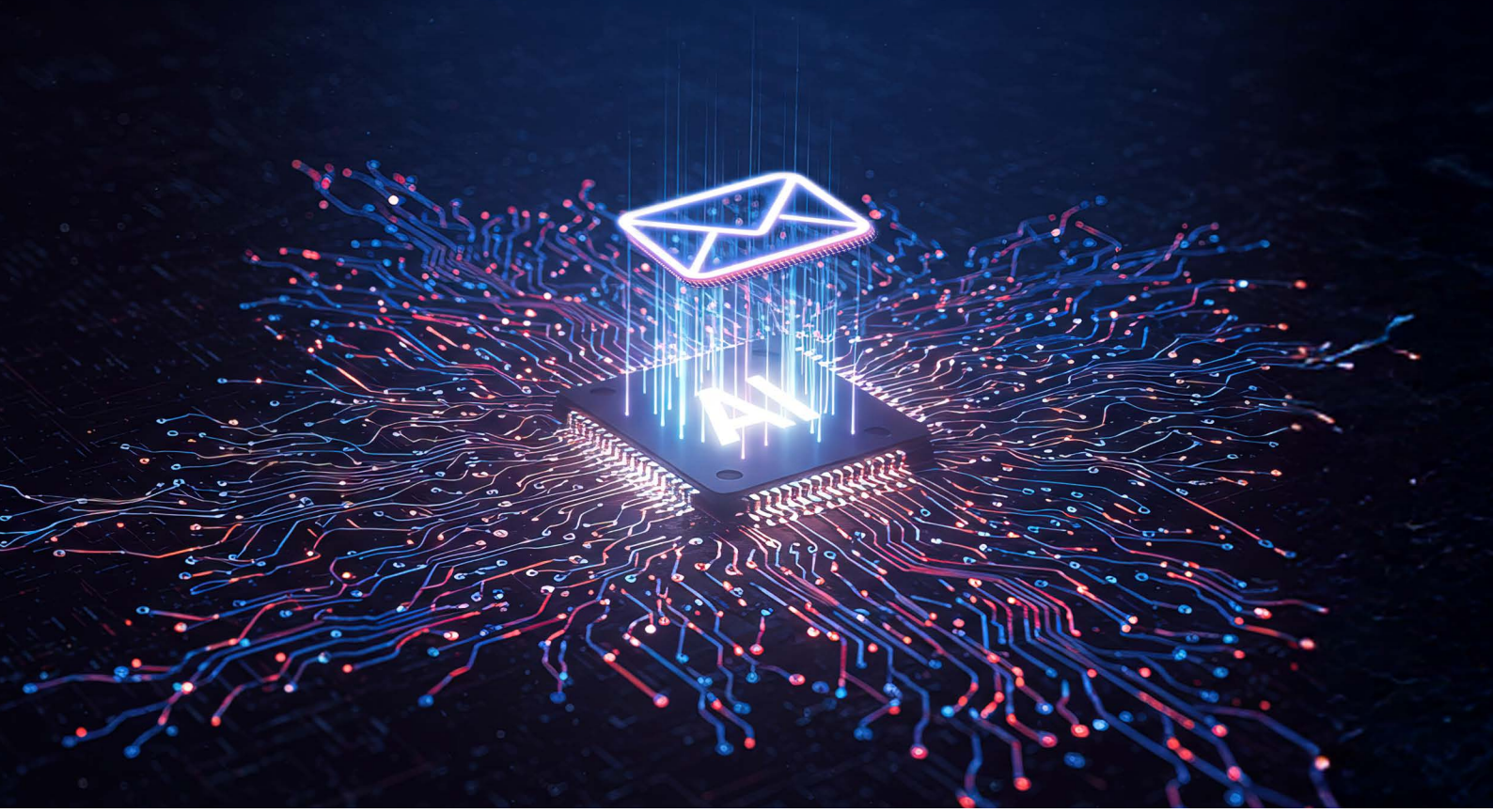
SENDMARC

2025 Cyberthreat Report:

Email security & DMARC in the age of AI



What's inside

Introduction

As generative artificial intelligence (GenAI) advances, its influence on cybersecurity is impossible to ignore. AI helps organizations detect and respond to attacks faster. Adoption has surged, with **72% of companies** integrating AI into at least one business function in 2024 - a 55% increase from the previous year.

