zivver

Email Security Trends 2025

THE WIDENING DISCONNECT BETWEEN EMAIL SECURITY AND RISK MANAGEMENT

Contents

Foreword

Email remains a cornerstone of organizational communication, enabling seamless collaboration and the exchange of sensitive information. However, we have observed a critical disconnect between the rapidly growing compliance requirements related to email and the development and adoption of the necessary robust security measures. While much attention has rightly focused on combating inbound threats like phishing and malware, the risks associated with outbound email deserve equal consideration. Misaddressed messages, unfit encryption practices, and accidental disclosures pose challenges that can impact security, trust, and productivity if left unaddressed.

The findings in this report reveal that effective email security should support—not hinder—the work of employees. Security solutions should empower users to operate safely and confidently, seamlessly integrating into existing workflows and unobtrusively leveraging suitable protective measures as needed. The insights in this report emphasize the importance of shifting perspectives: rather than trying to educate employees and expecting them to do the right thing at the right time, organizations can adopt tools and processes that reinforce good security practices and simplify compliance to meet evolving regulations like NIS2, DORA, GDPR and HIPAA.

This report invites businesses to reimagine their approach to email security. By fostering a culture of accountability and support, balancing user empowerment with robust safeguards and investing in supportive, smart, and integrated technologies, organizations can align their email practices with the demands of a fast-changing digital landscape. We hope these insights inspire actionable steps to create a safer, more efficient environment for your teams as you prepare for the challenges of 2025 and beyond.

Rick Goud, Co-Founder and Chief Innovation Officer, Zivver

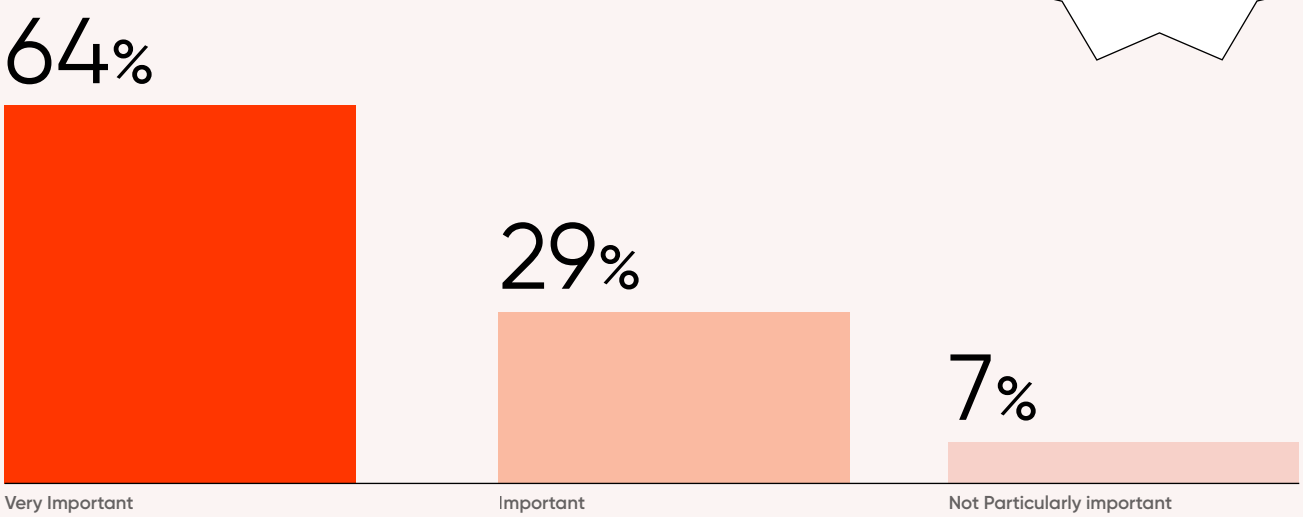
Executive Summary

Email remains the backbone of modern business communication. More than **90% of employees identify email as "important" or "very important" to their day-to-day work**, and as we approach 2025, it remains the number one channel for communication and the exchange of sensitive information - but could it also be an organization's biggest vulnerability?

Total Importance

93%

Employee: Importance of email in day to day job



There is a troubling gap emerging between the perceived risk of using email, and the reality of day-to-day security and risk management. IT leaders primarily focus on inbound threats such as phishing attacks, which 47% rank as their top concern. Yet two-thirds admit that outbound security breaches, often caused by innocent human mistakes, result in far more data loss than malicious social engineering attacks.

Outbound threat vectors can take many forms – a typo in the address field, a misdirected email, a CC or BCC error, or attaching the wrong file before hitting the send button. This isn't the fault of employees, but rather a clear sign that email is a silent threat vector that demands closer monitoring, training, and compliance oversight. **Only 34% of email incidents are formally reported**, and a staggering 67% of IT leaders claim that email doesn't get the security attention it deserves.

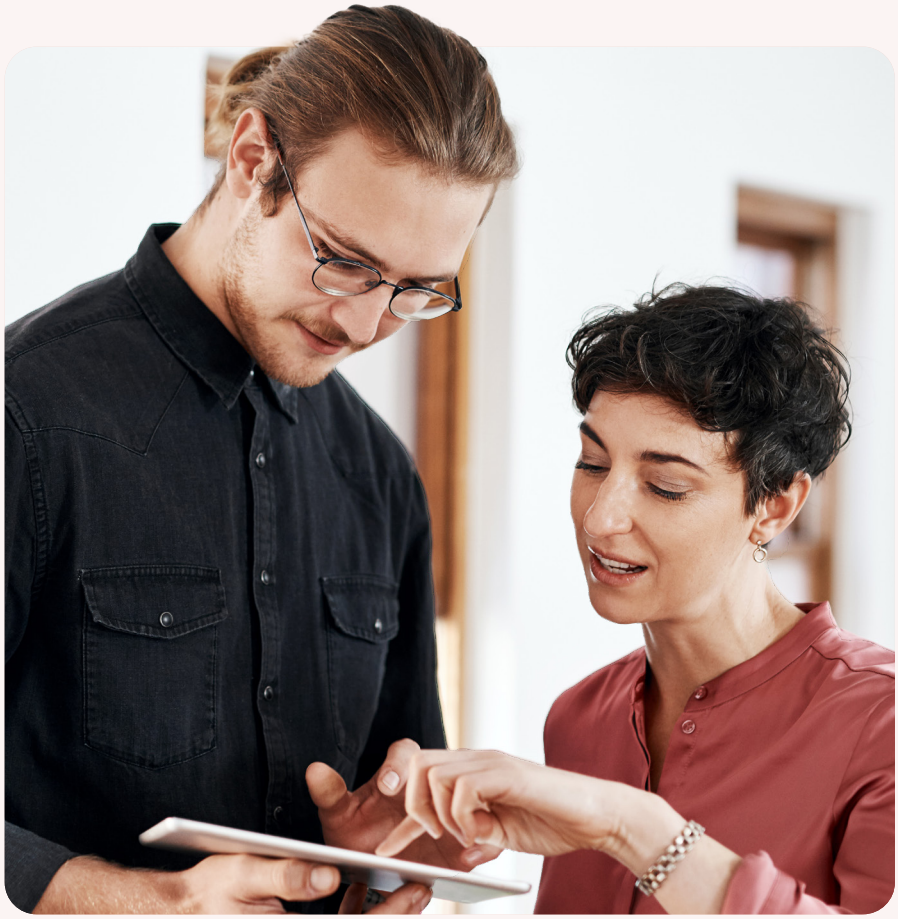
Their motivation for reevaluating email security and governance is now stronger than ever.

This widening security gap also poses problems from a compliance perspective. From NIS2 and GDPR in the EU to CCPA in the US, as well as industry-specific regulations like HIPAA in healthcare and global standards such as ISO/IEC 27001, which require email security to be considered as part of a broader risk management strategy, organizations have a lot to consider. These compliance objectives rightly take the form of internal company security policies, yet **while 73% of employees are aware of the security policies pertaining to email, only 52% adhere to them.** This suggests that the "silent threat" posed by email isn't necessarily a fault of a company policy, but how those policies are adopted and governed.

Efforts to mitigate email risks often rely heavily on training programs, but these too often fall short. **While 64% of employees report receiving training on email security, more than a third in large organizations find it ineffective or are dissatisfied with how training is delivered.** This dissatisfaction is more pronounced among frequent mistake-makers, many of whom also report confusion over company policies. Real-world scenario training and interactive workshops, which employees overwhelmingly prefer to more traditional "box-checking" exercises, could improve engagement, but training alone cannot bear the weight of securing such a vital communication channel.

The message is clear: rather than depend on training or the formation of email security policies or expect busy employees to manually bear the burden of email security on their own, businesses need to start introducing operational guardrails and intelligent security controls to secure email as a channel and empower employees to use it safely and confidently. IT leaders are hearing this message loud and clear. Over the next two to three years, their focus will shift toward automation and the use of AI-based tools to not only counter increasingly sophisticated inbound threats but give employees the support they need to mitigate the risks inherent to outbound email. These businesses will move away from a culture of blame, and toward a culture where employee mistakes aren't seen as individual faults, but as opportunities to evolve email security as a whole.

IT leaders are hearing the message, but are the security vendors they depend on? **More than two thirds (67%) of IT leaders believe vendors are not innovating fast enough to keep up with emerging risks,** leaving a critical gap in the market. This report, based on a study conducted in October 2024 with 400 IT decision-makers and 2,000 employees across the US, UK, Netherlands, France, Germany, and Belgium, offers an evidence-based exploration of these vital issues. By analyzing insights from organizations with 250+ employees across various sectors, it will provide actionable recommendations to help businesses to comply with regulatory requirements, reduce data leaks and improve security outcomes. Through smarter investments, empowered employees, and the seamless integration of smart technologies, businesses can maintain email's role as a vital – but safer – tool for communication.



Technology tools

Chapter 1

Email security: Threats, trends and solutions

Email is indispensable to modern business, but it also stands directly at the intersection of escalating cyber threats and tightening regulatory demands. Originally developed in the 1970s, even before the internet, email was designed as a basic messaging tool – not a secure communication platform. Over the years, protocols such as DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework) have been retrofitted to bolster security, yet despite these gains, it has resulted in a patchwork approach to security that has left email vulnerable. Malicious attacks, such as phishing, spoofing, and Business Email Compromise, lacking adoption of security standards like DANE (DNS-based Authentication of Named Entities), missing authentication and data loss through human error only compound email's inherent vulnerabilities.

> On average, an organization will experience 212 outbound email security incidents per month, yet only half (52%) of employees follow outbound email security policies to ensure compliance.

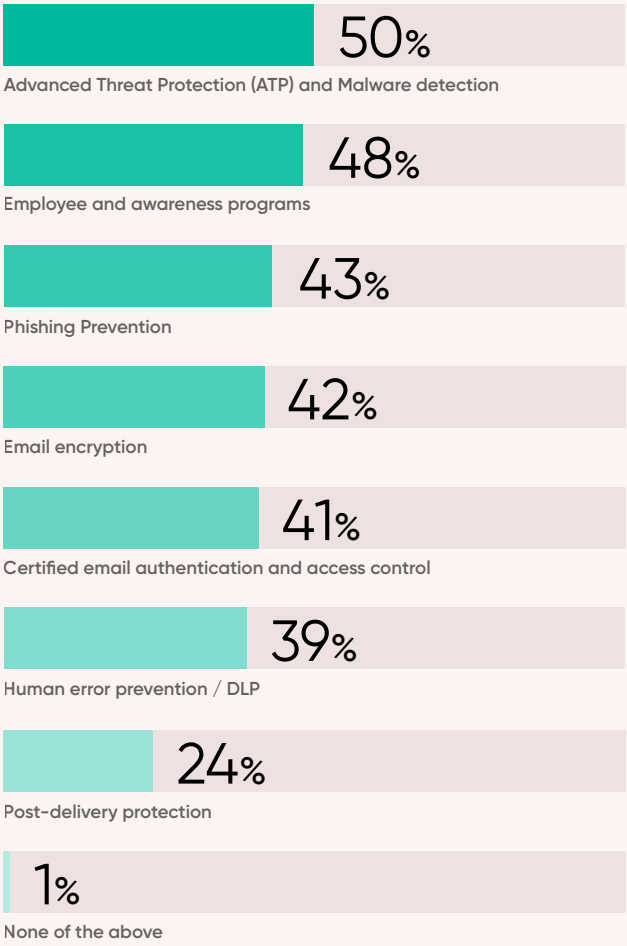
The inbound issue

Malicious attacks, or "inbound" threats, are considered the biggest threat vector to email amongst IT leaders, with 47% stating that inbound threats are a bigger concern to them than outbound email security. Phishing continues to dominate as one of the most prevalent and sophisticated cyber threats, accounting for over 80% of reported security incidents in 2024, with attackers leveraging increasingly convincing impersonation techniques, outpacing the defensive capabilities of even major providers like Microsoft.

