PONDURANCE

More Than Financial Loss —
Protect Your Healthcare Practice and Patients From Ransomware

INTRODUCTION

Healthcare is one of the largest and fastest-growing industries, consisting of hospitals, clinics, drug and medical devices, and insurance providers. Many healthcare providers operate 24/7 to provide necessary ongoing or emergency care for patients. The ongoing global pandemic affected millions of lives and shed light on the criticality of these services and the upstream supply chain in support of human survival. Opportunistic cybercriminals seized on this opportunity and doubled down on their attacks against healthcare organizations. While dedicated healthcare professionals worked around the clock to save lives in the fight against COVID-19, cybercriminals leveraged this time to launch ransomware attacks at a frenzied pace. In 2020, cyberattacks targeting healthcare organizations increased by 55%[1] and disrupted already-strained medical resources, costing the healthcare industry $20.8 billion in downtime.[2]

In 2021, **24 million** patient records were exposed as a result of healthcare cyberattacks.[1]

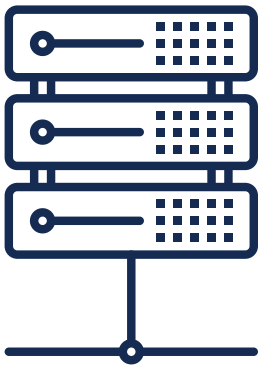
Healthcare facilities of all sizes continue to be prime targets for ransomware attacks, primarily due to the amount of patient data they process, outdated systems and devices, and lack of security awareness training. In a ransomware attack, sensitive data, systems, and other digital resources are held hostage by financially motivated bad actors who demand payment to unlock the information. These bad actors and their extensive network of accomplices pose multiple risks to healthcare organizations including: 1) impact of patient care and safety; 2) disruption of business operations; and 3) disclosure of sensitive information.

Attackers have proven their ability to paralyze an organization's daily operations, impacting the privacy and safety of its patients. The ransomware industry will continue to evolve, but the underlying techniques for gaining access to sensitive health data have primarily stayed the same. Once an attacker gains access to secure medical systems or devices, attackers will encrypt files using malware, locking out administrators and users. Ransomware gangs are becoming increasingly relentless in their tactics and have recently begun encrypting backup files before encrypting live systems, making it even harder for organizations to avoid paying the ransom.

Pondurance security analysts have spent a considerable amount of time analyzing common attack patterns within a complex healthcare landscape to improve cybersecurity defenses, reduce compromise, shorten dwell time, and prevent damaging ransomware outcomes. Healthcare organizations can still focus on elevating their cybersecurity programs by bringing *people, processes, and technology* together to prevent and stop the spread of ransomware within their IT and Internet of Things (IoT) devices and networks.

From a business perspective, implementing 24/7 monitoring, detection and response; securing the domain controller, often referred to as the heart of the network; and implementing signature-less endpoint detection and response are smart investments that healthcare executives can put toward defending their networks and assuring patient care.

A compromised domain controller is by far the most common denominator related to large-scale ransomware events. It verifies which users and endpoints are allowed to access resources on a healthcare network.



PONDURANCE

CHALLENGES IN THE HEALTHCARE INDUSTRY

Leaders in the healthcare industry face a myriad of challenges, with COVID-19 overshadowing critical cybersecurity challenges. The Centers for Disease Control and Prevention (CDC) advised a nationwide quarantine to reduce the spread of the virus. Today, post-pandemic, physicians deal with a significant increase in mental health issues and sicker patients because of the delayed care patients had to endure from the pandemic.

Unfortunately, securing medical devices and networks may not seem like a high priority compared to challenges that include saving lives, but the impact of cyber threats expands far beyond financial challenges.

Let's explore the top four cybersecurity challenges that security professionals in the healthcare industry anticipate in the second half of 2021, according to a recent Pondurance study:

HOW RANSOMWARE ATTACKS SUCCEED

Carrying out a successful ransomware attack involves a variety of moving pieces. Some bad actors leverage botnets to carry out their attacks, while others buy lists of compromised credentials used for credential stuffing. Hackers even sell ransomware software or direct network access on the dark web, simplifying ransomware attacks on healthcare organizations.

