KATALYST

DIGITAL OPERATIONS PARTNER

HEALTHCARE EDITION

2026 Katalyst Cybersecurity Executive Report

Securing Your Digital Backbone

How Healthcare Organizations Are Protecting Patient Care, Reducing Risk, and Strengthening Operational Resilience in 2026

In healthcare organizations, technology is not a back-office function. It supports patient scheduling, EHR and EMR access, diagnostic systems, clinical coordination, billing, and secure patient communication. When systems go down, care is delayed. The organizations building intentional digital backbones are reducing disruption risk and strengthening the patient trust that defines their reputation.

This report is your benchmark. Your baseline. Your starting point.

$10.93M
avg healthcare breach cost

1 in 4
hospitals report care disruption after cyber incidents

48+ hours
common EHR recovery delays after ransomware

HIPAA
compliance pressure continuing to rise

EXECUTIVE LETTER

A Message From Our CEO

Something has shifted in the conversations I have with healthcare leaders. They are no longer asking whether cybersecurity matters to patient care. They are asking why it feels so hard to get under control, and what it will take to get ahead of it.

- **Security is an operational resilience issue**
- **Boards are asking different questions**
- **Compliance intensity is accelerating**
- **Growth and security are colliding**
- **Vendor sprawl is compounding exposure**
- **Internal bandwidth has reached its limit**

The healthcare organizations that solve this in 2026 carry a durable advantage forward. They protect patient trust, pass audits with less disruption, and keep care running. The ones that don't keep paying in downtime, breach notifications, staff burnout, and the patient confidence they cannot easily rebuild.

Luke ohnson
CEO, Katalyst
Digital Operations Partner

The conversation in every healthcare boardroom has changed. Technology risk is no longer a footnote in the annual report. It is a standing agenda item in risk and quality committees across organizations of every size, because when systems go down, patient care is what stops.

> *"The Digital Backbone must be intentional. It cannot be inherited, assembled by accident, or managed by whoever has time."*

What does that mean in practice? It means the infrastructure your organization depends on, the network, the EHR and clinical systems, the cloud environment, and the Microsoft 365 platform your staff work in every day, needs to be owned, operated, and improved with the same discipline you apply to patient care.

Security is a discipline, not a purchase.
The healthcare organizations pulling ahead are not those with the most tools. They have the clearest accountability and the most consistent execution.

Compliance is a floor, not a ceiling.
Regulators, insurers, and patients are raising expectations faster than most organizations are raising their posture. HIPAA is the baseline, not the goal.

The co-managed model is how this gets solved.
Healthcare organizations cannot hire their way to security maturity. Embedded partnership with shared accountability is the answer.

Six Forces Reshaping Technology Leadership

Healthcare organizations are balancing growing cybersecurity threats, evolving patient expectations, workforce challenges, and increasing reliance on connected technologies. These are six forces reshaping technology leadership in 2026.

01

Security Leadership Has Changed

Cybersecurity has become an executive responsibility. Technology leaders are expected to protect patient care, manage organizational risk, and demonstrate operational resilience, not simply maintain IT systems.

02

Third-Party Risk Is Expanding

Healthcare organizations depend on electronic health record platforms, medical device manufacturers, cloud providers, and business associates to deliver care. Managing third-party risk has become essential to protecting patient information and maintaining operational resilience.

03

Connected Healthcare Is Expanding Risk

Electronic health records, connected medical devices, cloud platforms, telehealth solutions, and digital patient services continue to expand the healthcare technology ecosystem. Every new connection introduces additional security and operational risk.

04

Technology Priorities Continue to Expand

Technology teams are balancing cybersecurity, clinical operations, AI adoption, infrastructure modernization, and patient experience initiatives while maintaining critical healthcare systems. Strategic priorities increasingly compete for the same resources.

05

Operational Resilience Is Now a Strategic Priority

Healthcare organizations are expected to maintain uninterrupted clinical operations despite cyber threats, outages, and technology disruptions. Cybersecurity has become inseparable from patient safety and organizational resilience.

06

Digital Healthcare Is Expanding the Attack Surface

Cloud adoption, hybrid work, telehealth, connected medical devices, and AI-enabled workflows continue to expand the attack surface. Security must be integrated into digital transformation from the beginning.

