rubrik

EBOOK

Safeguarding Patient Care

A Healthcare Leader's Guide to Achieving Cyber Resilience

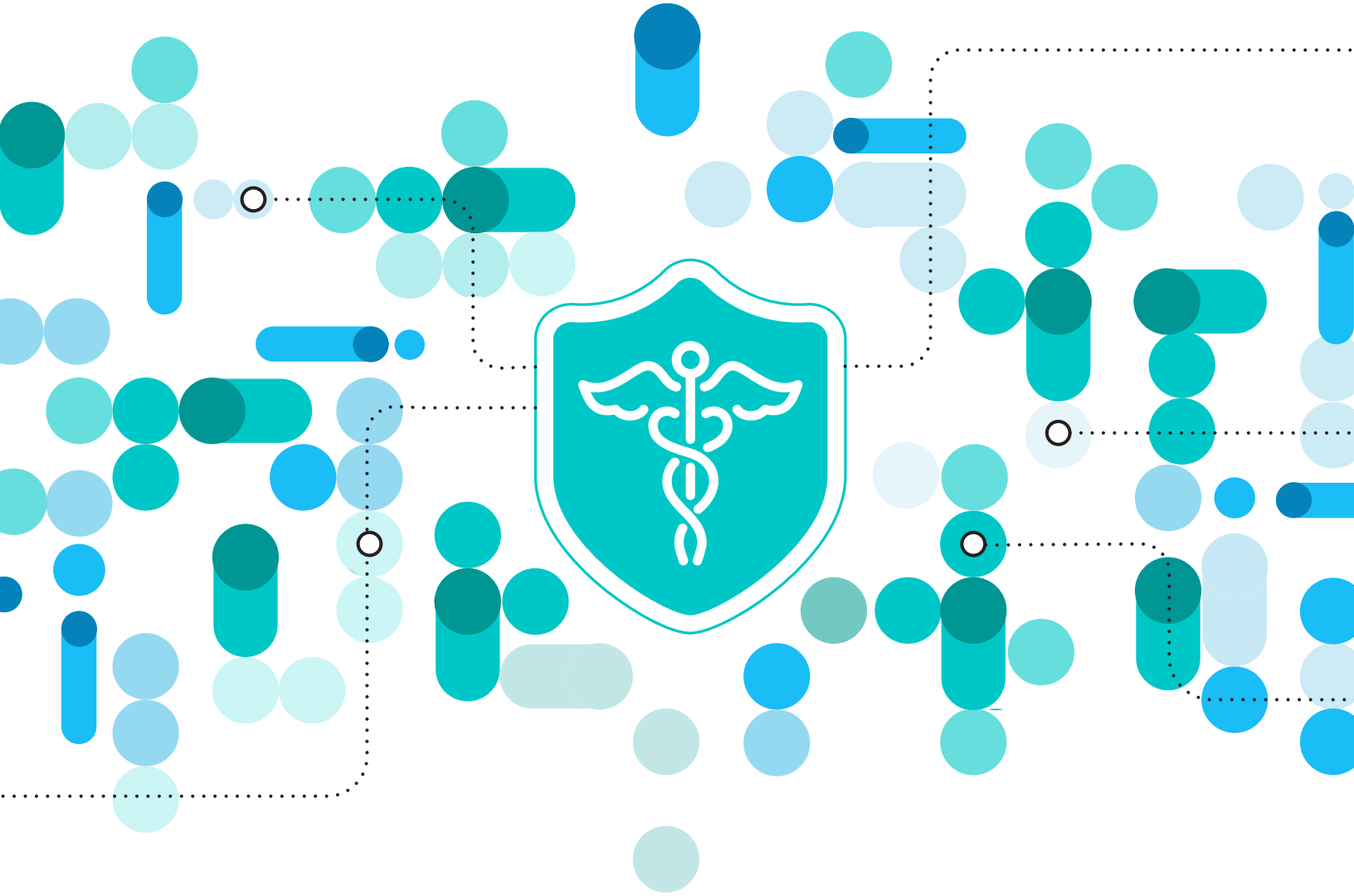


Table of Contents

Healthcare organizations today face an unprecedented surge in cyber threats that jeopardize not only sensitive patient data but also the very continuity of care. In the US alone, 389 healthcare institutions suffered successful ransomware attacks within the last fiscal year, according to Microsoft's 2024 Digital Defense Report. These attacks took systems offline, delayed critical medical operations, and caused appointments to be rescheduled.[1] According to another study from The University of Minnesota Twin Cities - School of Public Health, hospitals hit with ransomware took an average of two to three weeks to return to typical patient care levels following an attack.[2] The financial toll is equally staggering. A typical hospital lost between 0.5 and 1% of their total annual revenue as a direct result of a single ransomware attack.[3]

In short, prolonged system outages disrupt critical operations, delay procedures, force organizations to revert to manual paper-based processes, and divert patients to other facilities, ultimately compromising the quality of care and patient outcomes, as well as the healthcare organization's revenue. In an industry where every second counts, the stakes could not be higher.