These threats are smart and growing smarter, targeting employees with personalized messages that exploit human trust and technical vulnerabilities. And yet email does not offer sufficient defenses to protect against business email compromise, spoofing, or phishing. Our most relied-on digital communication platform must be enhanced to educate and arm employees to identify and counter harmful incoming attacks.

Understandably, malicious threats dominate the security agenda. Advanced Threat Protection and malware detection (50%), employee training and awareness programs (48%), and phishing prevention (43%) are the three main priorities for email security investment according to IT leaders, over and above encryption and human error prevention.

IT leaders: Priorities of security investment



While the focus on malicious attacks has spurred advancements in detection and prevention technologies, IT leaders still feel preventative measures are lacking; 67% of IT leaders say that security vendors are not innovating quickly enough with evolving AI risks. Furthermore, 59% of employees say that they are worried that AI will make it harder for them to know if an incoming email or link is legitimate.

> 67% of IT leaders say that security vendors are not innovating quickly enough with evolving AI risks

It is clear; while threat prevention is the focus for IT leaders, current tools and defenses are falling short. In addition to the inbound struggle, our research highlights an overlooked threat vector in email's security defenses requiring equal, if not more, attention from IT leaders this year.

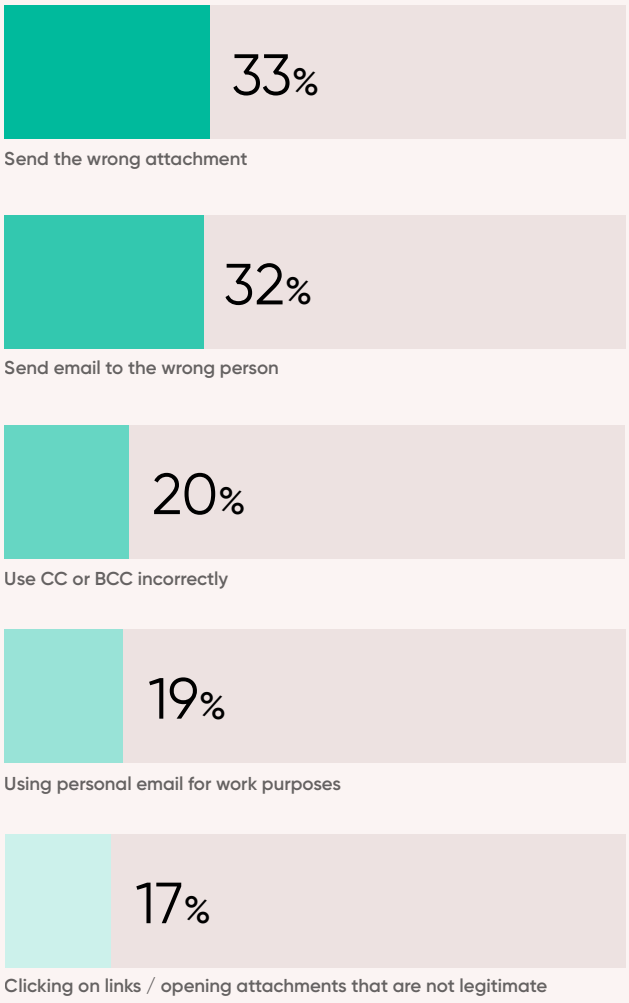
The outbound threat blind spot

As of January 2024, the Netherlands reported approximately 139,625 personal data breaches since the implementation of the GDPR In May 2018*. The UK's Information Commissioner's Officer (ICO) report that data leaks caused by human error, such as misaddressed emails, posed the single greatest threat among all cybersecurity incidents in 2024, accounting for over 85% of reported breaches*. This is a theme that is reflected across much of Europe and the US, yet inbound threats – due to their malicious nature – tend to receive the most attention. It is only recently, as the amount of sensitive data businesses gather and the compliance mandates around it have increased, that this "attention gap" has become glaringly apparent.

Our research shows that even the Dutch numbers only expose the tip of the iceberg and outbound email mistakes are alarmingly common. Employees frequently send the wrong attachment (33%), misaddress emails to unintended recipients (32%), or misuse CC and BCC fields (20%). These mistakes are more likely to happen when employees are tight on time (54%), when they are stressed (40%), or when they feel overwhelmed by too many messages (40%).

More than half of employees admit to making email mistakes of this nature at least once every few months, with 30% saying they make these errors on an almost weekly basis. Expecting busy employees to not make mistakes isn't viable, and while training can reduce the likelihood of mistakes occurring (a topic we will explore later in this report) the real focus should be on email as a channel and the risk-mitigating technology that supports it.

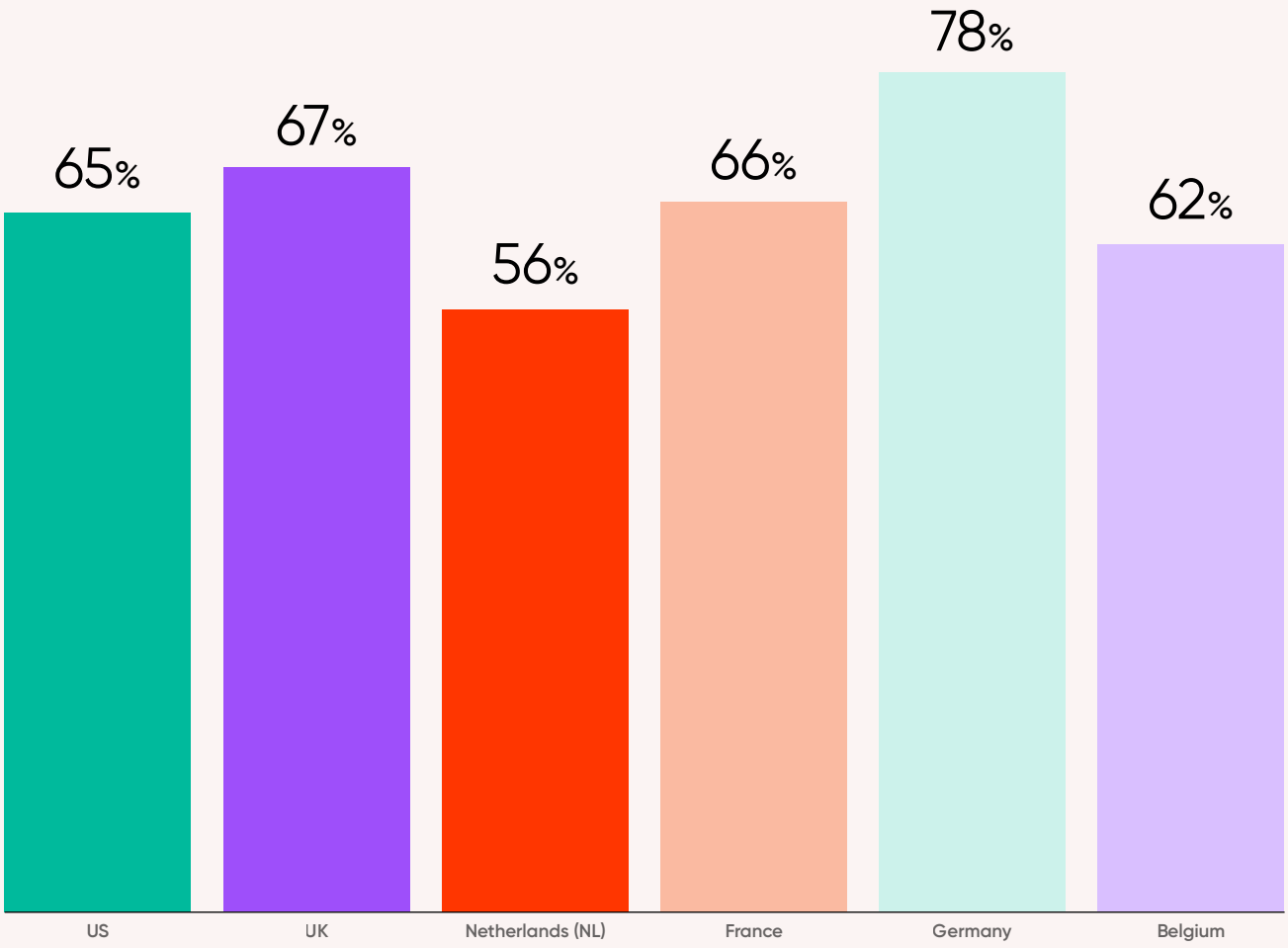
Employee: Most common types of email error



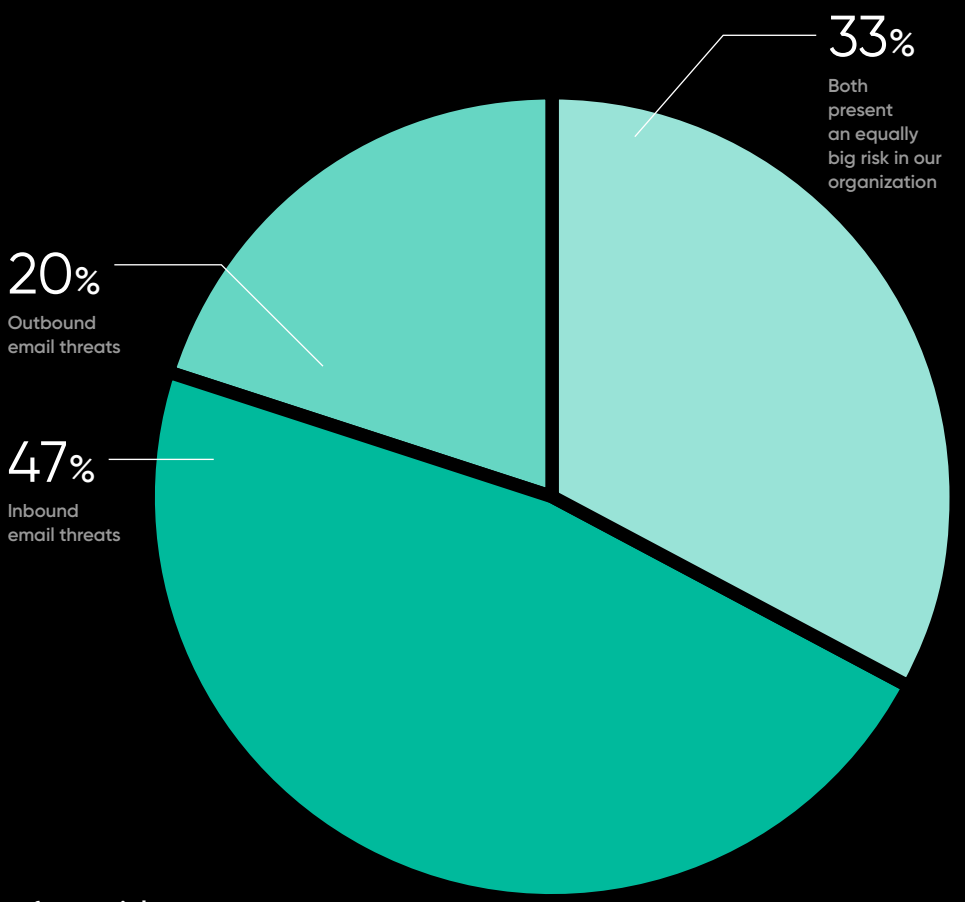
Misaligned email security priorities

While 47% of IT decision-makers identify phishing and malware as top threats to their data, only 20% prioritize outbound risks and just 39% of IT leaders point to data loss prevention/human error as an investment priority for email security. Yet, despite the low level of attention paid to outbound risks, two-thirds (66%) of IT leaders admit that employee mistakes in outbound emails result in more significant data loss than malicious inbound attacks.

