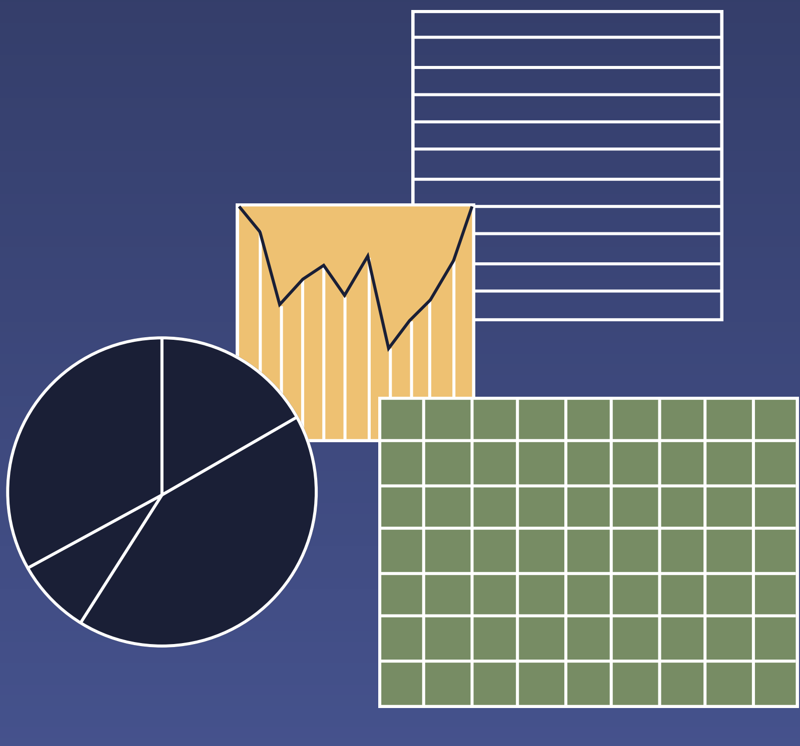
The State of Business Email 2025: Infrastructure, Risk, and IT's Next Opportunity



Exclaimer

2025

Table of contents

Executive summary

In 2025, email continues to anchor business communication across industries and regions. While instant messaging and collaboration platforms are on the rise, email remains unmatched in its role as the system of record. When the message matters—when accountability, auditability, and professionalism are required—businesses send it by email.

This year's State of Email report, based on insights from 4,009 IT leaders across the UK, US, Germany, and Australia —reveals a paradox: email is relied on more than ever, yet often managed with outdated processes and insufficient investment. IT leaders are expected to secure the most targeted part of the stack, modernize legacy workflows, maintain compliance, and support brand consistency—often without the tools, automation, or authority to do it effectively.

Email isn't just "still here"—it's still critical. And it's under pressure.

Key insights

1. Email still dominates communication

- **89%** of IT leaders rank one-to-one email as important—slightly ahead of collaboration tools **(86%)** and on par with instant messaging (IM) and video conferencing platforms.
- Email remains the go-to for **client communication, internal updates,** and **IT and security alerts** where reliability and auditability matter most.

Executive summary

2. Security and compliance gaps are widening

- **83%** of organizations reported email-related security incidents, with **48%** experiencing them in the past year.
- Only **47%** feel very confident in their compliance posture.
- Phishing and spoofing top the list of IT concerns, yet **fewer than one-third** have implemented DMARC, DKIM, or SPF—leaving a critical protection gap.

3. Time is being spent in the wrong places

- **37%** of IT leaders say reducing spam and unwanted emails takes up a disproportionate amount of their time.
- **35%** of IT teams say email signature management is one of their top two most time-consuming tasks—highlighting just how manual and inefficient governance remains across many organizations.
- Only **41% have integrated email with their security and compliance stack**—despite the operational load it represents.

4. Professionalism and compliance are on the line

- **92%** of leaders agree that consistent, well-managed email signatures build trust and professionalism.
- Despite this, **80%** still rely on manual methods or user self-service—undermining consistency, compliance, and control.

Executive summary

5. AI and automation are no longer optional

- **43%** of IT leaders believe AI-driven email automation will shape business communication in the next five years.
- Their top priorities: **stronger security (41%), more automation (38%), easier management (37%),** and **better integrations (36%)**—signaling a shift toward smarter, scalable email ecosystems.

This report outlines where email stands, where it's headed, and what IT needs to do next. Because when it comes to professional, high-trust communication, email still carries the message.

"

"Email touches every team, every customer, and every major milestone of your business. This report shows why it's time to stop thinking of it as background infrastructure, and start treating it like the operational system it really is."

— Vicky Wills, Chief Technology Officer, Exclaimer

Methodology

This report is based on original research commissioned by Exclaimer in partnership with Censuswide, with the aim of understanding how IT leaders are managing the evolution of business email—from infrastructure and governance to security, integration, and automation.

The study used a **quantitative, cross-sectional survey design,** supported by qualitative commentary from internal subject-matter experts. Fieldwork was conducted online **between April 4 and April 16, 2025.**

We surveyed **4,009 IT professionals** across four core geographies:

United Kingdom (1,003)
United States (1,000)
Germany (1,006)
Australia (1,000)

Respondents were selected using a **non-probability sampling approach**, targeting individuals with active involvement in managing email systems, communication policies, or security/compliance infrastructure. Quotas were applied to ensure a balanced mix of respondents by:

Company size: Micro (1–100 employees), small (101–250), mid-sized (251–500), upper mid-market (501–1,000), large (1,001–5,000), and enterprise (5001 or more)
Industries: Technology, financial services, healthcare, manufacturing, construction, education, hospitality, legal, media, retail/e-commerce, public sector, professional services, nonprofit, and more
Roles: IT Managers, Directors, CIOs, CTOs, Administrators, and Security/Compliance Officers
Email platform: Microsoft 365 (Office 365), Microsoft Exchange, and Google Workspace (Gmail for Business)

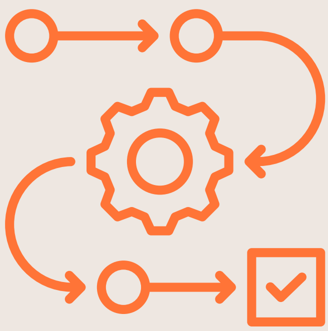
Methodology

The survey consisted of structured, multiple-choice questions focused on five areas:

1. **Communication tools and usage patterns**
2. **Email security, risk exposure, and compliance**
3. **Signature management and operational governance**
4. **Tech stack integration and workflow automation**
5. **Future trends: AI, personalization, and strategic email use**

Results were analyzed using standard descriptive techniques. While quantitative data formed the foundation of our insights, it was contextualized with qualitative commentary from Exclaimer's in-house experts.

This research complies with ESOMAR standards, and all respondents gave informed consent. While the survey provides a robust snapshot of IT sentiment in 2025, it reflects the views of respondents at a point in time and should be interpreted in that context.



Chapter 1

Email's role in the modern communication stack

Chapter 1

In 2025, IT leaders are managing a broader mix of communication tools than ever before—from instant messaging and video calls to collaboration platforms. But even as adoption grows, these tools aren't replacing email. They're building around it. When communication needs to be formal, consistent, and shareable across teams, email remains the default.

This chapter explores how email continues to anchor business communication, even as new tools gain ground. It looks at how IT leaders are balancing a shifting stack—supporting fast-moving platforms while relying on email to keep operations aligned and communication clear.

Even with growing adoption of messaging and collaboration tools, email remains the most important channel for business-critical communication.

89% of IT leaders say direct one-to-one email is important to their organization

In Germany and Australia, that figure rises to **94%,** followed by **86%** in the US, and **81%** in the UK. Importance also exceeds **90%** across key industries such as professional services, technology, and finance. Nearly half of all respondents **(48%)** consider it "very important."

Despite the rise of messaging apps, email remains the trusted default for professional communication. In fact, **48%** of respondents say **more than half of their internal and external communications rely on direct email**—underscoring its central role in day-to-day business interactions.

