Cymulate

Threat Exposure Management for Healthcare

Abstract

For over a decade, the healthcare sector has remained the costliest industry for data breaches. Though some of the elements that underline this poor performance are specific to healthcare, emerging technologies open new avenues for the industry to improve its ability to prevent breaches and, most importantly, to limit the extent of breach damages.

This paper examines the healthcare sector's structural drawbacks and explores how continuous threat exposure management can help prepare healthcare organizations before the next attack.

Table of Contents

01 Introduction

As threat actors continue to target healthcare providers, cyber leaders in the industry face heightened urgency to harden their defenses before the next attack while preparing their response and recovery capabilities for the potentially inevitable breach.

Healthcare data has long been a valuable target because it demands the highest level of sensitivity and includes detailed personal information that can be used for identity theft. But beyond the value of the data, the very critical nature of healthcare services makes the industry a prime target for ransomware attacks. Recent attacks highlight the impact of disrupting healthcare services (e.g., electronic health records and ordering systems) and business operations (e.g., insurance claims and payment processing) essential to providing care. The ultimate nightmare scenario would involve hospital operational technologies (OT) that regulate and manage life-supporting medical devices.

This paper briefly draws a cyber diagnostic of the healthcare sector before devising a list of preventive approaches and technologies that proactively seek out and validate potential weaknesses to fix them before attackers exploit them.

02 The Healthcare Sector's Digital Characteristics

From a structural perspective, the healthcare sector has several unique security challenges.

The Nature of the Data

Attackers target personal health data for its value – both in resale on the dark web and the essential nature of that data to deliver healthcare services.

- **The perennity of health data**
  Health data it remains valuable for extended periods, and there is no option to modify the data if it is stolen. For example, compared to financial data such as credit card numbers, the ability to cancel the card and order a new one means the stolen data has a short shelf value. The same is true for any credentials to access online accounts because it is easy to change passwords. Even other perennial data, such as an address or a social security number, can be modified in case of extreme abuse, but there is no way to modify health records.

- **The criticality of health data**
  When faced with a ransomware attack, healthcare institutions' freedom of movement is limited unless they have a backup system in working order. Any delay in recovering encrypted data might result in patient death. Other sectors might engage in complex negotiations, play for time to let forensic enforcement forces try and locate the hacker, or even decide to refuse to pay and manage the consequences, but for healthcare, this isn't an option.

The Nature of the Network

Managing patient health requires interacting with disparate contributors who need access to the patient's data to provide the required service. That range of services may include protected health information (PHI) and ambulatory medical records (AMR) shared between clinics, hospitals, family doctors, specialists, and other medical personnel, all with different systems and levels of protection.

To make matters worse, medical personnel are chronically short on time and, therefore, less likely to activate multi-factor authentication (MFA) and other time-consuming security measures. In addition, the multiple devices used to access patients' PHI might be shared or have dual personal/professional use, and some are BYOD (bring your own device), with all the inherent associated risks.

As the healthcare sector's prime directive is to provide patient care, budgeting priority for IT and cyber equipment is low, resulting in a higher proportion of legacy systems. These systems are ill-adapted to handle technology progress and the multiplication of connected services, such as:

- Telemedicine
- Appointment scheduling
- Online prescription services

An additional challenge is IoMT, the Internet of Medical Things, which includes:

- **On-body Devices –** Any device worn outside the body to monitor or interact with anatomic activities. These include all wearable devices, from personal wellness and fitness devices to FDA-approved wearables.
- **At-home Monitoring Devices –** Any activity that includes electronic interaction between the patient and a medical service provider. These include telehealth virtual visits, remote patient monitoring (RPM), and personal emergency response systems (PERS).
- **Medical Care Facility Devices –** This covers devices or systems that monitor or manage inventory and high-value assets such as infusion pumps, patient flow, environmental conditions, energy use, and optimization.

Any of these can be used as a potential attack point of entry.

The 24/7 Cycle

By its very nature, the healthcare sector must be running 24/7. This complicates remediation systems that require interrupting services and results in postponing mitigation, extending the time window open for attackers. It also increases remediation costs.

03 | The Healthcare Sector Threat Landscape

With the high value and long-lasting shelf-life data generated by the healthcare sector, it is unsurprising that it attracts a lot of unwelcome attention from cyber attackers.