Yet this rapid growth is also driving a new era of cybercrime. AI-enabled phishing campaigns, deepfake scams, and Business Email Compromise (BEC) schemes are growing more convincing and harder to detect. In one case, a deepfake video call was used to defraud a multinational company of over **$25 million**. Internal adoption also creates new attack vectors, giving malicious actors fresh opportunities to exploit unapproved or insecure tools.

In this shifting landscape, one fact hasn't changed: Email remains a cornerstone of global business communication, connecting employees, customers, and partners around the world. This means securing it is no longer optional - it's critical to business continuity.

The financial impact of cyberattacks in 2024 was significant, with the global average cost of a data breach exceeding **$4 million** for businesses, and cybercrime costing the world **over $9 trillion**. And with GenAI-powered email attacks advancing, the stakes are higher for organizations that don't take their email security seriously.

"In a world of GenAI, securing your email identity matters more than ever before."

- Sam Hutchinson, Sendmarc Co-Founder and CEO

This report explores how evolving threats, new global regulations, and authentication standards like **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** are reshaping the email security landscape in 2025.

Notes:

1. The statistics in this report are drawn from multiple studies and datasets. Each figure should be understood within the context of its original source.
2. All monetary amounts have been standardized and are shown in U.S. dollars (USD) for consistency.
3. DMARC protects against email-based impersonation, spoofing, phishing, and domain misuse but cannot stop all cyberattacks. Threats like ransomware delivered through other channels, insider breaches, and supply chain attacks require a layered approach that includes authentication, monitoring, user training, and broader security measures. This report aims to raise awareness and support Sendmarc's mission to make the Internet safer for all.

Key findings & trends

Global email by the numbers in 2024

361B+
emails sent & received daily

4.4B+
email users

Over 55%
of the global population used email

Trending cyberthreats

A world-record
$75 million ransom
was paid by a Fortune 50 company

A third of breaches
involved ransomware/extortion

BEC was the second-costliest cybercrime, totaling almost
$3 billion

68%

Human actions or errors played a role in
68% of breaches

AI

Experts warn that GenAI is accelerating credential theft and insider risks, making attacks faster, stealthier, and easier to scale.

40%

Percentage of **BEC attacks** that are AI-generated

78%

Amount of employees who used **unapproved AI tools** at work, fueling major cyber incidents

The state of DMARC

The global DMARC market
is projected to hit
$38.8 billion by 2032

DMARC adoption
increased by 60% after Google & Yahoo's 2024 mandates

DMARCbis
(DMARC 2.0)
is coming

Why email remains irreplaceable - and at risk

In 2025, email is still the backbone of business communication.

While collaboration platforms like Teams, Slack, and WhatsApp may have surged in popularity, they remain proprietary and siloed - you can't Slack someone on WhatsApp.

But email is an open and universal standard. It's essential for communication, transactions, customer support, and the countless processes that keep businesses running.

Email by numbers:
Billions of users, billions of risks

Email use reached extraordinary heights in 2024. People around the world sent over **361 billion** emails daily - that's almost 4.2 million every second. And the numbers are still climbing, with daily volumes projected to exceed **424 billion** by 2028.

The growth in email users tells a similar story. In 2024, there were more than 4.4 billion users – representing over half of the world's population at roughly 55.2%. By 2028, this is expected to rise to over **4.9 billion users**, reinforcing email's position as a key communication channel for both consumers and businesses.

Email remains critical for organizations - and a prime target for attackers. Left unprotected, it becomes a vulnerability that could devastate your organization.

Without security standards like **DMARC**, **Sender Policy Framework (SPF)**, and **DomainKeys Identified Mail (DKIM)**, companies of all sizes are vulnerable to email-based spoofing, phishing, and impersonation attacks.

This dependence on email, combined with weak authentication and the rise of GenAI, has driven the growth of increasingly sophisticated email threats over the past year.

To understand the true global impact, it's important to see how different regions are being targeted - something we explore in the following section.

The global picture:
Email security threats by region

United States

The United States reported the world's highest cybercrime losses in 2024, exceeding **$16 billion** - a **33% increase compared to 2023**. The Federal Bureau of Investigation's Internet Crime Complaint Center (FBI IC3) received over 800 000 complaints in 2024, with phishing/spoofing accounting for the highest complaint volume.

