Healthcare is one of the most targeted industries for cybercrime. Recent data suggests that hospitals account for 30% of all large data breaches! Defending against today's advanced cyberattacks starts with gathering intelligence on threat actors' methods and operations. Based on research from BreachQuest and case data from our incident response team, this report exposes the latest healthcare cybersecurity threats and provides insights into how these threats exploited healthcare business vulnerabilities in 2021.

With threat actors continuously innovating and utilizing upgraded variants of ransomware and malware healthcare organizations must explore how they can increase their preparedness. This report covers:

- Top healthcare threat actors and methods
- Observations from cyberattacks in Healthcare in 2021 vs 2020
- Insights on ransomware incidence in Healthcare
- Actions and practices you can take to be more secure

Take the first step toward improving your preparedness. After reviewing this report, consider what actions your organization has taken to ensure a rapid response and recovery to cyberthreats? Do you know have a plan and know who to call? Do you have an incident response retainer? Do you have experienced IT team that you can get onsite within hours? Do you have a team that understands your industry and environment that you can reach out to? If you can't prevent the attacks, at least build your preparedness so you know what to do. We are here to help.
Notes from our CIO / CSO

Complexities of Healthcare Cybersecurity

Healthcare Breaches are Always Newsworthy

Legal requirements, the substantial type of Protected Health Information (PHI) to protect, and the complexity of health organizations all contribute to headline cybersecurity news stories for healthcare. HIPAA privacy and Security Law Healthcare and financial institutions are mandated by Federal law to disclose breaches. Without reporting, there isn't a news story. This is one of the reasons why it is so important to recognize the courageous decision by Mandiant and their leadership with their disclosure in the SolarWinds Breach. There was no federal requirement for them to tell anyone.

Protected Health Information (PHI)

There are 18 HIPAA identifiers for PHI, which requires HIPAA-covered entities and their business associates to provide breach notification to all impacted patients following a breach. An impermissible use or disclosure of protected health information is presumed to be a breach. It is then up to the covered entity or business associate to demonstrate there is a low probability the PHI has been compromised. An organization should interpret this as follows; it's a breach if you can't prove you were not breached.

The 18 HIPAA Identifiers include sensitive medical data and have a patient's most personal information, making it newsworthy and headline-grabbing. In rare cases, the data exposed has actual medical information, but a hacker threatening to leak patients' therapy notes is heart-wrenching and alarming. Since HIPAA breach news stories rarely provide details on what data is disclosed and to who, a victim will find it difficult to determine the impact on their privacy or the risk to their personal or financial security information. Being notified that your name, address, and fax number was much different from having personal medical information disclosed.
Complexity and Size Matters

Few environments face the complexity of healthcare. The type of devices, the urgent situations faced by their users (a long password for an ER doctor could mean life or death of a patient), or potential life or health impacts if a device fails or works incorrectly. Hospital IT and cybersecurity professionals provide heroic services keeping environments running and rapidly implementing new services such as telehealth to support the COVID pandemic. When I attended the H-ISAC summit in December last year, I was awed and inspired by the technical security implemented and the speed and efficiency of one hospital cybersecurity team as they described their process and service provided to elderly patients for telehealth. They met the time urgency and the technical challenges, but they also drove and hand-delivered secured and sanitized devices to support patients who needed telehealth services.

There is also a size and scale consideration and connectivity. In Idaho, small hospitals and clinics are practicing in areas classified as frontier, and they face technical challenges for connectivity and receive appropriate technical support. IT support can be a challenge for any small practice in any area. Often, they rely on a single or part-time IT to protect them from the same internet full of danger as a large organization.

Without a Federal Data Breach Law and exploited complicated vulnerabilities such as logj4, we can anticipate continued healthcare headlines. As we recognize and appreciate everyone on healthcare’s front lines, remember the Healthcare and cybersecurity professionals tasked with the difficult challenge of protecting your health information.
Cyberattacks in the Healthcare Industry

49M

Individuals

In 2021 49.4 million individuals were reported from all types of healthcare related incidents. A 44% increase over 2020.

OCRportal.hhs.gov

5x

Increase in Attacks

Between 2017 and 2020, ransomware attacks on healthcare organizations were predicted to quadruple, and will increase by an astounding 5X by 2022.

Cybersecurity Ventures Report.