Highest Cost of Breach Across all Sectors

According to the 2022 annual IBM Cost of a Data Breach report, for the 12th consecutive year, the healthcare sector remains the infamous leader in breach cost, reaching an average of $10.10 million. This is a 42.6% increase compared to 2020, nearly twice as high as the second-highest cost attained by the financial sector's $5.97 million price tag.

Anything related to health seems to remain costly in terms of breaches, as the third contender for the highest breach cost is the pharmaceutical sector, with an average breach cost of $5.01 million.

Understanding the reasons behind those disproportionally high costs is key to minimizing them or at least understanding why this is impossible.

Ransomware

One of the reasons behind these prominent costs is the high likelihood that the healthcare sector will pay to recover data and maintain operations in case of a ransomware attack. According to a Sophos study, 61% of healthcare respondents whose encrypted data admitted to paying the ransom compared to the cross-sector average of 46%. Interestingly, in 2021, healthcare organizations that paid the ransom got back, on average, only 65% of their data—down from 69% in 2020. Similarly, only 2% of those who paid the ransom in 2021 got ALL their data back, down from 8% in 2020.

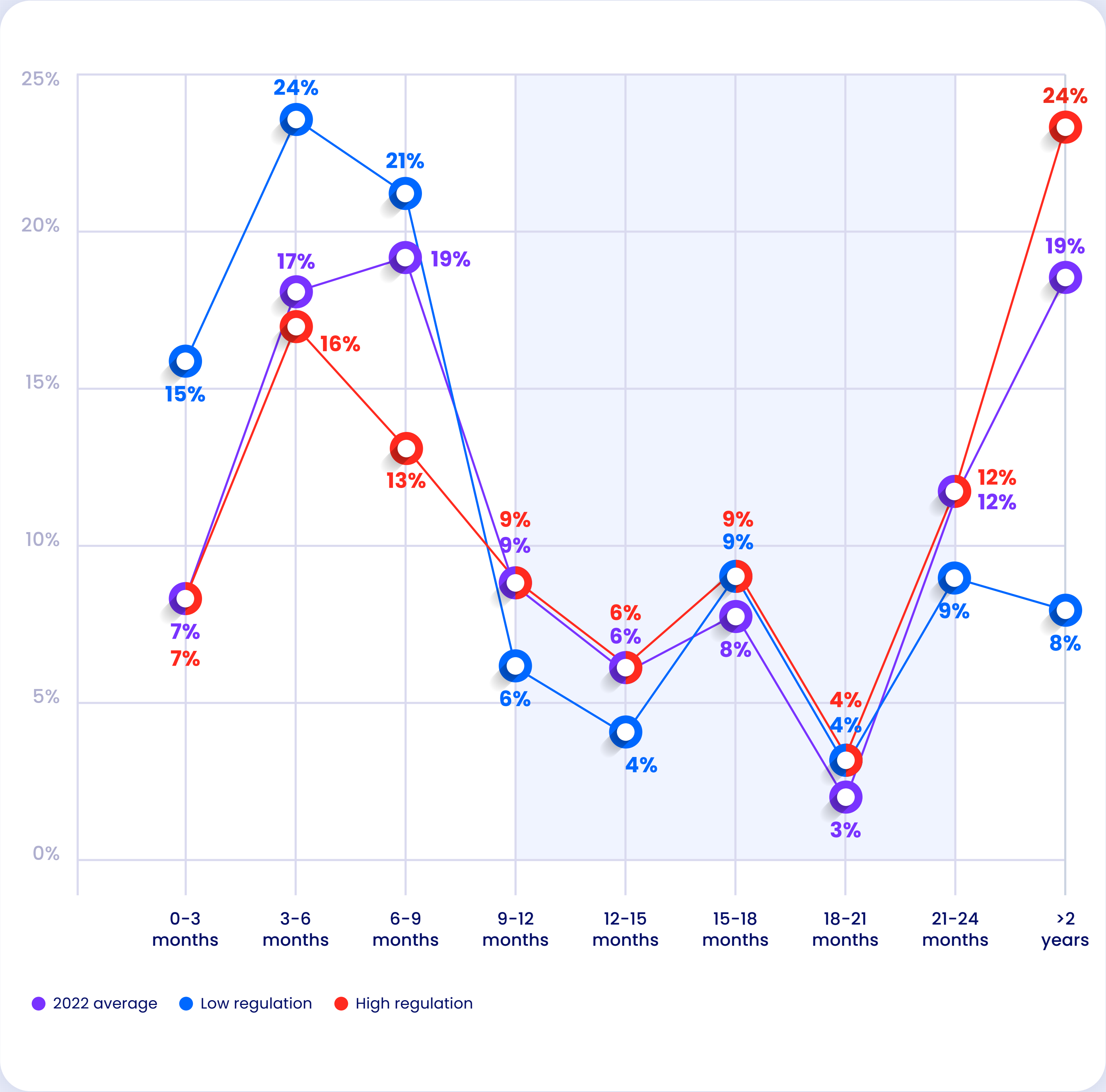
Remediation

The average post-attack remediation cost across all industries was US$1.4 million in 2021, down from US$1.85 million in 2020. Yet, the healthcare sector's average remediation cost increased from US$1.27 million in 2020 to US$1.8 million in 2021. As detailed above, these disproportionate costs are partially due to the healthcare sector's 24/7 structural nature, which complicates remediation procedures.

Regulation

The healthcare sector is highly regulated, and the figures above might be considerably undervalued as they only reflect the already calculated cost for breaches that happened less than two years ago. As shown in the graph on page 6, considering the higher-than-average long-term costs for highly regulated sectors, a steep uptick in those costs 18 months after a data breach can lead to a sharp increase in the total costs.

Average distribution over time of data breach costs in low vs. high data regulation environments



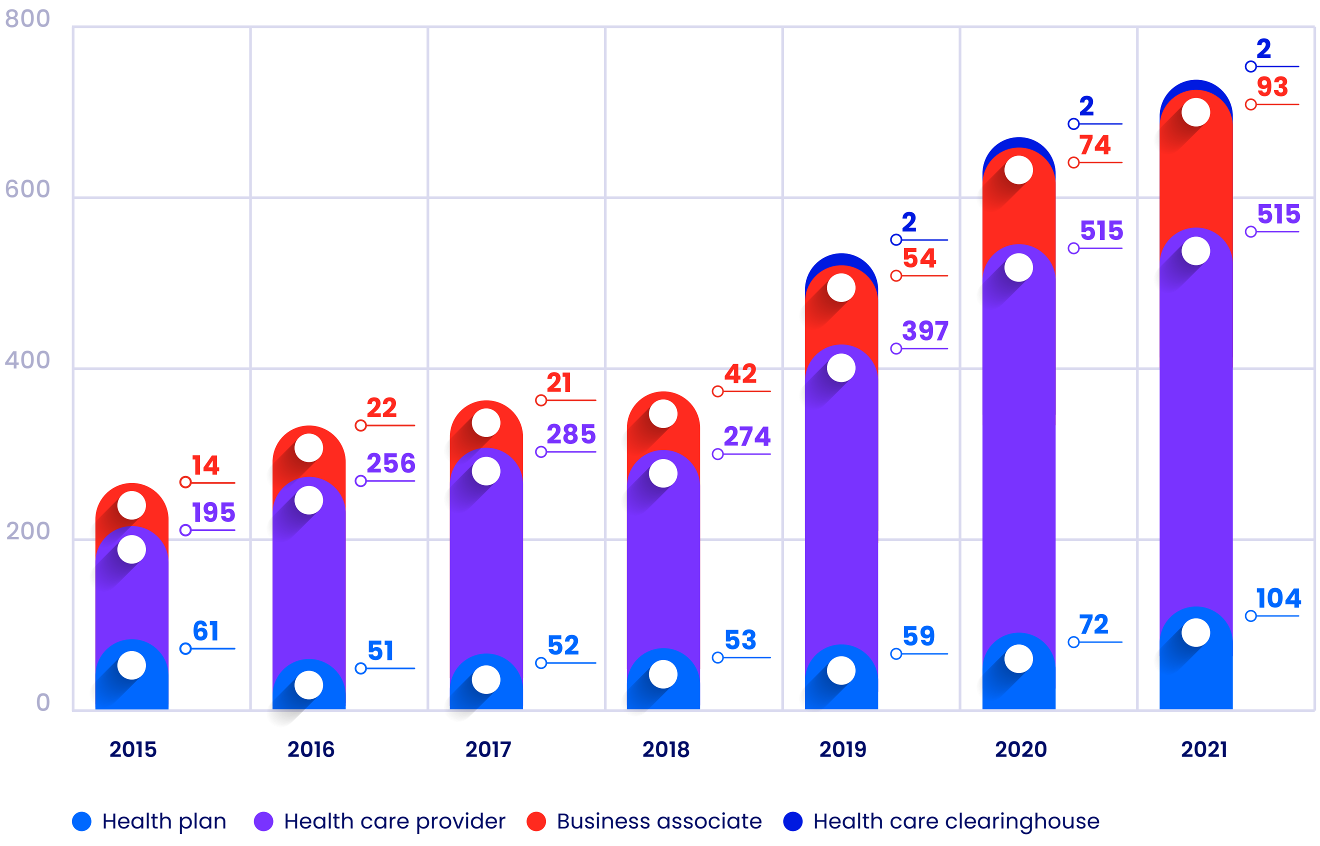
Data source: IBM Cost of a Breach Report 2022