Latin America

A major cyber readiness gap persists in Latin America: only **seven of 32 nations** have critical infrastructure protection plans, and just 20 have Computer Security Incident Response Teams (CSIRTs).

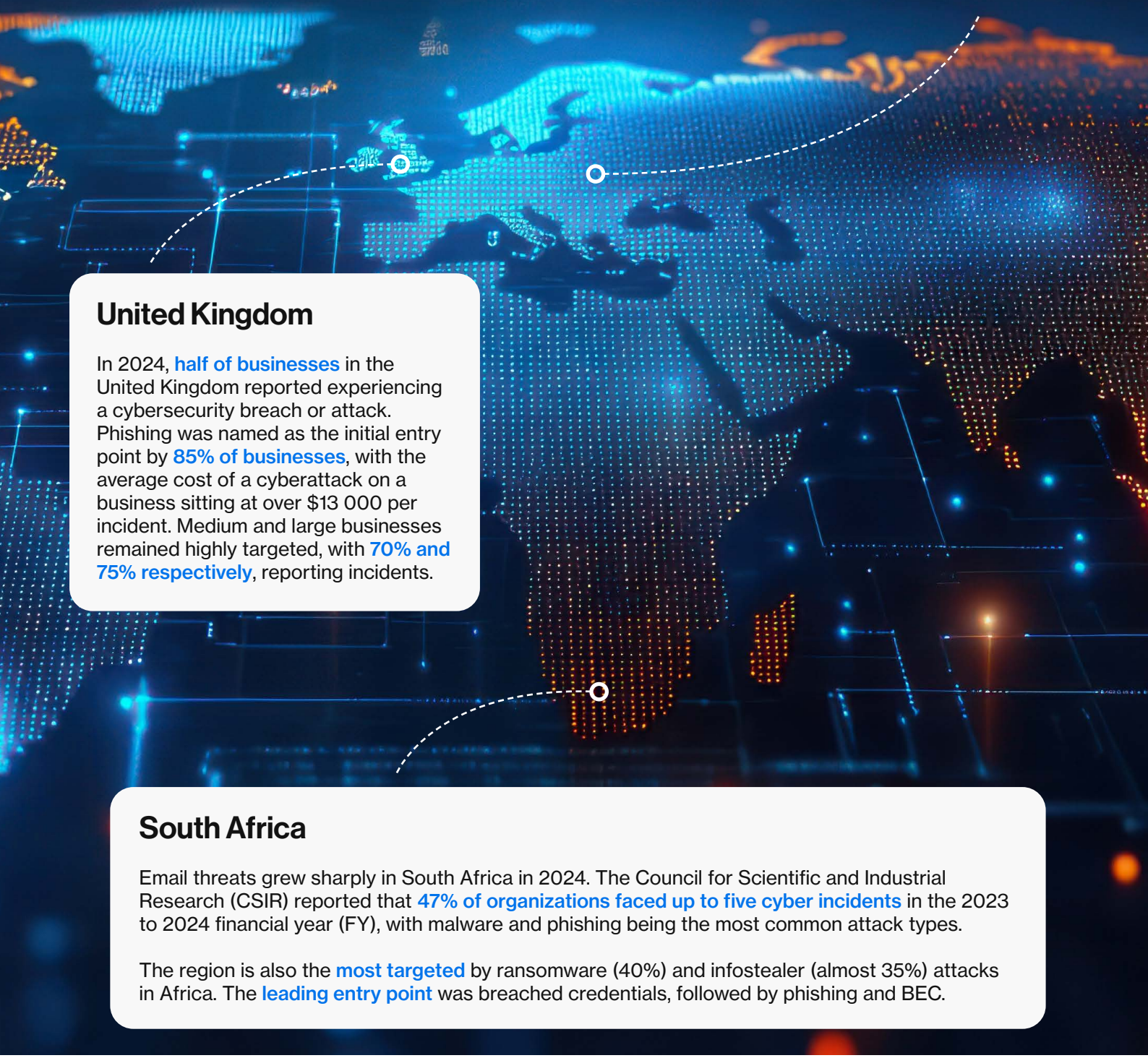
This vulnerability drives rising cybercrime, projected to cost over **$90 million** annually in 2025. While **94% of cybersecurity professionals** support adopting a risk-management framework, limited resources and stakeholder resistance continue to prevent progress across the region.