Faced with this new reality, healthcare IT and security leaders must shift their cybersecurity mindset from prevention only to one that focuses on complete cyber resilience. While preventing incidents remains crucial, organizations must also be prepared to quickly detect, respond to, and recover from inevitable attacks to maintain patient care continuity. By implementing a modern cyber resilience platform, healthcare organizations can dramatically reduce their recovery times from ransomware attacks and operational failures, minimize the impact to patient care, and protect their organizations from significant financial ramifications.

This ebook serves as an essential guide for CIOs, CISOs, and other IT leaders in the healthcare space navigating this complex landscape. We will explore the anatomy of modern cyberattacks affecting healthcare organizations, provide a framework for assessing your organization's risk exposure, and outline the key capabilities and best practices needed to achieve true cyber resilience. Through real-world case studies and practical insights, you will learn how leading healthcare organizations are leveraging modern cyber resilience platforms to safeguard their data, maintain operational continuity, and continue delivering excellent patient care in the face of growing threats.

The time for action is now. As a healthcare leader, you have a critical role to play in fortifying your organization's defenses and ensuring the resilience of your mission-critical systems. Let this ebook be your roadmap to a more secure, resilient future for your organization and the patients you serve.

1. Microsoft Digital Defense Report 2024
2. Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients
3. Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients

Understanding the Anatomy of a Healthcare Cyberattack

To effectively defend against cyber threats, it's crucial to understand the tactics and techniques employed by attackers targeting healthcare organizations. While the specific methods may vary, most attacks follow a common pattern.

Phishing and compromised credentials remain the top vectors for initiating an attack. In fact, 16% of breaches involved compromised credentials, and 15% involved phishing.[4] Hackers often prey on unsuspecting employees, tricking them into revealing login information or installing malware through deceptive emails or websites. Legacy systems with unpatched vulnerabilities also provide an easy entry point for attackers.

Once inside the network, attackers often lurk undetected for an extended period, known as the dwell time. During this phase, they move laterally across the environment, escalating privileges and identifying valuable targets such as electronic health records (EHRs) and medical devices.

The attack often culminates in data exfiltration and encryption. Sensitive patient data is silently siphoned off, possibly to be sold on the dark web or used for blackmail. Then, hackers may encrypt critical systems, rendering them inaccessible to the healthcare organization and grinding operations to a halt. Recent high profile attacks, such as the ransomware incident at Change Healthcare, a UnitedHealth Group subsidiary, underscore the devastating impact of these attacks. The Change Healthcare attack caused adverse financial impacts at 94% of hospitals[5] and cost UnitedHealth $870 million in just Q1 of 2024.[6]

4. IBM Cost of a Data Breach Report 2024
5. AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances
6. Forbes: UnitedHealth Paid Hackers $22 Million, Fixes Will Soon Cost Billions

Why Is Healthcare Data So Valuable?

Healthcare data has become an increasingly attractive target for cybercriminals, making the healthcare sector particularly vulnerable to cyberattacks.

There are several key reasons for this trend:

Healthcare records have high monetary value on the black market. A single healthcare record can be worth significantly more than other types of personal data, such as credit card numbers (Up to $500 for a medical record compared to $1 to $5 for a compromised credit card).[7]

Healthcare data's value is partly due to the wide array of sensitive information it contains, such as Social Security numbers, dates of birth, financial details, and medical histories. This comprehensive nature makes it highly valuable for identity theft and other forms of fraud. Unlike credit card numbers that can be quickly canceled, healthcare data has long-term misuse potential, often remaining exploitable for extended periods without detection.

The sensitive nature of healthcare data also adds another layer of vulnerability. Medical records often contain intimate details about a person's physical and mental health, making them potentially embarrassing if exposed. This sensitivity can make healthcare organizations more likely to pay ransoms quickly to prevent data leaks, further incentivizing cybercriminals.

7. Seattle Times, Why health care has become a top target for cybercriminals

Assessing Your Organization's Cyber Risk Exposure

To build an effective resilience strategy, you must first understand your organization's unique risk profile. Start by identifying and quantifying your sensitive data assets. EHRs are a prime target, containing a wealth of valuable patient information. And that's just one system.

Patient data likely exists in a host of different systems, including Microsoft 365, mobile devices used to capture patient data, and other applications used by medical staff—to name just a few areas. So, to properly assess your risk profile, you first have to take a thorough inventory of your data and assess the potential impact of data loss or exposure.