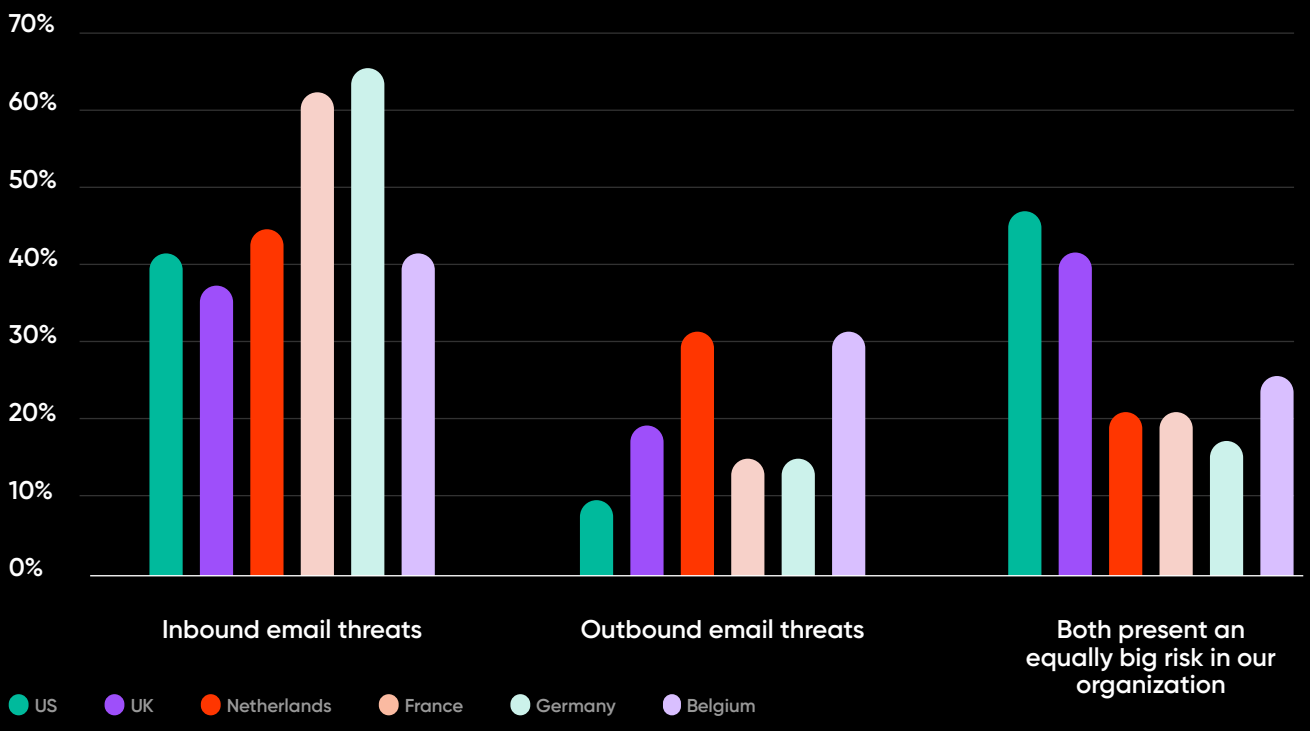
IT leaders: We lose more data every year through employee error than through any kind of malicious inbound threat



IT leaders: Biggest risk in terms of potential data loss



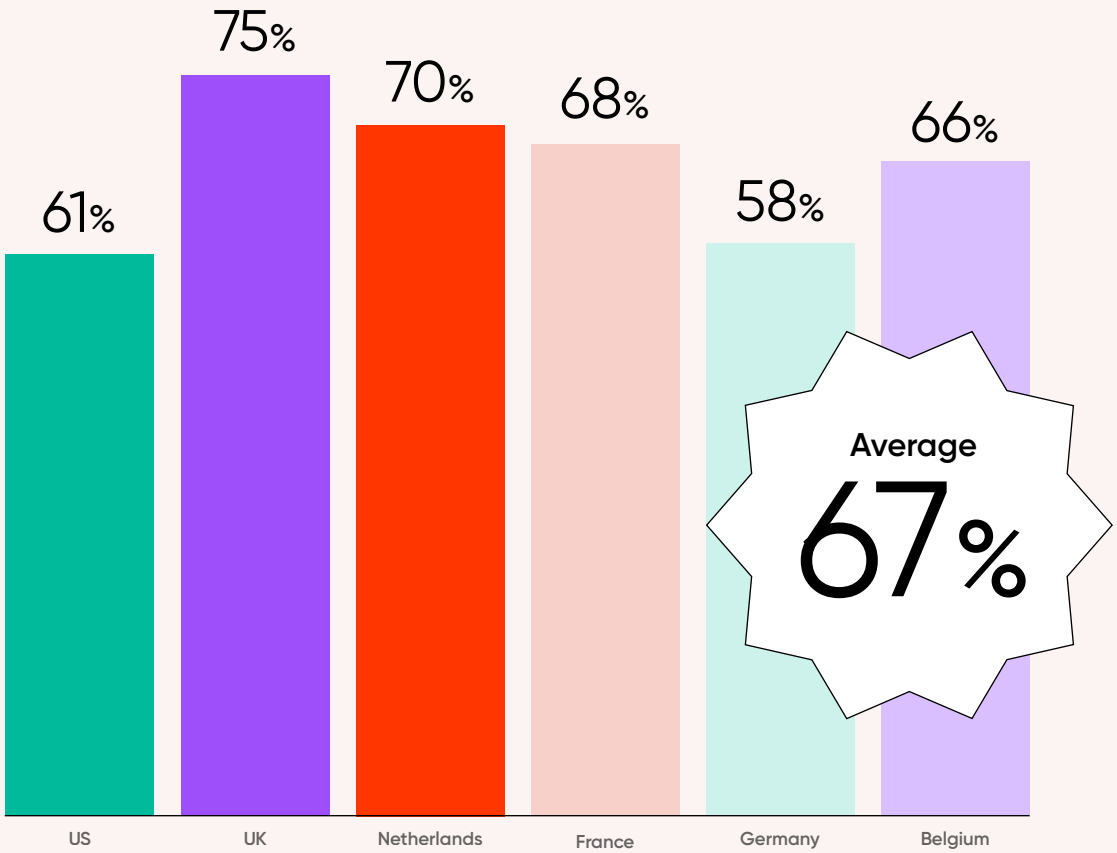
IT leaders: Biggest risk in terms of potential data loss - regional split



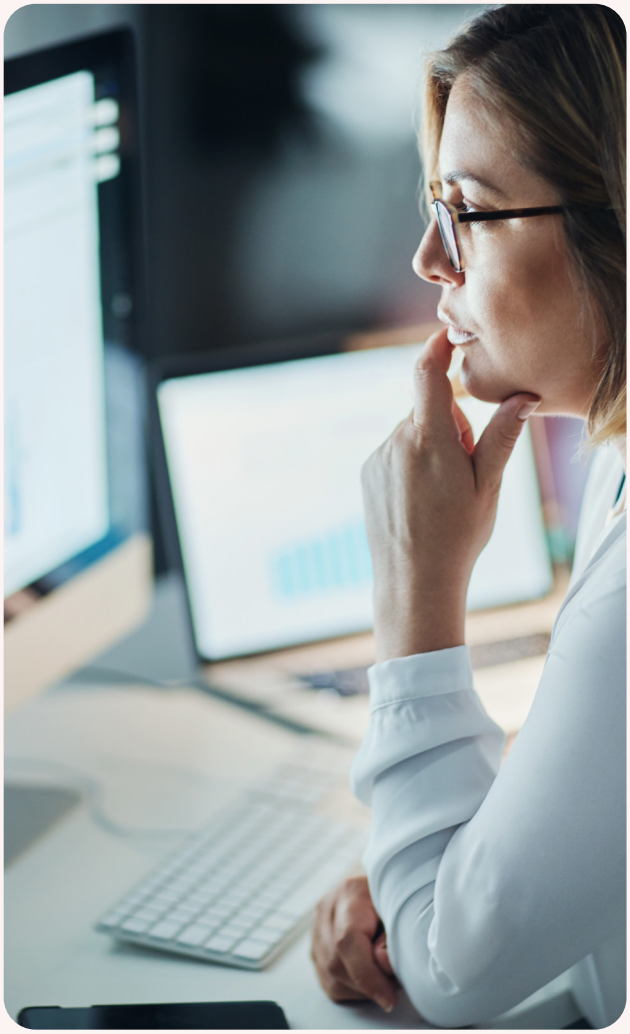
> 67% of respondents agree: "Outbound email security doesn't get as much attention beyond compliance, but it is the silent security killer. Sometimes we focus more on perceived risks rather than actual threat realities when it comes to email security."

This points to a dramatic misalignment of security policies. Maintaining inbound security is, of course, essential, but not at the cost of outbound security.

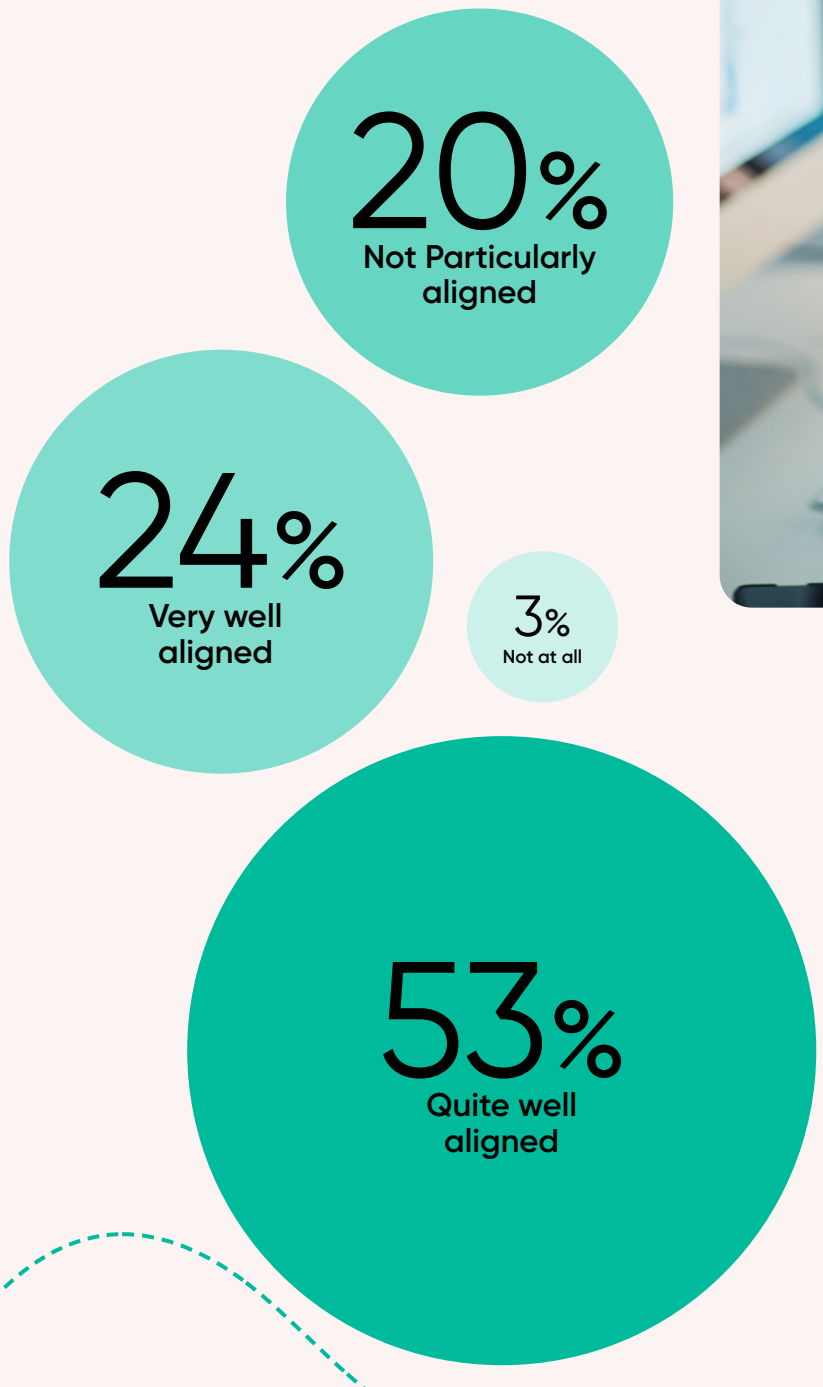
Outbound email security doesn't get as much attention beyond compliance, but it is the silent security killer



This misalignment extends beyond perception to investment: only 25% of IT leaders believe their security spending is “very well aligned” with actual risks. Adding to the complexity, 38% rank "employee misunderstanding of security policies" among their top vulnerabilities, while 60% of employees report using workarounds to bypass policy measures, highlighting a potential gap between IT leaders’ assumptions and the reality on the ground.



IT leaders: How aligned is data security investment with these actual security threats/risks to your organization?



Email security checklist:

The confluence of challenges—outdated protocols, human error, and the escalating threat of phishing—make email security a critical issue that must be addressed holistically. Rather than make email security burdensome for employees, organizations should consider tools and processes that empower employees to make better security choices. This includes:

Invest in advanced email security solutions

- **Adopt AI-Powered Security Platforms:** Implement intelligent email security systems that utilize artificial intelligence and machine learning to detect and block sophisticated phishing attacks, spear-phishing, and zero-day threats.

- **Real-Time Error Prevention Tools:** Equip employees with tools that provide real-time alerts for potential mistakes, such as misaddressed emails or incorrect attachments, helping to prevent data leaks before they occur. These tools must prioritize simplicity and user experience, such as providing one-click encryption or intuitive phishing alerts, to ensure employees can adhere to security policies without difficulty.

Implement robust encryption and authentication protocols

- **Upgrade to Advanced Security Standards:** Organizations must upgrade to Advanced Security Standards and fully adopt critical protocols such as DMARC for email authentication and DANE for enhanced transport security, ensuring emails are sent securely to the correct servers.