The global picture: Email security threats by region

Europe

In Europe, phishing attacks increased by **91.5%** between April 2023 and April 2024, and BEC incidents also rose by nearly **124%** in European enterprises.

The EU's Agency for Cybersecurity (**ENISA**) found that ransomware was the second most common attack type for H2 2023 to H1 2024, while threat actors relied on tools such as FraudGPT and large language models (LLMs) to generate more convincing scam emails.



United Kingdom

In 2024, **half of businesses** in the United Kingdom reported experiencing a cybersecurity breach or attack. Phishing was named as the initial entry point by **85% of businesses**, with the average cost of a cyberattack on a business sitting at over $13 000 per incident. Medium and large businesses remained highly targeted, with **70% and 75% respectively**, reporting incidents.

South Africa

Email threats grew sharply in South Africa in 2024. The Council for Scientific and Industrial Research (CSIR) reported that **47% of organizations faced up to five cyber incidents** in the 2023 to 2024 financial year (FY), with malware and phishing being the most common attack types.

The region is also the **most targeted** by ransomware (40%) and infostealer (almost 35%) attacks in Africa. The **leading entry point** was breached credentials, followed by phishing and BEC.

The global picture: Email security threats by region

China

Chinese businesses experienced a **70% increase** in cyberattacks from 2023 to 2024, with the cost of cybercrime in the region reaching **$15 billion**. The nation faced **five million** attack attempts per day and ranked **number one** globally for data breaches, with breached accounts skyrocketing 340 times compared to 2023.

India

Cybercrime in India surged in 2024, with financial losses up **206%** to over $27 billion as reported cases rose by **over 42%** from 2023 to more than **22 million**. Phishing was a leading driver: security researchers recorded over **80 million** phishing attempts against Indian users, placing the country second globally and accounting for one-third of all attacks across Asia-Pacific.

Australia

The Australian Signals Directorate (ASD) received over 87 000 cybercrime reports in the 2023 to 2024 FY, an average of one every **six minutes**. Data breaches hit a record high of **over 1 100 incidents**, while phishing attempts topped **30.2 million**, ranking Australia as the **eighth most-targeted country** worldwide.

Expert's point of view on email security

Not securing your business email is an **open door for threat** actors. There is enough social information available for scraping or buying to **social engineer** anyone these days. By not securing your email you're placing a 'come on in' sign for those looking to exploit.

James Abercrombie
Global Community Lead at Acronis

Acronis

Under attack: Top business threats in 2025

For businesses, the danger isn't just that cyberthreats are increasing - it's that they're becoming smarter.

AI is helping attackers fine-tune their methods, from impersonation to extortion, faster than many businesses can strengthen their defenses. In this section, we unpack the top threats to your business in 2025 and where AI is raising the stakes.

Top threats

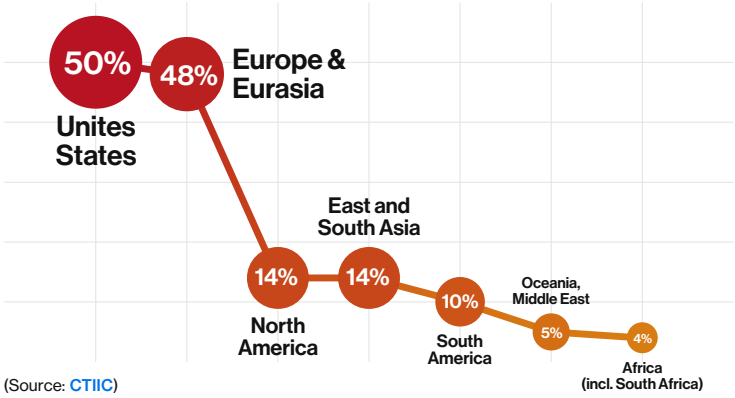
1 Ransomware & extortion attacks

Few threats were as disruptive in 2024 as ransomware and extortion. Nearly one in three breaches involved these attacks, which drove costs close to $5 million in just the first half of the year, making them one of the most persistent and costly global risks.

Over half of ransomware attacks in Q3 were delivered via email, which Hornet Security identifies as the most consistently used delivery channel between 2022 and 2024.

Worldwide ransomware attacks by region

Ransomware is most common in advanced economies, but emerging markets aren't risk-free - underscoring the need for stronger cybersecurity worldwide.



