SECURANCE CONSULTING

Advantage of Insight | AI

DIGITAL HEALING, DIGITAL THREATS:

WHY CYBERSECURITY ASSESSMENTS ARE CRITICAL TO PROTECTING HEALTHCARE SYSTEMS

www.securanceconsulting.com

HEALTHCARE'S CYBER CRISIS

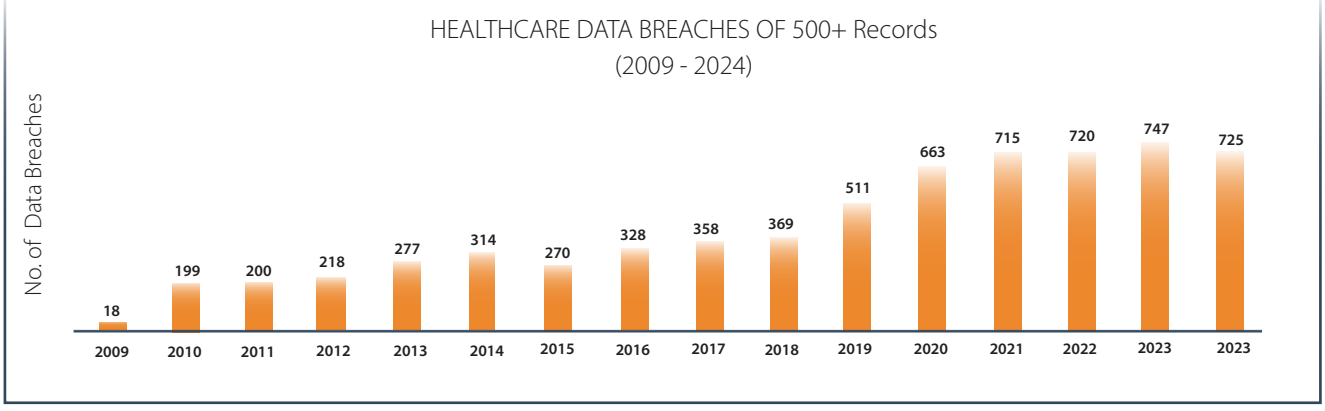
Electronic medical records (EMRs), telehealth, and cloud-based platforms power everything from patient scheduling to surgical planning. But this transformation comes at a cost. As healthcare organizations connect more systems, adopt more tools, and share more data, they also increase their exposure to cyber threats.

Healthcare is now one of the most targeted industries for ransomware and data breaches. These attacks don't just leak sensitive information; they delay diagnoses, cancel procedures, and endanger patients' lives. Unfortunately, many healthcare providers are still playing catchup when it comes to cybersecurity.

Protecting patients and keeping operations running takes more than firewalls and compliance. Organizations need a clear understanding of their risks. Cybersecurity assessments provide that clarity by uncovering weaknesses before attackers do.

Cyber Risk in Healthcare: At a Glance

Visualizing breach volume and cost trends over the past 10 years.[1]



DIGITAL CARE, DIGITAL RISK: IT AS A CLINICAL ASSET

A Perfect Storm of Risk

Regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), along with frameworks such as the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) and HHS' Health Industry Cybersecurity Practices (HICP), offer essential guidance for protecting healthcare systems and patient data. Compliance sets minimum safeguards, but attackers exploit gaps like unpatched systems, misconfigurations, and human error. Without ongoing testing and monitoring, organizations stay vulnerable, especially when documentation outweighs real defense.

This puts healthcare at a unique risk. The combination of digital transformation, regulatory demands, and operational pressures has created a perfect storm. The convergence of digital transformation, regulatory complexity, and operational pressure has created a perfect storm. While the sector continues to innovate in care delivery, many providers lack cybersecurity readiness. The result? An environment where attackers don't need to break in; they simply log in through overlooked gaps.

Key systemic challenges include:

- **Expanded Attack Surface:** IoT devices, telehealth portals, and third-party integrations increase exposure.
- **Legacy Systems:** Outdated infrastructure and weak segmentation are common.
- **Limited Resources:** Underfunded IT teams struggle, particularly in community and nonprofit hospitals.
- **Policy vs. Practice Gaps:** Written procedures often fail to match daily operations.
- **Operational Fallout:** Breaches can shut down labs, cancel surgeries, and delay treatment.
- **Patient Safety:** Cyberattacks directly threaten clinical outcomes and lives.

