Cyber Risks to The Healthcare Industry

INTRODUCTION - WHY ARE ATTACKS AGAINST HEALTHCARE INSTITUTIONS ON THE RISE?

> *"Threats against the U.S. healthcare system continue to be a long-running issue, made undoubtedly worse as the COVID-19 pandemic's spread continues."*

Kelvin Coleman, *Executive Director at the National Cyber Security Alliance*

Never in modern history has the need for properly functional healthcare and medical facilities been more critical. Thanks to the pandemic, hospitals, regional healthcare facilities, walk-in clinics, and emergency rooms have been pushed to the brink, doing their utmost to provide care for patients, despite untenable circumstances. And yet while medical institutions are locked in one battle saving lives, they are locked in another one, as cyber criminals use this overwhelming time as an opportunity to enter networks and systems unnoticed.

And so today, healthcare is facing a multitude of threats from cyber criminals, ranging from advanced malware to sophisticated phishing campaigns, to the targeting of medical devices, to complex data breaches, and so much more. In this white paper, we will explore the many challenges and threats facing the field and what can be done to combat them.

TODAY, HEALTHCARE IS A PRIME TARGET FOR CYBER CRIMINALS

The IT and security teams at medical facilities are acutely aware that they are increasingly in attackers' cross hairs and budgets allotted to remediating this issue have increased accordingly. According to Cybersecurity Ventures, a widely recognized cyber security research publication.

> *"global healthcare cybersecurity market will grow by 15 percent year-over-year over the next five years and reach $125 billion cumulatively over a five-year period from 2020 to 2025.The driving factor for this astronomical investment into cyber defence is triggered by the vast number of wide-ranging hacks and data breaches launched on hospitals and healthcare providers."*

For cyber criminals, healthcare is an attractive target for many reasons; the incredibly sensitive and valuable nature of the data these facilities hold; the fact that they cannot tolerate any amount of downtime, as it could put patients and their data at grave risk; the high rate of employee turnover; and of course, the pandemic, which has provided attackers with ample opportunity to infiltrate unnoticed, as staff grapples with life and death decisions.

LET'S EXPLORE THESE DRIVING FORCES IN GREATER DEPTH:

Considering the critical nature of hospital networks, it's not feasible, nor realistic or safe, to dismantle parts of the network to install relevant patches and security updates. But this can lead to major problems; To illustrate, a prime way ransomware attacks are deployed is by gaining access to hospital networks by leveraging a pair of VPN vulnerabilities found in Citrix ADC controllers, affecting Gateway hosts (CVE-2019-19781) and Pulse Connect Secure (CVE-2019-11510). By early 2020, both vulnerabilities had received security patches to prevent hackers from exploiting them but to this day, many healthcare organizations still have not applied the update.