(Source: CTIIC)

Manufacturing, healthcare, finance, and critical infrastructure were among the hardest hit industries. Notable cases included a $22 million ransom paid by Change Healthcare and a world-record $75 million ransom paid by an undisclosed Fortune 50 company.

Ransomware has become one of the most dangerous threats to healthcare, where disruption can mean more than financial loss - it can cost lives. Since 2015, attacks on hospitals and medical facilities have risen by more than 300%, forcing emergency services to divert patients, delaying urgent treatments, and in some cases contributing to fatalities.

When one hospital becomes a ransomware victim, nearby hospitals feel the impact too, with one study recording an 81% spike in cardiac arrest cases and decreased survival rates for those patients when a neighboring facility was under attack.

A recent example saw Synnovis, an NHS pathology provider in London, crippled by ransomware, halting blood tests, transfusions, and urgent cancer care across multiple hospitals.

These incidents underscore that in healthcare, ransomware isn't just a business or IT crisis - it's a direct threat to human life.

In recent years, attackers have escalated their methods with double and triple extortion schemes, pressuring not only the primary victim but also their partners and clients.

> **AI amplified these threats, powering adaptive malware, convincing phishing campaigns, and Ransomware-as-a-Service (RaaS) platforms that allowed less skilled cybercriminals to launch faster, more advanced attacks.**

Despite increased law enforcement pressure that forced some ransomware groups to rebrand and change tactics, the overall threat persisted. Across all sectors, organizations faced record financial and operational damage, as increasingly sophisticated, AI-driven attacks fueled a rise in global extortion activity.

Top threats

2 Human manipulation & deception

Cybercriminals continued to exploit the human factor in 2024, with manipulation and deception ranking among the most widespread risks worldwide.

Human actions or errors played a role in 68% of breaches, while social engineering and phishing drove at least 22%, affecting 42% of organizations globally.

The National Computer Emergency Response Team found that phishing was Argentina's top incident type in 2024 at 31%, down from 75% in 2023, a sign that attack methods are diversifying in the region.

Global campaigns also became more targeted and spread across email, voice, video, and messaging applications. Cybercrooks turned to LLMs and GenAI to automate spear-phishing, producing messages that looked more authentic than ever.

Attackers also used AI to automate open-source data harvesting and deployed deepfake video or voice calls to impersonate executives so they could divert payments or steal sensitive information. In one case, scammers created a fake WhatsApp profile and used an AI-cloned voice of WPP's CEO to lure executives into a fraudulent Teams call.

> **Companies across all industries worldwide faced persistent BEC and impersonation last year. The FBI reported losses of almost $3 billion, cementing BEC as the second most financially damaging cybercrime.**

High-profile incidents highlighted the dangers of human manipulation and deception: European retailer Pepco Group lost about $16.8 million in a phishing attack linked to BEC, while in Australia, a man was charged after a BEC scam drained roughly $1.35 million from a Sydney hospital through multiple fraudulent email-led transfers.

Top threats

3 Credential abuse & insider threats

Stolen credentials and insider threats proved especially damaging in 2024, giving attackers a direct route into organizations and causing disruption across businesses of every size.

About 88% of breaches in the Basic Web Application Attacks category involved stolen credentials, which, along with social engineering, remained key entry methods for financially motivated bad actors.

Research also shows that malicious insider incidents were the costliest initial breach vector, averaging $4.92 million per case, while compromised credentials, including account takeover (ATO) attacks, cost organizations $4.67 million on average per breach.

Email ATO was a growing concern, often following credential compromise. Hijacked accounts enabled internal phishing campaigns that were hard to detect and expensive to contain.

Across all regions, security specialists warn that GenAI is accelerating credential theft and insider risks, making attacks faster, harder to spot, and easier to scale. In South Africa, small and mid-sized businesses (SMBs) were hit especially hard, facing 143% more attacks per user than larger organizations, and 22% of those were forced to shut down.

Top threats

4 Supply chain & third-party risk

Supply chain and third-party attacks surged in 2024, driven by growing digital interdependence and complex vendor networks. As a result, protecting against these risks has become a top priority for cybersecurity teams worldwide.

According to IBM, compromises involving supply chain and external partners were the **second most common initial attack vector**, responsible for 15% of all breaches. These breaches were especially damaging, costing nearly $5 million per incident on average and taking the longest to resolve - about 267 days from identification to containment.