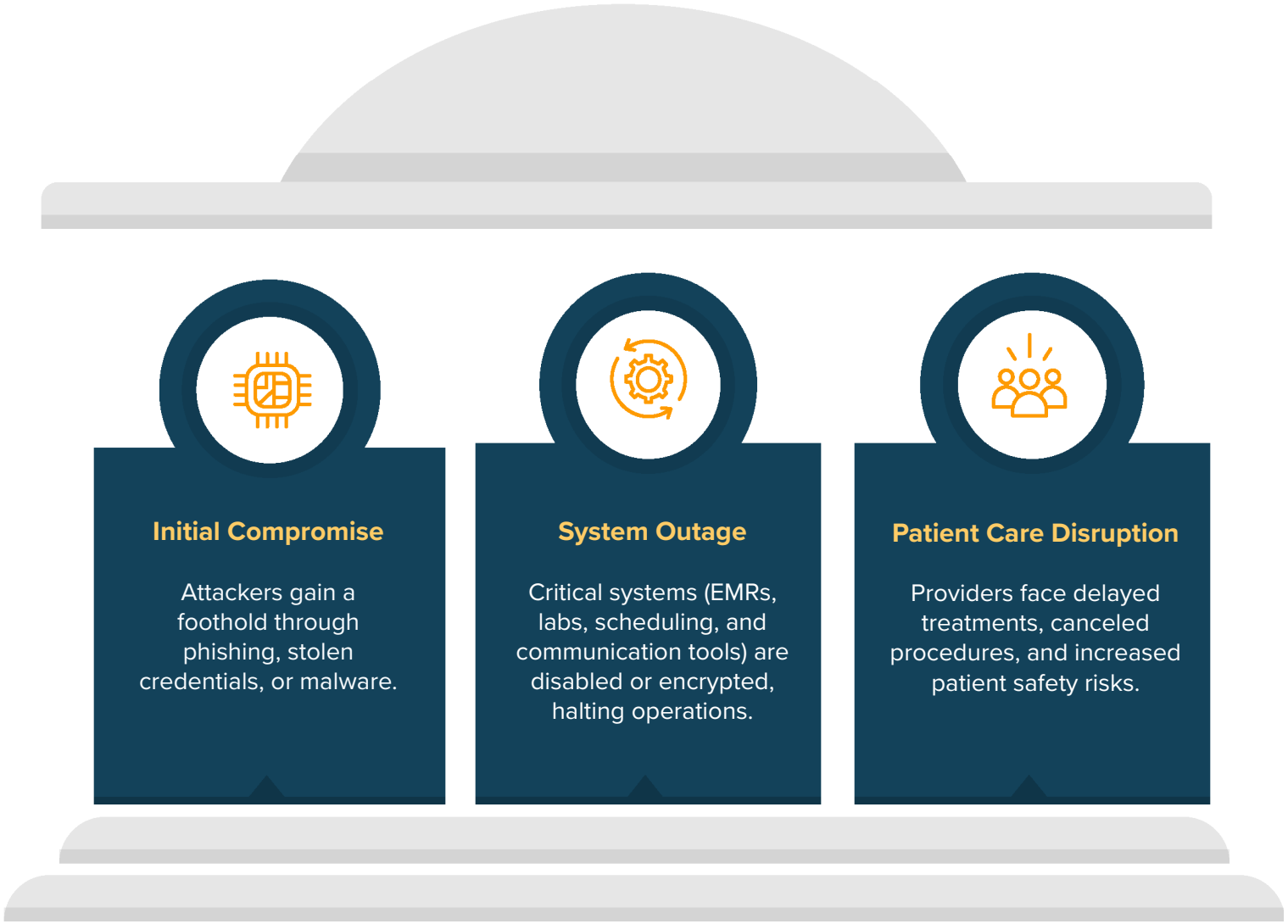
Individually, these risks may be manageable. Combined, they multiply in scale and impact, creating a threat landscape few organizations are prepared to navigate.

Small Oversights with Massive Consequences.

Cyberattacks rarely begin with sophisticated exploits. Most stem from basic lapses: a missed patch, an inactive user account, or a phishing email that evades filters. These seemingly minor cracks often go unnoticed until attackers exploit them at scale. The true danger lies not only in the breach but in how quickly it spreads and disrupts care.

Without regular cybersecurity assessments, vulnerabilities remain invisible. And when an attack hits, the damage extends far beyond IT. Patient trust, clinician efficiency, and organizational reputation are all at stake.

How One Weak Point Can Trigger a System-Wide Crisis



WHEN RISK BECOMES REALITY

The following incidents highlight the critical risks healthcare organizations face when security gaps are left unchecked.

CommonSpirit Health

A ransomware attack in 2022 forced CommonSpirit Health, one of the largest nonprofit health systems in the United States, to disconnect hospitals in 13 states from their electronic health record (EHR) systems.[2] This led to delayed procedures, canceled appointments, and patient care disruptions across emergency rooms, cancer centers, and outpatient clinics. Some hospitals were forced to revert to paper records for weeks. The incident exposed critical gaps in cyber resilience and ultimately cost the organization more than $160 million in remediation and operational losses.

Weak network segmentation allowed the ransomware to propagate across systems that should have been isolated. In addition, incident response plans were either outdated or untested, leading to delayed detection, slow containment, and a prolonged recovery timeline.

Change Healthcare

In early 2024, Change Healthcare, responsible for processing a significant portion of the nation's healthcare claims, fell victim to a ransomware attack that paralyzed billing, prescription services, and prior authorizations for hundreds of providers nationwide.[3] The attack created a supply chain crisis, delaying reimbursements and forcing many providers to front costs or halt services. Change paid a $22 million ransom, and downstream disruption has been estimated to exceed $6 billion, with long-term effects on both financial operations and patient trust.

