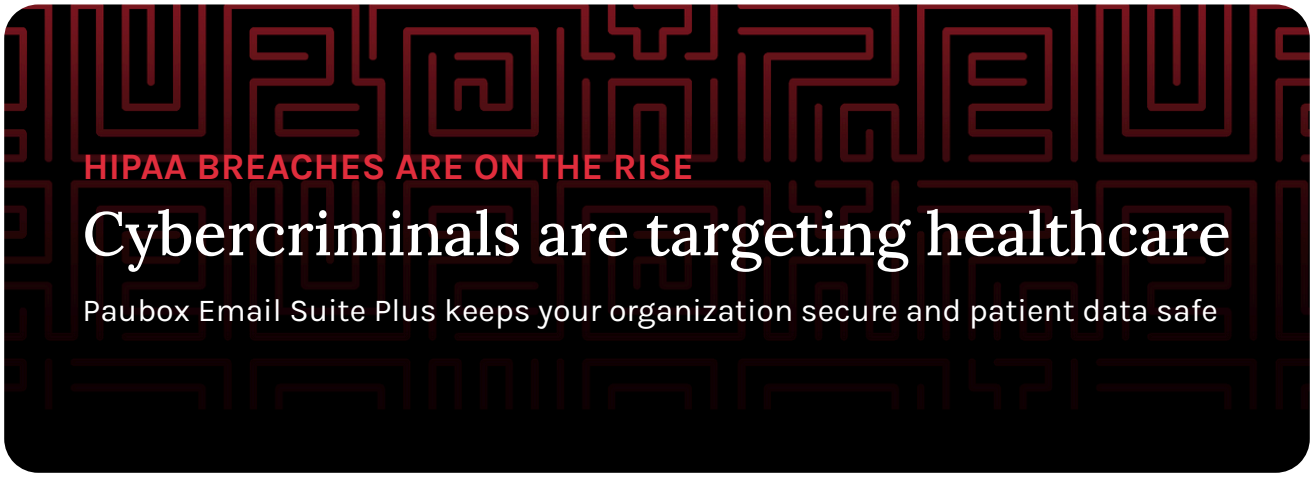
PAUBOX

2025 REPORT

Healthcare IT is dangerously overconfident about email security

Why Healthcare IT leaders are overestimating their email security and what the downstream consequences are.

Table of contents



Executive summary

Healthcare IT leaders are confident. Too confident.

Email remains healthcare's largest cybersecurity vulnerability, yet critical gaps persist, largely due to outdated systems and tools that generate significant user frustration.

The reality is clear: if an email security system creates friction or frustration, it will inevitably be bypassed by staff, undermining even the best-intentioned security efforts.

This report reveals the critical disconnect between perceived security readiness and actual vulnerability within healthcare email systems.

Leveraging first-party survey data, breach analysis, and audits, we show why baseline protections alone are insufficient. To truly safeguard patient data and ensure operational resilience, healthcare organizations must acknowledge these vulnerabilities and implement solutions designed for both effectiveness and seamless usability.

KEY INSIGHTS

92%
of healthcare IT leaders say they are confident in preventing email breaches

8 out of 10
admit they worry about their HIPAA compliance status

56%
of healthcare orgs spend less than 10% on cybersecurity efforts

86%
say their current email security tools cause workflow friction

“Hi, my name is Healthcare, and I have a security problem.”

92% of healthcare IT leaders say they’re confident in their ability to prevent email-based data breaches. That should be reassuring. It’s not.

When we dig beneath the surface to get past the checkboxes and into the configuration details, the story shifts.

- Encryption that depends on users checking a box, typing a word or jumping through other hoops
- Email authentication tools like DMARC or SPF half-configured
- No formal incident response workflows tied to email risks (A HIPAA violation, by the way!)
- No one is actually reviewing logs or email analytics

Many compliance failures are the result of false assumptions, not negligence. Teams think their vendor handles it. Or they’ve passed a one-time audit and treat that as an all-clear.

