omega systems
technology managed

# 2025 Healthcare IT Landscape Report

Threats, Blind Spots, and Opportunities for **Cybersecurity Transformation**

# Table of Contents



omega systems
technology managed

# Executive Summary

**Healthcare leaders are failing their patients – and not in the traditional sense.**

Organizations are increasingly facing sophisticated cyberattacks that endanger the very people they're tasked to care for. However, cybersecurity and IT priorities continue to take a backseat to other operational demands for healthcare teams. This creates a wave of vulnerability that is impossible to ignore.

To uncover these threats, blind spots and the opportunities for transformation, Omega Systems surveyed healthcare leaders on their cybersecurity posture, technology investments, HIPAA compliance challenges and more.

The findings reveal clear opportunities for healthcare organizations to **improve cybersecurity and compliance through deeper strategy, smarter investments, and trusted partnerships** with managed security service providers (MSSPs).

# Healthcare leaders underestimate cybersecurity's impact.

IT leaders across the healthcare industry grapple with a host of competing challenges, each vying for more attention and resources as years pass.

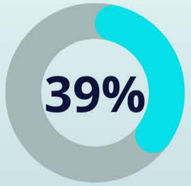
Unfortunately, a rise in concern for economic, regulatory and other factors has **pushed cybersecurity down to a disturbingly low priority level**.

**in fact:** Healthcare IT leaders report these challenges as the most significant hindering their business success in 2025:


**rising operational costs**
likely compounded by tariffs & inflation


**maintaining compliance**
with strict data privacy & protection regulations


**protecting patient data**
due to the rise of telehealth & remote patient monitoring




**implementing cutting-edge technology**
including artificial intelligence (AI) innovation


**ensuring patient safety and care**
at a time when competing priorities pull focus away from patients


**defending against advanced cyberattacks**
such as ransomware, phishing attacks, data breaches, etc.

**With cybersecurity ranking last, leaders may be underestimating how a successful cyberattack or data breach could impact nearly every other priority on the list.**

From safeguarding patient data and maintaining compliance to preserving care continuity and operational resilience, cybersecurity is a critical foundation to healthcare operations and progress.

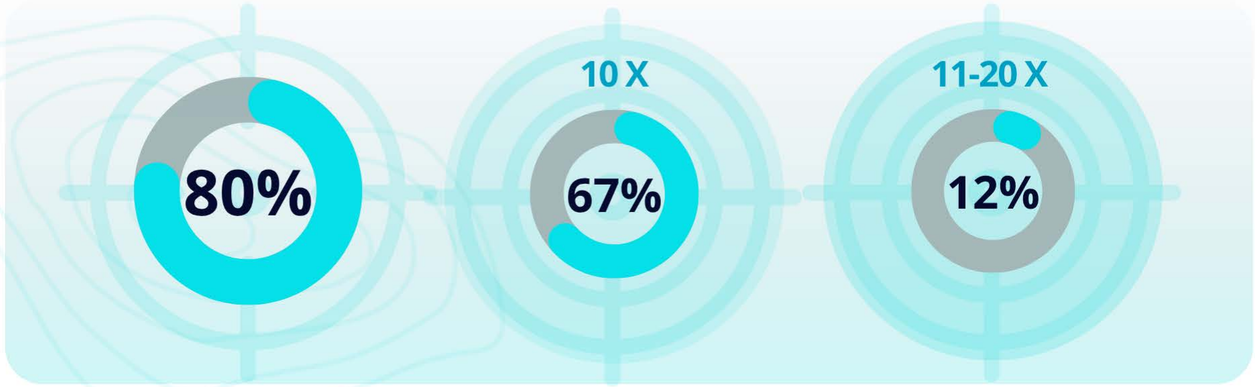
***concerning stat:***

*One in five (21%) managed care plans admitted they don't view cybersecurity as a critical business function.*

# Heightened risk is jeopardizing success - and patient safety.

It's alarming that healthcare IT leaders may not be focused enough on cybersecurity as a top business priority. This creates a dangerous precedent, placing organizations in the crossfire of attacks that are increasingly severe in both sophistication and frequency.