These are not isolated failures. They reflect a troubling pattern of systemic weaknesses that often go unnoticed until it is too late. From poor third-party oversight to insufficient network segmentation and inadequate response planning, these vulnerabilities are both avoidable and persistent.

The lesson is clear: the cost of inaction is high. Enterprise-wide cybersecurity assessments are essential. They provide the visibility, validation, and insight needed to anticipate threats, strengthen defenses, and prevent the kind of widespread disruption we continue to see.

> ***In 2024, industry sources found that U.S. healthcare providers lost an average of $2 million per day during ransomware-induced downtime.[4]***

From Blind Spots to Clear Strategy

Cybersecurity assessments are diagnostic tools that uncover hidden risks and challenge assumptions. In healthcare, systems are often presumed secure, backups assumed reliable, and vendors trusted implicitly.

Assessments provide verification. They test controls, evaluate readiness, and identify vulnerabilities before attackers do. For healthcare leaders, they offer clear data to guide decisions, justify investments, and strengthen accountability. The result is a more resilient, informed approach to protecting patients and operations.

What a Comprehensive Assessment Covers:

1. Foundational Security Controls

- Validate zero-trust architecture and enforcement of multi-factor authentication.
- Audit encryption, authentication, and access controls.
- Confirm reliable backups and sound data governance practices.

2. Infrastructure and Network Hardening

- Use vulnerability and penetration testing to identify unpatched systems, outdated software, and misconfigurations.
- Evaluate firewalls and network segmentation.
- Review VPN, remote access, and cloud configurations.

3. Operational Resilience

- Assess incident response and disaster recovery plans.
- Run breach simulations and tabletop exercises.
- Test end-user awareness with phishing simulations.

4. Vendor and Third-Party Risk

- Analyze vendor access management and audit capabilities.
- Verify third-party compliance.
- Ensure contract terms include breach response protocols and transparency.

These insights not only reduce the likelihood of a breach, but they also prepare organizations to respond effectively if one occurs.

> ***In 2024, healthcare had the highest average data breach cost of any industry at $9.77 million.[1]***

BEST PRACTICES

Conducting regular cybersecurity assessments is essential for ensuring your defenses can perform under real-world conditions. These assessments go beyond compliance checklists and test your organization's ability to prevent, detect, and respond to threats.

Penetration tests simulate attacker behavior to uncover vulnerabilities such as unpatched systems, weak access controls, and misconfigured firewalls. Configuration reviews evaluate whether security settings across technologies, like firewalls, network devices, and cloud platforms, align with best practices, internal policies, and regulatory requirements. Reviews of IT controls and processes examine how effectively security measures are implemented and maintained over time, ensuring that policies are followed in day-to-day operations. More specific assessments, such as application and database security reviews and endpoint evaluations, provide a detailed picture of your risk exposure.Together, these services validate that your cybersecurity protections work not just in theory but in practice, helping you identify gaps, prioritize remediation activities, and strengthen resilience.

Tracking progress over time, from one assessment to the next, allows organizations to monitor improvements, and measure risk reduction. This visibility helps leadership, allocate financial and human resources more effectively, and respond to evolving threats with confidence.

Security Starts with Assessment

Modern healthcare is digital at its core. That means cybersecurity is no longer just an IT issue; it's a matter of clinical safety, operational continuity, and institutional trust. Every healthcare organization, regardless of size or specialty, faces escalating cyber risks. The question is not whether you'll be targeted, but when.

Cybersecurity assessments provide the visibility, insight, and strategy needed to stay ahead of evolving threats. For healthcare leaders, they are the first step toward long-term resilience. If your organization has not been conducting regular assessments, start with a baseline evaluation. A baseline assessment should benchmark your current security posture, identify urgent risks, and highlight gaps across people and technology providing a broad view of risks across your environment.

As your security program develops, assessments should become more targeted and sophisticated. A more mature assessment will often include technical testing, detailed process reviews, and advanced threat simulations. From there, organizations can prioritize next steps based on risk, regulatory requirements, and available resources. Assessments form the foundation of a proactive strategy, guiding security investments and improving outcomes across the care continuum.

If you're ready to launch or mature your assessment program, click here to schedule an initial discussion.

ABOUT SECURANCE

Securance has more than two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://www.hipaajournal.com/2024-healthcare-data-breach-report
2. https://medcitynews.com/2024/12/healthcare-cyberattack-ransomware
3. https://www.chiefhealthcareexecutive.com/view/commonspirit-says-some-patient-information-accessed-in ransomware-attack
4. https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf
5. https://www.hipaajournal.com/biggest-healthcare-data-breaches-2024

Digital Healing, Digital Threats

© 2025 Securance LLC. All Rights Reserved.

SECURANCE CONSULTING
Advantage of Insight AI

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com