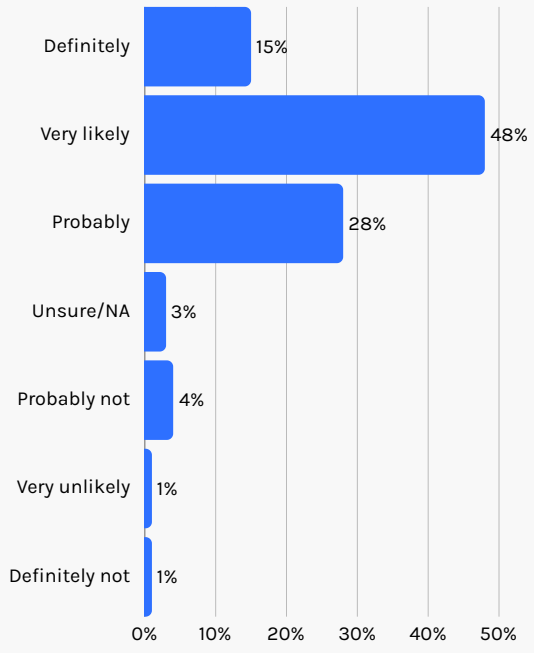
> “As a cybersecurity consulting practice engaging with hundreds of organizations annually, we consistently observe a critical gap in email security practices. Too often, organizations rely on infosec policies, user training, or manually enforced controls—rather than implementing automated, policy-driven email encryption solutions. This overreliance on human-dependent safeguards introduces unnecessary risk and undermines the integrity of outbound email protection strategies.”
>
> **Andrew Hicks,**
> Partner and National HITRUST Practice Lead, Frazier & Dieter Advisory, LLC

In fact, 8 out of 10 IT healthcare leaders admit they worry about their HIPAA compliance status.

Another layer to the confidence gap is the space between security goals and the reality of implementation. Many healthcare IT teams are working with resource limitations, competing priorities, and institutional resistance create a perfect storm of inaction. Despite growing awareness of email risk, these barriers prevent meaningful change.

Healthcare IT leaders identified a wide range of internal and external challenges that consistently stall their efforts to adopt HIPAA compliant email solutions.

PERCEIVED HIPAA COMPLIANCE



WHERE IT LEADERS FEEL CONFIDENT (VS. WHAT THE DATA SAYS)

Category	Confidence level	Actual risk
HIPAA compliance	92% say “we’re good”	Most configs fail audit
Threat detection	89% say AI matters	Only 44% use AI
Budget allocation	Majority say “email is covered”	56% spend <10% on cybersecurity
Tools	86% report friction	Process abandonment is common

54% cited implementation complexity as a top concern. Across a range of healthcare organization types and sizes, replacing legacy systems or layering new protocols on top of outdated infrastructure continues to be a challenge.

A lack of vendor support (53%) leaving teams to troubleshoot critical gaps alone. Staffing shortages (45%) and leadership resistance (44%) speak to broader institutional limitations, while integration issues (41%) reveal how deeply embedded old systems remain. Budget constraints (36%) and fear of disrupting user workflows (36%) show the balancing act IT teams are constantly performing, trying to protect data without slowing everything down.

Even end-user readiness is a factor, with 23% citing poor patient email literacy and 15% noting inconsistent security training. The data tells a clear story:
these barriers are persistent, layered, and deeply embedded in healthcare's operational DNA.

The problem isn't just technical, cultural and operational.

KEY TAKEAWAY

If your HIPAA compliance depends on end users remembering to encrypt, you're not compliant. You're pushing your luck.

Leadership resistance, internal silos, budget constraints, and implementation complexity stall progress. IT leaders are often set up to fail by a system that undervalues secure communication infrastructure, underfunds its modernization, and overestimates its resilience.

TOP BARRIERS TO ADOPTING HIPAA COMPLIANT EMAIL SOLUTIONS

Barrier	Percent
Complexity of implementation	54%
Lack of vendor support	53%
IT staffing shortages	45%
Resistance from leadership	44%
Integration challenges with legacy systems	41%
Budget limitations	36%
Fear of user disruption	36%
Poor patient email literacy	23%
Inconsistent security training	15%
Overreliance on outdated tech	3%
Other	1%

AI-powered threat detection is missing in action

Phishing attacks have evolved. They're faster, more personalized, and increasingly generated by AI. Attackers now use generative AI to craft messages that mimic the tone, structure, and urgency of real communication. They're going beyond the executive team to target billing teams, HR, and clinicians with surgical precision.