This isn't just about preference—it's about purpose. Email is the go-to for high-visibility, high-stakes communication where compliance, consistency, and accountability are non-negotiable:

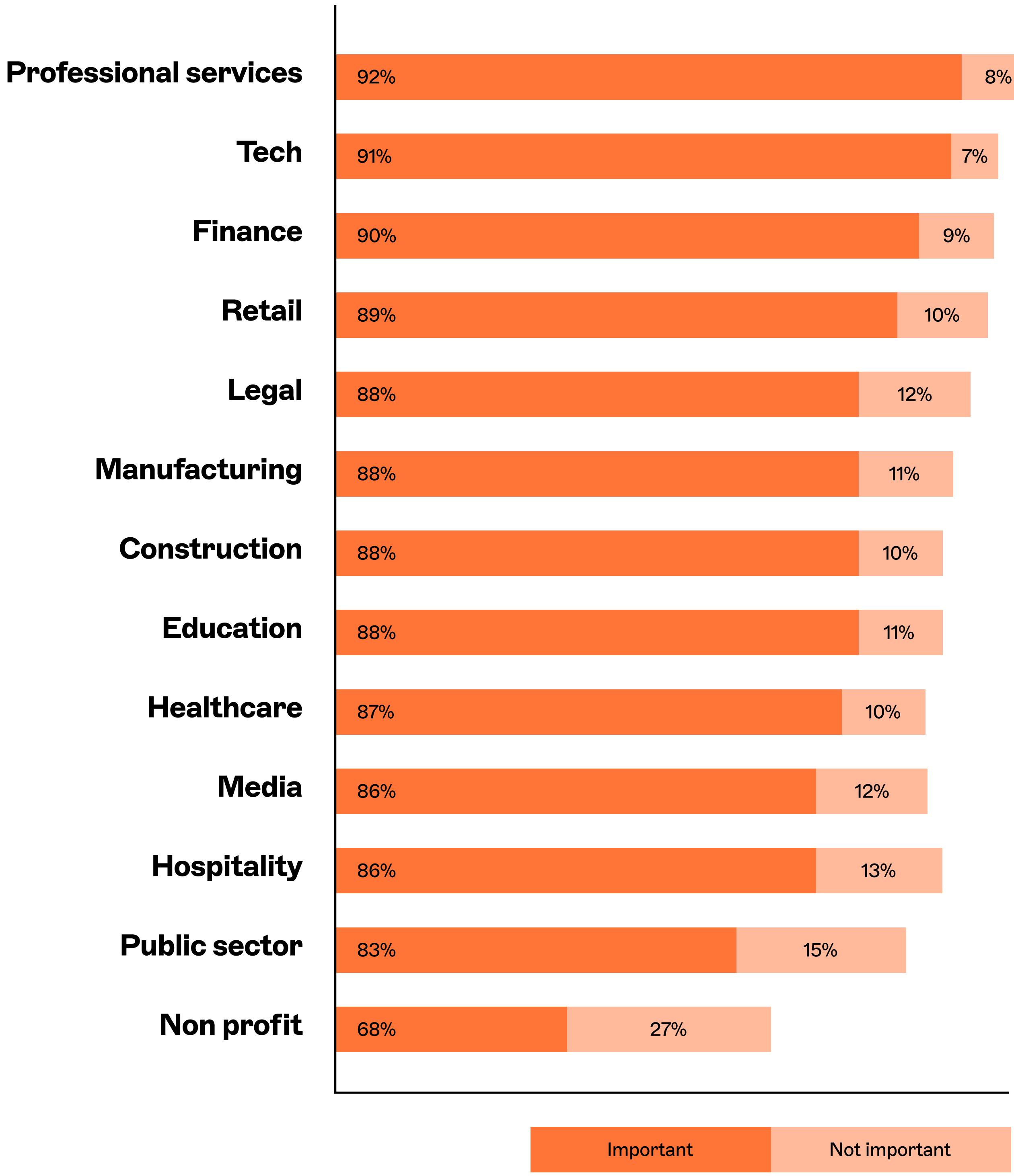
49% use email for IT and security alerts

36% use email for internal collaboration

34% rely on email for client or customer communication

These are messages that need a clear trail, guaranteed delivery, and consistent formatting. That's where email excels—and where chat apps fall short.

The importance of email, by industry



Key insight:

If it's important or professional, it's sent by email.

Email's importance also scales with complexity. Even in large organizations, where asynchronous collaboration tools thrive, email volume remains high. **49%** of IT leaders in enterprises with 5,001+ employees say typical users send **over 16 emails a day**—a signal that email is still powering cross-functional, high-volume workflows.

At the departmental level, its relevance is just as clear. The teams most reliant on email are those responsible for infrastructure, people, and service delivery:

Teams most reliant on email

56% **IT teams**

37% **HR and Internal Comms**

31% **Customer Success** and **Finance**

As digital tools proliferate, email retains a unique position: it works across roles, scales with complexity, and provides the clarity and auditability other platforms lack.

Tool usage: Comparing email to collaboration platforms and IM

Based on responses to: **"What percentage of your organization's internal and external communications relies on..."**

Usage Tier	Direct Email	Collab & IM Tools
High Use (51–100%)	48%	43%
Moderate (31–50%)	40%	39%
Low (≤30%)	11%	17%

Insight:

Organizations are more likely to rely heavily on direct email than on modern collaboration or messaging platforms:
Nearly **half (48%)** of respondents use email for **more than half** of all communications, compared to **43%** for tools like Slack, Teams, and Asana.

When the communication is sensitive, strategic, or high-risk—email is still the channel organizations trust.

What this means for IT

Messaging tools may be evolving, but they're not replacing email—they're reframing its role. For IT leaders, email isn't a legacy system to tolerate—it's a core asset to modernize. When communication really matters, email still carries the message.

Trend 2: Instant messaging is growing, but doesn't replace email

Instant messaging tools have become essential for fast-moving teams. For quick check-ins, triage threads, and on-the-fly updates, platforms like Slack, Microsoft Teams, and Google Chat help people move fast. But even as usage grows, IM isn't replacing email—it's complementing it.

> **Email vs. IM: What each tool does best**
> **Email:** Auditability, security alerts, client communication, internal policy comms
> **IM:** Speed, quick coordination, informal updates, project-specific collaboration

IT leaders see value in both. In fact, 89% say one-to-one email is important to their organization—and the same number say that about instant messaging. But when you look at how each is actually used, the picture gets clearer:

48% of organizations rely on **email** for **more than half** of their internal and external communications

43% say the same about **instant messaging** and **collaboration platforms**

17% use IM sparingly (**≤30% of communications**), compared to just 11% for email

Trend 2: Instant messaging is growing, but doesn't replace email

So while both channels are seen as critical, email continues to do more of the heavy lifting—playing a more consistent, foundational role across teams.

It shines when speed matters more than structure—think project huddles, support triage, or cross-functional standups. But when the message needs to be logged, shared up the chain, or meet compliance requirements, the inbox is still where it ends up.

Even in large enterprises, where IM has gained the most traction, email hasn't lost its grip. Among organizations with 5,000+ employees:

85% of IT leaders say IM is more important than email

78% still say email is critical

And team members send an average of 15 emails per day

IM isn't replacing email—it's evolving alongside it. Platforms like Slack, Teams, and Google Chat are moving from side channels to operational hubs. But email remains the system of record.

Confidence in IM is broad and growing, no matter the platform:

90% of Microsoft 365 users say IM is important.

89% of Google Workspace users agree.

86% of Microsoft Exchange users do too

This signals a platform-agnostic trust in IM as a core communication tool. But the takeaway isn't about picking a favorite. Email handles the high-stakes. IM handles the high-speed. For IT leaders, the real work is enabling both—securely, seamlessly, and at scale.

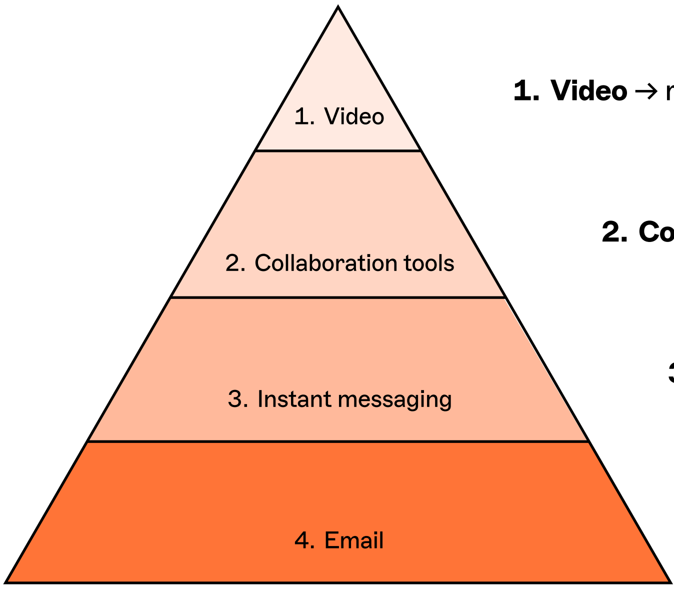
Speed may live in the chat window. But accountability still lives in the inbox.