In 2024, AI reshaped the landscape, weaponizing trusted business relationships to drive a surge in supply-chain email attacks.

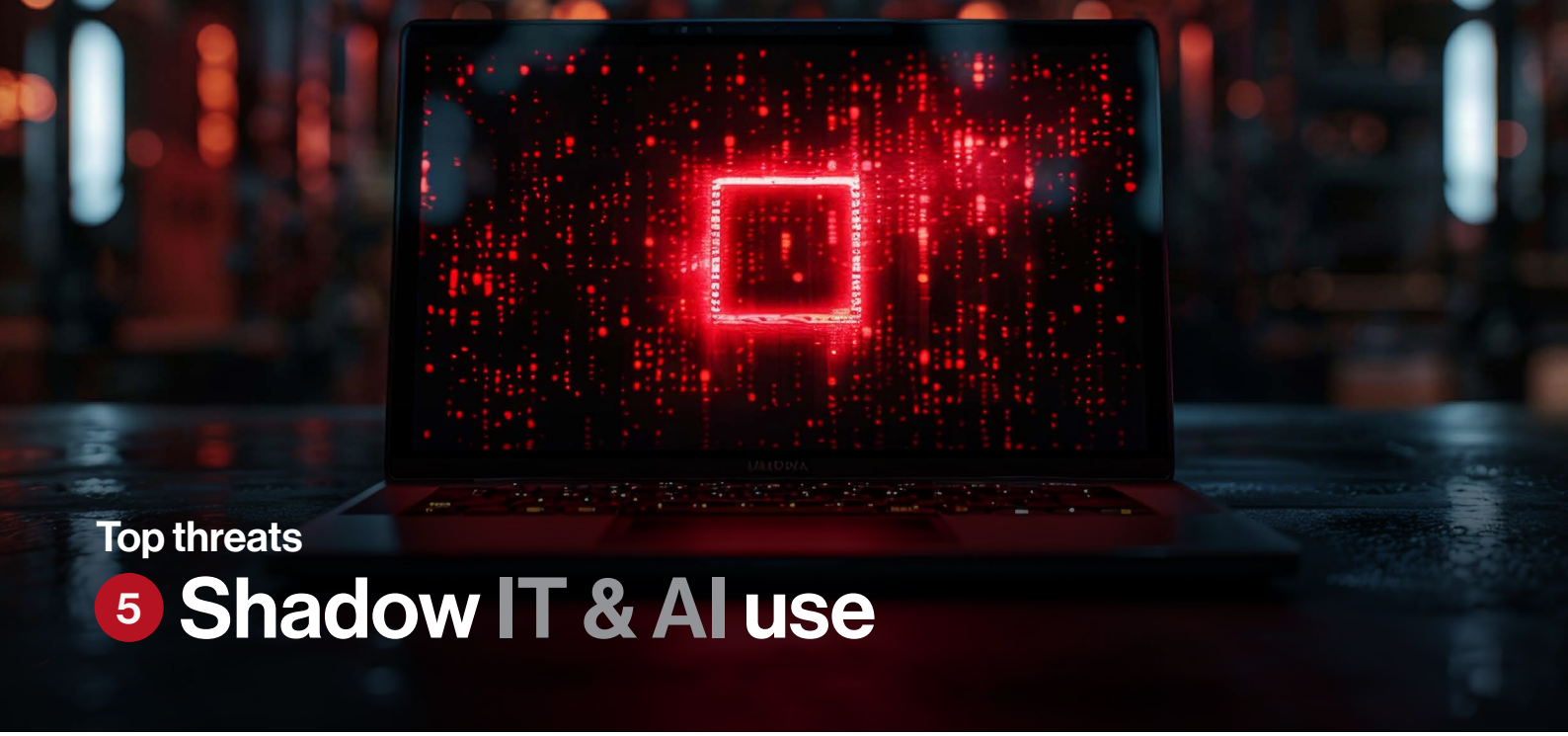
AI-powered campaigns evolved from phishing to sophisticated **multi-vector campaigns** that exploited vendor relationships, with **40% of BEC attacks** being AI-generated, and Vendor Email Compromise (VEC) incidents rising **66%** in the first half of 2024.

