 7.7 million breach records in July, and Opko Health notified regarding 423,000 patient records.

Ransomware attacks often compromise patient records and can also compromise medical devices used for administering care.

RANSOMWARE CAUSES DATA BREACHES

Ransomware attacks often compromise patient records and can also compromise medical devices used for administering care. Campbell County Health faced a ransomware attack in September 2019 that affected medical devices used for radiology, endocrinology and respiratory therapy, and was forced to transfer patients to other hospital systems while recovery efforts were undertaken on the affected devices.[xl] Health records were also unavailable, which meant, among other implications, that patients seeking prescription repeats had to bring previous medication bottles to prove entitlements.

MISCONFIGURATION OF CLOUD SERVICES AND ON-PREMISES SERVERS

Healthcare providers using new cloud storage services may inadvertently misconfigure the sharing settings to enable public access to protected health information. Such misconfigurations have been called out for Amazon Web Services S3 Storage Buckets across multiple industries, but other cloud services – and even on-premises servers – have created breach opportunities against healthcare providers. For example:

- Back in 2016, St. Joseph Health System adopted a new file-sharing application for storing patient records, but left the default sharing settings activated.[xli] The consequence was that more than 30,000 patient records were publicly available for more than a year – these records had been indexed by Google.

- An employee at Medico of South Carolina in June 2019 inadvertently misconfigured the sharing settings on a new server, leaving the medical information on the server accessible over the Internet.[xlii]

- When Sunshine Behavior Health set up a new AWS S3 Storage Bucket, the sharing settings were wrong, which resulted in 93,000 patient records being publicly accessible for at least the August to November 2019 timeframe.[xliii] Patient records included full names, dates of birth, postal and email addresses, phone numbers, credit card numbers, and health insurance details. The misconfiguration was noticed by an external party, but it took multiple notifications before Sunshine properly secured its patient records.

OPPORTUNISTIC COMPROMISE ATTEMPTS

Healthcare providers that fall victim to cyber attacks are often quick to state that no patient records were breached. However, the mere notification of an incident creates space for other malicious actors to attempt to profit from the situation. For example, the ransomware attack at DCH System apparently led to no patient records being accessed by unauthorized people, but a week after the attack patients in the area were reportedly being contacted by phone and email from supposedly DCH personnel requesting personal information.[xliv] It is unknown whether this was purely an attempt by unrelated threat actors to leverage the chaos and uncertainty of the situation to gather data from customers, or actions directly initiated by the original cyber criminals.

Diagnosis: Highly Attractive and Highly Vulnerable

The healthcare industry offers a potent mixture of threat factors that together make the industry a prime target for cyber criminals. Given factors such as life-and-death situations where every second counts, sensitive data available in great volumes, and medical devices vulnerable to cyber attack, among others, it is no wonder that healthcare is relentlessly targeted for financial gain through extortion and cybertheft. The industry is at the same time highly attractive to cyber criminals and highly likely to be compromised.

Interactions between patients and healthcare providers generate large volumes of sensitive health data.

- **Continual Collection of Sensitive Health Data**
  Interactions between patients and healthcare providers generate large volumes of sensitive health data, such as patient records, lab results, medical images, and other sensitive and confidential information. This data must be protected from unauthorized access and theft, typically for decades, all the while making it available to the right people at the right time for the right reasons. And, unlike compromised credentials, compromised medical data (e.g., a patient's blood type or health condition) cannot be changed by the affected individuals.

- **Medical Data Must Be Available**
  Healthcare providers hold troves of electronic medical data on patients, and if this data is unavailable, patient safety and even viability are threatened. From incorrect interventions, to wrong prescriptions, and even missed medical checks, non-availability of medical data is a big red flag. Cyber criminals who are able to compromise PHI through ransomware, for example, can often extort a ransom payment from the healthcare provider due to these business continuity requirements.