**Eighty percent (80%) of healthcare organizations were targeted by a cyberattack in the past 12 months,** while two-thirds faced threats as many as 10 times, and 12% were targeted as many as 20 times.




**consider this:**

Nearly all (92%) ambulatory care centers were **hit by a cyberattack in the last 12 months,** while residential and long-term care facilities reported the lowest attack figures – still at a staggering 71%.

**in fact:**

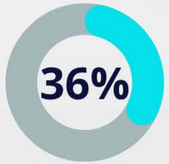
Twenty-seven percent (27%) of organizations report that **more than half of their sensitive patient data was at risk due to cyberattacks.**

Healthcare organizations fell victim to a wide range of advanced attacks in the past year, including:

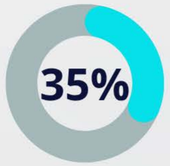
- **Phishing or smishing campaign (48%)**
- **Ransomware attack (34%)**
- **Business Email Compromise (BEC) attack (33%)**
- **Insider threat or data compromise (28%)**
- **Internet of Medical Things (IoMT) attack (19%)**
- **Supply chain attack (18%)**
- **Deepfake (10%)**

In the era of digital health, unpreparedness for cyber threats could have **drastic impacts on patient health**.

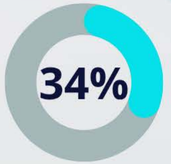
It's no surprise healthcare leaders report that numerous cybersecurity and IT weaknesses keep them up at night, including:



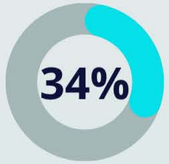

**Antiquated cybersecurity technology** that cannot adequately protect confidential patient data in the cloud




**Limited visibility into cyber risks** across an increasingly complex digital perimeter

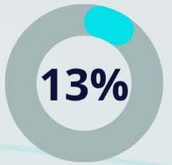



**Uncertainty around what data is at risk** within their digital networks




**Falling behind in leveraging AI** to combat evolving cyber threats


**Underestimating the severity and frequency of cyberattacks,** putting Protected Health Information (PHI) at risk




**Downplaying the risks and potential costs** of cyberattacks to avoid reputational harm

Nearly 20% of leaders believe their patients have not received proper care because their systems were impacted by a cyberattack.

**~20%**

**52%**

More concerning, 52% believe that a fatal patient incident caused by a cyberattack in a US healthcare facility is inevitable within the next five years.

# Top 4 cybersecurity gaps to beware of

Interestingly, many healthcare leaders believe their organizations are prepared to face today's security threats. Sixty-seven percent (67%) report they always or frequently prioritize cybersecurity investment in executive-level decision-making meetings.

Despite the prevalence of attacks experienced in the past year, 80% of leaders say they are confident or very confident their employees will effectively detect and prevent AI-powered attacks like phishing, deepfakes, or other advanced social engineering attacks. Seventy-six percent (76%) are confident in the security posture of their third-party vendors and suppliers.

**But reality shows a false sense of security.** Data indicates that specific cybersecurity gaps exist, putting healthcare organizations at greater risk.

1 Organizations do not maintain robust cybersecurity training programs.

2 Organizations have not implemented efficient incident response plans.

3 In-house cybersecurity / IT teams are not adequately staffed.

4 Organizations don't assess vulnerabilities across their attack surface enough.

## Healthcare organizations do not maintain robust cybersecurity training programs.

Data found that 30% of companies don't regularly train their teams on how to respond to cyberattacks or data breaches, and nearly half are still not utilizing simulated phishing exercises – one of the most impactful methods for testing employee security awareness.

Given that 81% of organizations were breached by an AI-driven social engineering attack last year, training needs to advance to meet the demands of the threat landscape.

Life sciences companies have the least faith in their employees' ability to identify advanced threats, with more than 13% indicating **low or no confidence** that users can detect and prevent social engineering attacks.