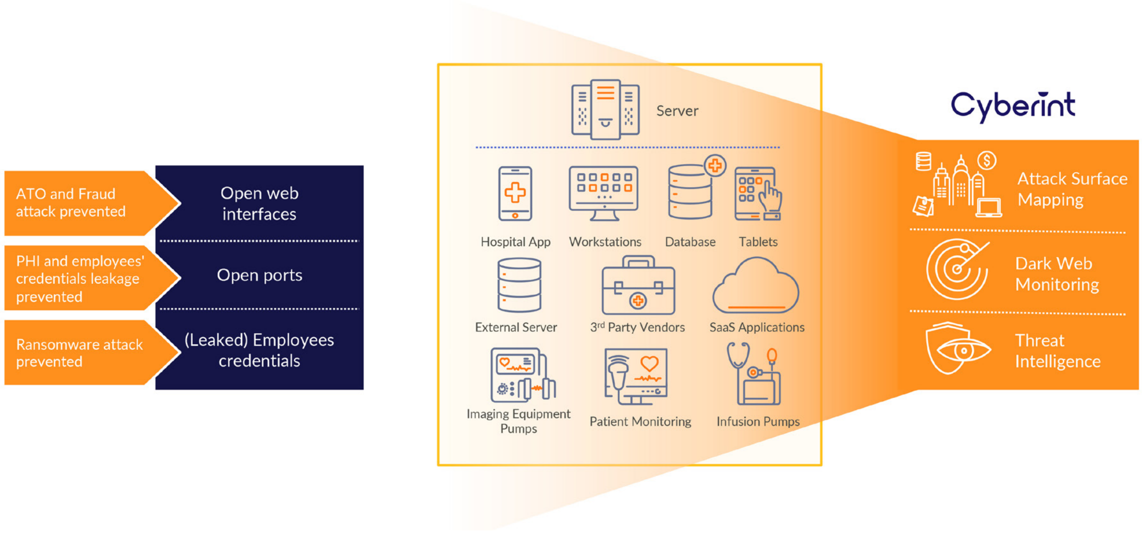
Another reason these sensitive networks are favoured targets for cyber criminals is due to the continual accessibility of the systems needed to provide patient care. To avoid loss of services, hospitals often quickly opt to pay ransom demands, to ensure patient health is not compromised, as well as to prevent cyber criminals from selling or publishing highly sensitive stolen healthcare data.

Then there is the issue of employees; perhaps now more than ever, nurses, doctors, therapists and even admins are overworked and exhausted. This weakened mental state makes it more plausible for unwitting employees to be tricked into clicking and downloading malicious attachments and files. And the high level of employee turnover of hospital employees not only creates a continuous stream of newly susceptible employees, but it further reduces the efficacy of phishing awareness training.

Next in line are the ever-expanding dangers associated with using third party vendors. Healthcare providers rely heavily on a wide range of suppliers to deliver core services and supplies. Hackers leverage these vendor platforms to get access to their more valuable partners. For example, in 2020, cloud services provider Blackbaud was hit with ransomware that subsequently infected over 20 medical institutions. Names, dates of birth, social security numbers, and the health information of millions upon millions of individuals may have been leaked in this massive and costly attack.

CYBERINT SOLUTION FOR HEALTHCARE

A typical Healthcare institution system is complex and combines various types of devices and end points, including patient monitoring, medical devices, and databases. As such, it may have inherent vulnerabilities, such as open ports or open web interfaces. Those vulnerabilities are exploited to perform Ransomware and other common attacks.



ATTACKS AND THREATS TO HEALTHCARE INSTITUTIONS

FAILING TO MEET REGULATIONS (HIPAA)

Every organization must ensure that all data is stored securely and that any possibility of data leakage or information theft are minimized as much as possible. Healthcare providers must also ensure that they comply with the Health Insurance Portability and Accountability Act (HIPAA). Fines for failing to comply with HIPAA can range up to $1.5M. Attacks such as ransomware can lead to the exposure of data, which can not only result in significant harm to patients, but to civil, and even criminal, penalties when considered as a breach of HIPAA.

Cyberint has identified a threat actor selling a database of internal information and patients' PII extracted from a healthcare organization system. The threat actor is offering the entire bulk, 3GB of documents, for $300. The documents contain sensitive information, including medical records, insurance information and more. It is unknown how this data was obtained by the threat actor, but it is believed to be one of the standard methods described in this section.

In another recent example, Cyberint identified an RDP (remote desktop) access for a server of an American hospital, which is currently for sale in an online marketplace. RDP access gives an attacker full control over a remote PC with almost no limitations, and the threat actor mentions that the hacked RDP server in question contains many patients' records and an active software showing full medical records of patients. A potential data exposure such as this constitutes a violation of patient privacy and can also be leveraged by threat actors to blackmail patients or the hospital.

EMAIL PHISHING AND SPEAR PHISHING

60% of data breaches in healthcare make use of phishing or other email-based attacks.
The main goal in these attacks is to obtain medical records, which rank among the most prized by identity thieves because they often contain data like names, addresses, birthdates, Social Security numbers, etc. Full medical record files can fetch as much as $1,000 per set.