- **Zero-Trust Encryption:** Utilize user-friendly encryption tools that make it easy for employees to encrypt sensitive emails, protecting data from interception and unauthorized access, ensuring that even vendors don't have access to sensitive information.

Establish Comprehensive Data Leak Prevention Strategies

- **Data Classification and Monitoring:** Implement systems that automatically classify sensitive information and monitor outbound emails for potential data leaks, with the capability to quarantine or block risky communications.

- **Policy Enforcement:** Clearly define and enforce email security policies, ensuring employees understand the importance of compliance and the procedures for handling sensitive information.

Compliance

Chapter 2

Regulatory storm on the horizon

There is a third element to email security that must also be considered, arguably the most pressing challenge for IT leaders in 2025 - the matter of compliance. Escalated by insubstantial security functionality inbuilt into email platforms, evolving malicious threats, and risks related to data loss prevention, human error, and security awareness, email, as a communication tool, is under the microscope of tightening regulatory demands.

As previously highlighted, email was not designed to be a secure communication platform; it was developed with the purpose of getting data from point a, to point b, as quickly as possible. As such, information security and data protection laws are rightfully challenging organizations to remedy email's flaws to protect sensitive data in transit.

In Europe, landmark legislations like DORA (Digital Operational Resilience Act) for financial institutions and NIS2 (Network and Information Systems Directive) for essential sectors, including government and healthcare, are set to take effect in 2025. The UK is introducing the Cyber Security and Resilience Bill in the same year. In the United States, federal laws such as HIPAA (Health Insurance Portability and Accountability Act) and GLBA (Gramm-Leach-Bliley Act) are undergoing continuous enhancements, with individual states enacting their own stringent data protection laws.

Each of these legislations include key requirements around risk management, information classification, secure information transfer, awareness training, and data leakage prevention – throwing email firmly under the regulatory spotlight.

Key legislative requirements for secure information management:

Various common denominators are explicitly detailed in the majority of new regulations that directly impact email. Outlined below, these factors require immediate attention to ensure requirements are met within the email environment to support compliance:

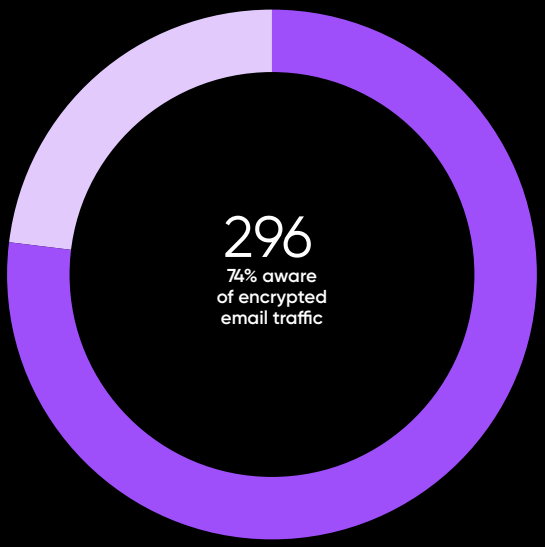
- Robust risk management practices: Organizations must adopt a proactive stance against phishing, integrating comprehensive risk management, incident response, and continuous monitoring into their cybersecurity strategies.
- Information classification: Organizations must classify information based on sensitivity to determine appropriate security controls for email transmission, preventing unintended exposure.
- Secure information transfer: Right-sized encryption and traceability are required to protect information during transmission from interception and unauthorized access.
- Access control: Access to sensitive information must be restricted to authorized individuals, necessitating reliable authentication for both senders and recipients.
- Awareness and training: Regular training and updates on information security policies are mandatory to maintain a security-conscious workforce.
- Data leakage prevention: Organizations must implement measures to minimize data leak risks due to human error, including monitoring and blocking or quarantining emails containing sensitive information with insufficient protection or potential errors.

Email visibility: How to manage hidden threats

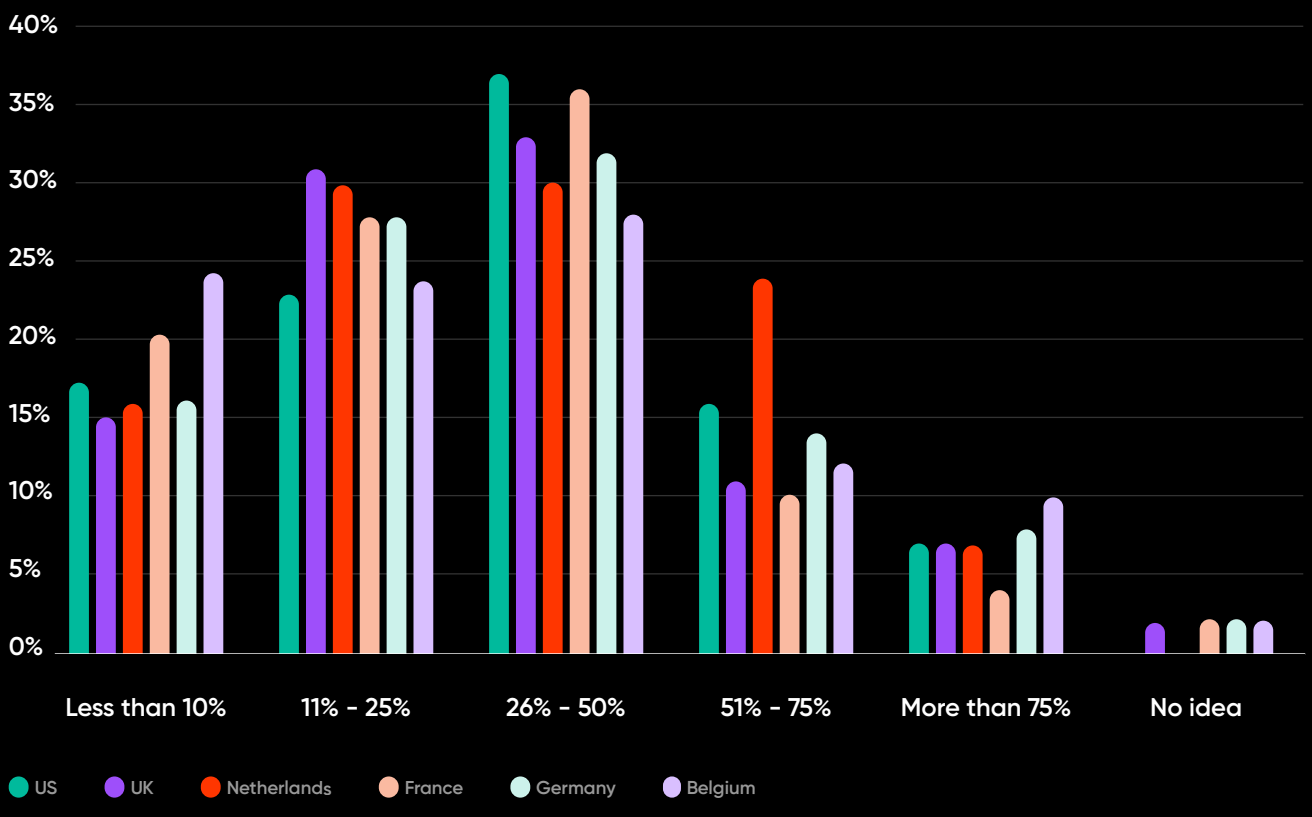
Supercharging the minimal security procedures within email will be key to closing the compliance gap. Two areas highlighted in our research which continue to prove difficult for IT leaders are transparency and reporting of email security threats.

Only 77% of IT leaders said they were aware of whether their emails were encrypted. Encryption should naturally depend on the sensitivity of email content; however, a lack of awareness points to a much deeper problem – a general absence of insight into email traffic.

Number of IT leaders aware of encrypted email traffic

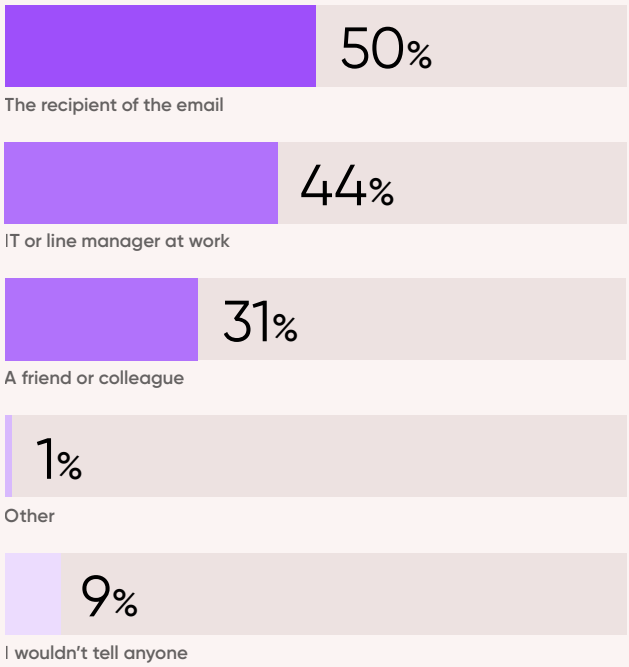


IT leaders: % of outbound email incidents through to be reported by employees - regional split



Similarly, many compliance frameworks mandate the monitoring and reporting of email incidents, yet informal employee practices often obscure the true scope of these events. While IT leaders estimate that only 34% of outbound email incidents are formally reported, many employees handle mistakes informally—50% say they would notify the unintended recipient directly, while just 9% would report the incident to IT. This behavior leaves IT teams in the dark about the true scope of email security incidents, undermining their ability to address systemic issues.

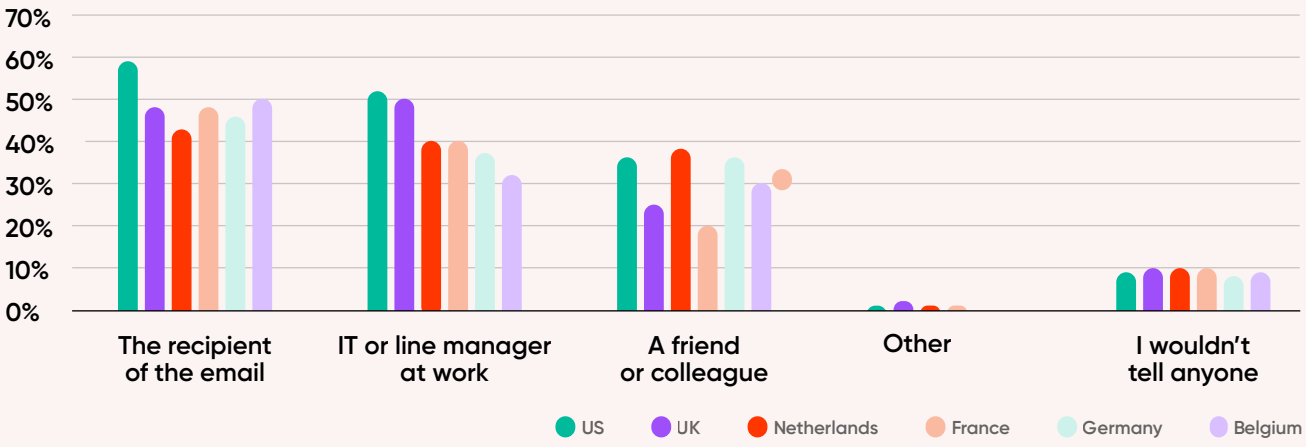
Employee: Who would you tell if you made an email error?



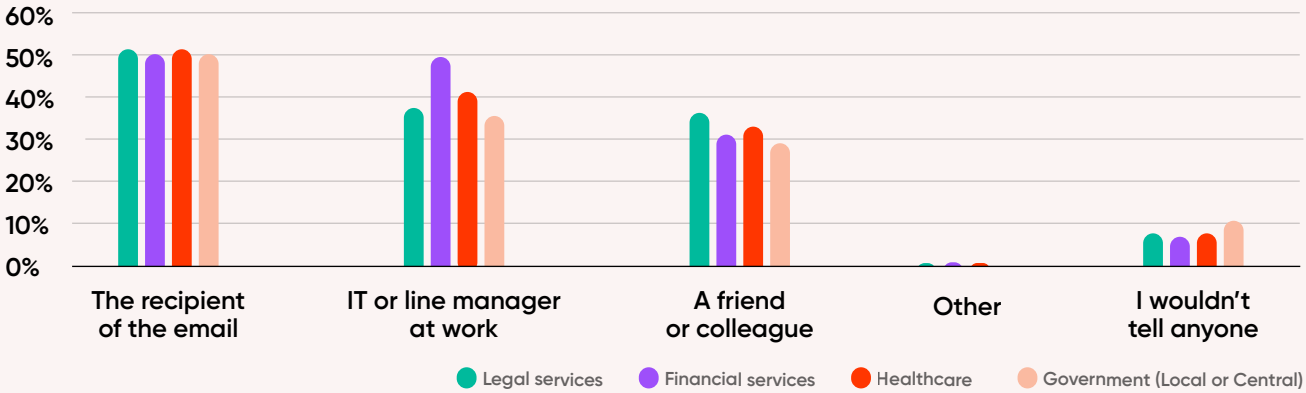
> Self reporting alone is not a solution. After making an email mistake, 50% of employees would notify the unintended recipient directly, and 9% state they wouldn't tell anybody at all.