> "We've seen email threats evolve faster than many tools meant to stop them. It's not just about phishing anymore—it's about deception at scale."
>
> **Hoala Greevy,**
> CEO, Paubox

Rules-based filters still form an essential baseline—establishing a necessary first layer of defense. However, 44% of healthcare organizations stop here, relying solely on legacy solutions.

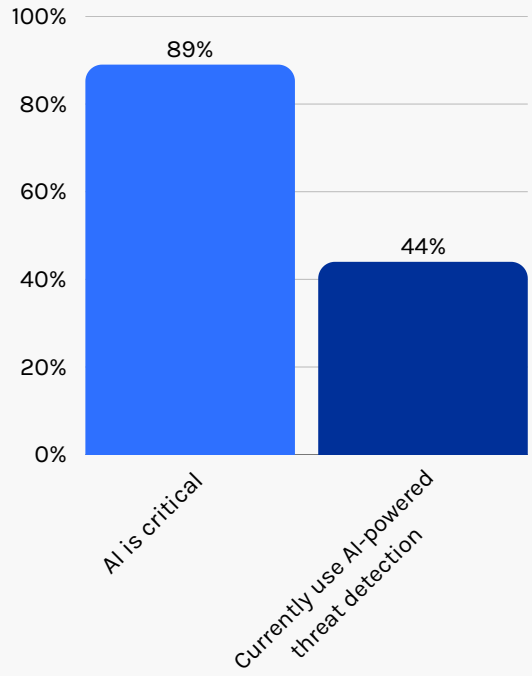
This leaves critical gaps in their defenses, as these systems alone can't match the sophistication and adaptability of AI-generated threats.

Attackers are scraping LinkedIn profiles and crafting spoofed messages that bypass outdated logic entirely. Proactive solutions, such as Paubox Email Suite Plus, build on this foundation with AI-powered threat detection, adding a crucial second layer that significantly enhances protection.

89% of healthcare IT leaders identified AI and machine learning as critical for detecting email threats. But knowing it's important and implementing it are two very different things.

> “Cybercriminals are exploiting the biggest vulnerability within any organisation: humans. As progress in artificial intelligence (AI) and analytics continues to advance, hackers will find more inventive and effective ways to capitalise on human weakness in areas of (mis)trust, the desire for expediency, and convenient rewards.”[1]
>
> **Amy Larson DeCarlo,**
> Principal Analyst, Global Data

AI THREAT DETECTION
PERCEPTION VS. ADOPTION



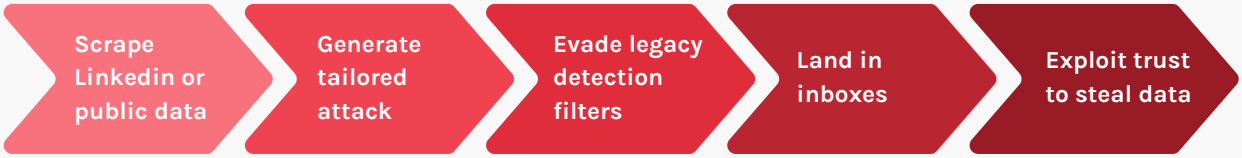
If your organization still relies on static filters, you’re a prime target. We’ve seen email attacks slip through tools that should have caught them.

One organization’s system flagged 200+ marketing emails as threats, but if not for the advanced detection solution in place, would have missed a spoofed email impersonating the CFO which could have been a $70,000 miss.

KEY TAKEAWAY

If your email security plan doesn’t already include AI, you’re giving attackers a head start.

ANATOMY OF AN AI-POWERED PHISHING ATTACK



Budgets lag risk

We're underinvesting in the fix.

Email is the single largest vector for cyberattacks in the healthcare sector. Despite that, most healthcare orgs allocate less than 6% of their IT budgets to cybersecurity.[2]

This wouldn't be so damning if healthcare were an outlier in the right direction—but it's not. Compare this to:

- Financial services, where cybersecurity budgets often exceed 10–12% of total IT spend[3]
- General industry, where cybersecurity takes up 21% of IT budgets on average[4]

Email security is buried inside broader IT budgets, making it easy to overlook and underfund the tools that matter most.

Meanwhile, HIPAA settlements for email-related breaches are climbing. The average cost of a breach is now $9.8 million in lawsuits, fines, and operational fallout. That dwarfs any line item on your IT budget.