## Organizations have not implemented efficient incident response plans.

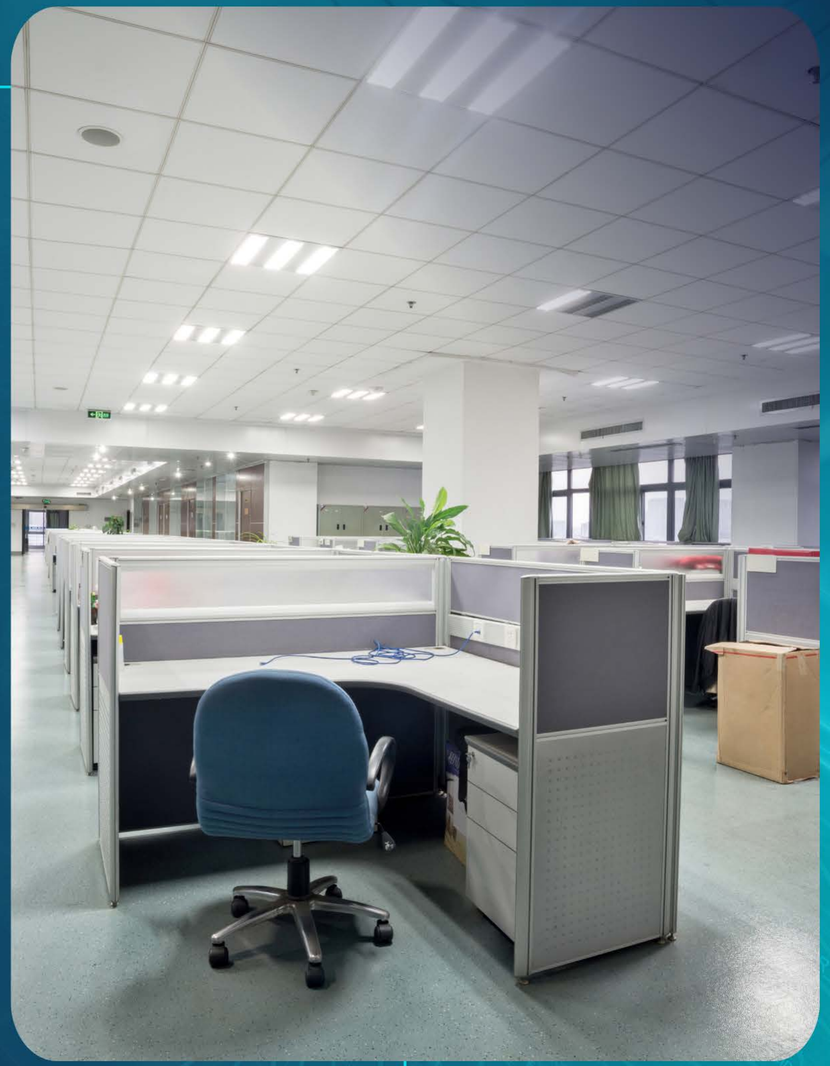
Nearly a quarter of organizations (23%) admitted it could take up to month to detect and contain a suspected data breach utilizing their current controls. For life sciences companies, response times are even longer, with 20% saying **it could take as long as months to quell the risk**.

Further complicating response efforts, 17% of healthcare companies surveyed don't have a current or effective incident response plan, and 16% say their team is not trained on incident response plans regularly.

## In-house cybersecurity / IT teams are not adequately staffed.

Nearly two-thirds (63%) of organizations have an in-house cyber or IT team, but staffing levels and expertise remain a concern for healthcare leaders. Our key findings include:

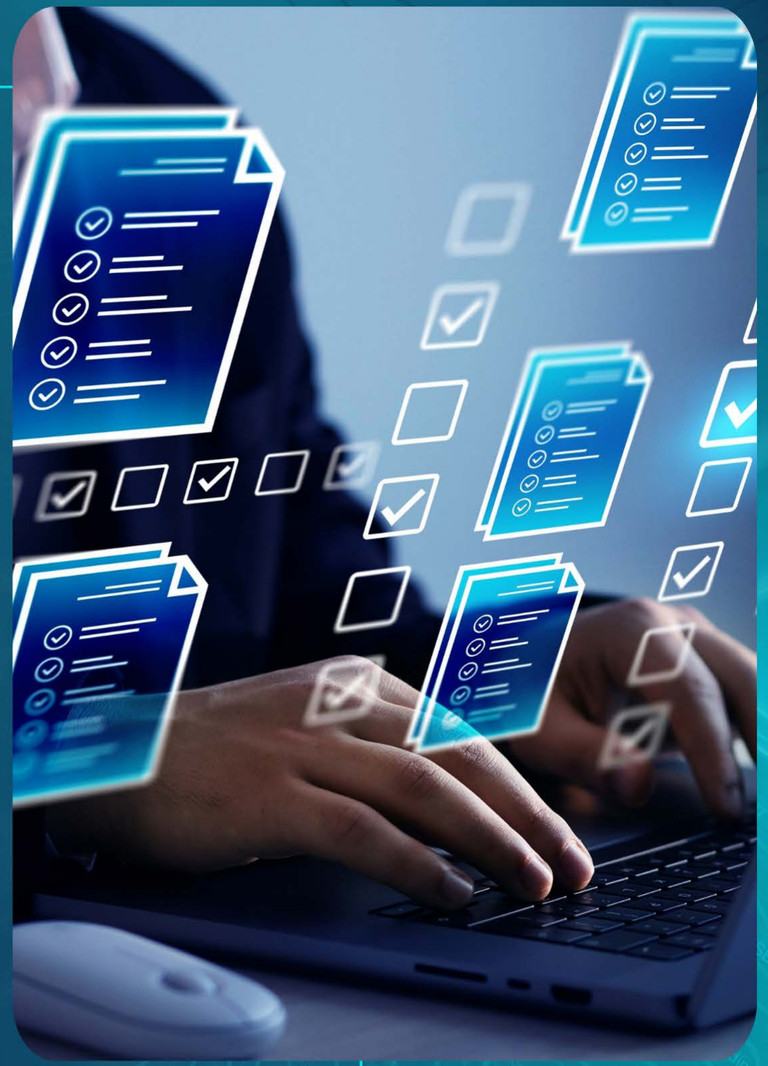
- 23% of organizations say their cyber/IT team is understaffed, including 38% of ambulatory care centers.
- 57% say they lack the time, resources or internal expertise to meet regulatory requirements and oversee the compliance process.
- 26% report their biggest challenge is employee retention and sourcing qualified talent.
- In the event of a cyberattack, 21% of healthcare leaders believe recovery would be delayed because they lack experienced in-house staff or do not have access to an outsourced 24/7 Security Operations Center (SOC).



## Healthcare companies don’t assess vulnerabilities across their attack surface frequently enough.

Forty percent (40%) of organizations indicated they do not currently conduct proactive IT risk assessments, and 8% of those have no plans to do so in the next 12 months!

Of those that are periodically assessing vulnerabilities, one in five (20%) do so less than quarterly. Given the rapidly changing threat landscape and complexity of growing attack surfaces, this poses a significant risk to operational integrity across the healthcare sector. Without continuous threat monitoring, cybercriminals can cause significant damage before they’re even detected.