- **Medical Data is Valuable**
  Data collected by healthcare providers for administering medical care has value to other actors beyond the original intent of its collection. For example, while a Social Security number can sell for $1, one patient record can sell for as much as $1,000[xlv]. While gaining this value is against data protection and data privacy regulations, both malicious insiders and external threat actors attempt to breach medical data to submit fraudulent claims to insurance providers, gather mistreated patients to include in class action suits, and streamline the identification of new patients for intake at other medical centers. Certain nation-state threat actors may be able to leverage deeply personal information contained in PHI for agent recruitment or coercion as well as medical research purposes.

- **Vulnerabilities Across Supply Chain Partners**
  Healthcare organizations rely on other firms to provide digital services, electronic records systems, lab services, billing collections, radiography, and more. Security vulnerabilities anywhere in the supply chain can result in non-operational systems (e.g., a ransomware attack against a supply chain partner) and breach notification requirements and expenses (e.g., when a billing collections firm is breached). Tight connections between businesses across a healthcare ecosystem can compromise an entire ecosystem.

- **Outdated Medical Devices**
  While general purpose computers, tablets and smartphones are used to coordinate healthcare, check schedules, and communicate with patients, a whole plethora of medical devices are used across the industry to monitor patients, supply health services, and diagnose conditions. Many of these medical devices are increasingly vulnerable to security threats, since they are based on legacy and unsupported operating systems that no longer receive security updates.

- **Stringent Compliance Obligations**
  Healthcare organizations are held to account to stringent compliance regulations, some of which have been in place for several decades (e.g., HIPAA in the United States, albeit with amendments over time) and the GDPR in Europe. Both require appropriate protections of health and sensitive personal data, both have breach notification requirements, both require formalized agreements when sensitive data is shared between firms, and both have a fines regime for non-compliance.

- **Systematically Poor Cybersecurity Readiness**
  Healthcare organizations exist to provide health care to patients, and while funding is frequently invested in new, cutting-edge treatments for patients, the industry has a history of systematic underinvestment in cyber security. Current IT and security infrastructures are increasingly outdated and vulnerable to new security threats, insufficient funding is allocated to new cyber security initiatives, and cybersecurity professionals with the right skillset can earn far more in other industries, thereby creating an industry-wide skills deficit. Moreover, with three out of five medical practices in the United States having fewer than 10 physicians, and another almost one in five being run by a sole physician, the industry structure means many medical practices lack the financial resources for high quality cyber security tools and dedicated security professionals.

Healthcare organizations are held to account to stringent compliance regulations, some of which have been in place for several decades.

Prognosis: Expectations of Changing Threat Dynamics

Healthcare organizations are in the spotlight for cyber criminals. In reviewing recent trends in cyber security, we expect to see the following threat dynamics against healthcare organizations over the next 24 months.

TIGHTENING THE SCREWS ON RANSOMWARE

Healthcare is already one of the top targeted industries for ransomware, but continued targeting only makes financial sense for cyber criminals if ransom demands are paid. Every time a healthcare organization pays the ransom (e.g., DCH Hospital System) this reinforces the ongoing return-on-investment opportunity from further ransomware attacks. Whenever a healthcare organization is able to recover without paying the ransom, or alternatively decides to go out of business due to the attack (e.g., Wood Ranch Medical, Brookside Medical), cyber criminals gain nothing and contemplate other targets. As there is no benefit to cyber criminals from ransomware attacks that don't lead to a ransom payment, we expect to see ongoing attempts to both frustrate recovery operations and raise the stakes on the extortion demand.

In terms of the first, recovery operations can be frustrated by encrypting backup systems, as well as the endpoints, or using multiple encryption keys to increase the likelihood of receiving a ransom payment. In terms of raising the stakes, the threat of releasing the encrypted data on the public Internet if the ransom demand is not paid is a tactic that has been used against government targets (e.g., City of Johannesburg in South Africa, October 2019),[xlvi] and the same is likely to be tried against healthcare too. Healthcare organizations have been quick to state that a ransomware attack didn't result in any patient data being breached through unauthorized access, but the threat of publishing the ransomed data if the ransom demand is not paid – whether the cyber criminals actually have the data to publish or not – is likely to increase the success rate of ransom demands being paid.