CYBERSECURITY IN IT BUDGET ALLOCATION

Industry	Percent of budget
Healthcare	<6%
Financial services	10-12%
General industry	21%

> "I see the gap in time between new vulnerabilities emerging and budgets catching up to them. That delay? That's where the attackers live."
>
> **Tony Cox, CIO**
> Henderson Behavioral Health

If email is your frontline exposure, your investment should reflect that. Instead, it's often treated as a sunk cost or a compliance tax.

This isn't about spending more. It's about spending right.

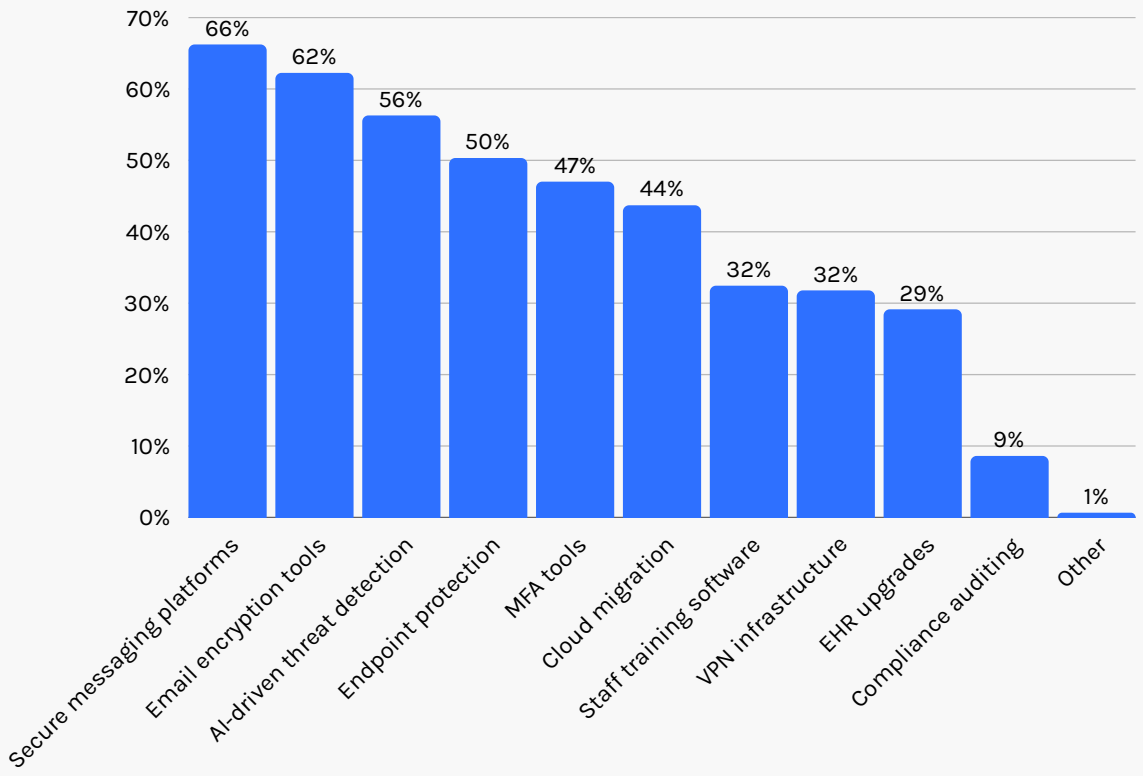
KEY TAKEAWAY

Treating email like a second-tier risk opens you up to top-tier costs.

> "Organizations that adopt risk-based budgeting frameworks demonstrate greater cybersecurity resilience, with structured investment strategies leading to a 40% reduction in security incidents."[5]