The convergence of AI automation, deepfake impersonation, and the complexity of modern supply chains enabled attackers to deliver convincing, personalized threats across **entire business ecosystems**, exposing critical gaps in traditional email security frameworks.

According to Verizon, third-party involvement accounted for **15% of breaches** last year - a sharp 68% jump from the previous year. These compromises extended beyond direct vendors to partner infrastructure and indirect software supply chains.

The impact has been particularly severe in Europe, where **ENISA** named supply chain compromise one of the region's "prime threats" for 2024. Organizations continue to struggle with visibility across expansive vendor networks, as attackers exploit weak links like misconfigured APIs, outdated systems, and unsecured open-source components.

> **The result is a rising wave of supply chain - driven breaches that ripple far beyond the initial victim, threatening entire business ecosystems.**



Top threats

5 Shadow IT & AI use

Unapproved technology - from shadow IT systems to unauthorized AI tools - created some of 2024's most overlooked but dangerous security gaps. IBM reported that breaches involving shadow AI affected 20% of organizations, adding an average of $670 000 to the cost of a breach.

These incidents carried serious consequences, exposing personally identifiable information (PII) in 65% of cases and intellectual property in 40%. The compromised data was stored across numerous environments, indicating that the use of just one unapproved AI tool can lead to far-reaching exposure.

Forrester predicted that 60% of the workforce would adopt AI tools without IT's approval in 2024, but the reality went even further.

Microsoft's data shows that the bring your own AI (BYOAI) trend was in full force, with 78% of employees already using personal AI tools at work - a trend even stronger in SMBs, at 80%. Why? Because AI helps employees in smaller teams scale and automate work. And BYOAI isn't just a Gen Z trend; it's taking hold across generations.

> **But while these tools are helping employees manage their workloads, the dangers of shadow AI use in businesses cannot be overstated.**

A Disney employee installed an unapproved AI art tool containing malware that led to a staggering breach exposing 44 million internal Slack messages and gave attackers access to credentials for Disney's internal systems stored in the employee's unsecured 1Password account.

In another example, Samsung engineers leaked proprietary source code by uploading it to ChatGPT without authorization, leading to an organization-wide ban on GenAI use on company devices and networks. This leak was the seed of broader concerns about the security risk of LLMs and the storage of user-submitted data.

The use of shadow IT and shadow AI each introduces serious risks – and when combined, they create a new wave of vulnerabilities. As unsanctioned tools spread faster than organizations can secure them, the potential for disruption only grows. Without oversight and clear security policies, businesses risk losing control of their technology environments.

The state of DMARC in 2025

DMARCbis: The next evolution of DMARC

What is DMARCbis?

DMARCbis, also known as DMARC 2.0, is the most significant update to the DMARC standard since its introduction. It's currently an IETF draft, designed to supersede older DMARC RFCs by elevating DMARC from an "Informational" document to a "Proposed Standard", reflecting its important role and broad adoption in email authentication for over a decade.

Why the update?

The updated standard provides clearer rules, more straightforward language, improved domain handling, and enhanced reporting, while ensuring backward compatibility with existing DMARC records.

When is it coming?

Expected publication:

2025

What's new?

- **Clearer rules and language:** Guidance is now precise, reducing confusion for both senders and receivers.
- **Defined participation rules:** Clarifies what full DMARC participation means - domain owners must publish a DMARC record and analyze reports. Emails must pass SPF and DKIM checks, while receivers must evaluate records and send daily feedback to domain owners.
- **Updated tags:** New tags add control; '`psd=`' (public suffix domains), '`t=`' (testing mode), '`np=`' (non-existent subdomain policy). Older tags like `pct`, `rf`, and `ri` are being retired. (See what new tags do)
- **Improved domain handling:** Uses DNS Tree Walk instead of the Public Suffix List to ensure DMARC application is correct and consistent for complex domains.
- **Refined reporting:** Aggregate XML reports are stricter and better aligned with how email works, improving visibility into delivery and security issues.

Why it matters for your organization

While `v=DMARC1` records remain valid, aligning with `DMARC 2.0` ensures stronger protection and prepares organizations for future compliance requirements. The updates are designed to provide clear guidance and improve defenses against spoofing, but interpreting new tags and reporting standards can be complex without a dedicated DMARC solution.

Early alignment delivers stronger security, better visibility, and regulatory readiness, benefits that can be achieved fully and simply through a managed approach rather than manual effort.