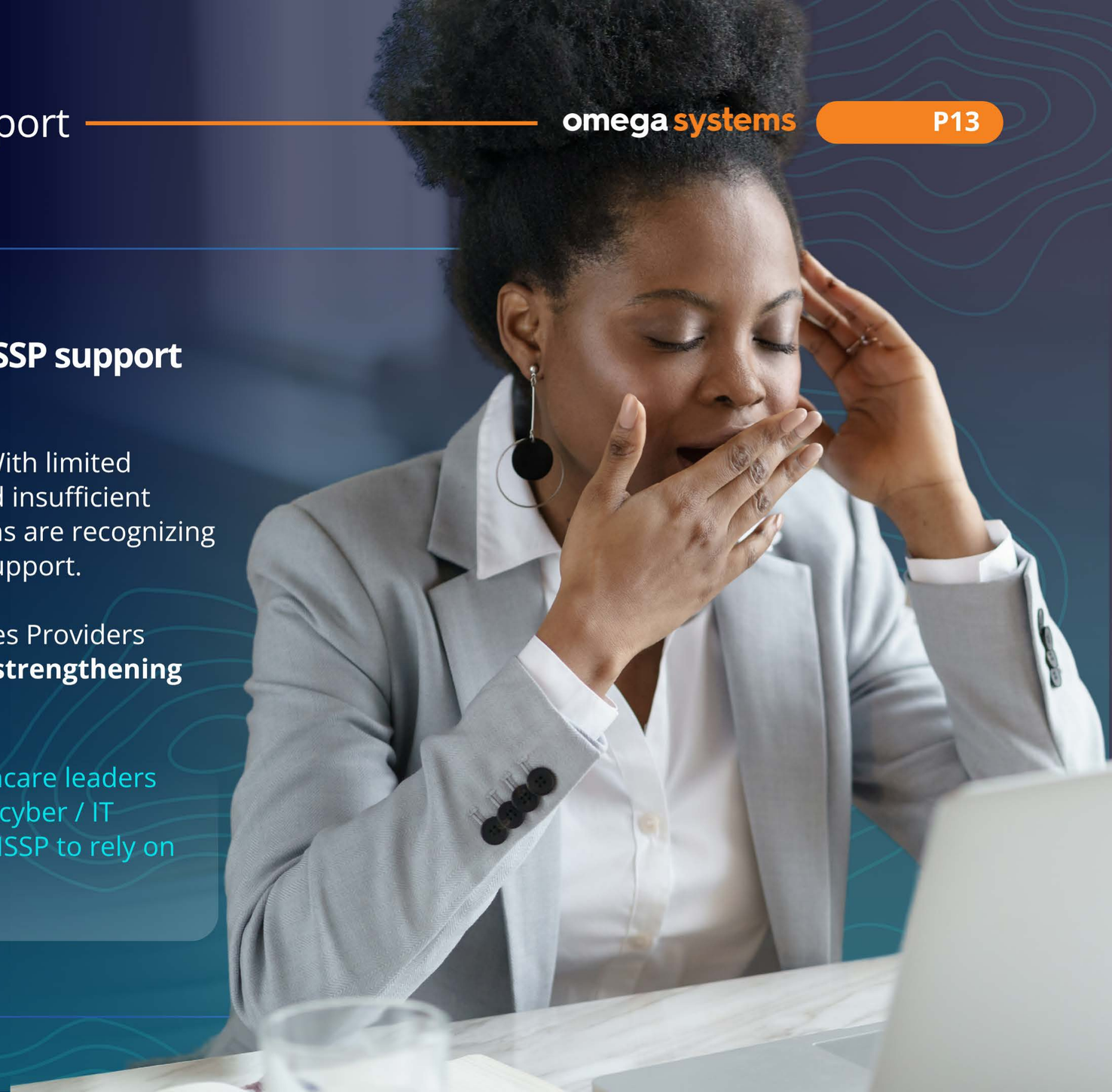


## The glaring need for professional MSSP support in the healthcare industry

These challenges won't be solved overnight. With limited internal resources, understaffed IT teams, and insufficient response plans, many healthcare organizations are recognizing the need to look beyond their four walls for support.

External experts like Managed Security Services Providers **(MSSPs) are becoming an essential part of strengthening cyber resilience**.

In fact, seventeen percent (17%) of healthcare leaders report losing sleep because their biggest cyber / IT weakness is not having an experienced MSSP to rely on for strategic risk management guidance.



# The cybersecurity and compliance conundrum

In a heavily regulated industry like healthcare, organizations need specialized expertise to manage both cybersecurity risk management and rapidly shifting HIPAA compliance requirements.

Eighty-one percent (81%) of healthcare organizations report they are prepared or very prepared to meet potential new HIPAA requirements in the next 12-24 months. **Yet, more than half (54%) are still relying on manual, in-house processes to benchmark their IT and security controls against HIPAA standards**, including the overwhelming majority of companies with less than 100 employees.