93%

Organization Affected

Over the past three years, 93 percent of healthcare organizations have experienced a data breach, and 57% have suffered more than five breaches during the same period.

HIPAA Journal 2021
Ransomware & Healthcare

Some ransomware groups themselves tend to target healthcare industries more than anyone else because of the value of the sensitive data, making the sector 2-3x more likely to be at risk.

An example of this is the "Hive" ransomware group. Hive primarily uses phishing emails to gain access to networks and remote desktop protocol ("RDP") to move laterally. The risk is so high simply because it has the most profitable resale value and tends to have more outdated systems than other industries.

The industry has been slow in updating its outdated systems and keeping up with cybersecurity technology, most dedicating a smaller portion of their budget to cybersecurity compared to other sectors.

Just 4-7% of a healthcare provider's IT budget is focused on cybersecurity. However, this number is expected to grow. Even though cybersecurity awareness may be increasing, cybercriminals are constantly finding ways to be better and faster.
Although ransomware remains a common attack vector, the healthcare industry overall is a prime target to cyber criminals for a number of reasons. 60% of the ransomware attacks in the healthcare industry took place within the US. Because of the sensitive information the medical databases contain, the data is seen to be more valuable and is sold for more money on the dark web or in most cases, is held hostage until a ransom is paid. During the event of encryption, organizations lose many hours in attempts to restore operations and regain access to the data. Most importantly, organizations lose the ability to care for its patients. Ransomware attacks are costlier than other types of breaches, since the data is so sensitive and valuable.
Ransomware & Healthcare

Who are the Threat Actors?

All ransomware groups are strictly financially motivated. Threat actors will execute phishing attempts and Remote Desktop Protocol (RDP) brute force attacks in hopes of some organizations falling for the attack. With the financial motive in mind, these attacks go as far as stealing patient data to jeopardize lives potentially. The speed of encryption and the sensitivity of the data is an effort to force a ransom payment from the victim.

The top ransomware groups in 2021 that targeted healthcare organizations are Hive, Pysa, Conti, and Lockbit. According to HC3, in the third quarter of 2021, Conti ransomware was the most active in the United States and globally. Conti is used as a ransomware service (RaaS) in high-profile attacks. Conti often weaponizes Word documents with malicious PowerShell scripts delivered by phishing emails.

2021 Q3 Incidents (Global)
Ransomware & Healthcare

Who are the Threat Actors?

On average, Conti bad actors are observed inside the network between four days to three weeks before deploying ransomware. Once inside the network, they tend to use scheduled tasks and batch files to execute on remote systems. Although tailored to the specific victim, recent ransom demands have been as high as 25 million dollars. If the ransom is not paid, the organization's data is published on the Conti's public site or sold.

Knowing all about this ransomware family is essential to protect against the threat. In February 2022, an employee of Conti leaked the chat logs, and details into the Conti organization. To learn exactly how this multi-layered organization works read our:

The Conti Leaks: Insight into a Ransomware Unicorn

https://www.breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/
In 2020, Thirty-four percent of all breaches were in healthcare.

Forgerock - 2021

Q1-2022 6,979,024 individuals affected by 136 healthcare Breaches.

HHS OCR

Healthcare breaches are the highest of any industry.

HIPAA Journal

Negligent breaches are still happening twice as often as malicious ones.

JOCS Vol2 Iss 1
Round Table Discussion

Answering the Hard Questions

We sat down with our guest expert Scott Koller, from Baker Hostetler, and a few of our Response Services team, and our new CIO / CSO to get their take on the threats facing healthcare.

Scott Koller
Privacy & Data security
Attorney Baker Hostetler

Alex Ondrick
Director of Security Operations for BreachQuest

Sandy Dunn | CIO /CSO
20+ Years in cyber security industry with the last 5 as the CISO of Blue Cross of Idaho

Sean Cordes
Associate Director of Incident Response for BreachQuest

Chris Pacenza
Associate Director of BreachQuests Recovery & Remediation Team.
In 2020, 47% of the cyber threats reported in healthcare were Probes/Scanning. What is the danger of this to the industry?

“An increase in this type of activity could be an increase in the number of threat actors seeking vulnerabilities to exploit, or an increase in the number of vulnerabilities being scanned for. While some threat actor groups specifically target the healthcare sector, more often than not, the threat actor does not know the target’s industry until after a vulnerability is found.”