When Technology Fails, Care Is Disrupted in Healthcare Organizations

- Patient care and EHR uptime
- HIPAA compliance and breach reporting
- Cyber insurance eligibility
- Vendor and third-party risk exposure
- Revenue cycle and billing resilience

In 2026, cybersecurity in healthcare is not an IT conversation. It is a patient care conversation. When systems go offline, appointments are canceled, clinical workflows break down, and billing cycles stall. Compliance is required, but operational continuity is what patients and staff depend on.

41% increase in connected medical devices

52% of providers report cybersecurity staffing shortages

24/7 clinical systems uptime expectations

The organizations that move from reactive IT support to intentional digital backbone management are gaining something their patients and staff depend on every day:

Confidence.

1 in 3 healthcare organizations hit by ransomware in the past 12 months.

72% of providers cite downtime as a patient safety risk

58% of breaches involve third-party vendors

93% of healthcare organizations experienced phishing attacks

Lean IT Teams. Greater Risk Surface.

4–6
disconnected security tools the average healthcare environment runs, with no unified view across them

78%
of breaches begin with identity compromise

67%
of providers rely on third-party platforms

95%
of healthcare organizations use connected medical devices

500+
records trigger HIPAA breach reporting

The challenge is not awareness. It is operational capacity.

Healthcare is among the most targeted industries for ransomware and data theft

Medical records command premium value on the dark web. Attackers know that healthcare organizations face immediate pressure to restore systems, and attackers price ransom demands accordingly.

EHR and EMR systems are both mission-critical and high-value targets

A ransomware event does not just lock files. It disrupts scheduling, halts clinical workflows, delays billing, and creates HIPAA breach notification obligations simultaneously.

Phishing and identity compromise remain the primary breach entry points

Shared credentials, inconsistent MFA enforcement, and access that outlasts employment are the most commonly exploited gaps across mid-sized healthcare environments.

94% of ransomware now includes data exfiltration

Even when systems are restored, the breach is not over. Stolen patient data creates downstream notification requirements, regulatory exposure, and patient trust damage that persists for years.

Cyber insurance underwriting is tightening specifically for healthcare

Insurers are requiring documented MFA enforcement, EDR deployment, and tested backup procedures as conditions of coverage. Organizations that cannot demonstrate these controls face denials.

Small internal IT teams are managing environments of growing complexity

Multiple locations, dozens of vendors, EHR consultants, telecom providers, and standalone security tools, all managed by teams that often lack the depth to monitor and respond proactively.

Identity Is the New Perimeter

Identity

60%+ of breaches involve compromised credentials

Shared credentials, weak MFA enforcement, and inconsistent access reviews are among the most commonly exploited gaps in mid-sized healthcare environments. A single compromised credential can provide system-wide access to EHR systems, billing platforms, and patient records. Identity governance is consistently cited as one of the highest-impact, most underdeveloped areas across healthcare organizations of every size. MFA enforcement and access rights reviews are now explicit requirements for HIPAA compliance and cyber insurance eligibility. Organizations that have not operationalized these controls are failing audits and losing coverage options. Vendor access governance is equally important. Third-party connections to clinical and billing systems that lack documented review processes are a primary path for attackers and auditors alike.

Email

75% of attacks originate through email

Billing teams, executives, and vendor contacts are the primary phishing targets in healthcare. Business email compromise leading to fraudulent wire transfers and insurance claim manipulation is a documented and increasing loss event across the sector. AI-driven phishing has dramatically increased sophistication. Attackers now reference real patient workflows, insurance processes, and internal staff names in ways that make messages nearly indistinguishable from legitimate communications. Email security without continuous tuning leaves significant gaps. Healthcare fraud and impersonation incidents are rising annually, and a configuration from 18 months ago does not reflect the current threat environment.

91%
cyber attacks begin with phishing

MFA
now required by HIPAA and cyber insurers

45%
of healthcare breaches involve hacking

$18M
patient records exposed annually

Recovery Is a Strategic Function

Many healthcare organizations reviewed had not conducted documented restore testing within the past year, even those with active backup systems running daily.

94%

of ransomware incidents include data exfiltration

In healthcare, backup failure is a patient care failure.

EHR systems, imaging archives, scheduling platforms, and billing systems are the operational core of a healthcare organization. When ransomware hits and backups are unavailable or untested, the path to recovery is measured in weeks. 20+ days of downtime in healthcare means cancelled appointments, delayed procedures, and billing disruptions that compound daily.

Backups alone are not protection. Tested, immutable, documented recovery processes are.

The backup job completing successfully is not the same as the backup restoring successfully within your required window. Quarterly restore tests, documented and reviewed by leadership, are the standard that cyber insurers, HIPAA auditors, and healthcare IT best practices require.