How to Assess the Potential Impact of Data Loss or Exposure

To conduct a thorough inventory and assess the potential impact of data loss or exposure, healthcare organizations should:

- Implement sensitive data discovery tools to identify and locate protected health information (PHI) and personally identifiable information (PII) across the organization's systems.
- Regularly scan and catalog data repositories, including user home folders, shared drives, and applications that may contain sensitive information.
- Assess and remediate "puddles" of PHI/PII found in unexpected locations, such as Excel spreadsheets created from data exports.
- Identify overexposed or stale data and remove what you don't need.
- Identify the organization's most risky users based on sensitive data access and implement least-privilege access.
- Quantify the number of patient records and sensitive data points to understand the potential scope of a breach.
- Evaluate the financial impact of a potential data breach, considering factors like:
  - Patient notification costs
  - Regulatory fines and penalties
  - Legal fees and potential class action settlements
  - Revenue loss during system outages
  - Long-term reputational damage and patient defection

By taking these steps, healthcare organizations can better understand their data landscape, quantify potential risks, and engage leadership, so they can make informed decisions about protecting their organizations' data.

Next, evaluate the resilience of your current backup and recovery systems. Legacy solutions often struggle to keep pace with the volume and velocity of healthcare data. They may lack the necessary immutability, isolation, and cyber recovery speed and capabilities to withstand a sophisticated attack.

Legacy solutions may also have a difficult time protecting data across disparate systems. Healthcare organizations often use numerous applications to care for patients and do business. This complex web of applications not only increases attack surface areas, it also makes it a challenge to act quickly when a breach does occur.

That's why it's important to assess your recovery time objectives (RTO) and recovery point objectives (RPO) against your current capabilities to identify gaps.

For instance, if your organization is relying on disparate systems to protect on-premesis, cloud, and SaaS applications, that can slow down your ability to restore all the impacted systems across the entire environment. If you don't know where to turn to find a clean copy of impacted data, you'll be forced to either deal with lengthy disruptions or pay a ransom. Make sure you know how long it will take to determine the blast radius, find and quarantine malware, and meet reasonable RTOs before an attack occurs.

Equally important is understanding the financial implications of an attack. IBM's annual Cost of a Data Breach Report has tracked the cost of data breaches for nearly two decades. According to its research, the average cost of a data breach for all industries globally is $4.88 million.

But for healthcare, that number is almost double at an average of $9.77 million per breach. In fact, healthcare has led all other industries for the average costliest data breach for 14 years in a row.[8] These costs include operational downtime, lost customers, and post-breach response efforts, among many other costs.

Because of the strict regulations surrounding healthcare data, regulatory fines around data breaches are particularly concerning for healthcare organizations. For instance, in the US, HIPAA penalties can reach into the millions-of-dollars range, depending on the severity of the violation.[9] Factor in potential legal liabilities, reputational damage, and patient churn for a comprehensive risk assessment.

Translating this risk into financial terms is key to gaining executive and board support for resilience initiatives. Quantify the potential impact using historical data and industry benchmarks. Then, present a compelling business case that highlights the ROI of investing in cyber resilience capabilities.

8. IBM Report: Escalating Data Breach Disruption Pushes Costs to New Highs
9. The HIPAA Journal: What are the Penalties for HIPAA Violations?

Risk Assessment Checklist

- **Conduct a comprehensive data inventory, identifying all sensitive information assets**
- **Evaluate the security posture of all on-premises, cloud, and SaaS applications**
- **Assess current backup and recovery capabilities against industry best practices**
- **Calculate potential financial losses from system downtime and data breaches**
- **Review regulatory compliance requirements and potential penalties**
- **Analyze the impact on patient care and organizational reputation**
- **Develop ROI models for proposed resilience investments**

Building a Cyber Resilience Game Plan

With a clear understanding of your risk landscape, you can develop a pragmatic cyber resilience strategy. Proactive preparation is the foundation.

Start by identifying and remediating sensitive data exposure.

Implement strict least-privilege access controls and measures to ensure sensitive information is properly secured.

Regularly test and validate the integrity of your backups to ensure they can survive an attack.

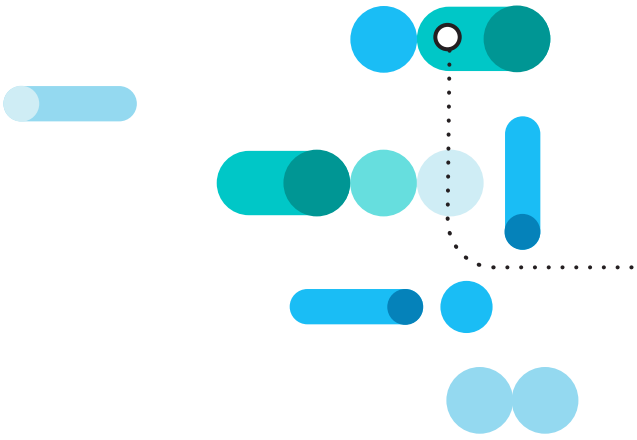
Develop and test a comprehensive incident response plan that outlines roles, responsibilities, and communication protocols.