Why IT should care

Email and IM now serve distinct, complementary functions. For IT, the job isn't to pick one over the other—it's to ensure both work together, securely and seamlessly. Because as teams shift between urgency and traceability, communication still needs to be consistent, auditable, and protected.

Trend 3: Other tools are gaining ground, but email anchors the stack

Beyond email and IM, organizations have embraced a broader toolkit: video conferencing, collaboration platforms, and external messaging tools. These channels are now essential for modern, distributed work. But they're not the foundation. They support workflows—they don't define them.



1. **Video** → real-time human connection
2. **Collaboration tools** → for sorting tasks/projects
3. **Instant messaging** → quick, casual
4. **Email** → formal, detailed, documented

Modern organizations have embraced a growing stack of communication tools. Globally, **89% of IT leaders** say video conferencing is important to their digital operations—with that number rising to **94% in the tech sector**, where remote and hybrid teams are the norm. Collaboration tools like Asana, Monday.com, and Notion also rank high, with **86%** of leaders calling them essential—especially in regions like Germany and Australia, and among upper mid-market companies.

But importance doesn't always equal consistency. These tools aren't embedded across every team or use case:

- **15%** of micro companies (1–100 employees) say video conferencing isn't important
- In the UK, only **79%** call collaboration tools important—and that drops to **60%** among nonprofits
- Even in large enterprises (5,001+ employees), **14%** say video is unimportant
- Nearly a third of nonprofit respondents **(31%)** call collaboration platforms unimportant

These gaps say a lot. Tools like video conferencing and project management platforms serve real, practical needs—but they're often situational. They work best when tied to specific workflows, team rituals, or remote environments. They're not universal—and they're not the default. Email is.

No matter the region, company size, or industry, email remains the one constant—used across teams, time zones, and tools. It delivers what others don't: visibility, traceability, and consistency. And it doesn't need a calendar slot, a shared board, or a permissions check to do its job.

Implications for IT

Video and collaboration tools are highly valuable, but their value depends on context. Email, on the other hand, is infrastructure. That means IT leaders need to focus on integrating these newer tools around email—not in place of it. Because when a task slips through chat, or a video call goes undocumented, it's the inbox that brings it all back together.

The stack may grow. But email still holds it together.

Key takeaways

Email still anchors business communication, but IT must support a multi-channel stack that's growing in complexity and policy risk. Here are our key takeaways on what's driving business communication in 2025:

Email remains the backbone of business communication.
Despite a growing ecosystem of tools, email is still the most widely used and most relied-on channel for high-visibility, auditable communication.

Instant messaging is essential—but not dominant.
IM tools like Slack and Teams are important for fast, real-time collaboration, but they serve different needs and haven't replaced email in most workflows.

Video and collaboration tools fill functional gaps.
Platforms like Zoom, Asana, and Trello support distributed work and team-based coordination, but usage and importance vary widely across industries and company sizes.

Tool adoption is contextual.
The importance of each communication channel depends on organizational structure, team function, and regional maturity—making integration, not standardization, the IT priority.

IT must orchestrate a multi-tool environment.
It's not about choosing one platform—it's about making the stack work together securely, efficiently, and at scale.

Securing the inbox: Email's evolving risk profile

Chapter 2

Email is still one of the most targeted entry points in the enterprise—and one of the most underestimated. While most IT teams have invested in protection, the inbox continues to account for a significant share of security incidents, and foundational safeguards like DMARC, DKIM, and SPF remain widely underused. The result: a threat surface that remains highly active and inconsistently defended.

The consequences of that exposure are growing. With the average cost of a data breach reaching $4.88 million in 2024[1]—the highest on record—email risk is no longer theoretical. And because threats vary by region, sector, and size, securing the inbox now demands more than policy. IT leaders need layered, context-aware defenses and systems that don't just protect—but prove they're doing so.

1 Source: Cost of a Data Breach Report 2023, IBM Security.
Available at: https://www.ibm.com/reports/data-breach

"Security and compliance pressures don't stop at the inbox. Yet email remains one of the most targeted, exposed, and under-managed parts of the stack. The insight here should inform how IT leaders prioritize the next wave of controls."

— Karl Bagci, Head of Information Security, Exclaimer

Despite years of investment in email security, the inbox remains a primary attack vector—and one many IT leaders still underestimate.

> **83% of organizations have experienced a security incident due to an email-related threat—nearly half happened in the past 12 months.**

These incidents aren't concentrated in specific regions or industries—they're happening everywhere. Email threats are not a diminishing problem. They're accelerating.

More critically, email isn't just part of the broader threat landscape—it's one of its most active and volatile surfaces. Over **53% of organizations say email is responsible for over a quarter—and in many cases, up to all—of their security incidents.** That's front-line exposure.

The top email security challenges cited by IT leaders include:

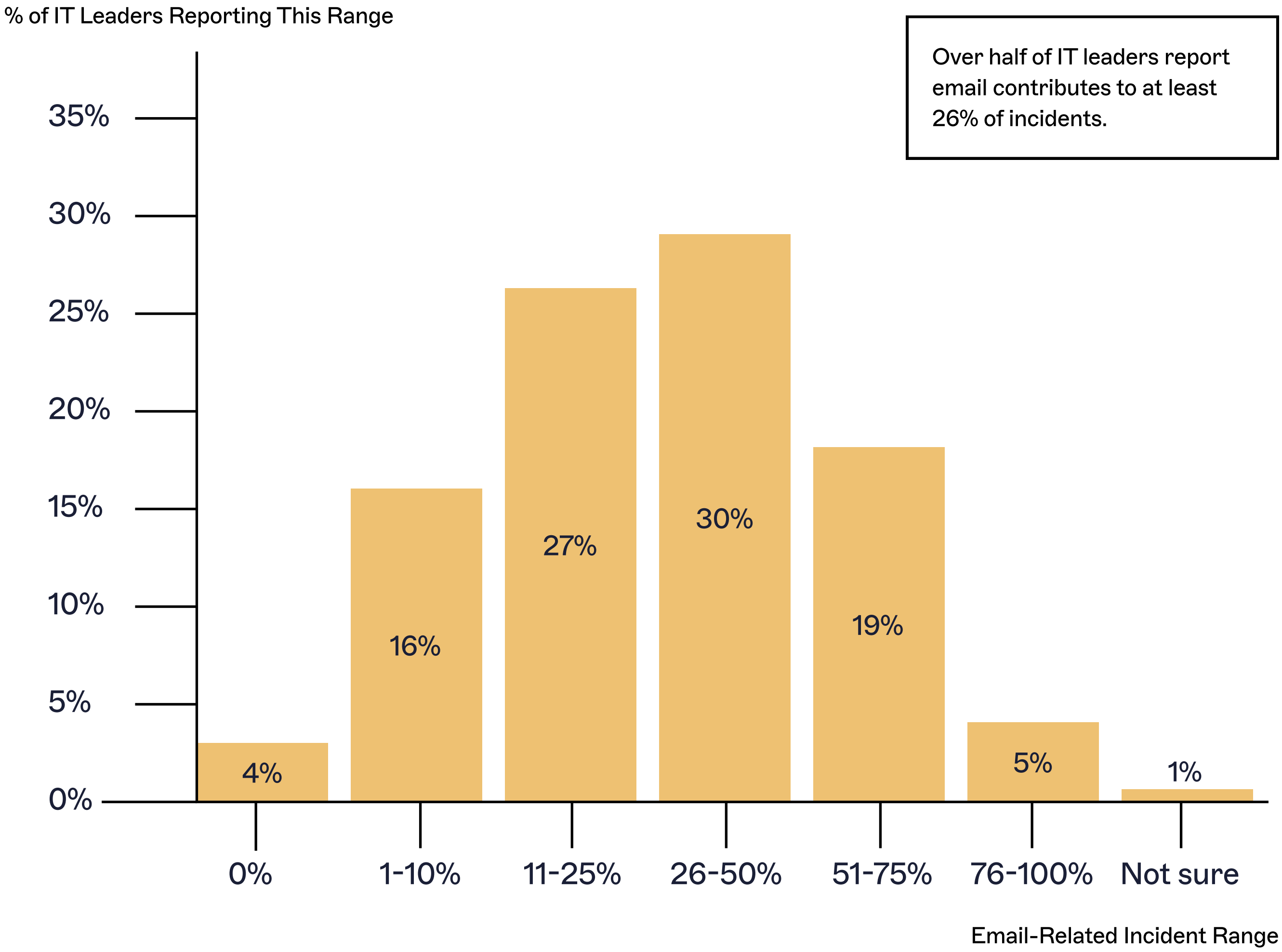
- **44%** **External threats** like phishing, spoofing, and spam
- **42%** **End-to-end encryption and security** gaps across email workflows
- **40%** **Balancing protection with usability,** particularly in hybrid setups

Even with this level of exposure, foundational protections remain uneven. Only **33%** of organizations report having implemented core protocols like **DMARC, DKIM**, or **SPF** —technologies designed specifically to protect against impersonation and spoofing.