In addition to the complexity and inefficiency of manual processes, 60% report that the biggest roadblock to compliance today is staying up to date on evolving regulations.

Other roadblocks include:

- **A lack of time and resources to meet stringent regulatory measures (33%)**
- **Limited budgets with which to implement compliant data privacy practices (29%)**
- **Limited or no internal expertise to oversee the compliance management process (24%)**

## The steep climb to cybersecurity and compliance readiness

With nearly half (48%) of companies managing the compliance process themselves, it's evident there is room for improvement when it comes to meeting current and future regulatory obligations.

Healthcare leaders report managed HIPAA compliance platforms would better aid their organization, with the most impactful features of a compliance platform being:

- **Data discovery and classification (59%)**
- **Control benchmarking, progress reporting, and task management (50%)**
- **Organized document management (46%)**
- **Automated evidence collection (35%)**

Given recent proposed changes to HIPAA requirements,[1] today's IT leaders appear to have significant work ahead of them in shoring up security programs. Current implementation rates for these proposed HIPAA controls indicate a sizeable gap ahead of impending changes.

**45%**
identity & access management (IAM) controls

**59%**
data encryption at rest & in transit

**65%**
multi-factor authentication (MFA)

Residential and long-term care facilities appear to have the largest hurdle to climb, with only a 36% adoption rate for IAM controls; while ambulatory care centers have the lowest implementation rate (54%) for multi-factor authentical protocols.

1 *https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html*

# The MSSP advantage for healthcare organizations

Perhaps most impactful, the healthcare organizations that outsource IT or co-manage alongside managed security partners are better positioned to defend against modern cyber threats.

Companies using MSSPs consistently outpace overall statistics in the following areas:

- Frequency of vulnerability assessments
- Speed of threat detection
- Use of security awareness training for employees
- Adoption of HIPAA proposed security controls
- Utilization of managed regulatory compliance platforms

Within specific sectors, MSSP partnerships appear most prominent among medical practices (45%) and least prominent within the ambulatory care vertical (4%).

- **Speed of threat detection**
- **Frequency of vulnerability assessments**
- **Utilization of managed regulatory compliance platforms**
- **Adoption of HIPAA proposed security controls**
- **Use of security awareness training for employees**

For companies that opt not to leverage MSSP support, the path to security and compliance will only continue to increase in complexity. Gaps across the IT and security tech stack may further widen because organizations don't have the time, resources, and expertise to develop a robust cyber program. Today:

**55%**

**rely on on-premise infrastructures** and/or legacy cloud systems that lack the capabilities to contain and resolve data breaches.

**54%**

**don't have Endpoint Detection and Response (EDR)** with automated moving target defense (AMTD) technology.

**54%**

**don't utilize data discovery and classification** to identify, track and organize data across their IT network.

**46%**

**don't have managed cloud/network connectivity solutions** for collaboration, accessibility, and secure scalability.

**41%**

**are not currently encrypting data at rest and in transit** to meet potential new standards set forth by HIPAA's Security Rule.

**35%**

**don't require multi-factor authentication (MFA)** to safeguard sensitive data and PHI from unauthorized access.

## The glaring need for professional support (MSSPs) in the healthcare industry

MSSPs deliver the skilled resources and premier infrastructure needed to reduce the systemic, financial, and reputational risks associated with security breaches through proactive cyberattack remediation and a strategic information security plan. Furthermore, MSSPs can help alleviate the compliance burden by automating core security functions and standardizing HIPAA monitoring and reporting, allowing organizations to adapt more quickly to regulatory change.

# Call to Action: Modernize security to protect patients, data, and compliance

Omega Systems' 2025 Healthcare IT Landscape report offers several imperative takeaways for healthcare leaders looking to elevate their cybersecurity and compliance posture.


- Make cybersecurity the foundation for reliable patient rare.
- Don't let HIPAA compliance become an afterthought.
- Advance cybersecurity capabilities to keep pace with emerging threats.
- Gain a competitive advantage by working with an MSSP.