TARGETING SUPPLY CHAIN FIRMS

Disrupting a single healthcare entity through ransomware is often effective at forcing a ransomware payment, but targeting supply chain firms that provide electronic services to healthcare organizations is even more lucrative. Targeting the hub firm enables ransomware to spread quickly through a trusted network of customers, putting entire healthcare ecosystems at risk. Both the Ryuk and Zeppelin ransomware variants are specifically used in targeted attacks against supply chain firms in healthcare (and other industries too), and the immediate discordant effects across many customers amplifies the heat against the supply chain firm to quickly pay the ransom demand and get customers back into normal operational status. It is a maliciously effective approach; we expect to see ongoing attacks of this nature.

Insiders will keep stealing PHI for a variety of motivations.

ONLINE DATA THEFT BY INSIDERS

Insiders will keep stealing PHI for a variety of motivations. Human desires for pleasurable company (e.g., Andrew Stewart in the UK),[xlvii] extra financial gain through selling records to injury lawyers and other medical clinics (e.g., the contractor at NSW Ambulance,[xlviii] the employee at NYC Health & Hospitals Corp.,[xlix] etc.), and attempting to satiate curiosity will not go away whatever the regulations say. The healthcare industry collects data on patients in sensitive, stressful and difficult situations, and there is value to be gained by malicious insiders by leveraging data they have access to for purposes other than that for which it was collected.

MEDICAL DEVICES UNDER ATTACK

Medical devices offer too good of an opportunity for cyber criminals to be left alone, particularly with the impending demise of security updates for Windows 7, which powers many of the medical devices across the industry. The ability for a compromised medical device to be controlled by an external malicious actor to initiate deliberate malfunctioning at the worst possible time in a surgical operation or other medical procedure would be devastating for healthcare organizations and patients alike. Creating life-and-death situations that demand either immediate financial payment to a cyber criminal or opening the healthcare facility to a medical malpractice suit from the relatives of a deceased patient due to the incident will create a gold mine for cyber criminals.

Prescriptions: Solutions to Consider for Improving Cyber Security in Healthcare

Cyber security protections appear to become vitally important to healthcare organizations immediately after a ransomware attack, data breach, insider malicious act, or other such incident. Breach notifications that proclaim "we take this very seriously" almost always precede the statement that "we have implemented additional security measures," such as heightened authentication approaches, better anti-malware approaches, and updated mandatory security awareness training. Of course, as solutions embraced after an incident, there are also additional costs incurred in attempting to clean up after the mess, such as engaging a third-party forensics firm, notification to law enforcement, notification to all affected patients, and annual costs for credit and identity theft monitoring. Interestingly, in a negative sense, rushed security measures after a data breach or other lapse have also been shown to increase the mortality rate among patients, indicating that in the rush to throw solutions at the problem in the harsh light of public scrutiny, the appropriate balancing of patient care with security precautions is not considered.

A more pragmatic approach is required, starting with following standard risk management processes. Step one is to complete an enterprise-wide risk assessment, followed by identifying appropriate controls, then prioritizing remediation efforts and expenditure, and finally monitoring the efficacy of mitigations over time. There should be nothing surprising to healthcare providers in this approach, as it is required by the HIPAA Security Rule. We have noted above a variety of risks that healthcare providers are facing across the world, and in light of this generalized risk assessment, the following controls (mitigations, solutions, safeguards) should be considered. We start with the two that are most commonly mentioned by healthcare providers immediately after a breach or other incident.

Security awareness training is an essential strategy for activating people as a layer of security.

HEIGHTENED AUTHENTICATION APPROACHES

Authentication approaches that rely solely on a username and password have been shown to be easily compromised through phishing attacks. Something more is needed, with multi-factor authentication (MFA) a very common recommendation for strengthening authentication. However, the way that MFA is enabled makes a difference, with SMS codes delivered to a phone and even Authenticator app codes being compromised during the past couple of years. Hardware tokens based on the FIDO2/WebAuthn standard are currently the best way of enabling MFA, because they are both phishing resistant and much faster than either SMS or app codes to use. Given that every second counts in certain medical situations, waiting for an SMS code to arrive is courting death.