The Fast and Consistently Growing Pace of Attacks

In parallel, the pace of breaches against the healthcare sector is accelerating. In the US, for example, the growth in the number of breaches affecting over 500 people's PHI between 2015 and 2021 has accelerated, as reported by the US Department of Health and Human Services (HHS).

Yet, despite the already sky-high rise in the number of cyberattacks against the healthcare sector in 2020 and 2021, that number nearly doubled in the first half of 2022 for the same period in 2021.

Number of breaches affecting 500 or more individuals



Data source: GAO analysis of Department of Health and Human Services - January 2022 data

04 How to Reduce Threat Exposure and Attack Impact

According to ThoughtLab 2022 "Cybersecurity Solutions for a Riskier World," the healthcare sector leads the world in terms of lack of preparedness for facing cyber threats. The fastest and most efficient way to accelerate getting to a higher level of cybersecurity preparedness is by identifying and closing breach and attack routes based on their degree of criticality.

Practically, this means adopting a Continuous Threat Exposure Management (CTEM) approach to continuously improve defenses before the next attack by focusing on the most critical weaknesses attackers will likely exploit.

Fundamentals of Threat Exposure Management

The essential shift of perspective underlying CTEM is to adopt a strategy that applies the attacker's view to:

- Identify gaps and weaknesses.
- Test and optimize the security controls, defenses, and incident response processes.
- Prioritize action based on validated proof that attackers can exploit the weakness and cause damage.

The CTEM framework includes five steps: scoping, discovery, prioritization, validation, and mobilization.

Scoping

Scoping provides the foundation for successful exposure management programs by aligning the cyber program with business risks, defining a clear focus, and establishing measurable goals and objectives.

Discovery

The discovery phase creates a risk-profiled asset inventory of the internal and external attack surface by identifying the assets, classifying their business context, and understanding potential cyber risk.

Prioritization

To mitigate the threats that your organization is most likely to face, prioritization within an exposure management program considers both external data like threat intel and vulnerability severity scores and internal factors such as compensating controls, business context, and the availability of mitigation.

Validation

Validation provides proof and evidence of actual exposure by testing the attacker's capabilities to exploit the identified weakness while assessing the effectiveness of controls and response processes to prevent, detect, and respond to the threat.

Mobilization

Mobilization is the execution of concrete steps to improve security posture, including patching vulnerabilities, updating system configurations, applying mitigating controls, or taking other actions that eliminate the weakness or strengthen defenses to enhance resilience.

05 | Threat Exposure Management Technologies

The Cymulate Security and Exposure Validation platform operationalizes threat exposure management with the following technologies:

Attack Surface Management

Cymulate Attack Surface Management (ASM) discovers vulnerabilities and misconfigurations to identify assets exposed to unapproved access, exploits, and other attacks. Cymulate ASM automates the attacker's view of your on-prem, cloud, and hybrid environments by scanning autonomous system numbers (ASN), domains (email and web), subdomains, IPs, ports, services, applications, and cloud platforms. The platform also scans the dark web for sensitive information and indicators of data leaks and cyberattacks.

Breach Attack Simulation (BAS)

Cymulate Breach and Attack Simulation (BAS) validates cybersecurity controls by safely conducting threat activities, tactics, techniques, and procedures in production environments. With automation and a library of realistic attack scenarios and simulations, Cymulate BAS gives security teams an easy-to-use interface to continuously test security architecture, people, and processes to assess cyber resilience.

Continuous Automated Red Teaming

Cymulate Continuous Automated Red Teaming (CART) provides cybersecurity teams a platform to increase operational efficiency and optimize their adversarial activities with production-safe methodologies. The implementation is easy, and the assessments can test any technique at any stage of the attack kill-chain independently – start with a well-crafted phishing email or begin from inside the network and move laterally in stealth, using a variety of exploits. The Cymulate CART solution supports automated testing for vulnerability validation, what-if scenario, targeted-, and custom-testing within a flexible framework for repeatable and scalable testing.