Conduct regular tabletop exercises to refine your processes and ensure team readiness. Evaluate cyber insurance options as part of your risk mitigation strategy.

To enable rapid recovery, you'll need a modern data protection architecture. Here are some qualities and capabilities to look for in a solution:

- Isolated and immutable backups that ensure data availability and integrity even if production systems are compromised
- Anomaly detection and alerting to quickly identify suspicious activities
- AI-driven threat hunting across backup data to proactively uncover hidden threats
- Fast threat detection and blast radius scoping to help teams minimize the impact of an attack
- Integration of your data protection solution with your broader security ecosystem, including SIEM and incident response tools, to help teams better coordinate their response to incidents
- Isolation of infected snapshots to reduce the risk of reintroducing the malware during a recovery operation
- Surgical recovery of only the impacted data and files to significantly reduce downtime
- Automated identification of clean recovery points for quick recovery of applications to production
- Automation and orchestration of recovery workflows to streamline the recovery process and minimize human error

As healthcare data becomes increasingly distributed across on-premises, cloud, and SaaS environments, a unified approach to data resilience is essential. Look for solutions that combine backup and recovery with cybersecurity to protect data, monitor for threats, improve your data security posture, and assist with cyber recovery—across your entire ecosystem. The ideal solution should include centralized management and policy enforcement, so your resilience strategy can seamlessly extend to new environments as your organization adopts cloud services and navigates M&A activities.



Rubrik Security Cloud: The Platform for Healthcare Cyber Resilience

Rubrik Security Cloud, a leading cyber resilience platform, aligns closely with the key capabilities needed for healthcare cyber resilience. Built on a zero trust architecture, Rubrik provides immutable, encrypted, and isolated data protection, ensuring the integrity of your backups.

With Rubrik, healthcare organizations can achieve rapid recovery for critical systems with quick restoration of EHRs, like Epic, drastically reducing downtime. Granular recovery options, including file-level restores, ensure you can quickly retrieve specific data sets as needed.

Rubrik Security Cloud also offers built-in sensitive data discovery and threat detection capabilities. Rubrik's AI-driven anomaly detection engine continuously scans backups for signs of ransomware and other threats. And Rubrik's sensitive data discovery and classification helps identify and remediate sensitive data exposure across your environment.

The combination of enterprise, SaaS, and cloud-native protection make Rubrik a seamless fit for hybrid and cloud-forward healthcare environments. Plus, Rubrik's unified platform allows you to centrally manage and protect data across these systems, simplifying operations and ensuring consistent policies.

Real-world healthcare customers have used Rubrik to significantly enhance their cyber resilience. For example, Kern Medical Center recovered 100% of its systems protected by Rubrik after a ransomware attack, with minimal disruption to patient care.[10]

Similarly, St. Luke's University Health Network credits Rubrik with reducing the time it takes to recover their data from months to minutes or hours.[11]

Check out these case studies:

- Learn how Rubrik helped Kern Medical Center defend against ransomware.
- Learn how Rubrik helped St. Luke's secure millions of patient records while saving money.

10. Learn how Rubrik helped Kern Medical Center defend against ransomware.
11. Learn how Rubrik helped St. Luke's secure millions of patient records while saving money.

Protecting Patients Requires Healthcare Organizations to Prioritize Cyber Resilience

As the threat landscape continues to evolve and healthcare data continues to grow, healthcare organizations must adapt their cybersecurity strategies to ensure the continuity of patient care. The alarming rise in attacks, coupled with the staggering financial and operational impact, underscores the urgent need for a paradigm shift from prevention to resilience.

By understanding the anatomy of modern attacks, assessing your risk exposure, and implementing a comprehensive resilience strategy, you can position your organization to withstand and quickly recover from inevitable incidents. A cyber resilience platform provides the critical capabilities needed to achieve true cyber resilience in healthcare.

With immutable backups, rapid recovery options, and intelligent threat detection, modern cyber resilience platforms empower healthcare organizations to minimize the impact of attacks and continue delivering vital services.

The time to act is now. As a healthcare leader, you have the opportunity and responsibility to champion cyber resilience initiatives within your organization.

By making strategic investments in modern cyber resilience platforms and fostering a culture of resilience, you can safeguard your organization's mission and protect the well-being of the patients you serve.

The stakes have never been higher, but with the right approach and tools, healthcare organizations can rise to the challenge and thrive in the face of evolving threats.

Learn more about cyber resiliency and other strategies for safeguarding your patient data in this collection of sessions from our Healthcare Summit. Click here to check it out.

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik (NYSE: RBRK) is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.

safeguarding-patient-care / 20250221