This signals a growing disconnect: while the threat volume is high and rising, many environments are still operating with outdated or incomplete protections. That's not just a technical shortfall—it's a strategic one.

As long as email remains a weak link, attackers will exploit every angle—whether it's external threats like phishing, or internal failures like misdirected emails, human error, and compliance oversights.

Email's Role in Security Incidents, According to IT Leaders



Source: Exclaimer survey of 4,009 IT leaders

What IT needs to do

Start treating the inbox as a high-risk asset, not a support function. That means putting layered protections in place—protocols like DMARC, yes, but also continuous training, automated policy enforcement, and platform-wide visibility. Email systems need the same attention and resilience IT gives to network perimeters or identity systems. The risk profile demands it.

Trend 2: Email threats look different by region, size, and sector

IT leaders agree email is a major concern—but the nature of that concern varies widely depending on where an organization operates and what it does.

Globally, **76%** of IT leaders say up to half of their security incidents are tied to email. On average, they estimate email accounts for **33%** of all incidents. That number climbs to **36%** in the UK and falls to **29%** in Australia. That 7-point difference may not sound large, but it reflects how local regulations, adoption of cloud systems, and regional threat actors shape the experience of risk.

When asked, 'What are the biggest email security challenges your IT team faces, if any?,' here's how IT leaders in the US, UK, Australia, and Germany responded.

UK:

US:

46% Managing external email threats (e.g., phishing, spoofing, spam)

40% Ensuring email encryption & security

42% Balancing security with ease of use for employees

32% Unauthorized email access

32% Compliance violations

33% Data leakage

AUS:

47% Managing external email threats (e.g., phishing, spoofing, spam)

47% Ensuring email encryption & security

42% Balancing security with ease of use for employees

35% Unauthorized email access

36% Compliance violations

31% Data leakage

DE:

42% Managing external email threats (e.g., phishing, spoofing, spam)

42% Ensuring email encryption & security

36% Balancing security with ease of use for employees

32% Unauthorized email access

32% Compliance violations

25% Data leakage

The percentage of security incidents that are related to email, by sector:

Construction →	35%
Education →	40%
Finance →	32%
Public Sector →	41%
Hospitality →	38%
Healthcare →	35%
Legal →	34%
Manufacturing →	32%
Media →	30%
Non-profit →	42%
Professional services →	33%
Retail /e-commerce →	26%
Tech →	29%

Industry verticals show even sharper variation in the specific email challenges they face.

- **Media and entertainment (55%**) and **manufacturing (51%)** cite phishing, spoofing, and spam as their top issues.
- In **finance**, the story shifts: encryption (**42%)** and usability (**42%**) rank alongside phishing (**41%**)—reflecting dual pressure to protect sensitive data without obstructing day-to-day operations.
- **Nonprofits** stand apart, with only **31%** listing phishing and spoofing as top concerns. This could reflect different levels of maturity, staffing, or even perceived threat relevance.

Then there's organizational size. In **enterprises** with 5,001+ employees, **49%** of IT leaders say phishing and spoofing are their biggest challenge. Compare that to **42%** for mid-size firms (101–250 employees) and **41%** for micro firms (1–100 employees).

Larger organizations face three distinct challenges:

1

Exposure grows with workforce size—more inboxes, more potential targets

2

Enforcement is tougher—policies are harder to roll out and maintain at scale

3

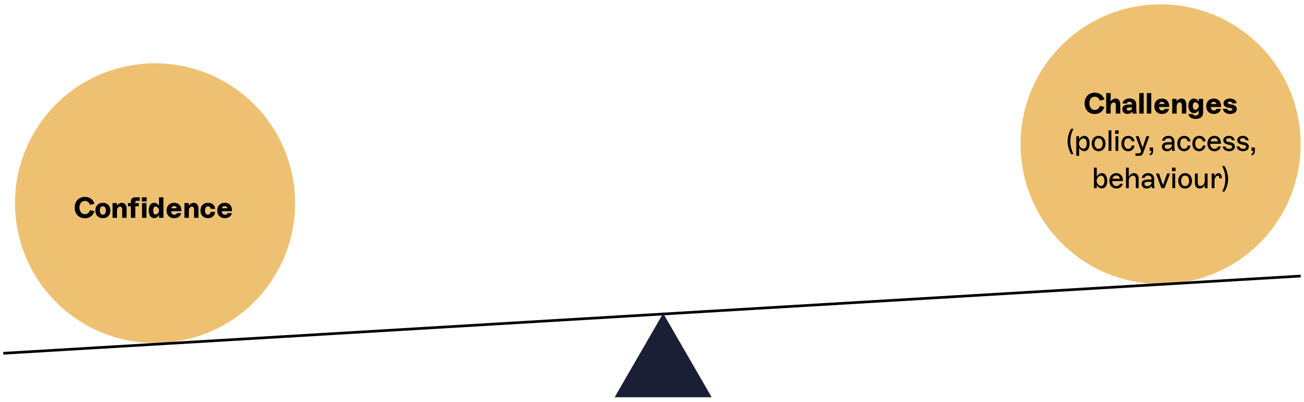
Human error increases—more variability in user behavior leads to more misdirected emails, weak passwords, and missed red flags

The result? A fragmented risk landscape where a one-size-fits-all security model can't keep up.

What IT needs to do

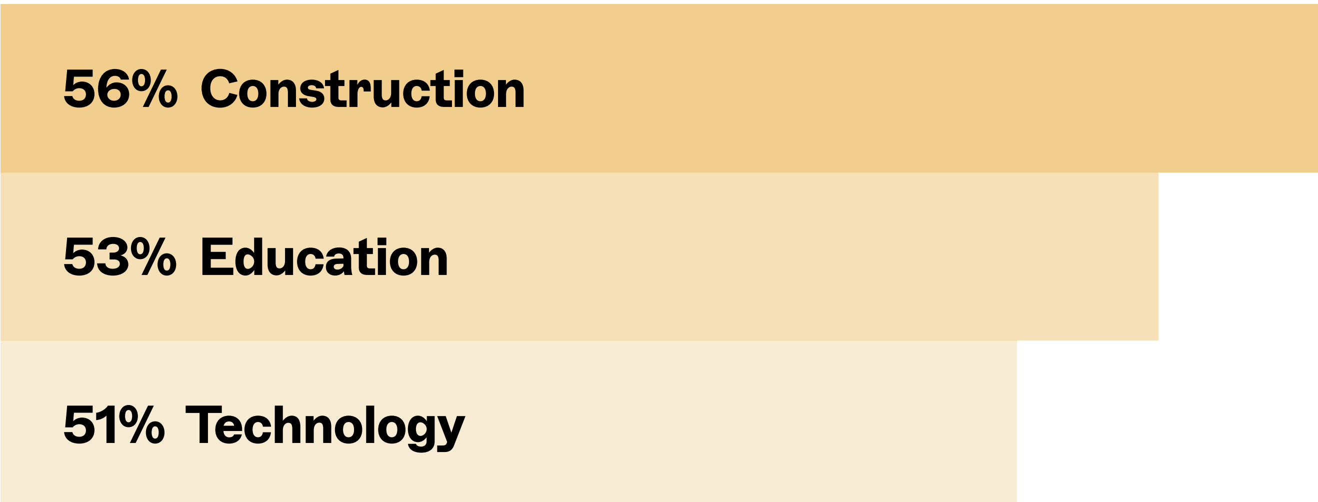
Threat mitigation isn't one-size-fits-all. IT teams need to map the specific threats most relevant to their sector, size, and region—and align protections accordingly. That might mean investing in advanced anti-phishing tooling for large enterprises or focusing on encryption in industries like finance or education. Broad coverage is good. Tailored enforcement is better.

Most IT and business leaders say they're confident in their ability to meet compliance requirements—but behind that confidence is a different story: resource constraints, complex systems, and uneven visibility.



93% of respondents say they feel confident in their compliance posture against frameworks like GDPR, HIPAA, SOC2, and ISO27001. While confidence is high on the surface, the breakdown reveals nuances. Only 47% of IT leaders say they are very confident, meaning more than half are relying on a more tentative, "somewhat confident" stance—leaving room for gaps in actual preparedness.