The low reporting rate stems from a culture where employees fear blame or simply view their errors as too minor to report. Organizations must foster a culture of openness where employees feel encouraged to report incidents without fear of repercussions in order to meet security benchmarks and compliance obligations. Clear reporting channels and regular reminders about their importance can help bridge this gap and improve IT visibility.

Employee: Regional split of incident reporting



Employee: Sector split of incident reporting

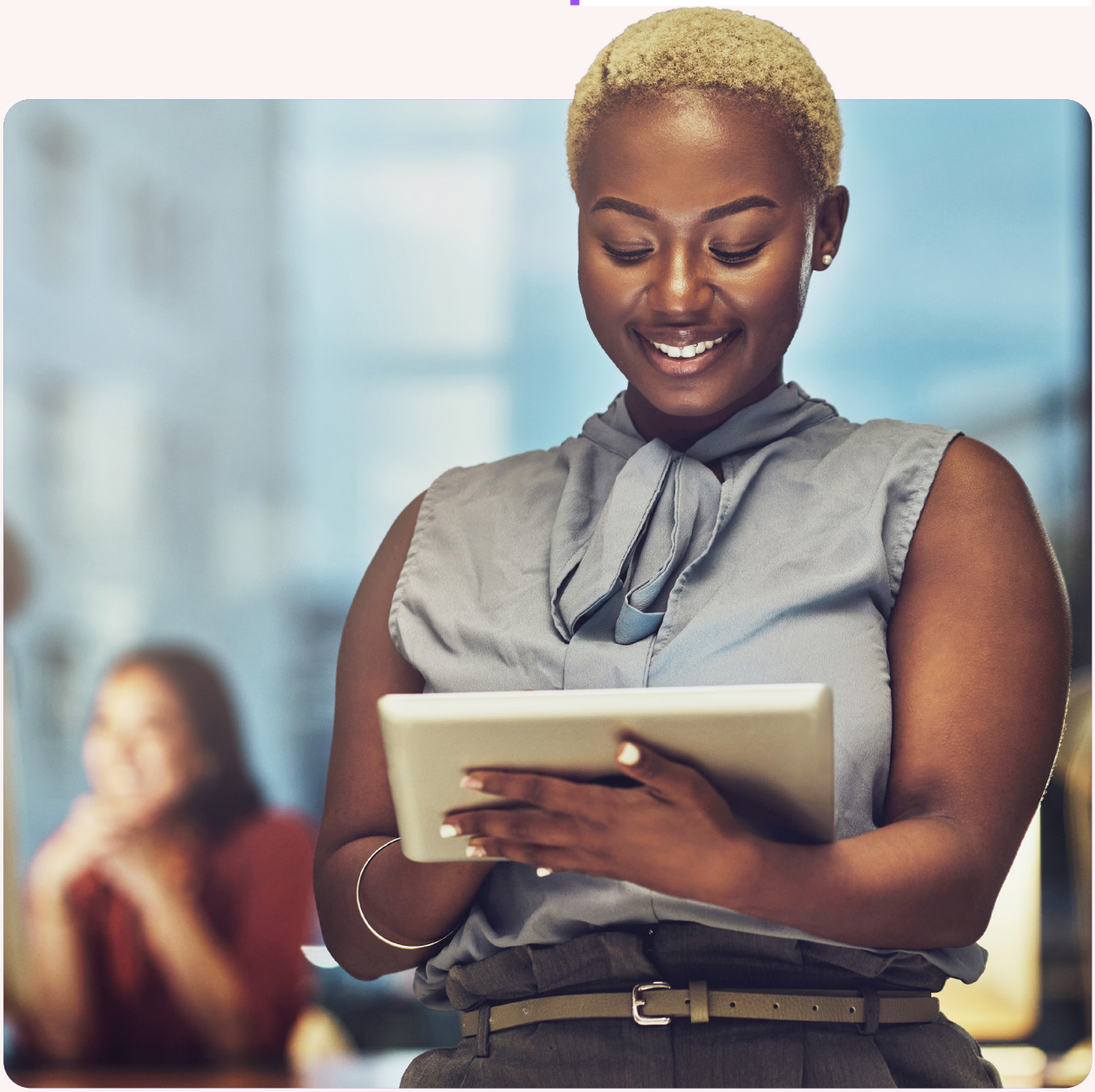


Making compliance a cultural norm

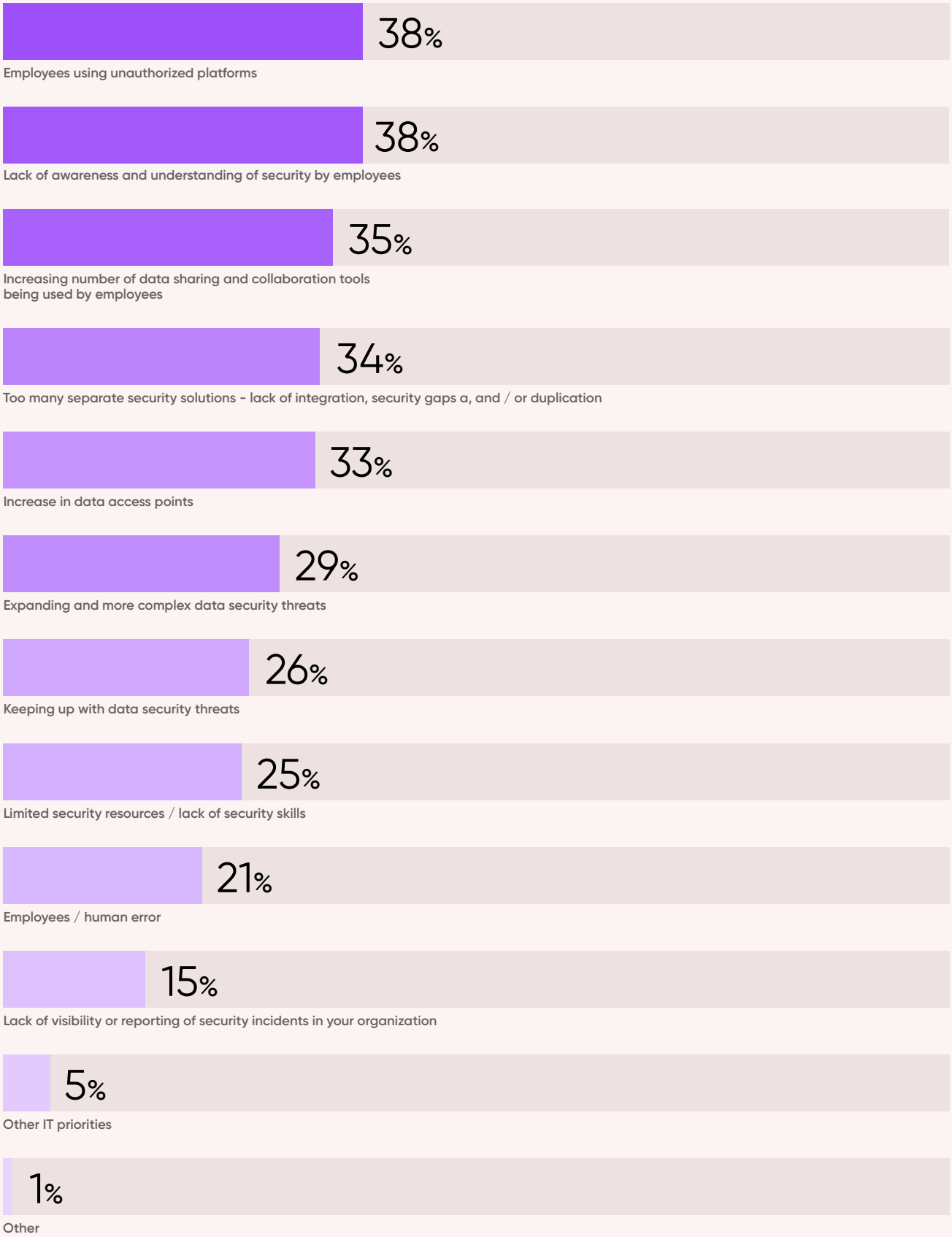
Employees using unauthorized platforms, a lack of security awareness among employees, and the increasing number of tools being used by staff are consistently ranked among the top three security vulnerabilities by IT leaders.

Employees are the common thread running through these top-ranked vulnerabilities, but they are the symptom rather than the cause. Employees simply reflect the environment in which they operate, and if the tools, training, and processes aren't in place to instill security as a cultural and operational goal, these vulnerabilities will persist.

> 54% of employees say that email accidents are most likely to happen when they are busy or tight on time, followed by feeling overwhelmed by too many messages or communication tools at 40%.

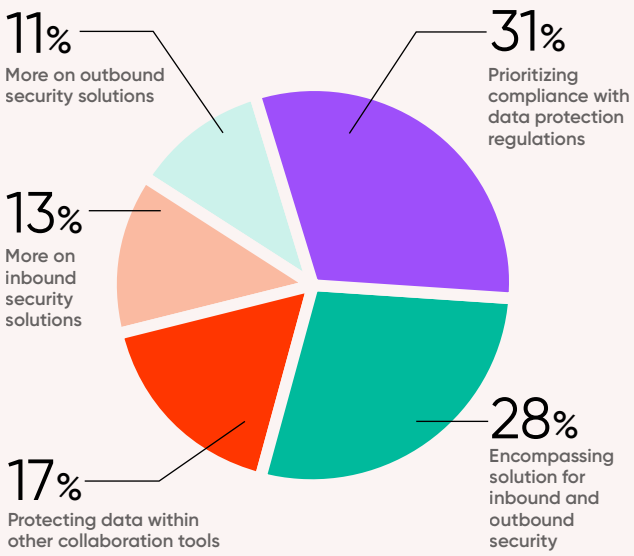


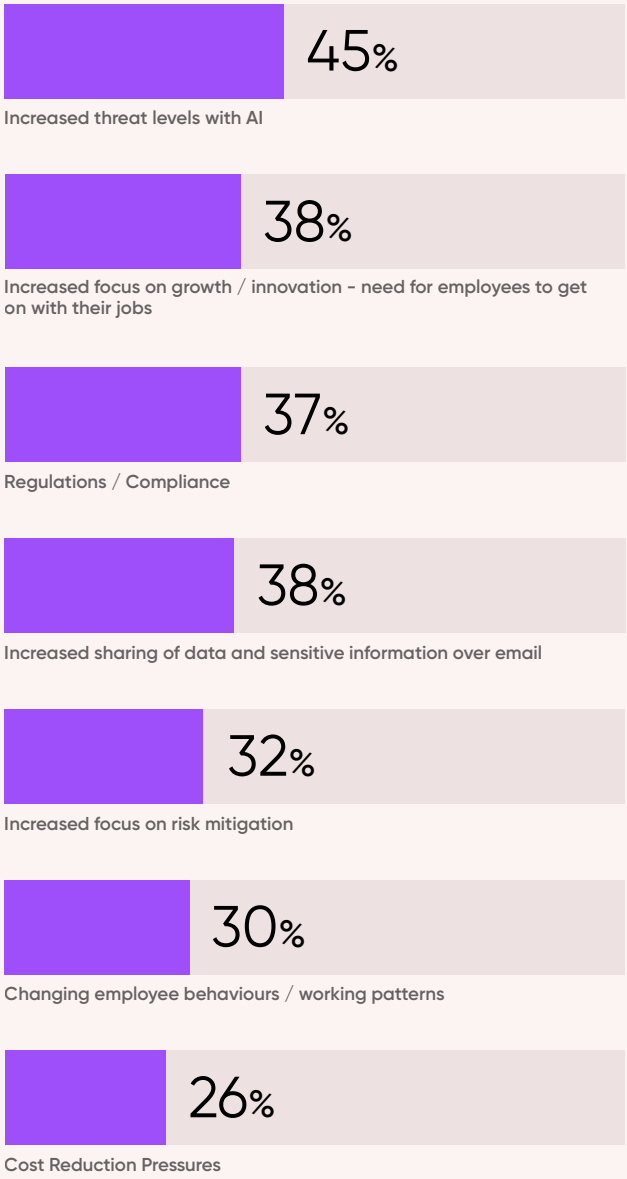
IT leaders: Biggest security vulnerabilities in organization



When asked what their primary email security focus for would be over the next two to three years, almost one-third of IT leaders (31%) said they would prioritize compliance with data protection regulations, and 28% said they would be looking for an "all encompassing" solution inbound and outbound security. Increased threat levels from AI, which is constantly being used to refine and sharpen phishing methods and tactics, was noted as the primary driver of these changes, with 45% of leaders citing it as their motivation for change. However, 4 in 10 (38%) cited regulatory pressures and concerns about compliance as their number one driver for change.