50%

of organizations fail to test backups annually (2025 findings)

Recovery readiness determines whether disruption is measured in hours or weeks.

Organizations with documented, tested recovery procedures recover faster, incur lower breach costs, and face reduced regulatory exposure. The difference between a recoverable incident and a reportable disaster often comes down to whether the backup was tested before it was needed.

Complexity Increases Cost. Katalyst Reduces It.

> *"Leveraging a partnership in this way allows for faster, more productive progress since the team is already built and can expand as needed. They sit down onsite with you for strategic planning sessions, taking the time to learn the context of your business and understand what's most important to you."*
>
> -- Director of IT, Graystone Eye

1

No Unified Monitoring

Multiple IT vendors, separate EHR consultants, independent telecom providers, and standalone security tools, with no single view of what is happening across the environment.

When something goes wrong, no one has a complete picture. Ownership is unclear, response is slow, and the gap between detection and containment widens while the clock runs.

How Katalyst Helps:

Centralized monitoring creates unified visibility across clinical systems, infrastructure, and vendors, improving detection speed and incident response coordination.

2

Misaligned Accountability

Fragmented vendor relationships mean unclear ownership when incidents occur. Each vendor manages their piece; no one owns the whole environment.

In healthcare, ambiguous accountability during an incident is not just an operational problem and a HIPAA exposure. Breach response requires documented ownership of every system.

How Katalyst Helps:

Clear ownership across vendors, systems, and internal teams improves response coordination and strengthens operational accountability during incidents.

3

Compliance Stress

Disconnected tools, inconsistent controls, and manual reporting processes create ongoing compliance friction, particularly around HIPAA, cyber insurance documentation, and audit preparation.

Lean IT teams supporting 100-500+ users cannot sustain continuous compliance posture without structure. Fragmentation forces compliance into a recurring scramble instead of a maintained state.

How Katalyst Helps:

Standardized controls and centralized reporting reduce HIPAA and audit complexity while making compliance easier to maintain continuously.

16+
connected systems common across healthcare operations

75%
of providers cite staffing shortages as a top risk

1:100+
IT staff-to-user ratios common in healthcare

AI Is Not a Future Problem. It Is a Present Multiplier.

AI-Generated Phishing

AI-generated phishing campaigns are becoming more convincing, personalized, and difficult to detect across healthcare organizations.

Attackers use AI to mimic executives, clinicians, billing teams, trusted vendors, and patient-facing communications. Technical controls remain essential, but ongoing security awareness training is becoming equally important.

Deepfake Impersonation

AI-generated voice and video are making executive impersonation and payment fraud easier than ever.

Fraudsters are using increasingly realistic voice and video impersonation to manipulate payment approvals, vendor requests, and employee actions. Verification procedures and identity controls are becoming critical safeguards.

AI-Powered Vulnerability Discovery

AI is dramatically reducing the time between finding vulnerabilities and exploiting them.

New AI-powered vulnerability discovery tools can identify weaknesses and generate exploit paths in hours instead of weeks. Healthcare organizations relying on periodic scans or delayed remediation are increasingly at risk of falling behind.

AI isn't just creating new threats. It's dramatically accelerating how quickly attackers can exploit existing ones.

Recent demonstrations from AI-powered vulnerability discovery platforms such as Mythos show that vulnerability discovery and exploit development can now happen in hours instead of weeks. Healthcare organizations need an ongoing vulnerability management program to continuously identify, prioritize, and remediate risk before attackers can take advantage.

The Risk to Healthcare Organizations Is Immediate

AI is increasing the speed, scale, and sophistication of attacks targeting healthcare organizations. Providers are seeing more AI-generated phishing, executive impersonation, credential theft, ransomware, and AI-powered vulnerability discovery. At the same time, employees are increasingly using public AI tools without understanding the security implications, creating new avenues for patient information and organizational data to be exposed.

Healthcare organizations that combine security awareness training, secure access controls, behavioral monitoring, centralized visibility, and a mature vulnerability management program are significantly better positioned to reduce risk before attacks disrupt care delivery or compromise patient information.

Security Awareness Training

Build a security-aware culture through ongoing phishing simulations, end-user education, and reporting workflows that help employees recognize evolving AI-powered social engineering attacks.

Secure Access (SASE)

Protect patient information by applying consistent access policies, web filtering, and data controls across users, devices, and cloud applications. This also helps reduce risk from Shadow AI and unintended data exposure.