Some industries report the high levels of very confident responses:

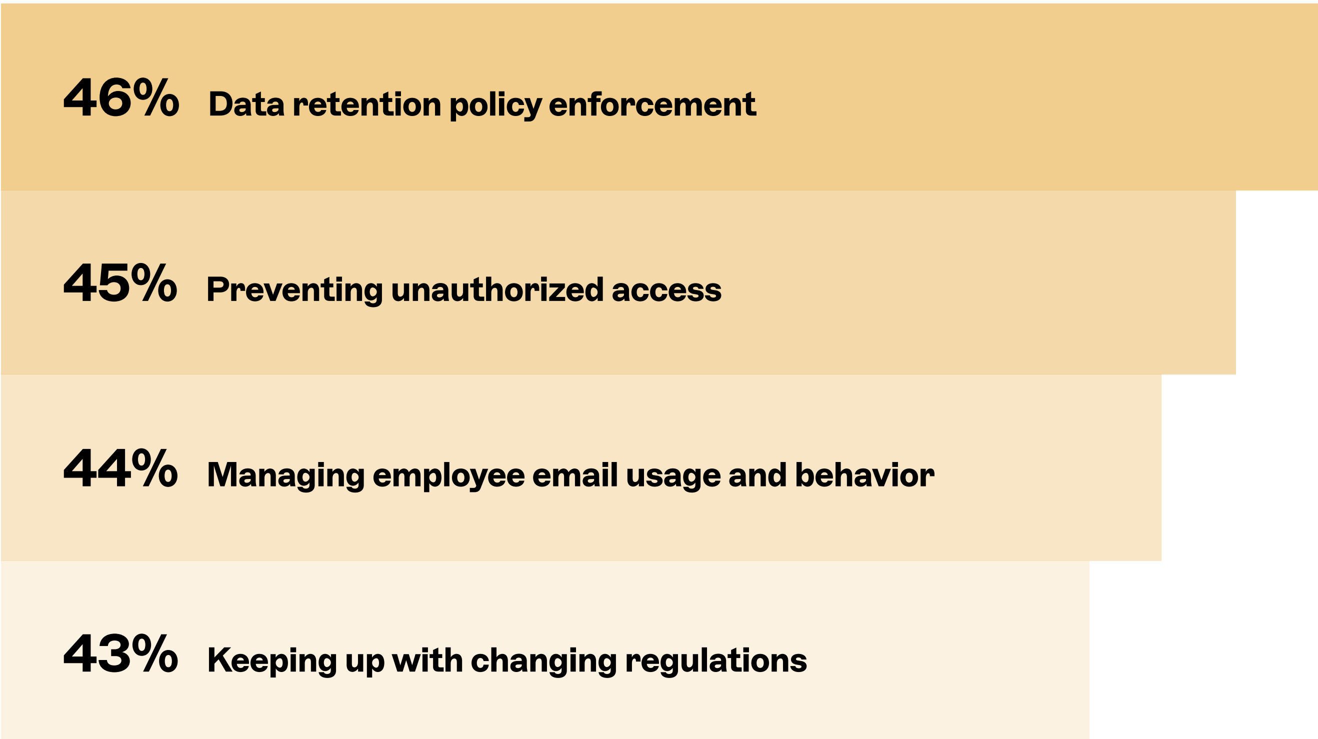


Others lag behind. Just **40%** of respondents in these sectors are very confident in their posture.

- **Nonprofits** and **hospitality** struggle with staff turnover, lean budgets, and legacy infrastructure—constraints that weaken their ability to enforce compliance.
- **Manufacturing** often faces the added hurdle of integrating compliance into physical systems with complex data flows—making enforcement especially difficult.

Even geography plays a role: **U.S. IT leaders** show the strongest confidence, with **54%** claiming to be very confident. The **UK (48%), Germany (43%),** and **Australia (42%)** trail slightly, likely due to more rigorous national data protection laws. What’s notable is that **platform choice doesn’t seem to shift the outlook**. Whether organizations use Google Workspace, Microsoft 365, or Exchange, confidence levels are nearly identical.

Still, the strain shows up in day-to-day operations. The top compliance management challenges reported by IT leaders include:



These pressures compound in large organizations, where systems sprawl and user oversight becomes more difficult. Nearly half of leaders at firms with 5,000+ employees say user behavior is their top concern.

Confidence without clarity won't cut it. Regulators—and internal stakeholders—expect documentation, auditability, and consistent enforcement. That's where the real lift comes in.

What IT needs to do

Turn compliance from a statement into a system. That means automating policy enforcement, capturing audit trails, and reducing reliance on manual oversight. Being confident isn't enough—IT leaders need email compliance to be provable, programmed, and ready for scrutiny at any moment.

Key takeaways

Email is one of the most active—and exposed—risk surfaces in the modern enterprise. It demands more than passive monitoring or confidence in policy. IT leaders must govern it deliberately, secure it systematically, and prove compliance under pressure. Here's what matters most:

Email threats are both frequent and underestimated.
Over half of organizations say email is responsible for a quarter to the majority of their security incidents. Despite this, many still lack basic protections like DMARC, DKIM, and SPF.

Context changes everything.
Risk perception and threat type vary by geography, industry, and company size. What's critical in finance or manufacturing may not be as urgent in education or nonprofits. Security strategies need to reflect those differences.

Larger organizations face layered challenges.
With more inboxes, more endpoints, and more variability in behavior, enterprises are especially vulnerable to phishing, misdirected emails, and inconsistent policy enforcement.

Compliance confidence doesn't guarantee control.
While most leaders report feeling confident in meeting requirements, enforcement remains heavily manual, and visibility gaps persist—particularly around employee behavior and data retention.

Proving readiness is the new standard.
Confidence is no longer enough. IT leaders need systems that automate policy, enforce standards, and generate audit-ready documentation. Because when failure happens, it's the proof—not the posture—that protects the business.

Chapter 3

Managing email at scale: Integration, efficiency, and purchasing behavior

Chapter 3

Email remains essential to how work gets done—but in too many organizations, it's still operating in a silo. As IT teams take on broader mandates for security, compliance, and digital transformation, email must evolve from a communications tool to an integrated part of the enterprise tech stack.

Yet there's a growing disconnect between what IT teams need—automation, interoperability, efficiency—and what their current email systems actually deliver. In many cases, email management remains manual, fragmented, and slow to scale. And as IT leaders take on more strategic ownership of the tools they deploy, the way email technology is procured is shifting too.

This chapter explores why outdated workflows are costing teams time, how integration gaps are stalling progress, and why buying decisions around email now demand long-term architectural thinking—not just feature comparisons.

IT leaders know where the time sinks are—spam filtering, compliance checks, signature updates—but too often, these tasks still fall to manual intervention. The result is a growing burden on already stretched teams.

Globally, IT leaders cite the top email-related drains on time and productivity as:

And these challenges scale with complexity. Yet, most IT leaders have failed to integrate tools that could automate these processes.

Just **29% of all respondents automate email workflows** with tools like Zapier or Power Automate, under half (**41%**) **have integrated email with security and compliance tooling**, and only **20% currently leverage an email signature management solution** for automatic updates.

That's a critical mismatch. Nearly half (**48%**) of all IT leaders say they want better automation and integration from their email ecosystem, **49%** say the same of security and compliance features, and **42%** want more options for signatures—yet relatively few have the connections in place.