IT leaders: Main security focus for next 2-3 years | Drivers for security focus





Email security should be regarded as an operational challenge rather than a burden placed on employees. Almost 8 in 10 (78%) agree that it is vital to empower employees with tools and processes that allow them to share data securely and compliantly.

Email security checklist:

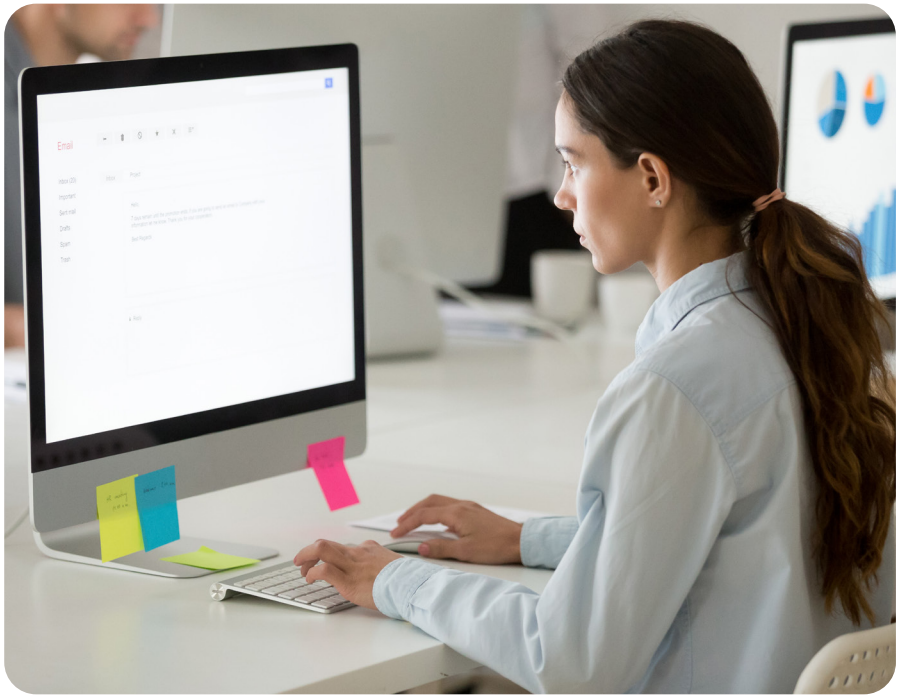
Given the evolving threat landscape and looming regulatory demands, it is clear that incremental improvements and reliance on legacy systems are insufficient. Organizations must make serious investments in advanced tools designed to assist employees and proactively prevent errors. This includes:

Align Security Practices with Regulatory Standards

- **Proactive Compliance:** Stay ahead of upcoming regulations like NIS2, DORA, and state-specific data protection laws by aligning security measures with international standards such as ISO 27001.

- **Regular Audits and Updates:** Conduct frequent security audits to identify vulnerabilities and ensure that policies, procedures, and technologies are up-to-date with the evolving regulatory landscape.

These proactive measures will not only address compliance obligations such as DORA and NIS2 directly but also reduce reliance on manual processes and improve employee confidence in email security.



People

Chapter 3

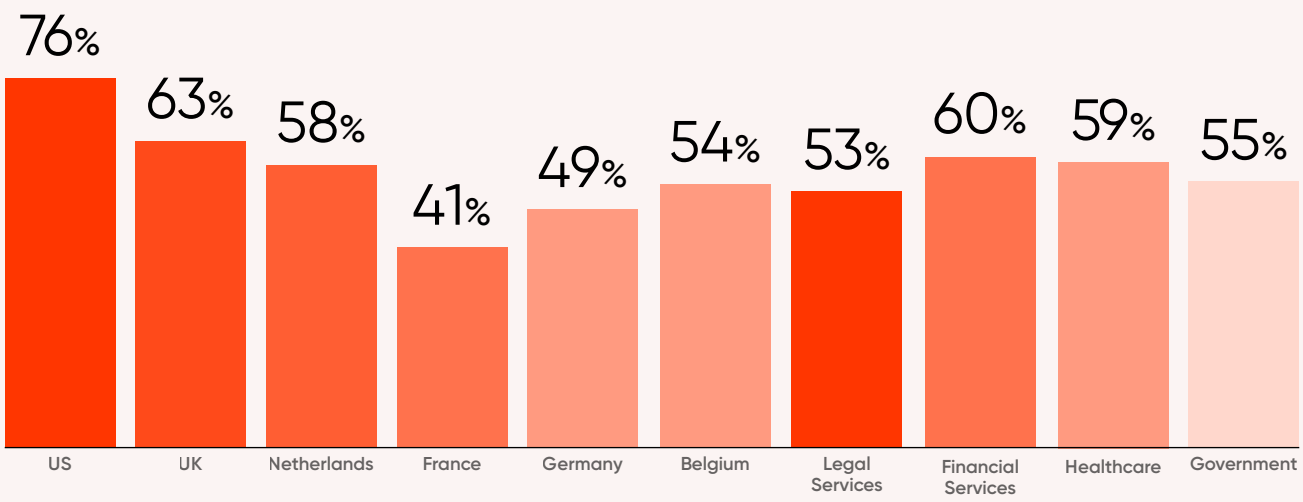
The power of integrated email security

Employees are calling out for more supportive measures to help them in meeting their organization's compliance requirements. We asked employees what the impact would be if their organization were to invest in technology that meant they do not need to worry about security when using email: 30% said they would be able to focus more on the quality of their work, 28% stated they would be more productive, and a further 28% said they would feel trusted by their employer.

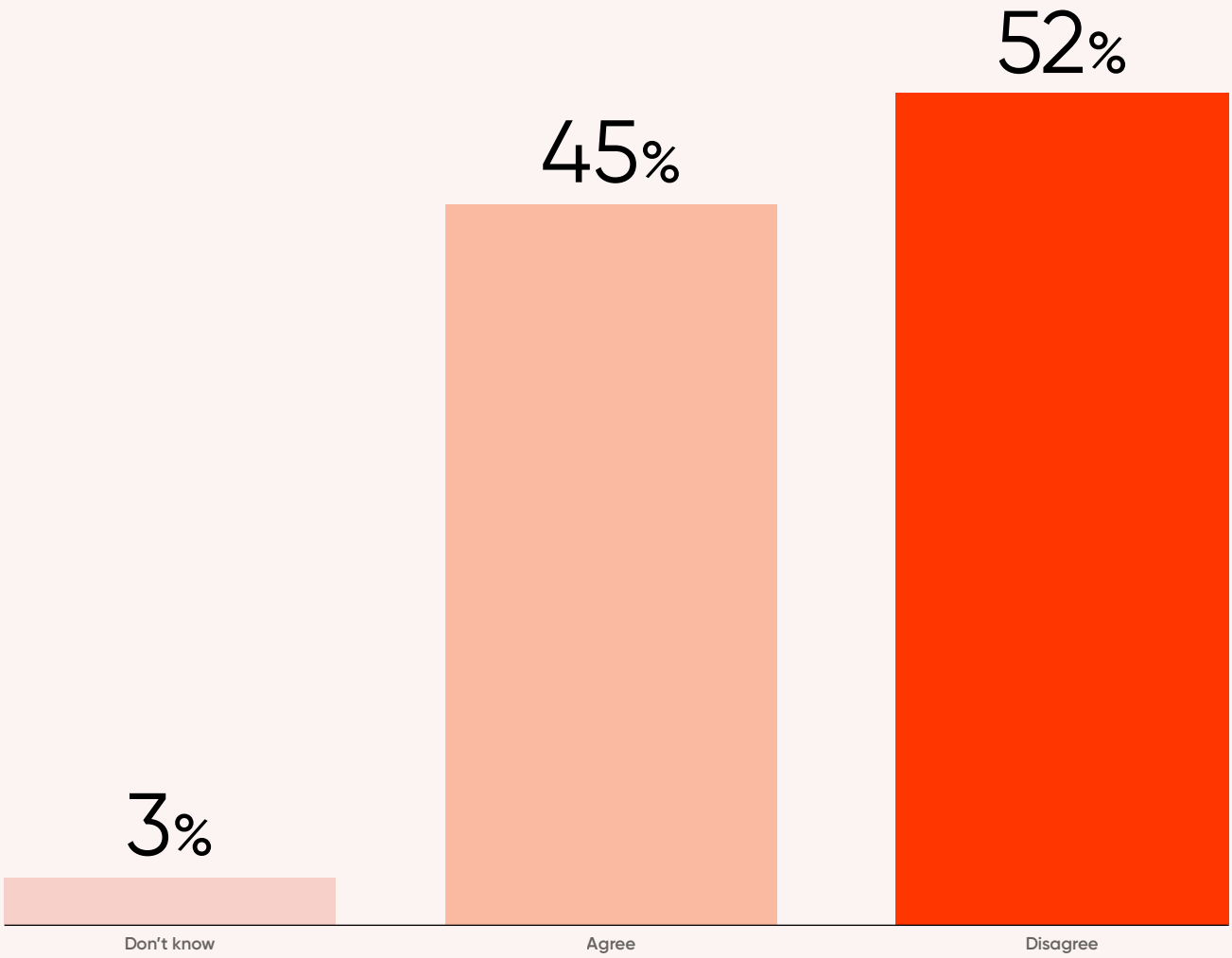
If employees truly are an organization's greatest security asset, policies must be clear and cohesive with their day-to-day workflows; otherwise, they will continue to make the wrong decisions. This is commonly known as the workaround problem.

Around 60% of employees say they frequently use IT policy workarounds to "get the job done" and save time or effort. When employees resort to manual workarounds, organizations lose visibility into the full scale of email-related risks and potentially expose themselves to compliance breaches. To bridge this gap, companies need to reevaluate how policies are communicated and executed in employee workflows.

% of employees agree: Most employees have their workarounds with IT policy to save time or effort | regional and sector split



Employee: I'm not clear on our company policy around email security



More than a third (34%) of workers in large organizations with more than 1,000 employees agree, "I'm not clear on our company policy around email security," increasing to 41% among smaller businesses with 250-999 employees.

Policy awareness gaps

Many employees lack a clear understanding of their organization's email security policies, with 38% saying they don't fully comprehend them. Among those who frequently make email mistakes, this confusion climbs to 52%, creating a direct link between policy understanding and the likelihood of making errors. Policies that are overly complex or not reinforced regularly can leave employees unsure, frustrated, and likely to see security policies as a barrier – rather than a support mechanism – in their day-to-day work.