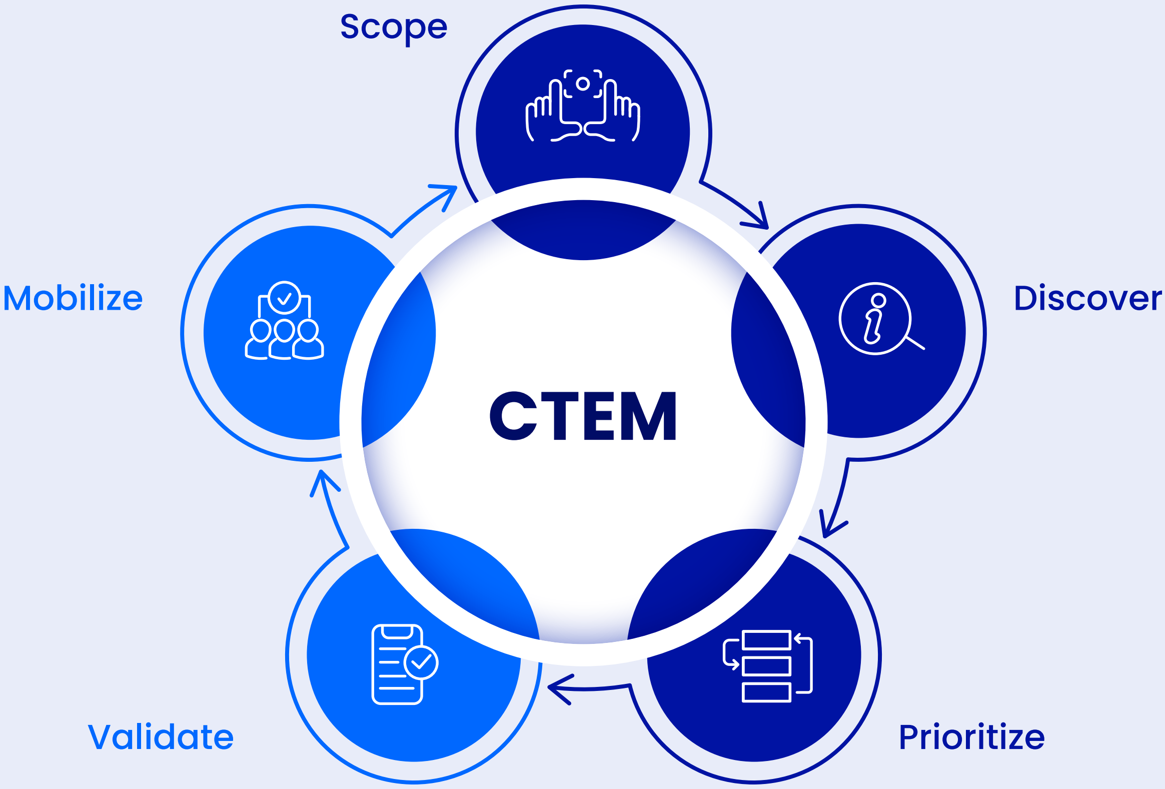
Exposure Analytics

Cymulate Exposure Analytics is a data aggregation and exposure intelligence solution that collects data from across enterprise IT, clouds, and the security stack to support exposure management programs to measure and baseline cyber resilience, focus on the most significant risks, and accelerate mitigations. Cymulate Exposure Analytics pulls data from vulnerability management platforms, asset inventories, clouds, security controls, and the IT infrastructure. Data are aggregated to contextualize the information with business relevance, prioritize remediation, and measure and optimize cyber resilience.

06 Conclusion

While attackers may always target the healthcare industry because of its valuable data and requirement for always-on systems, Continuous Threat Exposure Management (CTEM) offers the best opportunity for security leaders to prevent the next breach. This proactive approach to cybersecurity provides security teams with the strategies and technologies to identify and fix the most critical issues before attackers can find and exploit them.

To accomplish this goal, security teams must rely on automated discovery and assessments to continuously discover the attack surface and validate security effectiveness with offensive testing of breach and attack simulation and automated red teaming.



CTEM program framework as defined by Gartner

About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 500 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.