“Probes and scanning are typically an attacker doing reconnaissance see the first item in the MITRE ATT&CK https://attack.mitre.org/”

“We often discover there are open ports that are vulnerable to attacks. To assist with minimizing this issues clients can use a monitoring tool that can pinpoint these vulnerabilities and then IT can take action to fix them.”

“Healthcare orgs and network defenders need to be vigilant about protecting networks and devices from the open internet, and maintaining regular patching schedules to minimize the risk posed by vulnerabilities.”

Healthcare Sector Threats

- **Botnet**: 32%
- **Probes/Scanning**: 47%
- **Malicious Host**: 11%
- **Other**: 10%

Source: Looking Glass, 2021
How is the healthcare industry unique when it comes to cybersecurity?

Round Table Discussion

“The healthcare industry has one of the oldest statutory frameworks and a very active, and engaged regulatory oversight body. The Office of Civil Rights frequently publishes guidance to the healthcare industry and has not hesitated to impose significant fines and penalties on offenders.”

“All organizations need to consider minimizing user friction for security solutions, but user efficiency and ease of use is especially important for doctors, nurses, and medical personal. When an ER team is faced with a life and death situation and need information immediately 16 character passwords user passwords with a screen which locks in five minutes are not a good solution.”

“Healthcare adds another dimension. The devices that can be affected have the possibility to be hooked up to a life saving device. I was on a case where the hospital had to divert cancer patients to another hospital as they were not able to perform chemo treatments.”

“Healthcare organizations are often in-scope of HIPAA, thereby increasing the org's levels-of-effort (time, people, money) required to maintain compliance.”
Round Table Discussion

How do healthcare organizations protect themselves when 60% of their breaches are from vendors? Is the IoT a problem for healthcare? Is Legislation the answer?”

“Healthcare organizations must have a high bar for third-party vendors who have any level of access to their operations. Vendors should be required to undergo a thorough assessment prior to gaining access, and recurring checks in order to maintain that access.”

“Most healthcare institutions depend on outside vendors to provide critical services. They will always have a level of vulnerability.”

“The underlying contract with the vendor should also require cyber liability insurance, full cooperation with any investigation, specify who does what during the investigation/notification process, and require indemnification for costs and expenses associated with a breach. Once the vendor is engaged, the healthcare organization needs to supervise the collection and use of data by the vendor, and regularly audit their practices to ensure continued compliance with security requirements.”
Round Table Discussion

What makes healthcare data so valuable to threat actors?

“While someone’s medical history, blood type, or allergies may not be inherently valuable to a threat actor, that information is absolutely critical to a physician providing care, which makes it a target for ransom. No other information has the same potential for misuse.”

“Healthcare environments often contain systems which maintain patient health records, PII, and financial records: Although systems should be secured and segregated, any system which contains all three should be considered a ‘critical asset,’ and a lucrative target for threat actors.”

“Having Protected Health Information (PHI), PII and possible facial data is exactly what the TA’s are looking for. When they hit a jackpot like this they feel the will have a big pay day.”

“Healthcare records are one of the most complete identity records each of us have. Birth date, age, current address, previous address, social security number, relatives, often credit card, insurance plan numbers, as well as sensitive medical diagnosis and information. An attacker has multiple possible options to convert the records into income which include identity fraud, credit card fraud, tax refund fraud, medical card fraud, ransom to the healthcare entity with threat of exposing the breach, ransom threats to patients with sensitive medical conditions.”
A botnet, put shortly, is a collection of internet-facing devices that a threat actor has compromised. They act as a collective group of computing power to be leveraged for further large-scale and distributed attacks. The type of attack used by botnets most often is DDoS ("distributed denial of service") attacks.

IoT devices (Internet of things) are the most common victim of exploitation for botnet use. Certain types of devices, like security cameras or printers, have very little computing power and often are not very secure, making them a great target. Think of security cameras or smart refrigerators, or printers. Threat actors will take over hundreds of thousands of these devices and become part of the network that will be used to carry out attacks.

In 2020, 32% of reported threats in the healthcare sector were from Botnets.
Botnets & Healthcare

A Risk that should not be Ignored

In 2021 there was a significant increase in botnet activity against healthcare-related websites. Websites used to book COVID-19 vaccines were often subject to service interruptions due to malicious botnet traffic.