## Make cybersecurity the foundation for reliable patient care.

Patient health increasingly depends on the reliability of digital systems. From electronic records to connected medical devices, any disruption caused by a cyberattack can have real clinical consequences. Healthcare leaders should **treat cybersecurity as a core operational priority** to ensure systems remain secure, accessible, and fully functional at all times.

## Don’t let HIPAA compliance become an afterthought.

In a heavily regulated industry like healthcare, compliance never gets easier. Regulatory standards will continue to evolve, and organizations must be prepared to implement IT security controls that prioritize data privacy and operational resilience. Healthcare leaders should look to modernize technology stacks, allowing them to **stay agile in the face of changing requirements**.

## Advance cybersecurity capabilities to keep pace with emerging threats.

As cyber threats become more sophisticated, particularly with the rise of AI-driven attacks, IT leaders will need to **evolve their tactics to keep pace**. Next-gen practices like data discovery & classification, endpoint security (EDR) with automated moving target defense and advanced phishing detection capabilities will become must-haves in order to adequately safeguard sensitive data.

## Gain a competitive advantage by working with an MSSP.

Modern threats require modern solutions. MSSPs deliver robust solutions and proven expertise that allow C-Suite and IT leaders to focus on their core business functions rather than managing cybersecurity and compliance programs on their own. Healthcare organizations should consider outsourcing critical cybersecurity functions to trusted experts who can deliver faster detection, response, and remediation capabilities. This co-managed approach strengthens resilience and helps internal teams stay focused on delivering superior patient care.

**As evidenced by these findings, MSSPs are strategic enablers of business growth and success.**

**With trusted support, it's time for healthcare organizations to leverage cybersecurity as a competitive differentiator.**

## Final Takeaways

Cybersecurity is no longer a back-office concern – it's central to delivering safe, reliable patient care. As highlighted in this report, healthcare organizations must treat cybersecurity as a core operational priority. From safeguarding electronic health records to keeping connected medical devices running, digital infrastructure is now directly tied to clinical outcomes. Any disruption caused by a cyberattack can have real – even life-threatening – consequences.

Meanwhile, compliance demands are only growing more complex. HIPAA continues to raise the bar, and healthcare organizations must be agile in adapting to these new regulatory pressures. Outdated systems and reactive strategies won't be enough to meet rising standards, and IT leaders will need modern, compliance-ready technologies and processes to keep pace. Meanwhile, continued pressure and limited bandwidth will make it increasingly difficult for understaffed and overstretched IT teams to stay ahead of emerging threats and evolving compliance demands.

Leveraging a trusted Managed Security Services Provider (MSSP) thus becomes a strategic enabler. MSSPs offer scalable, enterprise-grade protection and managed compliance support – capabilities that most healthcare organizations admit they can't maintain on their own. By outsourcing key security and compliance functions, healthcare teams can stay focused on their core mission while strengthening their defense posture.

More than just a safeguard, cybersecurity (when done properly) is a strategic asset that fuels growth, protects patient trust, and sets forward-thinking organizations apart. **Now is the time to modernize, secure, and lead.**

omega systems
technology managed

## About Omega Systems

As a trusted MSP and MSSP to healthcare organizations across the U.S., Omega Systems is passionate about delivering the security and compliance expertise today's businesses need alongside the responsive and reliable managed IT support they deserve. Omega's service-driven IT solutions are designed to help customers leverage technology to fuel efficiencies, mitigate risk, and empower growth and success. We support that commitment by injecting trust, innovation and service excellence into every engagement – delivering a superior and satisfying customer experience unparalleled by other MSPs.

Learn more at **www.omegasystemscorp.com.**

### About this study

These findings are based on an Omega Systems April 2025 online, qualitative survey of 250 healthcare business leaders in the United States. Titles included CEOs, CISOs, CIOs, CTOs, COOs, CFOs, and other IT leaders. Survey respondents work at organizations with between 50 and 500 employees and in specific healthcare sectors including medical practices & clinics, ambulatory care centers, specialty care practices (treatment centers, mental/behavioral health, etc.), life sciences (e.g, biotech, pharmaceutical, or medical devices), residential and long-term care facilities, and managed care, insurance, or medical billing companies.