There are many forms of phishing emails targeting healthcare facilities: business email compromise or BEC phishing, wherein an attacker sends an email impersonating a senior company executive; email account compromise, a BEC attack which is launched from an impersonated sender’s email account; clone phishing, which leverages a legitimate email previously sent by the purported sender; and spear phishing, a highly targeted attack which can take weeks to months of research and preparation.

All of these methods rely on the principles of familiarity and/or urgency. This is especially true in healthcare, where overworked employees, rushing between patients or meetings, may check email on mobile phones and respond to malicious messages without thinking to verify legitimacy. Any employee clicking malicious links will be directed to a fake login page, where the employee will enter login credentials, which are collected and transmitted to attackers. The attackers will then use the employee’s login credentials to access the organization’s financial and patient data.

DENIAL OF SERVICE

In healthcare, system and network availability is critical. Distributed Denial of Service (DDoS) attacks aim to disrupt or otherwise impact availability, which may lead to the loss of patients' lives. To illustrate, in 2014, Boston Children's hospital experienced a highly damaging DDoS attack after the hospital recommended that custody be withdrawn from a patient's parents. The attack persisted for at least two weeks, interrupting Internet access and harming day-to-day operations and research capabilities. BCH spent more than $300,000 mitigating the damage from this attack.

CONNECTED MEDICAL DEVICE TAMPERING

Modern hospitals have an incredible amount of connected medical IoT devices and there has been a significant increase in the number of cyberattacks carried out against healthcare organizations via these less-than-optimally secured devices.

Connected devices have become critical to patient care in recent years, but inherent issues, such as hardcoded passwords, misconfigurations, outdated firmware, and design flaws, can make them vulnerable to cyber-attacks. Communication between medical devices and servers that is not properly protected can lead to the corruption or exposure of critical information. Sophisticated methods, such as man-in-the-middle (MiTM) attacks, can alter data from crucial connected devices, leading to devastating effects.

CRYPTOJACKING / MEDJACKING

Malicious mining of cryptocurrency, otherwise known as cryptojacking, is the use of stolen computing power (CPU) to mine for cryptocurrencies, such as Bitcoin and Ethereum. Cryptojacking involves the infection of general purpose IT infrastructure and Medjacking refers to the infection of IT-based medical equipment. Medical equipment typically requires real time communications, and doctors and nurses also require fast response time when searching for patient information. Rogue mining for cryptocurrency can significantly slow down equipment and harm performance.

Though popularity of this methodology tends to wax and wane, it remains a significant threat to medical facilities because it is very hard to detect such attacks, and they can go unnoticed for very long periods of time.

MEDICAL IDENTITY THEFT

According to The Ponemon Institute, approximately 65% of victims pay more than $13,000 to stop having their medical identity compromised. Hackers steal personal information to make claims against insurance policies and after filing fraudulent claims, they take the money. In some cases, they may even get medical services since they do not have their own policies. All the attackers must do is get access to personal information, such as a Social Security number.

Another use case is stealing personal information for buying drugs. Attackers then sell these drugs or use them for their own purposes. In recent months, Cyberint has identified a darknet-based threat actor, offering to forge documents on demand, such as medical records, birth certificates, and drug prescriptions.

RANSOMWARE ATTACKS

According to the latest statistics, ransomware is now responsible for almost half of the data breaches in the healthcare industry. The virulent ransomware strain dubbed Ryuk is responsible for more than 75% of ransomware infections. According to Forbes.com, The gang's aggressive negotiating tactics and highly-targeted attacks have generated around $150 million in cryptocurrency pay-outs from its victims. Average Ryuk ransom payments are estimated to ring in somewhere around $110,000!