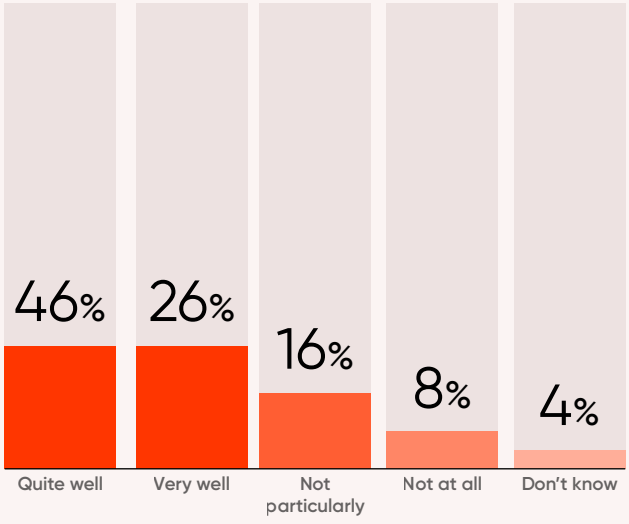
Employee: Attitudinal statements

Re-thinking email security training

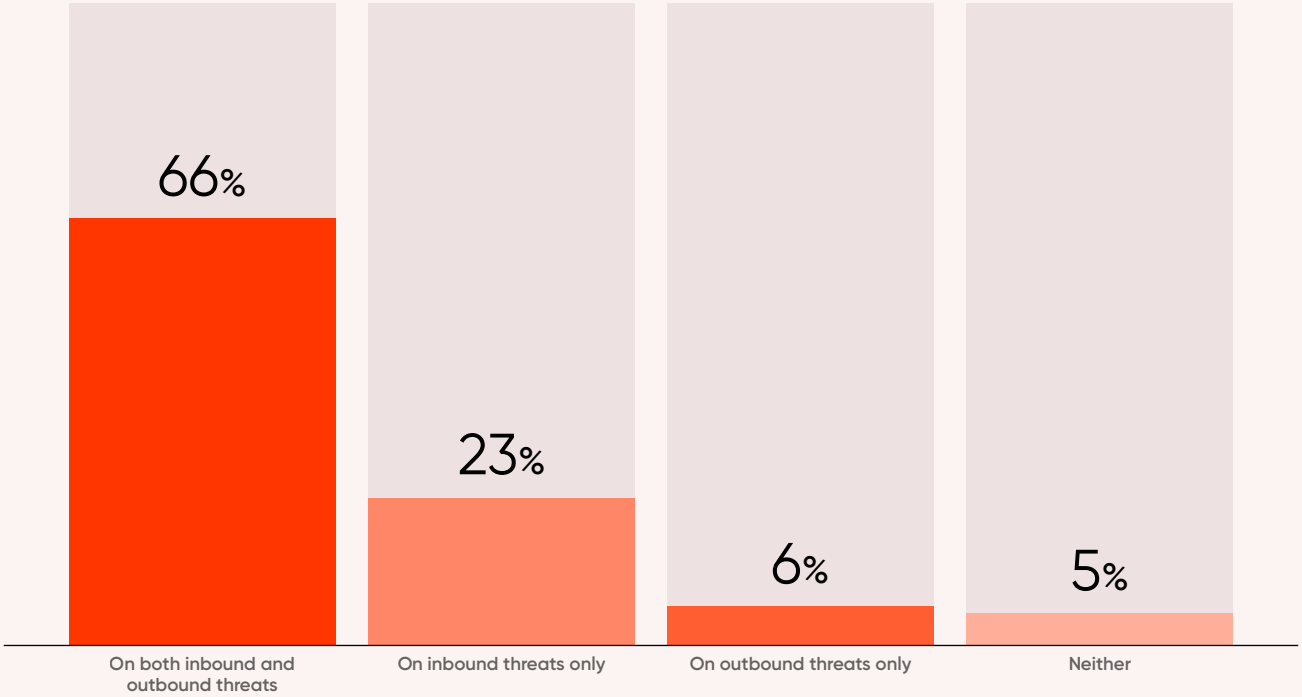
When it comes to email security policy, traditional training simply is not working. Regulations emphasize that employee awareness is key to compliance. However, while nearly all organizations provide some form of training, its effectiveness remains stubbornly limited, leaving employees dissatisfied and their organizations exposed.

Organizations recognize the importance of email security training, with 95% of IT leaders confirming its availability within their companies. Yet only 26% believe it drives significant improvements in employee behavior to safeguard data, and nearly half (46%) acknowledge that there is room for improvement. This rift between the prevalence of training and its perceived effectiveness points to fundamental flaws in its design and delivery.

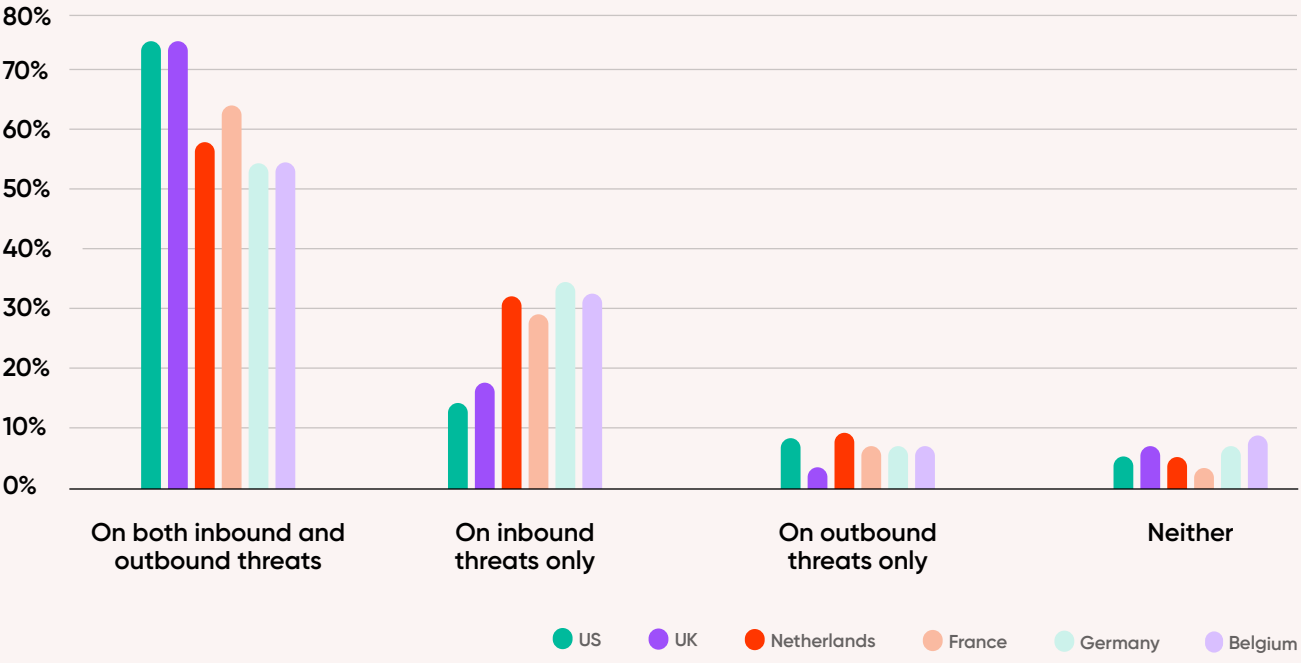
IT leaders: How well training impacts employee email behaviors



IT leaders: inbound and outbound email security training provision



Training provision - regional split



One critical issue is the static nature of many training programs, which often focus on broad compliance objectives rather than practical, actionable skills. As advancements in technology, such as AI-driven threats, continue to evolve, training programs must keep pace. Without addressing emerging risks or equipping employees to recognize and respond to potential data loss incidents, these programs will become outdated and ineffective.

Part of the reason training falls short is that it is often shaped around the organization rather than its employees. More than a third (36%) of employees across large organizations describe email security training as ineffective or a waste of time, and dissatisfaction increases to 54% among those who frequently make email mistakes. This group, which stands to benefit most from effective training, often feels that programs are overly generic and fail to address the specific challenges they encounter in their roles.

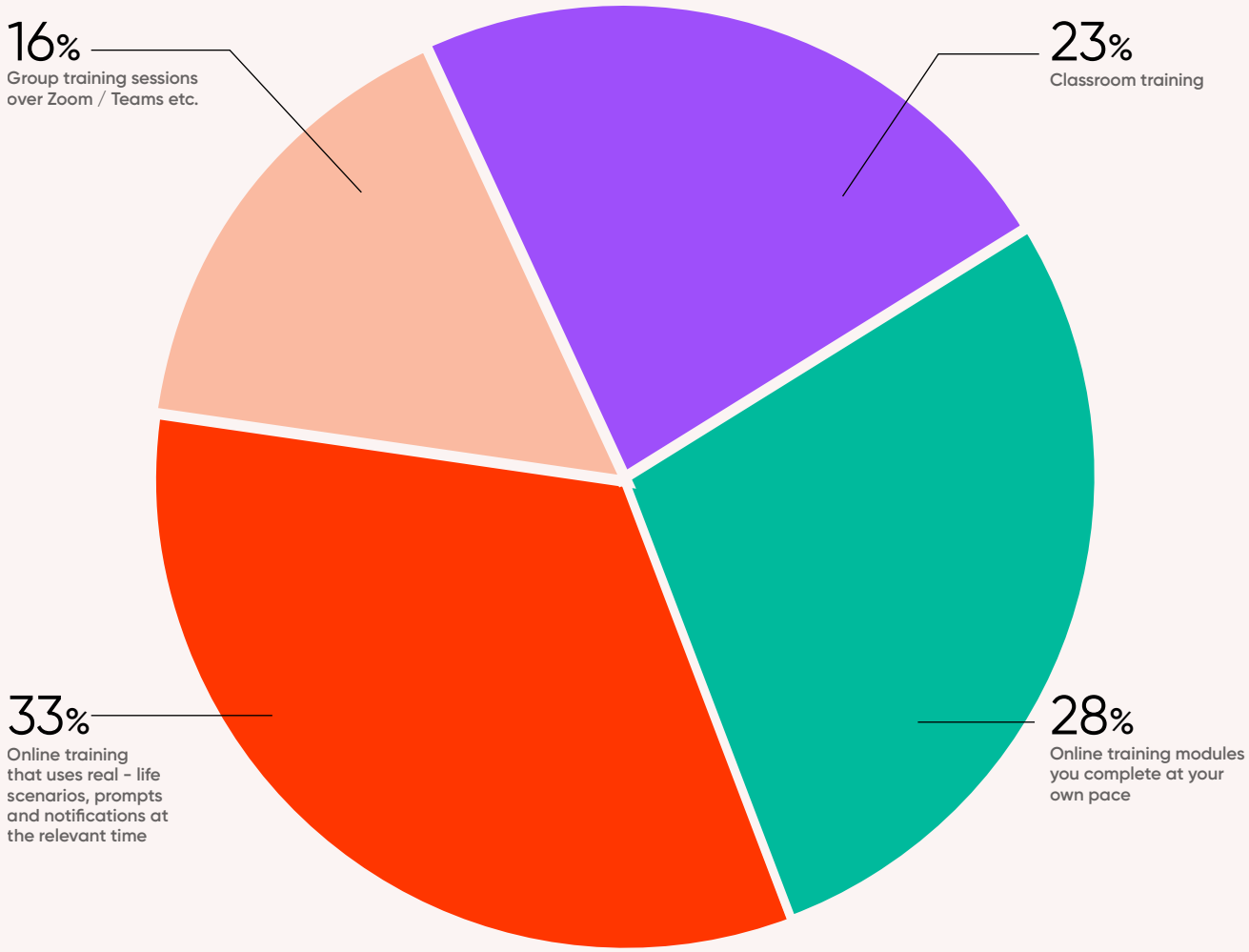
Employees also report frustration with training formats that rely on lengthy online modules or classroom-style lectures. These methods may fulfill compliance requirements but rarely engage employees or leave them with actionable takeaways. The lack of relevance to daily tasks only reinforces the perception that training is a box-ticking exercise rather than a valuable learning opportunity.

A lesson in training

Organizations need to consider how employees prefer to learn and how they can use those learnings to close compliance gaps. Our research shows that employees overwhelmingly prefer interactive and scenario-based training formats that mimic real-world situations. Immediate prompts and contextual feedback, integrated into their daily workflows, are particularly effective for reinforcing secure behaviors.

For example, interactive simulations that replicate phishing attempts or outbound email mistakes can help employees identify risks and understand the consequences of errors in a controlled environment. Role-specific training modules tailored to different job functions can also make sessions more relevant and engaging. These approaches not only improve retention but also foster a greater sense of responsibility and confidence among employees.

Employee: Most engaging / effective email security training format



Email security checklist:

Enabling compliant, secure workflows goes hand in hand with training. For lasting change, organizations must embed these practices within a broader cultural shift toward openness and accountability. This involves:

Investment in Advanced Email Security Solutions

- **Adopt AI-Powered Security Platforms:** Implement intelligent email security systems that utilize artificial intelligence and machine learning to detect and block sophisticated phishing attacks, spear-phishing, and zero-day threats.

- **Real-Time Error Prevention Tools:** Equip employees with tools that provide real-time alerts for potential mistakes, such as misaddressed emails or incorrect attachments, helping to prevent data leaks before they occur. These tools must prioritize simplicity and user experience, such as providing one-click encryption or intuitive phishing alerts, to ensure employees can adhere to security policies without difficulty.

- **Policy Enforcement:** Clearly define and enforce email security policies, ensuring employees understand the importance of compliance and the procedures for handling sensitive information.

Enhance Employee Training and Awareness Development

- **Interactive and Engaging Training:** Develop training that is interactive, scenario-based, and tailored to various employee roles and age groups to increase engagement and retention.

- **Continuous Education:** Implement ongoing training initiatives, integrated into daily workflows, rather than one-time sessions to keep employees educated and updated on the latest threats and best practices in email security.

When combined with improved training methods, these cultural changes can drive a more engaged and security-conscious workforce, significantly reducing the risks associated with email communication.