COVID-19

The pandemic played a huge role in launching successful ransomware attacks against healthcare organizations. While frontline medical workers continued to work on-site, the majority of healthcare organizations connected with patients through telehealth services. As more hospitals and providers rely on telehealth, 76% of U.S. hospitals utilize these applications to communicate with patients and other consulting practitioners.[3] This accelerated digitization increased the attack surface by exposing more network ports, adding new software dependencies, and increasing the use of cloud services.

LIMITED FUNDING

Healthcare organizations are understaffed and underfunded when it comes to cybersecurity. As new threats emerge, it can be difficult for healthcare leaders to know where they should invest funding. Most small and midsize health organizations do not have the capacity or the capital to invest in a 24/7 internal security operations center (SOC).

IMPERSONATION

From phishing and business email compromise (BEC) to stolen credentials and social engineering, impersonation is a classic way for attackers to access sensitive health data. Amid the COVID-19 pandemic, security professionals saw a significant increase in phishing attacks related to COVID-19 topics. In fact, phishing was the top attack vector seen by the Pondurance security analysts. Attackers are exceptionally skilled in the art of impersonating individuals and taking advantage of humans and system weaknesses. It can be challenging for healthcare professionals to stay vigilant, especially when a day in the life of a physician can consist of dealing with critical medical emergencies.

PONDURANCE

DOUBLE EXTORTION

Ransomware gangs are sophisticated and highly organized. They break access into healthcare infrastructure to encrypt files and demand a ransom payment to decrypt the data, including threatening to leak the stolen information if an additional payment is not made. Recently, attackers have been favoring this method of extortion to maximize return on investment as hospitals continue to digitize more and more patient and medical data.

RANSOMWARE-AS-A-SERVICE

Ransomware attacks are becoming more widespread than ever and have proven to be a lucrative business for cybercriminals. Rogue developers are selling or leasing malware to users, operating a ransomware-as-a-service (RaaS) model. The developer gets a portion of the ransom payment. RaaS allows low-level attackers to launch ransomware campaigns on healthcare organizations while having a direct customer support line to ensure a successful attack.

DOMAIN CONTROLLER

The domain controller is seen as the heart of any distributed network, making it a valuable asset within any medical IT infrastructure. The domain controller is a server that verifies requests and confirms the users on a healthcare network are who they say they are by checking the usernames, passwords, and other credentials and then deciding whether to allow or deny access to the users.

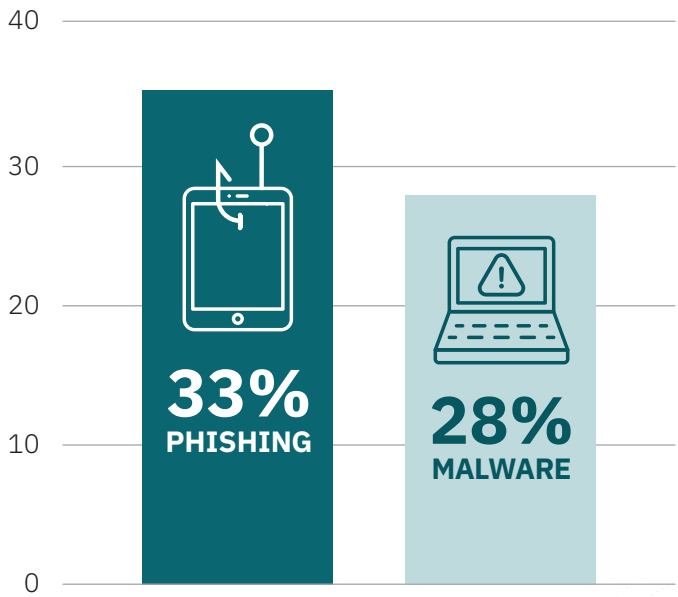
Cybercriminals use the domain controller as a gateway to access the domain administrator or enterprise administrator privileges to gain wide access and spread malware for a successful ransomware attack. Compromising the domain controller can result in unauthorized access to:

- Financial and payment information.
- Electronic health records (EHR).
- Medical intellectual property and medical research.
- Medical staff's user credentials.

WHY ARE HOSPITALS THE PRIME TARGET FOR RANSOMWARE?