PROTECT THE EMAIL CHANNEL

Because email continues to be a key threat vector for ransomware, phishing, breaches of PHI, and so forth, it is essential to provide the appropriate controls for email in every healthcare organization in the supply chain. These controls include encryption of sensitive content like PHI; data loss prevention controls to monitor, and when necessary block, what is being sent; preventing "type ahead" errors in which emails can be inadvertently sent to the wrong person; and so forth.

SECURITY AWARENESS TRAINING

Effective protections cover the gamut of the people, process and technology triad, and so security awareness training is an essential strategy for activating people as a layer of security. The FBI has recently stressed the importance of awareness and training for people, in addition to technology-based solutions and process revisions for improving a security posture. Security awareness training must cover topics like warning signals for phishing and other social engineering attacks, being alert to where PHI is stored and how to protect these places, and reinforcing the correct way

of sharing or disposing of health data. The importance of confidentiality and appropriate access to all PHI is equally important to stress, as happened at the Aegis Medical Group, for example, after an incident of employee theft of patient records in 2019.[i]

EVASIVE THREAT PROTECTION

No amount of training will make humans perfect, so appropriate compensating controls must be put in place for the cases when an employee clicks on a link or opens a document. Moreover, in targeted attacks, cyber threat actors are willing to work stealthily to extend an initial foothold across as wide an attack surface as possible. Victims targeted by Ryuk ransomware, for example, may be compromised for months or years before the ransomware attack is initiated, during which time the cyber threat actors are mapping network resources and gaining control of additional footholds. Advanced adversaries employ highly evasive techniques, such as living-off-the-land tools, fileless or in-memory only malware and are not reusing known malicious attributes that antivirus and traditional endpoint detection and response (EDR) tools rely upon. Reliance on threat intelligence (patient zero) and past attacks may not protect organizations from advanced, evasive and novel threats. Healthcare organizations must seek solutions that offer endpoint and server protection without the reliance on any known TTPs, attacks or IOCs. Instead of using behavior or machine learning models, those solutions typically leverage a positive security model.

MONITORING AND PROMPTLY ADDRESSING VULNERABILITIES

As soon as vendors advise of vulnerabilities in operating systems and applications, cyber threat actors go to work developing kits to leverage these vulnerabilities. Ongoing monitoring of all endpoints, servers and medical devices for known and discovered vulnerabilities gives up-to-date insight on where remediation activities are needed, either through patching if available or isolation until an update can be implemented.

STRENGTHEN IDENTITY ACCESS CONTROLS

While creating strong, frequently changed and unique passwords is a recommended best practice, it often is inadequate. Users will forget them, incrementally numerate passwords to simplifying recall, or write them down. Once credentials have been compromised – even if it's a long password or a passphrase – cyber criminals still can gain access. Strengthen access controls through new approaches that do not rely on passwords, either by removing passwords altogether in favor of FIDO2-enabled passwordless authentication or some other modern authentication mechanism.

STRONG MULTI-FACTOR AUTHENTICATION (MFA)

Reliance on a username and password for controlling access to systems is no longer enough for any employee with access to sensitive data like PHI. If access credentials can be compromised simply by asking for them through a phishing campaign, an attacker can take whatever data they want, when they want it, or use modular malware to extend from an initial foothold to compromising additional systems and planting malware for a subsequent and more devastating attack. Approaches for MFA are available on a good-better-best continuum, with good (SMS code, email notification) and better (Authenticator app) approaches still being vulnerable to carefully designed phishing attacks. At present, the best approach, which ideally would be provisioned for all employees who have access to PHI and other sensitive data, is to use modern hardware security keys based on FIDO2/WebAuthn that use public-key cryptography. These also provide an additional promise of secure passwordless logins – the "holy grail" for authentication. Some security keys provide multi-protocol support so that organizations can easily bridge between legacy systems and those supporting modern authentication protocols. While any approach to MFA is better than doing nothing, continuing with approaches that have already been compromised and expecting a different outcome is not advised.

Reliance on a username and password for controlling access to systems is no longer enough for any employee with access to sensitive data like PHI.