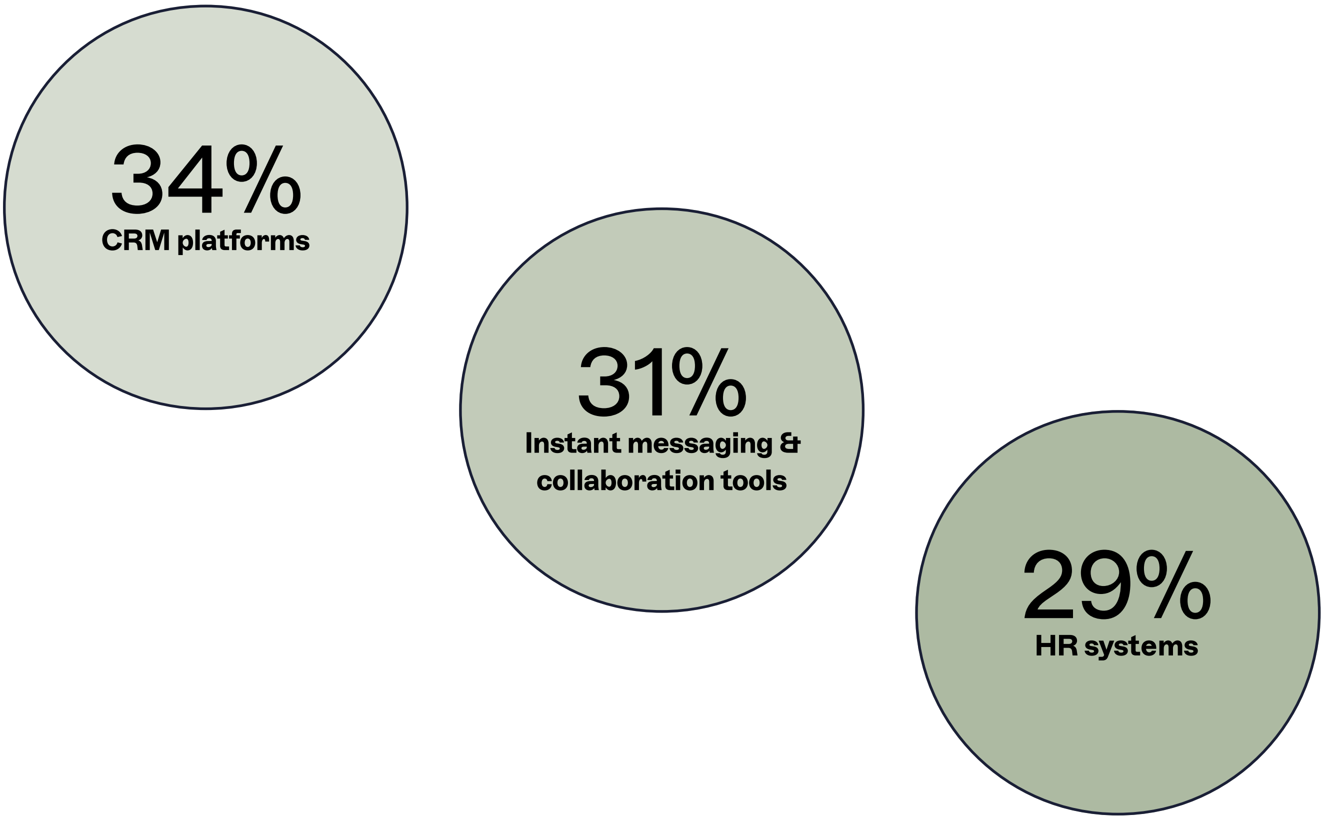
The tools exist. What's missing is connection. Teams are stuck firefighting routine tasks instead of investing in automation that could reduce risk, reclaim time, and unlock bandwidth for higher-impact projects.

The IT implication

Reframe email management as a system, not a set of chores. Tasks like spam filtering, compliance enforcement, and signature updates are repeatable and rule-based—which makes them ideal candidates for automation. By prioritizing automation in these areas, IT can streamline processes, reduce friction, and free up resources to drive broader transformation.

Email doesn't exist in a vacuum—but in too many organizations, it's still treated like it does. While business teams adopt new platforms and workflows, email often remains isolated from the tools it needs to connect with most.

Less than half of IT leaders **(41%)** say email is integrated with their **security and compliance stack.** Other integrations are even lower:



Just **29%** have integrated email into any kind of workflow automation, and **28%** have connected to marketing automation or appointment booking tools. That's despite the fact that **89%** of IT leaders view email as a critical communications tool.

When email operates in a silo, teams suffer. Marketing has to manually update signature campaigns. HR has to track and transfer employee changes in disconnected systems. Legal and compliance lose audit visibility. And IT is left stitching things together—responding reactively instead of building proactively.

What business applications, if any, does your organization integrate with direct email?

41% IT security & compliance solutions

34% Customer Relationship Management (CRM) systems (Salesforce, HubSpot, etc.)

31% Instant messaging tools (Slack, Microsoft Teams, etc.)

31% Collaboration tools (e.g., Asana, Trello, Monday.com)

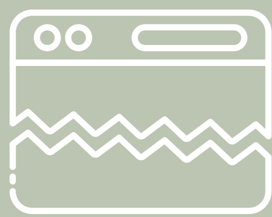
29% HR & onboarding systems (Workday, Bob, etc.)

29% Workflow automation tools (Zapier, Power Automate, etc.)

28% Marketing automation tools (Marketo, Pardot, etc.)

28% Appointment booking tools (Calendly, MS Bookings, Chili Piper, etc.)

Disconnected systems don't just slow down workflows. They introduce gaps in visibility, enforcement, and accountability—gaps that attackers can exploit and auditors can question.



What this means for IT

Email should be embedded in the architecture of how the business runs—not floating beside it. That means integrating it with core systems like CRM, HR, messaging, and security tools. Tight integrations strengthen governance, reduce redundancy, and improve operational resilience. The goal isn't to reinvent email. It's to make it work better—by making it work with everything else.

Trend 3: Buying email tech is now a strategy, not a transaction

IT still owns email procurement—but the criteria are shifting. Today's buying decisions are less about vendor reputation or feature checklists and more about how tools fit into a larger, more integrated stack.

Across the board, the top drivers for email tech selection are:

- **42%** **Security and compliance protections**
- **40%** **Ease of integration**
- **38%** **Automation and AI value**
- **37%** **Scalability and flexibility**

Traditional considerations like **cost (33%)** and **vendor reputation (32%)** now rank lower —especially in large enterprises, where nearly half **(47%) prioritize security first.**

But buying still comes with friction. Barriers preventing IT from investing in new technology include:

- **43%** **Security and compliance concerns**
- **41%** **Migration and implementation complexity**
- **41%** **Internal approvals and process delays**

These friction points slow down progress and make it harder for IT to deliver on transformation goals—even when the benefits are clear.

Why IT should care

Treat email procurement like infrastructure planning. Every tool should align with the business's broader architectural and security strategy—not just solve a narrow problem**. IT's role is shifting from administrator to strategic advisor,** guiding decisions, validating integrations, and ensuring every solution fits into the larger ecosystem. It's not just about approving tools—it's about orchestrating how they work together to support scale, security, and long-term value.

Key takeaways

**The gap between IT's priorities and what's been optimized is widening. Automation, integration, and smarter purchasing are the levers IT must pull to reduce drag and deliver value.
Here's what matters most:**

Automation is overdue.
IT teams are still spending too much time on repeatable tasks like spam control, compliance enforcement, and signature updates. Automation isn't a luxury—it's the next step.

Integration isn't optional.
Email is still operating in isolation in most organizations. Without tight connections to systems like CRM, HR, and IM, IT carries the burden of stitching together fragmented workflows.

IT still owns procurement—but strategy now outweighs price.
Security, integration, scalability, and AI value now drive purchasing decisions more than brand or cost. The buying process is about long-term fit, not short-term deals.

Execution depends on orchestration.
From prioritizing automations to coordinating across departments, IT leaders must ensure every tool aligns with business priorities and simplifies the stack—instead of adding complexity.

Email signatures for professionalism, consistency, and control

Chapter 4

Email isn't just a communication tool—it's a brand vehicle. Every message an employee sends reflects the business: its standards, its consistency, and its credibility. But in most organizations, signatures are still managed like an afterthought: decentralized, manually updated, and full of inconsistencies.

For IT leaders, this isn't a cosmetic issue. It's an integration problem. Signatures sit at the intersection of infrastructure, governance, and professional standards—but often lack a system to support them. Without integration into the wider tech stack, they generate tickets, add risk, and pull IT into requests they shouldn't have to manage.

This chapter explores why signature management is stuck in reactive mode, how fragmented ownership creates operational drag, and how IT can lead the shift—automating, standardizing, and embedding signature control into everyday workflows.

Trend 1: Everyone agrees signatures matter—but few are managing them well

IT leaders overwhelmingly agree on the value of professional, consistent email signatures. **92%** say that well-managed signatures build trust and credibility. But the day-to-day experience tells a different story—one of fragmented ownership, outdated processes, and a steady flow of formatting requests that eat into IT's time.

Ownership is a core issue. When no one fully owns signatures, everyone owns the mess

Only **55%** of organizations say IT owns signature management.