Hospitals are a 27/4 operation. Attackers are human, and they look for the lowest-risk, highest-reward opportunities. Ransomware is more profitable when lives are at risk. Modern ransomware techniques have proven that it is not only about the data when attacking a hospital. The goal is to paralyze the network to ensure executives pay the ransom to get hospital operations back online. The following factors are contributing to the recent and ongoing surge of ransomware attacks:

- **Human error and misconfiguration.** Often the medical staff is fatigued from working long hours, which makes it easier for the staff to be susceptible to weak passwords, phishing emails, and system misconfigurations. The medical staff needs to be trained to identify security threats such as phishing and social engineering tactics. Still, at the same time, it is easier said than done when you have little time on your hands to determine if an email is a phishing email.
- **Phishing is a common gateway to ransomware.** It only takes one infected email to gain access to the network. Phishing attacks continue to be the top attack type seen by the Pondurance security analysts. In the first quarter of 2021, 33% of attacks detected were phishing attacks.



- **EHR is a valuable commodity.** Hospitals are leveraging digital technology to digitize medical records, Social Security numbers, payment information, and medical data to improve patient services. EHR enables hospitals to ingest and provide more accurate, up-to-date information to document and forecast the progress of treatments and practices and prevent disease. Attackers see this information as a gold mine for medical identity theft.
- **Legacy systems and medical devices are nearly impossible to harden.** The fear of disrupting patient services is often the primary reason healthcare organizations fail to keep their systems up to date. Medical devices could run outdated vendor firmware that represents a more significant threat to the network. Often these devices are not created with security in mind, having weak authentication and, in some cases, hardcoded credentials. In addition, the data transfer firmware is unsecured and unencrypted, resulting in the risk of exposing electronic protected health information (PHI) in patient monitors, MRI machines, VoIP phones, printers, and more.
- **Limited cybersecurity staff is an epidemic in the fight against cybercrime.** The medical industry is not the only sector that is affected by the lack of cybersecurity talent. Healthcare is struggling to find employees with cybersecurity-related skills, and overall it is expensive to hire and retain cybersecurity professionals. On average, it takes 70% longer to fill cybersecurity positions in the healthcare industry than IT jobs.[4]
- **Third-party risks.** Organizations of all sizes have experienced their fair share of cyberattacks due to third-party and vendor risks. The healthcare industry is not any different, and third-party risks are among the most significant vulnerabilities that providers and payers face. In fact, according to a Pondurance study, 42% of enterprise healthcare organizations say third-party and vendor risks are the leading cybersecurity and privacy challenges they face in today's threat landscape.

RANSOMWARE COSTS TO CONSIDER

In 2020, ransomware attempts against the healthcare sector rose by 123%, while attackers collected more than $2.1 million in ransom payments.[5] The ransom payments are only part of the total cost of the attack, while other contributors such as downtime, legal, and public relations have a significant impact on a healthcare organization's bottom line.

Downtime costs are some of the most considerable financial losses associated with a ransomware attack. It can take days, even weeks, to get a hospital back online after an attack. To reduce the costs associated with downtime, having an incident response plan is critical to react, respond, and recover from an attack.

Ransomware costs the healthcare industry **$20.8 billion** in downtime.[2]

Security upgrade costs are major contributors when recovering from ransomware. Healthcare organizations face unavoidable costs to upscale an entire IT staff with more security analysts and compliance managers. Those costs run even higher if healthcare leaders plan to upgrade healthcare technology and tools because they may need to hire more staff to manage and implement these tools.

Legal costs and reputation damage can cost the healthcare industry on average $20.8 billion in lawsuits[4] and other recovery costs. Ransomware attacks, including data breaches, often result in reputation damage, legal damages, and financial loss and can affect a healthcare organization well after a ransomware attack concludes.

HIPAA and regulatory costs are major cost factors of a ransomware attack. Organizations that are HIPAA-covered entities are subject to high fines if PHI is involved in a cyberattack. Fines for violating HIPAA can range from $100 to $50,000 per violation or per record, with a maximum penalty of $1.5 million per year for each violation.[6]

$7.13 million is the average total cost of a data breach in the healthcare industry.

PROTECTING HEALTHCARE FROM RANSOMWARE

Cyber threats can penetrate a healthcare network in a variety of ways. However, prioritizing people, processes, and technology can make a significant difference in protecting the most vulnerable avenues of a medical network. Healthcare organizations can follow the recommendations below to prevent ransomware.