AUTOMATED ADHERENCE TO SECURITY PROCESSES

A Cloud Access Security Broker (CASB) provides capabilities for automatically checking the security posture of discovered cloud services, and can alert when anomalous behavior and settings are identified. For example, leading CASBs can check the sharing settings on Amazon S3 storage buckets (and other cloud sharing services), and alert if these are set inappropriately so corrective actions can be taken. Likewise, if unusual IP address access is identified, or impossible travel conditions for simultaneous logins are noticed, heightened authentication requirements can be automatically requested (and logged for subsequent analysis). In the face of a systemic storage of cybersecurity professionals in healthcare, tools that support automated adherence to security policies amplifies the abilities of these limited people resources.

PHISHING PROTECTIONS

Phishing attacks are commonly used by cyber threat actors to compromise account credentials, plant ransomware, and gain access to systems containing sensitive health data. Protecting against phishing attacks through analysis of attachments and links for malicious behavior patterns, hardening email authentication using SPF, DKIM and DMARC policy settings, and scanning for impersonation offer technology solutions to decrease the likelihood of a successful phishing attack. Combined with security awareness training and strong multi-factor authentication approaches, anti-phishing protections enable healthcare providers to reduce the likelihood of being compromised.

REDUCE THE ATTACK SURFACE

Various approaches exist for reducing the space in which an attack can successfully execute. Security awareness training is an effective approach we have already discussed. For managing endpoints, application whitelisting and data encryption plays a role in reducing the space for compromise and the space for unauthorized access to sensitive data. For network access, using pre-defined IP addresses and IP ranges reduces the ability for threat actors to gain a foothold. For application access, the principle of least privilege ensures that people can access only what they need when they need it, rather than having open access to everything.

Supply chain attacks during 2019 have wreaked havoc on healthcare providers.

HARDEN MEDICAL DEVICES

Catalog the medical devices within a network estate, and ascertain the risks associated with each device or collection of devices. For example, known vulnerabilities that have not been patched are risks. Equally, devices that run on Windows 7 are risky as well, and will become riskier from mid-January 2020 when Windows 7 goes out of active support from Microsoft and security updates are no longer provided. If risky devices cannot be updated or upgraded - and capital costs are a factor in these calculations - look for solutions that layer security protections on medical devices, for example, by limiting the processes that can be executed. Any devices that can be patched should be enrolled in automated patching processes, and any devices or applications that are obsolete and no longer required should be decommissioned appropriately.

HARDEN THE SUPPLY CHAIN

Supply chain attacks during 2019 have wreaked havoc on healthcare providers, indicating that security audits and attestations are not fully factored into supply chain decisions. Both HIPAA and GDPR require a due diligence process for any supply chain firm that will have access to personal and sensitive data. Various industry certifications – for example ISO 27001 and ISO 27018 – provide independent evidence that a firm has appropriate processes and protections in place. Cost of service must not be the only decision factor in selecting supply chain partners; maturity of security processes are even more important. Equally, security audits and attestations are not a one-time event; the need for up-to-date evidence is ongoing.

AUTOMATED DATA CLASSIFICATION

Implementing protections for sensitive health data requires the ability to identify the presence of such data. In structured systems, such as electronic health records (EHR), classification can be undertaken by design. In unstructured systems, such as email accounts, which are easier for an external actor to compromise through a phishing attack than an EHR, classification must be tuned for the specific organization by policy settings. Automatically identifying sensitive data through common alphanumeric patterns or regular expressions (regex) enables automated protections to be applied, such as encryption or other rights management.

RANSOMWARE-RESISTANT BACKUPS

Recovering from a ransomware attack usually requires paying the ransom demand to obtain the decryption keys, or using viable backups to restore normal operations. If viable backups or not available, a healthcare provider must either pay the ransom demand (and hope for the best) or cease operations (which we saw a couple of times during 2019, e.g., at Wood Ranch Medical). How backups are created is vitally important, because if the backup system is also compromised by ransomware or fails for other purposes, recovery is compromised, e.g., the backups at Wood Ranch Medical were also encrypted in its ransomware attack, and the attack at Brooklyn Hospital Center in late July 2019 resulted in unrecoverable PHI, indicating the lack of a proper backup system. Onsite backups are a good first step, but offsite backups held by a third-party are even more important.