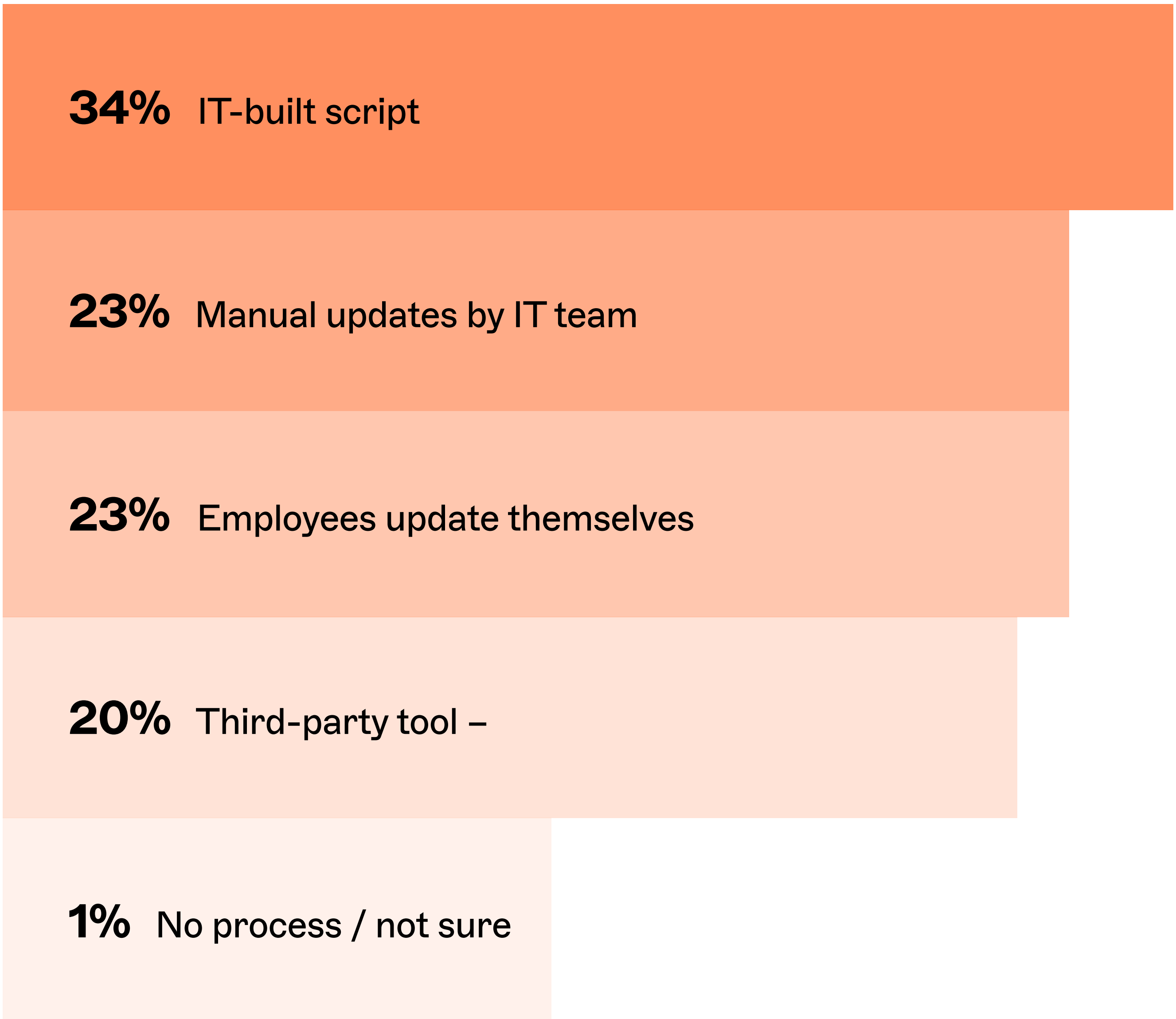
The rest split responsibility across HR **(16%)**, marketing **(14%)**, or individual employees **(14%)**.

In large enterprises, IT ownership drops to **47%**; in the public sector, it's just **34%.**

And the management methods reflect this fragmentation. Instead of streamlined tooling, 80% of organizations rely on patchwork processes:

- **34%** use IT-built scripts
- **23%** update signatures manually
- **23%** ask employees to manage their own

How are email signatures managed?



These methods of management result in frequent issues:

- **33%** say employees ignore signature guidelines
- **32%** report formatting that varies across clients and devices
- **31%** lack centralized control and visibility

Despite this, only **20%** of organizations use a dedicated signature management solution.

Trend 1: Everyone agrees signatures matter—but few are managing them well

Top challenges in managing email signatures:

- **33%** Employees not following guidelines
- **32%** Inconsistent formatting (devices/clients)
- **31%** No centralized management
- **31%** Can't use for marketing/engagement
- **31%** Slow update process
- **28%** Poor brand governance
- **24%** No insights into performance
- **3%** No major challenges

For IT, that means repeated interruptions, mounting support requests, and a growing disconnect between the tools they're managing and the professional standards they're expected to uphold.

Implications for IT

To reduce friction and reclaim control, IT must shift signature management into the infrastructure layer. That means enforcing consistency through automation—not approvals—and giving business users controlled access to update content. The goal isn't to micromanage—it's to create a scalable system that upholds professional standards without becoming another support burden.

Even though signatures are one of the most visible parts of external communication, they're rarely treated as part of a business's strategic planning processes. Updates usually come after something breaks—a change in structure, a security audit, or internal pressure from other teams. The fix is manual, rushed, and often temporary.

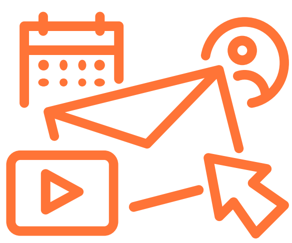
Top triggers for email signature updates include:

These reactive updates often fall on IT's shoulders, even when the need comes from other areas of the business. And because most systems aren't built for scale, what should be a simple change becomes a multi-day task—chasing down templates, updating code, fixing formatting errors, and fielding support tickets from confused users.

This approach doesn't just consume time—it creates risk. Inconsistent signatures can lead to outdated information, non-compliant disclosures, or unprofessional impressions in key communications. For IT, it's another example of unmanaged infrastructure masquerading as a design problem.

IT takeaway

Rather than waiting for audits or rebrands to force rushed fixes, IT can implement a signature management solution that brings control and consistency to the process. With centralized policy enforcement and automated updates, business teams can manage content within guardrails, while IT ensures consistency and compliance. This shifts signatures from a recurring disruption to a routine part of operations—reducing overhead and freeing IT to focus on higher-value work.



Key takeaways

Email signatures are one of the most visible—and most operationally neglected—components of business communication. For IT, they represent a clear opportunity to replace reactive service work with strategic system design.
Here's what matters most:

Ownership is fragmented.
Signatures are managed by a mix of teams, leading to inconsistency and placing support pressure on IT.

Fixes are reactive.
Signature changes are typically driven by events—not process—which makes updates harder and slower than they should be.

Manual methods dominate.
Most organizations still use scripts, manual edits, or rely on employees to manage their own—creating more overhead than necessary.

IT can lead the shift.
With centralized control, automation, and integration into broader workflows, IT can improve consistency, reduce inbound requests, and elevate signatures from a formatting task to a system-level asset.

The future of business email

Chapter 5

Email isn't disappearing. It's evolving. While AI, automation, and messaging tools are changing how teams communicate, email remains the foundation for formal, high-trust, and high-stakes interactions. For IT leaders, this isn't about defending legacy systems—it's about modernizing a channel that still carries critical business value.

Today's email environment is defined not just by its staying power, but by its growing complexity. Threats are more sophisticated. Expectations are rising. And the tools supporting email—from gateways to AI engines—need to do more, faster. This chapter explores where business email is heading, and how IT can shape that future by investing in security, leveraging AI, and enabling more integrated, adaptable workflows.

For all the noise around AI, automation, and UX enhancements, one priority cuts through across roles, regions, and industries: email security. It isn't a secondary consideration—it's the anchor of everything else. As threats escalate and regulatory demands increase, IT leaders continue to view enhanced security and encryption as the single most important force shaping the future of email.

Across platforms, regions, ranks, and org sizes, security leads.

47% **of all IT leaders say enhanced security and encryption will shape the next five years of business email**

53% **of ITs in the tech sector prioritize future investments in email security**

51% **of primary decision-makers rank encryption as a top strategic priority**

38% **want stronger phishing and spam protection built directly into their systems**

Legal **(47%)**, manufacturing **(49%)**, and media **(52%)** industries all elevate security above other key improvements to business email

While AI and collaboration features are gaining ground, they don't override the fundamentals. Email still carries contracts, credentials, system alerts, and regulatory disclosures. And the risk of exposure grows with every user, endpoint, and vendor integration added to the stack.