Shahan Ahmed
Montclair State University

IT INVESTMENTS IN THE LAST 12 MONTHS



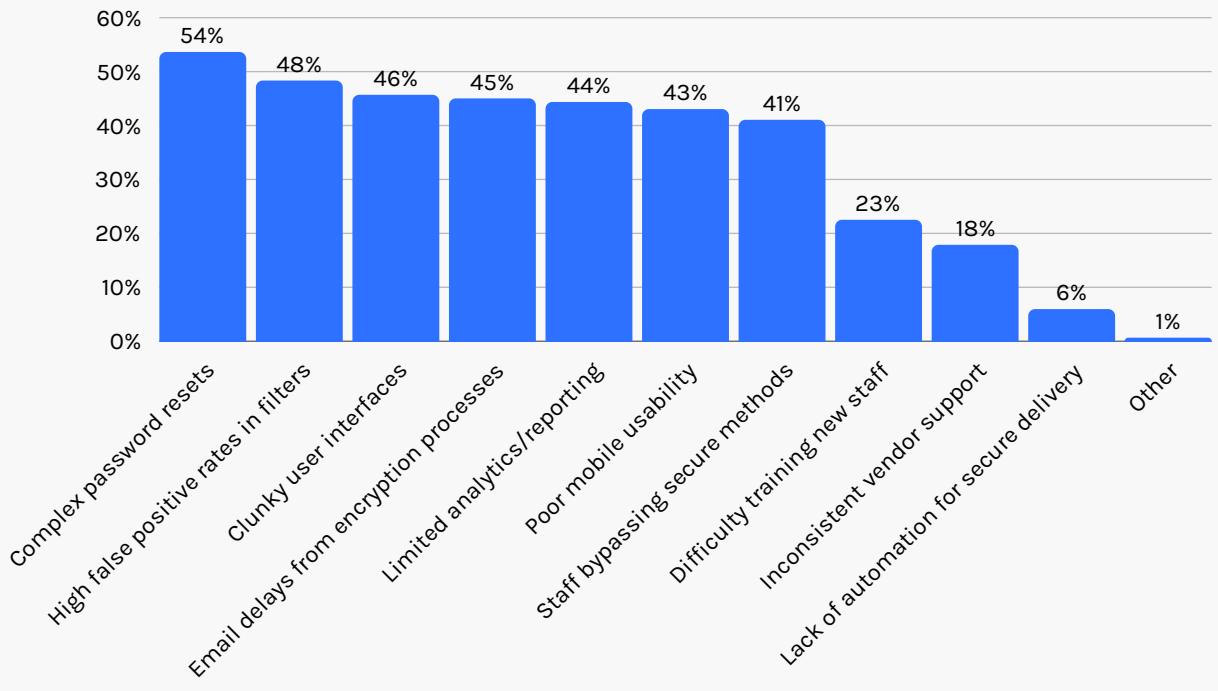
When security plans create friction

If an email security system creates frustration, it will be bypassed. We've seen it time and again—patients giving up on portals and administrators manually sending PHI because the official system is too slow.

86% of IT leaders say their current tools cause workflow friction.

These tools were supposed to help—but too often, they get in the way. The best ones? You don't even notice they're there. Tools that make secure communication seamless—not stressful—are the ones that actually work.

TOP FRUSTRATIONS WITH EMAIL SECURITY TOOLS



Complex logins. Forgotten passwords. Delayed access. These aren't minor usability bugs. They're reasons users go rogue.

We've heard it all:

- "Patients keep calling saying they can't open the message."
- "Our funders asked us to resend reports another way."
- "Our doctors are just texting files instead."

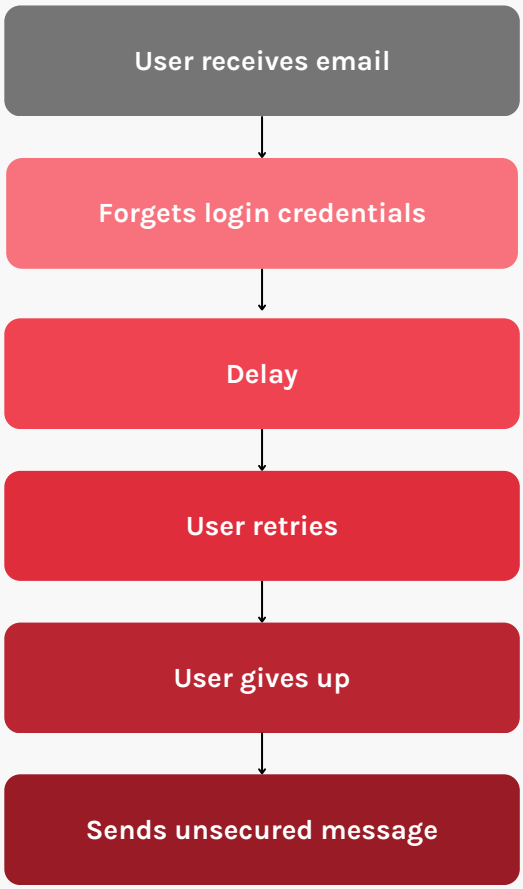
This is the inflection point: do we keep tolerating broken systems in the name of tradition? Or do we admit that usability is part of security—and build for both?