Summary

The healthcare industry is currently – and will remain – a high-value target for cyber criminals. There are too many opportunities ripe for the picking to extort ransom payments, breach sensitive health data for insurance fraud, and find disaffected patients for class action suits. The industry has a record of systematic underinvestment in cyber security protections, and the increased rate of attacks and successful incidents during 2019 is a sad testament to its vulnerability. Given the evidence and fallout from incidents during 2019, all healthcare providers must take urgent action to protect the vulnerable patients they serve by shoring up effective cyber security protections.

Sponsor of This White Paper

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

Balancing security and usability has always been a challenge, and many existing authentication methods today struggle to deliver on both. Software-based authentication solutions, including passwords, SMS, and mobile apps, are all increasingly vulnerable to malware, phishing scams, or man-in-the-middle attacks. On the other hand, more secure hardware authentication solutions, like traditional smart cards, are difficult to use and deploy. Yubico's flagship product, the YubiKey, changes this.

The YubiKey is a hardware-based authentication solution that provides superior defense against account takeovers and enables compliance. The YubiKey offers strong authentication with support for multiple protocols, including FIDO U2F, PIV (smart card authentication), OpenPGP, one-time password, and WebAuthn/FIDO2, the new open web standards enabling the replacement of weak password-based authentication with public key cryptography. With its unique multi-protocol support, the YubiKey delivers strong hardware protection across any number of IT systems and online services — all with just a simple touch. The YubiKey is easy to use, fast and reliable, and is proven at scale to significantly reduce IT costs and eliminate account takeovers.

yubico

www.yubico.com

@Yubico

+1 844 205 6787

sales@yubico.com

Yubico also offers the YubiHSM 2, an ultra-portable hardware security module that enables organizations of all sizes to protect secrets stored on servers. It enhances cryptographic key security throughout the entire lifecycle, reduces risk, and ensures adherence with compliance regulations.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.

REFERENCES

[i] Meera Narendra, Another Healthcare Organisation Struck by Ransomware, November 2019, at https://gdpr.report/news/2019/11/28/privacy-another-healthcare-organisation-struck-by-ransomware/

[ii] Meera Narendra, French Hospital Hit by Ransomware, November 2019, at https://gdpr.report/news/2019/11/21/privacy-french-hospital-hit-by-ransomware/

[iii] Government of Victoria, Cyber Health Incident, October 2019, at https://www.vic.gov.au/cyber-health-incident

[iv] Stephen White, US Study Reveals Leading Healthcare Cybersecurity Challenges, November 2019, at https://gdpr.report/news/2019/11/21/privacy-us-study-reveals-leading-healthcare-cybersecurity-challenges/

[v] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[vi] Ionut Ilascu, Over 38 Million Healthcare Records Exposed in Breaches Over 2019, November 2019, at https://www.bleepingcomputer.com/news/security/over-38-million-healthcare-records-exposed-in-breaches-over-2019/

[vii] Ionut Ilascu, Over 38 Million Healthcare Records Exposed in Breaches Over 2019, November 2019, at https://www.bleepingcomputer.com/news/security/over-38-million-healthcare-records-exposed-in-breaches-over-2019/

[viii] Meera Narendra, French Hospital Hit by Ransomware, November 2019, at https://gdpr.report/news/2019/11/21/privacy-french-hospital-hit-by-ransomware/

[ix] Danny Palmer, Ransomware: These four industries are the most frequently attacked, May 2017, at http://www.zdnet.com/article/ransomware-these-four-industries-are-the-most-frequently-attacked/

[x] Allen Kim, In the Last 10 Months, 140 Local Governments, Police Stations and Hospitals Have Been Held Hostage by Ransomware Attacks, October 2019, at https://edition.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html

[xi] Dan Kobialba, Ransomware Attack Count Total for 2019 (So Far), October 2019, at https://www.msspalert.com/cybersecurity-research/ransomware-attack-count-2019/

[xii] Ionut Ilascu, Brooklyn Hospital Loses Patient Data in Ransomware Attack, November 2019, at https://www.bleepingcomputer.com/news/security/brooklyn-hospital-loses-patient-data-in-ransomware-attack/