What this means for IT

Email security isn't a future concern—it's a present imperative. IT teams should prioritize solutions that offer layered protection, enforce compliance policies automatically, and scale across geographies and business units. From encrypted delivery and domain authentication to real-time monitoring and audit trails, the next generation of email infrastructure will be defined not by how modern it looks—but by how safe it keeps the business.

AI in email has turned a corner. Once a forward-looking experiment, it's now a standard that modern IT leaders expect to see—built in, not bolted on. Across sectors, regions, and company sizes, artificial intelligence is no longer seen as an optional upgrade. It's a critical part of how email will evolve to meet rising demands around automation, efficiency, and risk detection over the next 5 years.

43% of IT leaders identified AI-driven email automation as one of the top trends shaping the future of business email. That number climbs in sectors where email management is especially complex or sensitive, reflecting a shift in mindset: AI isn't about convenience—it's about capacity.

Who's already thinking ahead?

52% **of tech companies say AI will define the future of email**

49% of large enterprises (5,001+ employees) expect more AI and automation in their email stack

43% of primary decision-makers list AI-driven email automation among their top strategic priorities

45% of legal sector leaders and **44%** in manufacturing back AI as a defining force

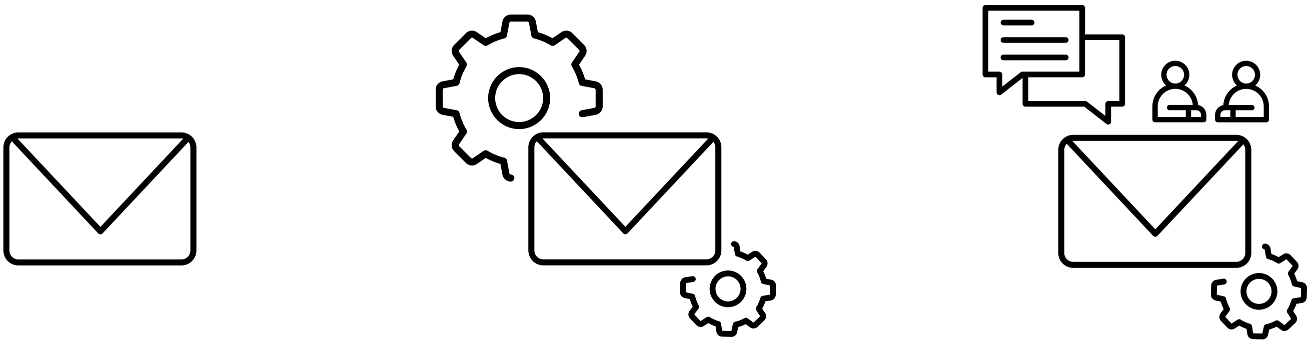
This goes beyond smart replies or subject-line suggestions. IT leaders want AI to optimize email delivery, triage messages by priority, detect threats, and reduce repetitive workflows. AI isn't just expected to keep up—it's expected to think ahead.

Considerations for IT

IT teams should evaluate AI tools based on practical outcomes, not just feature lists. The goal is to reduce overhead, boost accuracy, and detect problems before they escalate. That means choosing platforms that use AI for real-time routing, intelligent filtering, behavioral analysis, and automation of low-value tasks. The future isn't about whether email uses AI—it's about how well it does. And IT's role is to make sure it delivers.

Messaging platforms are gaining ground, but email remains essential —especially for external, formal, and auditable communication. Rather than being replaced, it's being repositioned within a blended communications ecosystem.

Email is evolving



90% of IT leaders say email will remain a primary business tool through 2030, even as real-time messaging platforms grow in popularity. This shift isn't about choosing one tool over another—it's about integrating them effectively and clearly defining how teams use them.

What's emerging is a hybrid model:

- **Email for formal, documented, compliance-sensitive communication**
- **Messaging for quick, internal collaboration and real-time feedback loops**

The integration between these systems is already underway:

42% **of IT leaders** expect tighter integration between email and real-time collaboration tools

41% say personalization will define the future email experience

34% want more customization and modularity in email environments

Email isn't static. It's adapting to meet new expectations—while preserving the professionalism and auditability that make it indispensable.

What this means for IT

IT must support a communications stack where email, chat, and collaboration platforms work in sync. That means deploying tools that integrate seamlessly across workflows, adapt to user roles, and maintain a high standard of professionalism and security. Email's future isn't in competition with messaging—it's in complementing it.

Key takeaways

Email is entering a new era—defined by smarter tools, stronger protection, and more strategic integration. For IT, this isn't about maintaining the status quo. It's about shaping what comes next.

Security remains the top priority.
As threats grow and regulations evolve, securing the inbox is more essential than ever.

AI is the new norm.
Automation, classification, and risk detection are no longer enhancements—they're baseline expectations.

Email is evolving—not being replaced.
It remains central to business communication, especially in high-trust, regulated, and customer-facing scenarios.

IT leads the transformation.
From adopting secure platforms to enabling integrated workflows, the path forward is proactive, not reactive. Email still carries the message when it matters most—and IT is the team that makes sure it arrives safely, consistently, and intelligently.

Conclusion

Email isn't going anywhere—but how it's managed, secured, and scaled is changing fast. Across industries, geographies, and business sizes, IT leaders are being asked to do more than just keep email running—they're expected to evolve it. The data from this report paints a clear picture: while threats persist and complexity grows, opportunities abound to automate, integrate, and govern more strategically. To keep pace, IT must shift from maintenance to orchestration—actively shaping the systems that support communication, compliance, and consistency across the business.

And as newer platforms emerge, email still holds its ground—for good reason. It remains the default channel for communications that matter. Whether it's legal agreements, client outreach, security alerts, or executive briefings, email provides the professionalism, auditability, and control that other tools can't. Its future isn't about replacement—it's about refinement.

1. **Treat email security as a core system, not an accessory.**
   With more than half of all security incidents tied to email in many organizations, IT must lead with layered, proactive defenses. This includes adopting foundational protocols like DMARC, DKIM, and SPF, building automated threat detection, and investing in employee training to minimize human error.

2. **Customize defenses to match your organization's risk profile.**
   Email threats vary by region, industry, and company size. IT leaders should map their risk landscape—phishing in manufacturing, encryption in finance, usability in nonprofits—and tune their tooling accordingly. One-size-fits-all solutions leave blind spots.

3. **Automate high-friction, low-value tasks to free up IT resources.**
   Managing spam, email signatures, and archiving are still huge time drains for IT—especially in larger enterprises. Automating these repeatable processes with purpose-built solutions reduces overhead, cuts down on support tickets, and allows IT to shift from admin to strategic advisor.

4. **Centralize signature management to enforce consistency and reduce complexity.**
   Fragmented signature ownership leads to inconsistent messages and excessive support load. IT should implement a signature management solution that allows business teams to manage content within compliance-approved guardrails—without relying on manual fixes or scripts.

Conclusion

5. **Future-proof your email stack with integrated, AI-enabled infrastructure.**
   Nearly half of IT leaders say AI and automation will define the future of email. At the same time, **90%** still see email as a critical business channel through 2030. IT must evaluate tools not just for functionality, but for their ability to adapt—supporting hybrid communication environments, smarter workflows, and scalable governance across the ecosystem.

Email is built for the communications that matter—and its evolution starts with IT. Modernizing how it's secured, automated, and governed isn't just a technical upgrade. It's how businesses stay protected, connected, and ready for what's next.

About Exclaimer

Email is built for the communications that matter—and Exclaimer helps IT manage it that way.

Exclaimer is the leading provider of email signature management solutions for Microsoft and Google email services. Its scalable, cloud-based platform enables organizations to centrally manage and automate email signatures—ensuring regulatory compliance, operational efficiency, and professional consistency across every message.

Built for IT teams, Exclaimer simplifies administration by eliminating manual updates, reducing security risks, and maintaining full control over business email communications. With powerful automation and integration capabilities, it helps IT teams modernize a critical part of their communication stack—without adding complexity.

Key capabilities include:

- **Centralized oversight** across devices, platforms, and users
- **Scalable automation** for formatting, role-based updates, and policy enforcement
- **Built-in compliance features** to support audit readiness and governance
- **Seamless integration** with Microsoft 365, Google Workspace, and other business-critical tools

Exclaimer delivers over 20 billion email signatures annually from 9 million email accounts across 70,000 organizations, including Sony, Mattel, Bank of America, NBC, the Government of Canada, the BBC, and the Academy Awards.

Visit www.exclaimer.com or follow us on Facebook, LinkedIn, and X (formerly Twitter).
For media enquiries: press@exclaimer.com

Book a demo

The State of Business Email 2025: Infrastructure, Risk, and IT's Next Opportunity

Exclaimer