

CHARTIS TOP READS

Healthcare's vulnerability to cybersecurity reflected in rising threats and soaring costs

Week of August 20 - August 26, 2023

| **AUG 25, 2023**

<https://www.chartis.com/insights/healthcares-vulnerability-cybersecurity-reflected-rising-threats-and-soaring-costs>

The Buzz This Week

A recent report from Moody's Investors Service highlights the healthcare industry's susceptibility to cyber threats and data breaches. The healthcare sector is a prime target for such breaches, earning it the label of being "cyber poor." Nonprofit healthcare organizations are rated as having a "very high risk," while for-profit healthcare organizations are considered "high risk."

Healthcare data breaches have consistently been the most expensive across all industries for 13 consecutive years. IBM's Cost of a Data Breach Report, released last month, reveals that over the past 3 years, the average cost of breaches to healthcare organizations has risen by more than 50%. Healthcare organizations lose an average of \$10.93 million for each data breach that occurs. Factors like environmental complexity, staffing shortages, and the time taken to detect and manage breaches contribute to this high cost. On average across all industries, the data breach life cycle for companies is 277 days to identify and contain a data breach—this life cycle is often higher for regulated industries like healthcare.

Federal records indicate that between 2010 and 2022, 385 million patient health records have been exposed in healthcare data breaches. One of the largest data breaches since 2010 occurred this summer—impacting an estimated 11 million patients. Ransomware attacks, an alternative form of cyber threat known as a "threat-to-life crime," can be especially dangerous for patients and healthcare facilities due to their direct impact on a hospital's capacity to provide patient care. A 2021 survey of nearly 600 IT professionals found these attacks have the potential to result in adverse patient outcomes. Among those surveyed who encountered ransomware attacks, most reported extended hospital stays, procedural and testing delays, and diversions. Over a third of respondents noted heightened complications, while nearly a quarter raised concerns about increased mortality rates.

Why It Matters

The [digitization of healthcare](#) infrastructure has driven significant improvements in patient care while also introducing vulnerabilities to potential cyberattacks due to the rapid adoption of technologies. The risk was further heightened during the pandemic, driven by the swift adoption of telehealth and the shift to remote work. Given the evolving landscape and a wide array of threats, it is essential to [integrate cybersecurity](#) into established governance, risk management, and business continuity frameworks.

Policymakers must continue to strengthen the regulatory environment for healthcare cybersecurity. Last month, the White House [announced a federal plan](#) to work alongside the private sector and other entities to put into action the [National Cybersecurity Strategy](#), which was released in March in an effort to improve the nation's cyber defense. The National Cybersecurity Strategy Implementation Plan (NCSIP) details more than 65 federal initiatives, each corresponding with the [strategy's 5 pillars](#): “defend critical infrastructure, disrupt and dismantle threat actors, shape market forces to drive security and resilience, invest in a resilient future, and forge international partnerships to pursue shared goals.”

Healthcare organizations must enhance their investments in cybersecurity and readiness to counter cyber threats in an effort to safeguard patient data, maintain crucial operations, and uphold community confidence. According to the [2022 HIMSS Healthcare Cybersecurity Survey](#), despite significant progress, challenges like limited security budgets, workforce issues, and insufficient training persist. This survey, which included responses from 159 cybersecurity professionals, highlighted that healthcare leaders indicate workforce challenges are a key concern. Notably, 84% of respondents identified recruiting qualified cybersecurity staff as their top concern, followed by concerns about budget constraints. A recent [Gartner study](#) highlighted that Chief Information Officers (CIOs) are prioritizing cybersecurity investment, with 66% planning to increase spending. Ultimately, healthcare organizations, together with government agencies, must take proactive measures to secure their operations and patients by effectively implementing protective measures.

RELATED LINKS

HHS:

Modern Healthcare:

Healthcare Dive:

Wall Street Journal:

Editorial advisor: [Roger Ray, MD](#), Chief Physician Executive.

Chartis Top Reads

[View All](#)

Our services

[STRATEGIC TRANSFORMATION](#)

[PERFORMANCE TRANSFORMATION](#)

[DIGITAL & TECHNOLOGY TRANSFORMATION](#)

[CHARTIS CENTERS FOR AI & STRATEGIC INTELLIGENCE](#)

[PAYER TRANSFORMATION](#)

[STRATEGIC COMMUNICATIONS & CHANGE MANAGEMENT](#)

LEARN MORE ABOUT THE AUTHOR



Emily Nevarez
Research Manager