[xiii] Lawrence Abrams, DCH Hospital Pays Ryuk Ransomware for Decryption Key, October 2019, at https://www.bleepingcomputer.com/news/security/dch-hospital-pays-ryuk-ransomware-for-decryption-key/

[xiv] Bill Toulas, French Hospital Had 6000 Computers Locked Down by Ransomware Attack, November 2019, at https://www.technadu.com/french-hospital-6000-computers-locked-down-ransomware-attack/85569/

[xv] Great Plains Health, Great Plains Health Page on Facebook - for November-December 2019, December 2019, at https://www.facebook.com/GPHealth/posts/3783101891715576

[xvi] Meera Narendra, Sentara Hospitals to Pay $2.175m Fine Over HIPAA Violation, December 2019, at https://gdpr.report/news/2019/12/03/privacy-sentara-hospitals-to-pay-2-175m-fine-over-hipaa-violation/

[xvii] DataBreaches.net, Fine Against Hospital Due to Data Protection Deficits in Patient Management, December 2019, at https://www.databreaches.net/fine-against-hospital-due-to-data-protection-deficits-in-patient-management/

[xviii] Ionut Ilascu, Over 38 Million Healthcare Records Exposed in Breaches Over 2019, November 2019, at https://www.bleepingcomputer.com/news/security/over-38-million-healthcare-records-exposed-in-breaches-over-2019/

[xix] Bay City News, Privacy Breach Involving Meal Tray Tickets at Zuckerberg SF General Hospital, December 2019, at https://www.nbcbayarea.com/news/local/san-francisco/privacy-breach-involving-meal-tray-tickets-at-zuckerberg-san-francisco-general-hospital-dph/2192937/

[xx] https://www.hipaajournal.com/another-employee-is-fired-for-emailing-phi-to-a-personal-account-3581/

[xxi] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[xxii] Gus McCubbing, NSW Ambos Win $275,000 Class Action Payout After Major Data Breach, December 2019, at https://www.smh.com.au/national/nsw/nsw-ambos-win-275-000-class-action-payout-after-major-data-breach-20191210-p53ihu.html

[xxiii] DataBreaches.net, NYC Health & Hospitals Corp. Investigating Alleged Employee Wrongdoing, December 2019, at https://www.databreaches.net/nyc-health-hospitals-corp-investigating-alleged-employee-wrongdoing/

[xxiv] Payne Ray, Mount Dora Medical Company Reports Minor Data Breach, November 2019, at https://www.gainesville.com/news/20191111/mount-dora-medical-company-reports-minor-data-breach

[xxv] Ionut Ilascu, Over 38 Million Healthcare Records Exposed in Breaches Over 2019, November 2019, at https://www.bleepingcomputer.com/news/security/over-38-million-healthcare-records-exposed-in-breaches-over-2019/

[xxvi] Nicole Perlroth, Two From China Are Charged in 2014 Anthem Data Breach, May 2019, at https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html

[xxvii] Maxine Bernstein, Premera Blue Cross to Pay $74M Over Data Breach, July 2019, at https://www.govtech.com/security/Premera-Blue-Cross-to-Pay-74M-Over-Data-Breach.html

[xxviii] Jessica Kim Cohen, Banner Health Agrees to $6 Million Settlement over 2016 Breach, December 2019, at https://www.modernhealthcare.com/cybersecurity/banner-health-agrees-6-million-settlement-over-2016-breach

[xxix] Jessica Davis, Ransomware Attack Forces Great Plains Health to EHR Downtime, November 2019, at https://healthitsecurity.com/news/ransomware-attack-forces-great-plains-health-to-ehr-downtime

[xxx] DataBreaches.net, Kalispell Hospital Sued Over Data Breach, December 2019, at https://www.databreaches.net/kalispell-hospital-sued-over-data-breach/

[xxxi] Melissa Cunningham, Fears Over Patient Data Breach After Cyberattack on Monash IVF, December 2019, at https://www.smh.com.au/national/fears-over-patient-data-breach-after-cyber-attack-on-monash-ivf-20191203-p53gj0.html