Attacks such as Ryuk are typically carried out through emails which appear to have originated from a legitimate company (like a credit card company). The user is directed to a fake website and tricked into downloading a security update or a link to a Google drive and by opening and "enabling" the documents, the victims then download malware. The so-called security update is a malicious program designed to find and encrypt data, rendering them inaccessible. The program then instructs the user to pay a ransom to unlock or decrypt the data.

Cyberint has identified a database uploaded to a darknet marketplace, where a hacking group published a portion of sensitive information, they allegedly obtained from the systems of a healthcare device manufacturer. The group stole approximately 320 GB of data, and to date they have uploaded to their website a sample containing 5% of it. Should a targeted facility refrain from paying, the group will continue publishing the rest of the database.

HOW CAN YOU MITIGATE THESE RISKS?

Leverage Measures To Handle Leaked Information

To minimize the impact of information leakage, it is important to ensure that provisioning and maintenance processes follow organizational policies and principles, especially in the healthcare environment. HIPAA describes key principle of minimum necessary, which states that organizations should take reasonable steps to limit uses, disclosures, or requests of PHI to the minimum required to accomplish the intended purpose.

In case employees' credentials are exposed apply pre-defined procedures for resetting the passwords or terminating the accounts altogether. Consider employing specialized tools to automate this process for accuracy and reliability. Leverage IT ticketing systems by building the provisioning workflow into the ticketing system.

Receive accurate and actionable threat intelligence on leaked information in the deep and dark web from Cyberint. Such evidence is based on the wide range of sources that Cyberint monitors, including Social Media feeds, online cyber-dedicated sources (XSS, Exploit, hackforums etc.), paste sites (such as pastebin.com, pastie.org, etc.) and an updated list of dark net marketplaces, chat rooms and forums which are known locations for hackers, across different industries.

Monitor Your Digital Assets Continuously To Minimize Exposure. For example: Scan Your Digital Assets To Make Sure You Avoid Using RDP and other Internet Facing Services

Several successful ransomware families such as SamSam, BitPaymer and CrySiS target RDP servers to initiate an attack.20 Unfortunately, many organisations still use RDP instead of the more secure Virtual Private Network (VPN) for remote access. RDP is known to suffer from vulnerabilities that can be exploited and may rely on internet-facing servers which are easily accessed. More than 800.000 systems with RDP services have been reported to be unpatched and vulnerable (ENISA ETL2020 Ransomware).

Implement an attack surface mapping module like the one provided by Cyberint to offer a process of discovery and continuous scan of all externally facing digital assets such as domains, IP addresses, websites, and cloud storage. Cyberint runs **discovery and scans to present** the issues and vulnerabilities, **prioritizes and act** on all issues discovered and **monitors** the constantly changing digital presence on an ongoing basis.

Employ Advanced Solutions That Provide Indications On Phishing Sites And Help Take Them Down

Advanced solutions that rely on threat indications, such as the registration of domains that impersonate the target brand by duplicating the web site or by manipulating the domain name, phishing kits that are developed and sold in the darknet, and so on. This can provide early indication on a planned phishing attack.
Cyberint with its advanced domain typosquatting capabilities, Phishing beacon technology and other advanced anti-phishing technologies can alert on such domains in an early stage of the campaign and effectively take the site down.

Cyberint provides Digital Risk Protection and Threat Intelligence. We believe in making the digital world a safer place to conduct business, by protecting our customers from cyber threats beyond the perimeter. We provide a rich set of external digital threat protection solutions, all automated or tailored with human expertise.

Cyberint provides targeted insights into threat actor activity, brand protection, phishing attacks, data leakage, and exploitable attack surfaces. Customers benefit from actionable recommendations seamlessly connected to their ecosystem - with minimal noise.

Cyberint serves leading brands worldwide including Fortune 500 companies across industries such as finance, retail, ecommerce, gaming, media, and more, with proprietary Argos™ technology enriched by dedicated cyber and intelligence analysts.

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

Cyberint