Threat actor “FritzFrog” has recently attacked healthcare, government, and education sectors, resurfacing after more than a year dormant. Since resurfacing in recent months, this group has seen a 10x growth. This group is leveraging a P2P Golang botnet to target and infect those that have exposed devices or servers running a Secure Shell Protocol(SSH). BreachQuest highly recommends disabling SSH anywhere it is not critically needed.

35-51%
Increase in 6 months

1H 2021 Botnet activity increased from 35% of malicious activity to 51% in only 6 months.
Fortinet

60%
Reported Phishing

Nearly 60% of healthcare organizations reporting phishing attacks in 2020
HIMSS, 2020
Cyber Insurance and Healthcare

The Insurance Market is hardening due to the following:

- Increasing number of ransomware cases
- Increasing severity of ransomware cases
- Aging end-of-life devices

Healthcare Data Breaches Annually
Cyber Insurance and Healthcare

The criteria to get and maintain a cyberinsurance policy is becoming more and more difficult and expensive. Marsh (2022) released twelve controls that are key to insurability, mitigation, and resilience. Without the first five categories covered, obtaining cyber insurance coverage would likely be called into question. As cyber threats continue to intensify healthcare organizations should focus on adopting all twelve controls to maximize their insurability and mitigate risk.

Top Cybersecurity Controls

The key to insurability, mitigation, and resilience.

- Multifactor authentication for remote access and admin/privileged controls
- Endpoint Detection and Response (EDR)
- Secured, encrypted, and tested backups
- Privileged Access Management (PAM)
- Email filtering and web security
- Patch management and vulnerability management
- Cyber incident response planning and testing
- Cybersecurity awareness training and phishing testing
- Hardening techniques, including Remote Desktop Protocol (RDP) mitigation
- Logging and monitoring/network protections
- End-of-life systems replaced or protected
- Vendor/digital supply chain risk management
Help is out there!

There isn't a simple solution for healthcare organizations and privacy. The complexity faced with nation-state attacks, zero-day attacks, spying, stolen trade secrets, misinformation, and stolen finances will continue to be a problem for healthcare organizations. But there are great people and organizations providing guidance, frameworks, and information and knowledge sharing to help businesses and organizations, including healthcare.

The National Council of Information Sharing and Analysis Centers

ISACs are trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats and mitigation. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

As a healthcare organization, joining H-ISAC is a lifeline. Joining H-ISAC provides access to healthcare security and privacy teams and individuals with the same challenges and can help you find answers. With H-ISAC, you can join mailing lists, attend summits, and join subgroups for specific areas of your program.

National Institute of Standards and Technology

NIST provides comprehensive information on all aspects of security and technology. NIST SP 800-66 r1 is specifically for healthcare organizations and HIPAA.


CIS Top 18 Center for Internet Security (CIS) controls

With a variety of frameworks such as ISO, NIST, and SOC2, it can be overwhelming to know where to start. The CIS Top 18 is the solution for smaller healthcare organizations or larger organizations. The CIS prioritizes security controls and breaks them into implementation groups based on the organization’s risk profile and resources available to them. https://www.cisecurity.org/case-study/26-year-healthcare-industry-veteran-and-the-cis-controls/

MITRE has a comprehensive site dedicated to healthcare https://healthcyber.mitre.org/, focusing on ransomware readiness.
BreachQuest is reimagining incident response with an elite team of cybersecurity veterans, including former NSA, DoD and US Cyber Command operators that have serviced more than 40 percent of the Fortune 100. BreachQuest was founded in response to the growing threat of ransomware, offering organizations the ability to minimize the cost and downtime associated with breaches through a re-engineered approach to incident response and recovery. Built around the proprietary PRIORI Platform, BreachQuest improves organization’s security posture with automated end-to-end readiness and response capabilities which enhances cyber resilience and reduces attacker dwell time. To learn more about BreachQuest, visit: https://breachquest.com/.

Get in Touch

Shawn Melito | CRO
smelito@breachquest.com

Jake Davidson | Director Sales
jdavidson@breachquest.com

24/7 Breach Response
US 888 409 5811
UK +44 800 260 6804

IR@breachquest.com