[xxxii] HIPAA Journal, Great Plains Health Ransomware Attack Prevents Access to Patient Medical Records, November 2019, at https://www.hipaajournal.com/great-plains-health-ransomware-attack-prevents-access-to-patient-medical-records/

[xxxiii] Adam Janofsky, Smaller Medical Providers Get Burned by Ransomware, October 2019, at https://www.wsj.com/articles/smaller-medical-providers-get-burned-by-ransomware-11570366801

[xxxiv] Meera Narendra, Over 100 Nursing Homes Across the US Struck by Ransomware, November 2019, at https://gdpr.report/news/2019/11/26/privacy-over-100-nursing-homes-across-the-us-struck-by-ransomware/

[xxxv] DataBreaches.net, Ransomware at Colorado IT Provider Affects 100+ Dental Offices, December 2019, at https://www.databreaches.net/ransomware-at-colorado-it-provider-affects-100-dental-offices/

[xxxvi] Meera Narendra, Ryuk Ransomware Hits 400 Veterinary Hospitals, November 2019, at https://gdpr.report/news/2019/11/21/privacy-ryuk-ransomware-hits-400-veterinary-hospitals/

[xxxvii] https://www.healthcareitnews.com/news/hackers-hit-nuance-again-2017-while-notpetya-cost-98-million-lost-revenue

[xxxviii] DataBreaches.net, More Details Emerge on Magellan Healthcare Breach, December 2019, at https://www.databreaches.net/more-details-emerge-on-magellan-healthcare-breach/

[xxxix] Taylor Armerding, Cost of Data Breaches in 2019: The 4 Worst Hits on the Corporate Wallet, December 2019, at https://securityboulevard.com/2019/12/cost-of-data-breaches-in-2019-the-4-worst-hits-on-the-corporate-wallet/

[xl] Adam Janofsky, Smaller Medical Providers Get Burned by Ransomware, October 2019, at https://www.wsj.com/articles/smaller-medical-providers-get-burned-by-ransomware-11570366801

[xli] HIPAA Journal, St. Joseph Health to Pay OCR $2.14 Million to Settle HIPAA Case, October 2016, at https://www.hipaajournal.com/st-joseph-health-pay-ocr-2140500-settle-hipaa-case-3638/

[xlii] DataBreaches.net, Months After Notifying Patients of a Leak, Medico Issues Press Release, December 2019, at https://www.databreaches.net/months-after-notifying-patients-of-a-leak-medico-issues-press-release/

[xliii] Meera Narendra, Over 90K Patient Billing Files Exposed Online, November 2019, at https://gdpr.report/news/2019/11/15/privacy-over-90k-patient-billing-files-exposed-online/

[xliv] DCH Health System, DCH Ongoing Response to Cyberattack and IT System Outage, October 2019, at https://www.dchsystem.com/Articles/dch_ongoing_response_to_cyberattack_and_it_system_outage.aspx

[xlv] https://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html

[xlvi] Tom Jowitt, City of Johannesburg Threatened With Ransomware Data Release, October 2019, at https://www.silicon.co.uk/security/cyberwar/city-of-johannesburg-threatened-299737

[xlvii] Sophie Law, NHS radiographer, 32, faces jail after illegally accessing more than 200 female patients' personal records before hounding them for dates, December 2019, at https://www.dailymail.co.uk/news/article-7764599/NHS-radiographer-32-faces-jail-illegally-accessing-records-hounding-dates.html

[xlviii] Andy Park, NSW Ambulance Contractor Stole 130 Paramedics' Personal Files and Stole Them, October 2016, at https://www.abc.net.au/news/2016-10-21/nsw-ambulance-contactor-stole-paramedics-workers-comp-files/7956046

[xlix] DataBreaches.net, NYC Health & Hospitals Corp. Investigating Alleged Employee Wrongdoing, December 2019, at https://www.databreaches.net/nyc-health-hospitals-corp-investigating-alleged-employee-wrongdoing/

[1] HIPAA Journal, Former Aegis Medical Group Employee Potentially Accessed 9,800 Records Without Authorization, November 2019, at https://www.hipaajournal.com/former-aegis-medical-group-employee-potentially-accessed-9800-records-without-authorization/