Managed Security Services

Behavioral monitoring, anomaly detection, and centralized visibility across identity, email, endpoints, EHR systems, and infrastructure enable faster detection and response before incidents affect patient care.

Vulnerability Management

Continuously identify, prioritize, and remediate vulnerabilities across your environment to reduce the growing window of exposure created by AI-powered discovery tools.

The Accountability Gap Is Not Tool Access. It Is Operational Discipline.

High Performers

- **MFA enforced across all users, vendors, and remote access**
  Not just enabled, but enforced consistently, with access rights reviewed against the full user list quarterly.
- **Centralized endpoint monitoring across all locations**
  A single view of all devices and systems with documented escalation paths and defined response SLAs.
- **Documented quarterly backup and restore testing**
  Restore tests are scheduled, executed, and results reviewed by leadership, not filed and forgotten.
- **Clear incident response runbooks and ownership**
  Every role knows what to do when an incident occurs. Runbooks are documented, practiced, and current.
- **Structured vendor accountability and reporting**
  Vendors have documented access rights, defined SLAs, and regular performance reviews, not open-ended relationships.

Lower Performers

- **Rely on reactive IT support without proactive monitoring**
  The first indication of a problem is a staff complaint or a system outage, not an alert. By then, damage is already done.
- **Lack documented recovery procedures for clinical systems**
  Backups exist but have never been tested against EHR and billing systems within actual recovery windows.
- **Maintain overlapping tools with unclear ownership**
  Multiple vendors, multiple dashboards, nobody accountable for the complete picture.
- **Have no executive-level visibility into technology risk**
  Leadership is making capital decisions about technology without visibility into the risk exposure those decisions carry.
- **No structured reporting to leadership or the board**
  When an incident happens, it is the first time leadership has heard about the underlying gap.

Moving from Downtime Risk to Operational Dependability

FROM

Reactive IT support

Issues are addressed after users report outages, tickets pile up, or clinical workflows fail. In healthcare, delayed response does not just impact operations. It impacts patient care, scheduling, billing, and staff productivity simultaneously.

TO

Proactive monitoring

Healthcare organizations cannot afford to learn about incidents when clinical systems go offline. 24/7 monitoring means threats are identified before they disrupt patient care.

FROM

Vendor sprawl

Separate EHR consultants, telecom providers, cloud vendors, MSPs, and security tools create fragmented ownership across the environment. When incidents occur, teams spend more time coordinating vendors than resolving the issue itself.

TO

Structured accountability

Every vendor touching patient data or clinical systems should have documented access rights, defined SLAs, and a named internal owner. Ambiguity is a compliance and security risk.

FROM

Untested backups

Backups may exist, but recovery procedures are often undocumented or never validated against real clinical systems. Organizations assume they can recover until a ransomware event or outage proves otherwise.

TO

Recovery confidence

A backup that has never been tested against your EHR and billing systems is an assumption. Documented quarterly restore testing is the difference between knowing and hoping.

FROM

Compliance anxiety

HIPAA, cyber insurance requirements, vendor risk reviews, and audit requests create constant operational pressure for lean IT teams. Without standardized processes and clear documentation, compliance becomes reactive instead of sustainable.

TO

Operational clarity

HIPAA compliance should be a maintained posture, not a recurring project. Organizations with structured digital backbones pass audits faster and with far less disruption to operations.

Patient trust is built on reliability. Reliability is built on structure.

Resilience Is Built Intentionally

High-performing healthcare organizations treat their IT environment as critical infrastructure, not overhead. A resilient digital backbone is designed with patient care continuity in mind, operated with discipline, and improved continuously.

01

CONNECT

Hybrid infrastructure, cloud platforms, and network connectivity managed as one cohesive environment. From on premises infrastructure and Azure to SD WAN, branch offices, and remote access, Katalyst standardizes, monitors, and optimizes how everything connects. Katalyst is accountable for keeping the digital backbone connected, stable, and operational end to end.

- SD-WAN & Networking
- Cloud Connectivity
- Branch & Remote Access
- Managed Infrastructure

02

PROTECT

Security is not a standalone product. It is an operational discipline. Katalyst aligns identity controls, endpoint protection, email security, compliance requirements, monitoring, and incident response into one managed security posture. Katalyst is accountable for continuously reducing risk, validating controls, and strengthening resilience across the environment.

