INDUSTRY BRIEF

ThreatQ for Healthcare

Healthcare organizations are attractive targets for today's hackers due to reams of personal and health information providers process and store on behalf of consumers. Electronic Health Records (EHR), which include valuable data, such as a person's full name, birth date, SSN and billing information, are like digital gold to adversaries given the lucrative opportunities associated with selling personal information on the black market.

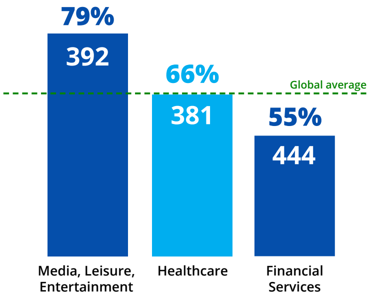
Sophos, a security software and hardware company, conducted a vendor agnostic survey and their findings showed that 66% of healthcare organizations were hit by ransomware last year, up from 34% in 2020.[1] This is a 94% increase over the course of a year, demonstrating that adversaries have become considerably more capable at executing the most significant attacks at scale. These campaigns often involve credential theft and infect multiple machines before detection, wreaking havoc on health system operations. According to a report from the New York Times in 2020, Russian hackers carried out a ransomware assault on United Health Services, a healthcare organization with a network of over 400 facilities. This attack marked the most extensive incident of its kind at that point in time.[2] Attacks like these and more recently a group by the name of Clop[3], serve as a warning for healthcare providers and emphasize the urgent need for better cybersecurity defenses in health systems worldwide. Which in turn may be causing more healthcare organizations are buying cyber insurance policies, which require them to invest in more robust cybersecurity defenses.[4]

KEY CHALLENGES

DATA AVAILABILITY

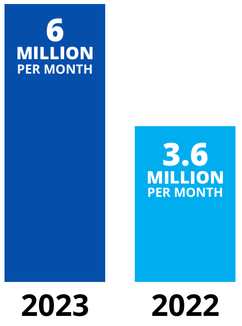
Instant and reliable access to accurate patient data saves lives. Clinicians need to see patient records on demand. An unwavering focus on patient well-being and health outcomes nearly always outweighs data protection. Hence the ongoing reliance on some insecure information-sharing processes and outdated communications technologies. But vigilance is mandatory. Confidential medical data is particularly vulnerable to malware and ransomware attacks, and therefore mandates stringent security controls. Threat intelligence can provide valuable details on attackers' motives and their tactics, techniques and procedures (TTPs) that can be used to determine how to most effectively strengthen defenses.

RANSOMWARE ATTACKS BY SECTOR



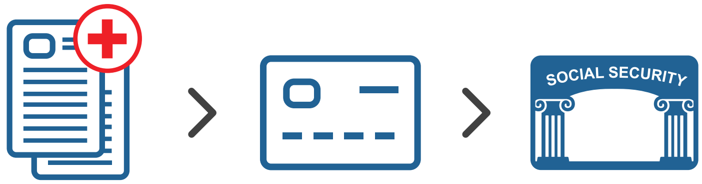
Source: Sophos[6]

INDIVIDUALS AFFECTED BY CYBER ATTACKS PER MONTH



Source: Chief Healthcare Executive® [5]

COMPARISON ON THE DARK WEB: SSN = $1, CREDIT CARD = $5, HEALTH RECORD = $1,000 PRICE PER RECORD[7]



Health Record **$1000**

Credit Card **$5**

SSN **$1**

Due to the amount of time that it takes for a health record to be recognized as stolen, it is much more valuable because it can be used for a much longer time than a credit card would be before the breach is discovered according to The HIPAA Journal, a HIPAA compliance provider.[8]

LEGACY SYSTEMS

Medical facilities and clinicians typically rely on outdated systems and devices, often running older versions of software and security tools that are highly vulnerable to compromise. Needing anytime anywhere access to patient information, healthcare workers and administrators are often reluctant to upgrade devices given potential interruptions in care delivery. However, a single outdated or compromised system can result in a major breach.