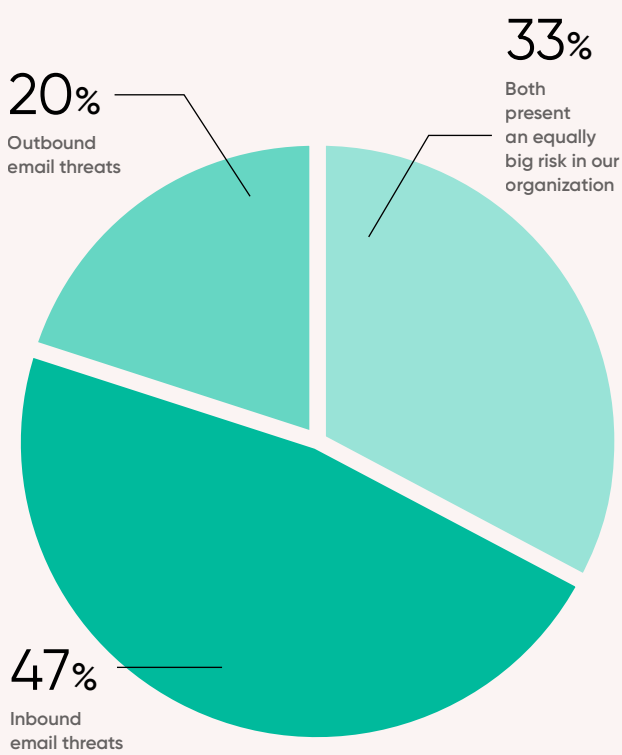
Conclusion

A call to action for leadership

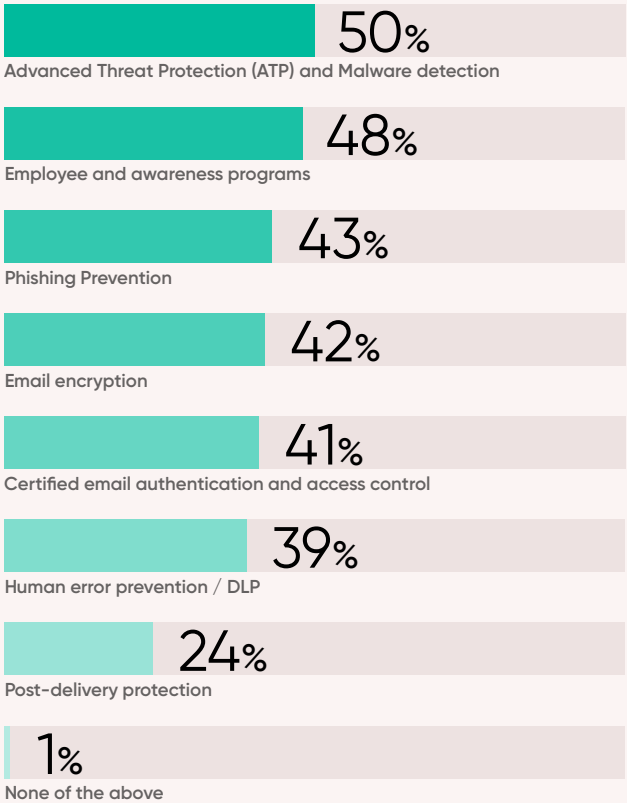
Improving email security must be an urgent priority for leadership. The risks of inaction are clear and costly: rising data breaches, substantial financial penalties, erosion of customer trust, and even personal liability for executives under new regulations.

Leadership must ensure that security investments are strategically aligned with the most pressing threats facing their organization. With only 24% of IT leaders highly confident in their current alignment, this gap leaves critical vulnerabilities unaddressed. Outbound email security, often sidelined in favor of inbound threat mitigation, demands equal attention to protect against data leaks and human error. Redirecting investments toward comprehensive solutions that address these overlooked risks is essential to building a resilient and effective security framework; solutions that not only support compliance but demonstrate tangible business value: a key factor in securing leadership buy-in for future investments. Fewer than one in four IT leaders believe their current security spending aligns well with the risks their organizations are encountering.

IT: Biggest risk in terms of potential data loss



Priorities of email security investment



Leaders must adopt a structured, proactive approach to secure email systems, focusing on five critical pillars:

1. **Conduct a Comprehensive Email Security Audit**
2. **Invest in Advanced Email Security Solutions**
3. **Adopt Robust Encryption and Authentication Protocols**
4. **Enable Staff through Comprehensive Data Leak Prevention Strategies**
5. **Foster a Culture of Security**

IT: Biggest risk in terms of potential data loss

By taking these steps, organizations can transform email security from a silent vulnerability into a powerful strategic asset. This shift not only ensures regulatory compliance but also strengthens competitive positioning, enhances operational resilience, and builds trust with customers and stakeholders.

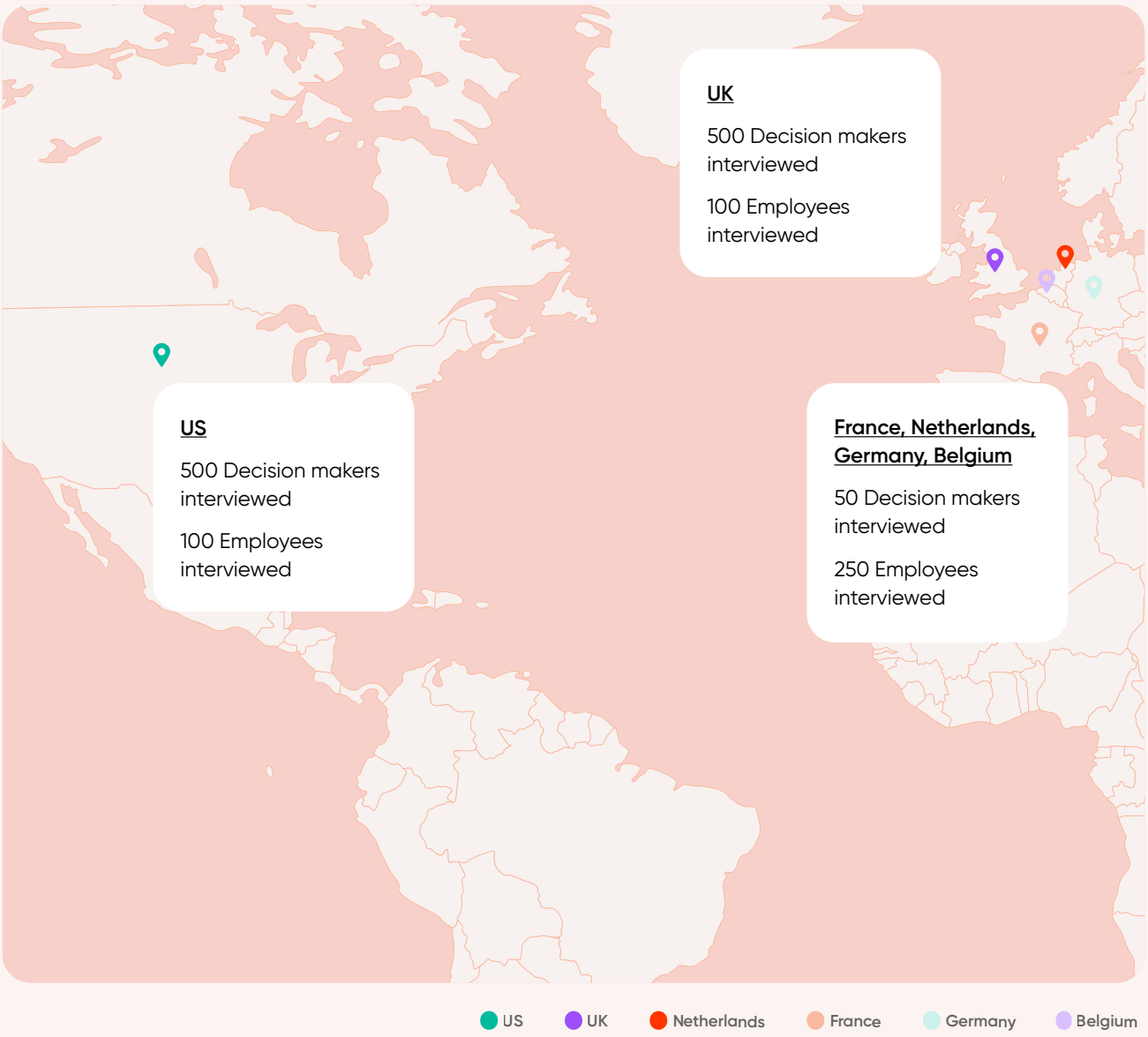
As 2025 approaches, improving email security is not just a strategic imperative—it is a compliance necessity. New legislations now hold board members personally liable for cybersecurity failures, making decisive action essential. Robust encryption and authentication are no longer optional but critical to securing communication channels against the escalating sophistication of cyberattacks.

In a world where the margin for error is narrowing and the consequences of negligence are escalating, the time to act is now. By investing in robust security solutions, advancing employee education, and aligning practices with international standards, organizations can mitigate risks, protect their most critical communication channels, and ensure email remains a trusted cornerstone of business success.

Methodology

The study was conducted in October 2024 and surveyed 400 IT decision-makers and 2,000 employees across multiple regions, including the US, UK, Netherlands, France, Germany, and Belgium. The IT participants were responsible for or heavily involved in their organization's email security strategy and represented companies with 250 or more employees across various sectors. Employees who participated also worked in organizations with over 250 employees, providing insights into daily email security practices. The study balanced responses from both groups to capture contrasting perceptions on email security risks, training effectiveness, and evolving threats, focusing on top-level insights to ensure reliable, actionable findings across all sectors.

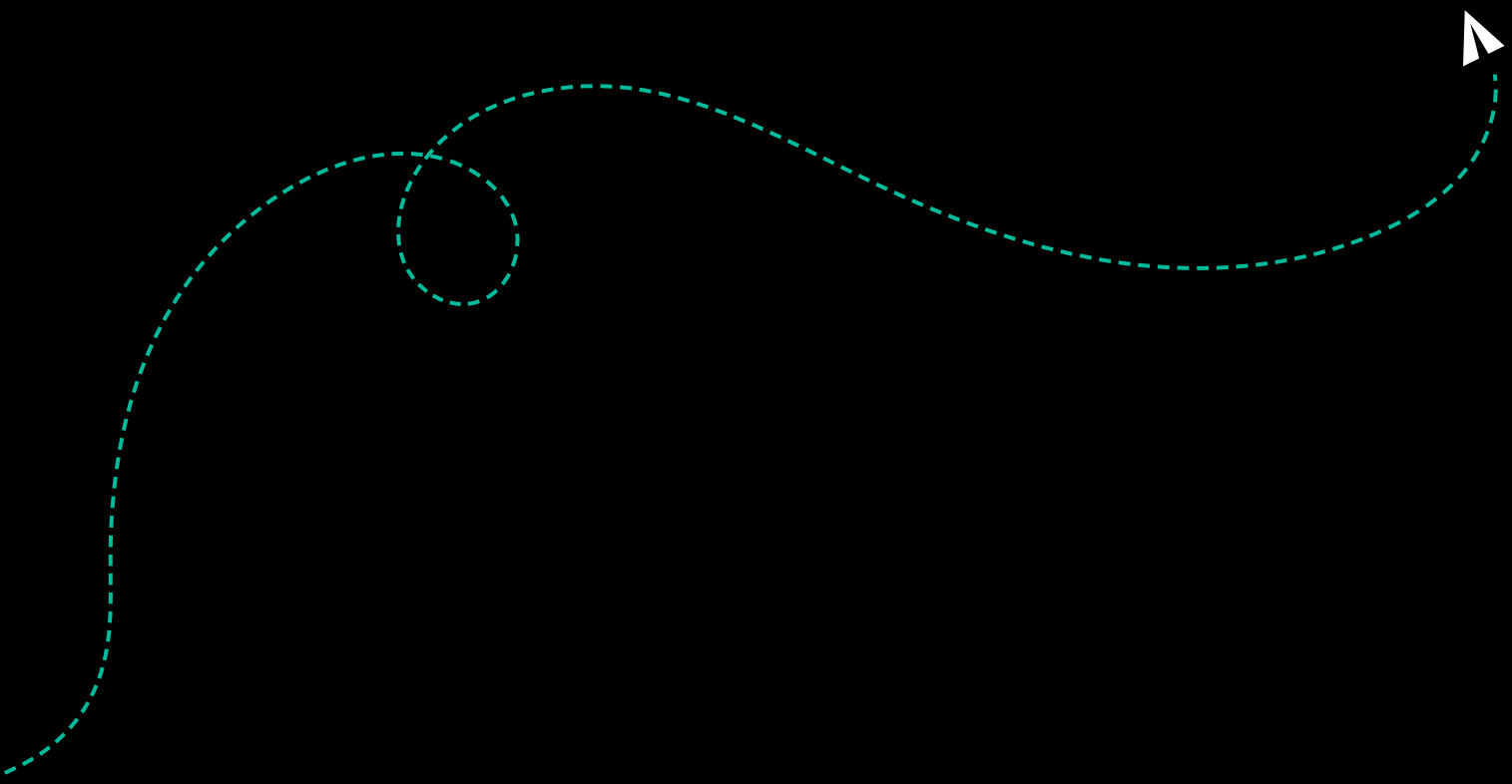
IT and Employee Regional sample breakdown



Index

statista.com/statistics/1203667/total-personal-data-breaches-europe

ico.org.uk/action-weve-taken/data-security-incident-trends



zivver