PAUBOX RESEARCH

PAUBOX

Email breach workload for healthcare IT directors

48% of healthcare IT and security leaders at recently breached organizations say email security work delayed other security projects, against 19% with no breach.

What we found

Recently breached organizations were more than twice as likely to report delayed security projects: 48% against 19%.

October breach notices from Brightmoor Hospice and VNA Health Group show the work: outside specialists, mailbox reviews, then record searches for addresses, all sitting beside IT's existing projects.

What it means for IT directors

Burnout belongs in the budget case

53% of recently breached organizations tie email security work to staff burnout or turnover, against 25% with no breach.

Overtime belongs on the cost side

45% of recently breached organizations report increased IT overtime or after-hours work, against 29% with no breach.

Automation is the top resource ask

44% of recently breached organizations pick better automation to reduce manual work, also the top no-breach answer.

WHY PAUBOX

9,000+

healthcare organizations trust Paubox to secure every email they send and receive.

Inbound Email Security catches phishing

Generative AI detects phishing, spoofing, and BEC in inbound email.

Encryption with no manual step

Every outbound email is encrypted by default, with no portals, passwords, or plugins.

HITRUST certified

Independently certified against the HITRUST framework.

Paubox survey of 170 healthcare IT and security leaders, March 2026 | Brightmoor Hospice, Notification of Data Security Incident, PR Newswire (October 16, 2026) | VNA Health Group, Notice of Data Privacy Event (October 19, 2026).