- Identity & MFA
- EDR & Endpoint
- Email Security
- MDR
- Cybersecurity
- Compliance
- MSSP
- SIEM

03

OPERATE

24/7/365 operational management backed by strategic guidance and measurable accountability. Katalyst provides continuous monitoring, help desk support, Microsoft 365 management, backup validation, security oversight, and operational reviews focused on ongoing improvement. Katalyst is accountable for helping organizations operate more efficiently, recover faster, and continuously strengthen their digital backbone over time.

- Help Desk
- Backup & DR
- Microsoft 365
- Advisory & QBRs
- vCIO
- Managed Security
- Managed Infrastructure

The backbone is not about adding tools. It is about operating them intentionally.

A Practical Roadmap for 2026

1 Immediate
0-90 Days

- **Review Identity and Access Management (IAM)**

  Review how identities are managed across employees, clinicians, administrators, third-party vendors, and remote access. Verify MFA is consistently enforced, validate privileged access, and identify inactive or unnecessary accounts that increase organizational risk.

- **Confirm backup immutability and restore testing**

  Review your most recent backup restore test for EHR, clinical, and critical business systems. Verify backups are immutable, regularly tested, and capable of supporting timely recovery during a cyber incident.

- **Review vendor and third-party access privileges**

  Map which vendors have active access to your systems and patient data. Identify which relationships lack a formal security review or documented access policy.

2 Mid-Term
3-6 Months

- **Implement a Vulnerability Management Program**

  Establish a consistent process to identify, prioritize, and remediate vulnerabilities across clinical systems and medical devices. Continuous vulnerability management helps reduce risk before threats can be exploited.

- **Establish centralized monitoring across all locations**

  Create centralized visibility across hospitals, clinics, remote locations, medical devices, and critical infrastructure. Every alert should have a documented owner, escalation path, and response procedure.

- **Formalize incident response documentation**

  Document who does what, in what order, when an incident occurs across IT, clinical operations, compliance, legal, and executive leadership.

3 Long-Term
6-12 Months

- **Implement digital backbone governance model**

  Define clear ownership for Connect, Protect, and Operate across your organization. Document accountability, performance metrics, and how security posture is reported to leadership.

- **Align IT strategy with organizational growth**

  Every new location, clinical service, acquisition, or technology initiative should include cybersecurity planning from the beginning. Integrating security early reduces operational risk and supports long-term resilience.

- **Continuously Align Executive and Board Reporting**

  Leadership should receive regular reporting that demonstrates measurable improvements in cybersecurity posture, operational resilience, and risk reduction. Reporting should support informed business decisions, not simply satisfy compliance requirements.

Ready to strengthen your digital backbone? Schedule a conversation with Katalyst.

KATALYST

DIGITAL OPERATIONS PARTNER

Your Digital Backbone. Owned. Operated. Continuously Improved.

katalystng.com
704-790-4440
Charlotte, NC | Spartanburg, SC

Assess.
Benchmark your environment across Connect, Protect, and Operate.

Transform.
Build and execute a practical, prioritized roadmap.

Manage.
Ongoing ownership, visibility, and continuous improvement — 24/7/365.

> *"There was no sales team looking for opportunities to take advantage of our vulnerable situation -- just a partner willing to support us."*
>
> **Ted Bayack · Director of IT, Graystone Eye**

> *"They will sit down onsite with you to provide strategic planning sessions. They will learn the context of your business and what is important to you."*
>
> **Ted Bayack · Director of IT, Graystone Eye**

> *"Leveraging a partnership in this way allows for a more productive effort quicker, since the team is already built and just expands as needed."*
>
> **Ted Bayack · Director of IT, Graystone Eye**

SOURCES & REFERENCES

1 IBM Cost of a Data Breach Report -- Healthcare, 2025
2 Sophos State of Ransomware Report, 2025
3 Verizon Data Breach Investigations Report, 2025
4 HIPAA Breach Notification & Compliance Guidance
5 Cyber Insurance Underwriting Research -- Healthcare 2025
6 Healthcare Identity & Access Management Studies 2025
7 AI Phishing & Healthcare Fraud Threat Analysis 2025
8 Ransomware Recovery & Backup Studies 2025
9 HHS Office for Civil Rights Breach Portal -- 2025 Data

This report is produced by Katalyst for informational purposes. Statistics sourced from publicly available industry research. Verify against primary sources before formal reporting.

Digital Backbone Assessment
Benchmark your full environment across Connect, Protect, and Operate.

30-Day Satisfaction Guarantee
If we are not delivering, we make it right or we refund you.

Start the Conversation
katalystng.com · 704-790-4440
Charlotte, NC | Spartanburg, SC