Security gaps observed across breached organizations

Authentication and sender validation

DMARC enforcement remains inconsistent across healthcare. In 2025, nearly three quarters of breached organizations either lacked DMARC entirely (41%) or operated in monitoring-only mode (33%).

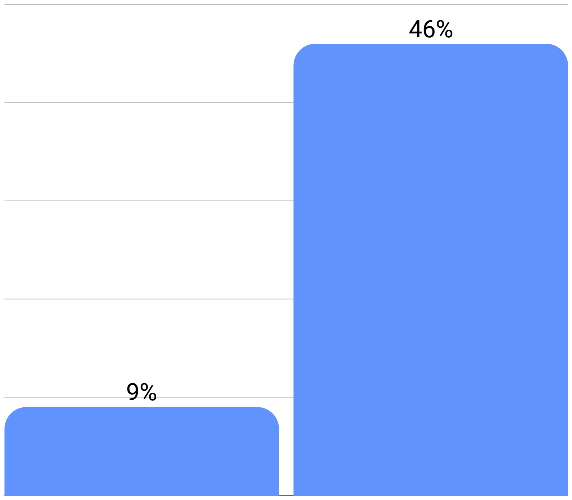
Without enforcement, an attacker can send emails that appear to come from a trusted domain, and the receiving system has no instruction to block them.

> **74% of breached orgs** had missing or unenforced DMARC (41% missing entirely, 33% monitor-only)

SPF adoption was more common, but often permissive. Over half of breached organizations used soft-fail policies (46%) or had no SPF record at all (9%).

A soft-fail policy means that even when a message is sent from an unauthorized server, it may still be delivered to the recipient's inbox rather than being rejected. Tightening SPF to a hard-fail policy ensures unauthorized messages are blocked outright.

These misconfigurations are the specific conditions that allow phishing emails to land, spoofed messages to appear legitimate, and credential harvesting campaigns to succeed.



56% of breached orgs had permissive or missing SPF records (9% missing, 46% soft-fail)

Transport security

None of the breached organizations analyzed enforced MTA-STS. As a result, email delivery relied on opportunistic TLS, a setting that attempts encryption when the receiving server supports it but falls back to sending messages unencrypted when it cannot encrypt.

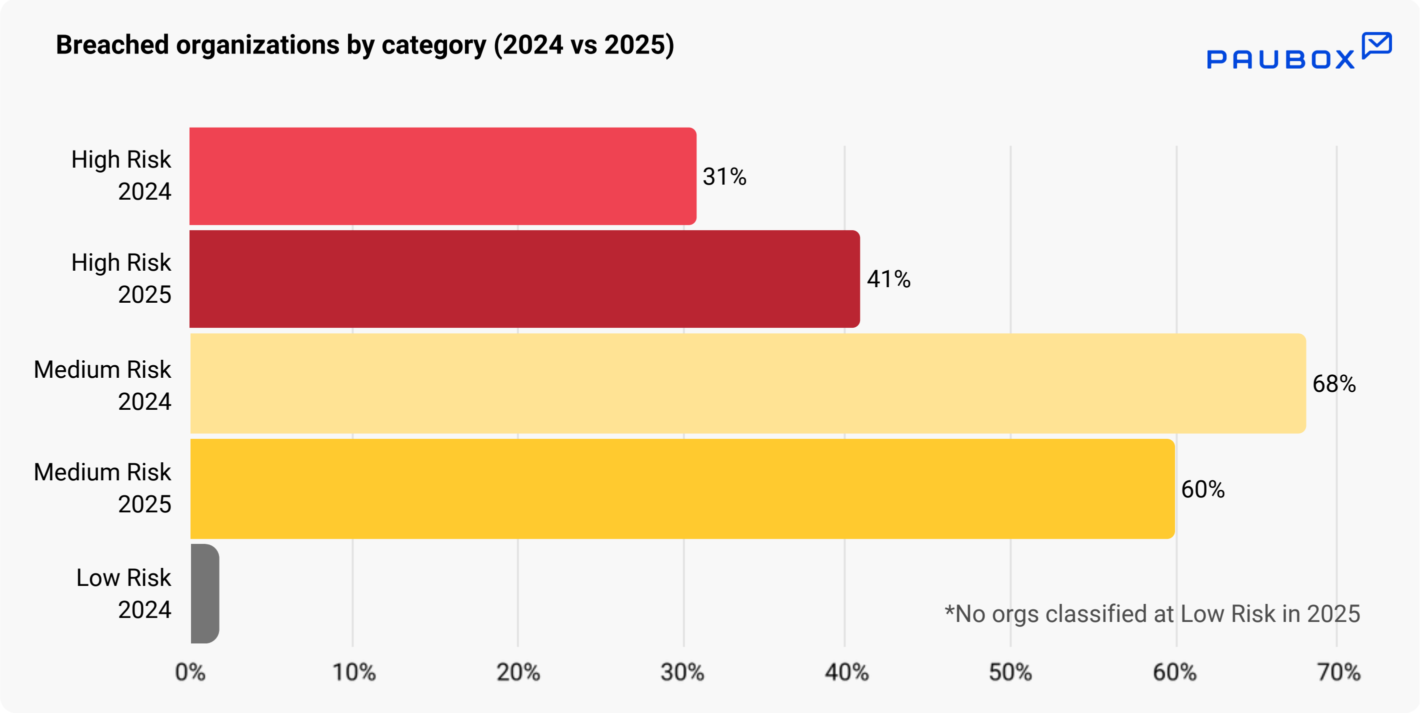
This means encryption is attempted but never guaranteed. In a downgrade attack, a bad actor intercepts the connection between two mail servers and forces that fallback, allowing them to read or alter the contents in transit. MTA-STS prevents this by requiring that connections between servers are encrypted, and refusing delivery if they are not.

This is a critical but often overlooked gap. Encryption in transit is only as strong as the policies that enforce it.

Reliance on user-driven controls

Many healthcare organizations continue to rely on portals, manual encryption triggers, or staff judgment to protect sensitive email content.

These approaches introduce friction. Over time, friction leads to workarounds. When speed and convenience conflict with security, staff behavior predictably favors speed.



Breached organizations by category (2024 vs 2025)

*No orgs classified at Low Risk in 2025

PAUBOX

Stop email phishing attacks with AI security

Surface hidden threats with generative AI email security that learns and evolves.

Talk to an expert