In order to effectively prioritize remediation efforts aimed at protecting both old and new assets, a health system must correlate threat intelligence data with potential security weaknesses in its environment. This enables a provider with limited security resources to focus on addressing critical infrastructure vulnerabilities that pose the greatest risk to the organization.

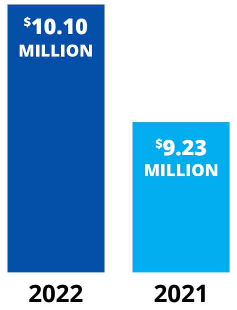
MODERN ASSETS

Modern technologies, like Internet of Things (IoT) medical devices and EHR applications, are delivering unprecedented accessibility, connectivity and scalability to improve efficiency and enhance patient care. But at the same time, they are expanding the attack surface and sensitive data is repeatedly being exposed to threats involving theft and misuse. Striking the optimal balance between advanced digitization and enforced security policies to protect assets across the growing attack surface remains difficult. Automatically recalculating and re-evaluating priorities and threat assessments based on the latest threat intelligence and a changing internal environment, helps to ensure ongoing focus on the most relevant risk mitigation strategies.

CREATING A LEADING DATA-DRIVEN SECURITY OPERATIONS

A robust security operations platform gives healthcare providers the context, customization and prioritization they need to make better decisions, accelerate detection and response and advance team collaboration. Serving as the hub of intelligence operations for many industries, the ThreatQ Platform aggregates and combines unstructured and structured data from any source, internal and external. There's no need to alter existing security infrastructure or workflows; all tools and technologies work seamlessly with ThreatQ's open architecture. Automation eliminates repetitive, time-consuming tasks so analysts can focus on high-priority and strategic work. The platform also provides flexibility to share curated threat intelligence, advisories and reports with a range of internal and external stakeholders, including the healthcare industry, quickly.

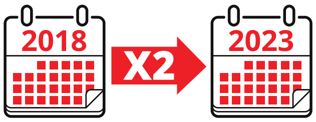
AVERAGE COST OF A DATA BREACH BY INDUSTRY



Source: IBM[9]

In 2022, an average of 1.94 healthcare data breaches* were reported each day.

Between 2009 and 2022: **5,150 healthcare data breaches*** were reported.



The number of healthcare data breaches* being reported has **doubled over the last 5 years** (2018 to 2023).

Source: The HIPAA Journal[10]

*Breaches involving 500 or more records.

ACHIEVE MORE WITH THREATQ:

- **CONSOLIDATE** external (e.g., NH-ISAC) & internal (e.g., SIEM) threat intelligence and vulnerability data in a central repository.

- **ELIMINATE** noise and easily navigate through vast amounts of threat data to focus on critical assets and vulnerabilities.

- **PRIORITIZE** what matters most for the health system environment.

- **INTEGRATE** only relevant indicators into your HIPAA-related security policies.

- **PROACTIVELY HUNT** for malicious activity which may cause significant harm to patient records and healthcare organizations.

- **FOCUS** on known security vulnerabilities in currently active exploits which may impact regulatory status.

- **ACCELERATE ANALYSIS** and response to attacks against multiple targets including network-connected medical devices.

- **AUTOMATICALLY** push threat intelligence to detection and response tools.

Request a live demo of the ThreatQ Platform and ThreatQ TDR Orchestrator at www.threatq.com/demo.

1. https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf
2. https://www.nytimes.com/2023/08/05/us/cyberattack-hospitals-california.html
3. https://www.chiefhealthcareexecutive.com/view/after-a-lull-ransomware-attacks-on-hospitals-are-rising-again
4. https://www.healthcareitnews.com/news/ransomware-attacks-have-doubled-2-years-report-shows
5. https://www.chiefhealthcareexecutive.com/view/after-a-lull-ransomware-attacks-on-hospitals-are-rising-again
6. https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf
7. https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=393f4dcd6c88
8. https://www.hipaajournal.com/healthcare-data-breach-statistics/
9. https://www.ibm.com/downloads/cas/3R8N1DZJ
10. https://www.hipaajournal.com/healthcare-data-breach-statistics/

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.