One tool designed with both usability and protection in mind is Paubox's ExecProtect+. By blocking display name spoofing and phishing attacks before they reach employee inboxes, ExecProtect+ removes the burden from end users entirely. It works in the background—no portals, no extra steps—giving healthcare organizations the security they need without adding friction to everyday workflows.

KEY TAKEAWAY

The most secure email system is the one your users actually use.

WHAT HAPPENS WHEN SYSTEMS GET IN THE WAY



> "Our company is as strong as the weakest employee link. HIPAA compliance depends on awareness and proper training—but also the right systems."
>
> **Ryan Winchester**
> Director of IT, CareM

Misconceptions are constantly undermining effective email security. Too often, healthcare IT leaders rely on outdated beliefs—assuming that compliance equals protection, that staff training alone can stop phishing, or that buying a HIPAA compliant tool checks all the boxes. But assumptions don't stop breaches. In reality, what sounds secure on paper often falls apart in practice—especially when systems create friction, rely on human behavior, or aren't fully configured. The myths are persistent, but the stakes are too high to let them go unchallenged. Below, we break down the most common false beliefs, and the facts that every security leader should know.

MYTH	FACT
"Portals equal compliance."	Most portals introduce friction—leading to non-compliance workarounds.
"Our staff are well-trained, so we're secure."	Human error is inevitable. You need tools that compensate, not just train.
"Email is just a communication tool."	Email is your most common PHI exposure point—and your biggest risk.
"More training will solve our readiness against phishing attacks."	Training helps, but 95% of phishing still goes unreported. You need better detection.
"Buying a HIPAA compliant platform checks the compliance checkbox."	Configuration gaps are common. Compliance isn't guaranteed without oversight.

WHY IT MATTERS

Patient data doesn't just live in EHRs. It flows through inboxes, attachments, referrals, and care coordination chains every single day. If your email system isn't locked down, your HIPAA posture is a house of cards.

Perception ≠ Protection

Healthcare IT teams aren't blind to risk. They're overwhelmed by it. But believing you're covered is no substitute for proving it.

Right now, too many healthcare IT leaders are placing their trust in outdated frameworks, unverified configurations, and assumptions that haven't been tested in real-world breach conditions.

it's time to re-evaluate. The platforms you trust. The tools you use. The training you assume is working. Confidence without clarity is dangerous. And in healthcare, it means lawsuits and lost trust.

5 MOVES TO MAKE NOW

- Audit your secure email configurations. Don't assume.
- Stop making users choose encryption—make it automatic.
- Upgrade detection systems to keep up with AI-powered threats.
- Fund email security in proportion to its risk.
- Choose tools that disappear into the workflow—not ones that disrupt it.

Methodology

This report is built on survey responses from 150 U.S.-based healthcare IT leaders gathered in Q1 2025, representing a range of healthcare organizations and settings. We also incorporated insights from real-world breaches, configuration audits, and user behavior data collected through internal security reviews.

These insights represent more than just trends—they offer a reality check on where the industry's email security posture truly stands, from frontline challenges to strategic oversights.

Sources

[1] “2024 Enterprise Predictions: Secure by Design”, globaldata.com

[2] “2023 HIMSS Healthcare Cybersecurity Survey”, himss.org

[3] “Cybersecurity Spending: Who’s Investing–And how much?”, patentpc.com

[4] “Cybersecurity Spend Is Now More Than 20% of the Average IT Budget”, knowbe4.com

[5] “Cybersecurity Challenges In IT Infrastructure And Data Management: A Comprehensive Review Of Threats, Mitigation Strategies, And Future Trend”, researchgate.net

PAUBOX EMAIL SUITE

Send email as normal, but HIPAA compliant

- Setup in 15 minutes
- HITRUST certified since 2019
- No portals, no passwords
- Top rated U.S. support

Start for free

PAUBOX