- **Keep all computers and medical devices patched** as frequently as possible. Run scheduled checks to ensure all software is up to date.
- **Multi-factor authentication (MFA)** is a valuable tool to protect against the rise in credential theft. Ensuring medical staff is leveraging MFA for all logins is an added layer of security for domain-level systems and can eliminate credential stuffing attacks by botnets.
- **Limit user access.** Users should only have regular access to the resources they need and level of access.
- **Allow only authorized applications.** Configure operating systems and/or third-party medical services to run only approved applications.
- **Network segmentation** is a key strategy to securing connected medical devices. Isolating them as much as possible from non-communicating devices can limit the risk of infection if a ransomware attack is deployed. Blocking external communication and avoiding the connection of devices to the internet unless required by the vendor can also reduce risks. Devices that cannot be patched should also be isolated from the network to reduce the attack surface associated with that specific device. Lastly, restricting personally owned devices on medical networks is key to preventing ransomware attacks.
- **Limit remote access as much as possible.** If remote desktop protocol is enabled, ensure there are compensating controls associated with it, such as registered origin IP addresses, destination-only access, and individual credentials with MFA added. Medical IT staff must limit remote access as much as possible to reduce the attack surface.
- **Establishing 360-degree visibility** to medical networks and devices, logs, and cloud infrastructure is key to eliminating blind spots. Monitor and analyze logs to ensure in-depth 360-degree visibility is properly implemented. HIPAA requires that healthcare-covered entities have the proper technical safeguards in place to protect and monitor electronic health information (EHI) adequately.
- **Monitor and analyze logs.** Logging alone is not sufficient, and healthcare organizations require trained security analysts to triage any and all incoming security alerts. Monitor your medical IT infrastructure, medical devices, and domain controller at a system and application log level. In addition, monitoring access logs for anomalies such as nondomain IP addresses for failed attempts is key to stopping bad actors. Implementing endpoint detection and remediation can provide visibility into all endpoints such as laptops and computers being used within a medical network.
- **Constant security awareness training** is critical to consistently arm medical staff with the much-needed knowledge of detecting and responding to common phishing and social engineering techniques. In addition, educate the staff on why creating a strong password can protect EHI and reduce the probability of a data breach or attack caused by human error.
- **Encrypt endpoints.** The use of full disk encryption makes a great deal of sense on a number of levels when dealing with medical data. A healthcare organization should not make it easy for a bad actor to access protected and regulated HIPAA information successfully.

CONCLUSION

Ransomware affects more than financial loss. These attacks can affect patient services and paralyze medical operations with little to no physical damage. As healthcare budgets continue to be strained, healthcare organizations are turning to outsourced cybersecurity to help lessen the burden of these attacks. Healthcare organizations need to invest in an SOC that offers 24/7 monitoring and a managed detection and response (MDR) service that acts as an extension to their existing security team.

The odds of organizations recovering from a ransomware attack without paying ransom are slim to none these days. Bad actors want to get paid for their efforts, and their tactics are getting even more relentless in today's threat landscape.

Healthcare leaders need a comprehensive cybersecurity model that incorporates 24/7 monitoring to reduce blind spots at the highest level. As ransomware attacks continue to increase in frequency and evolve in sophistication over time, it is critical that healthcare security professionals be aware of current attack patterns that lead to unauthorized access to medical networks. The cost of ransomware has only increased year over year. Healthcare organizations should monitor their assets with a holistic cyberdefense solution and prioritize security awareness training throughout the entire organization.

ABOUT PONDURANCE

Pondurance delivers world-class MDR services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your team can focus on what matters the most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk.

Sources:
1. Healthcare Cyber Attacks Rise by 55%, Over 26 Million in the U.S. Impacted, CPO Magazine, February 26, 2021.
2. 2020 offered a 'perfect storm' for cybercriminals with ransomware attacks costing the industry $21B, Fierce Healthcare, March 26, 2021.
3. Fact Sheet: Telehealth, American Hospital Association, 2021.
4. Why hospitals, health systems are facing a cybersecurity talent shortage, Becker's Health IT, November 13, 2020.
5. 2021 SONICWALL Cyber Threat Report, SONICWALL, 2021.
6. What are the Penalties for HIPAA Violations?, HIPAA Journal, March 9, 2020.

pondurance.com
500 N. Meridian St., Suite 500, Indianapolis, IN 46204