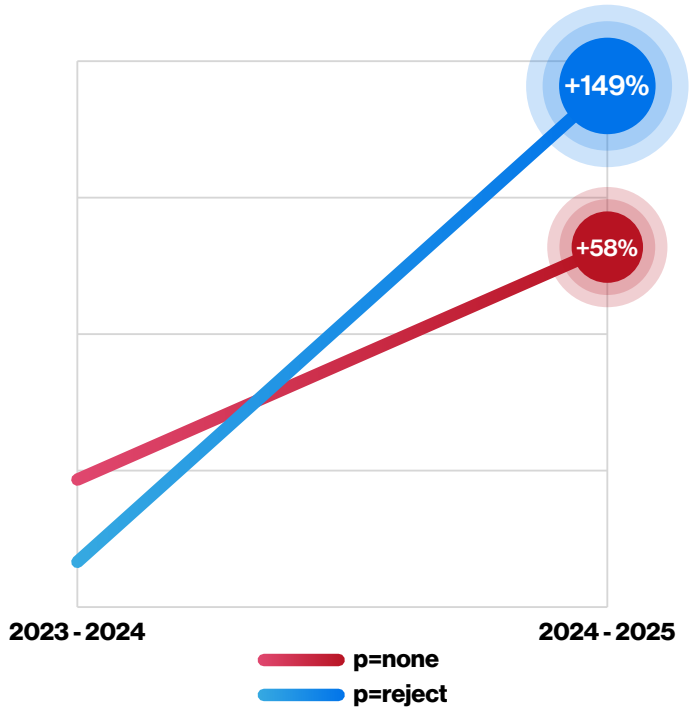
Read more about DMARCbis

DMARC adoption accelerates:
Global shift toward p=reject

Sendmarc observed a **58% increase in DMARC adoption** worldwide between July 2023 to 2024 and July 2024 to 2025. Even more significant is that the number of domains enforcing a **p=reject policy grew by 149%** over the same period.

This sharp rise reflects a global shift away from monitoring-only policies (p=none) towards full enforcement with p=reject, the strongest form of email authentication. The trend signals that more organizations are prioritizing protection against spoofing, phishing, and email-based impersonation attacks, aligning with regulatory momentum and growing awareness of email security risks.

Domain policy percentage increase:



Data from Sendmarc
(July 2023 to 2024 vs. July 2024 to 2025)

Key changes & announcements

In 2024 and 2025, DMARC has evolved from a best practice to a formal requirement across various sectors worldwide.

February 2024:

Google & Yahoo mandate DMARC for bulk senders (p=none)

December 2024:

CISA BOD 25-01 requires U.S. federal agencies to implement DMARC (p=reject)

Ongoing since 2024:

United Kingdom/European public sector guidance strongly recommends DMARC

March 2025:

PCI DSS v4.0 requires the adoption of anti-phishing mechanisms for organizations that process card payments, and recommends DMARC

May 2025:

Microsoft mandates DMARC for bulk senders

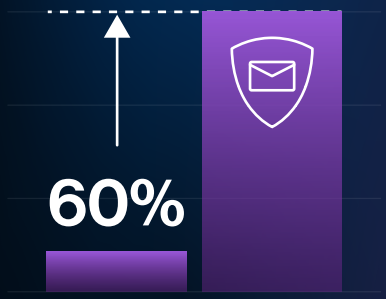
July 2025:

Cloudflare requires all emails sent through its Email Routing platform to pass SPF or DKIM and strongly recommends DMARC

November 2025:

Google tightens enforcement of its sender rules, resulting in temporary and permanent rejections for non-compliant emails, a sign that all senders (not just bulk) must comply for reliable deliverability

See a breakdown of international DMARC mandates and email security regulations here.



Google & Yahoo's Feb 2024 DMARC deadline drove a 60% rise in email domains with valid DMARC records in just two months.

$38.8B
Expected global DMARC market value by 2032

14.34%
Compound Annual Growth Rate (CAGR) of the global DMARC market from 2025 – 2032

Expert's point of view on DMARC regulations

Over the past few years, the email landscape has undergone significant shifts. What began in 2024 with Google and Yahoo mandating DMARC for bulk senders has now been reinforced by Microsoft in 2025, signaling a **growing global movement** toward stronger email authentication.

These developments mark the start of a fundamental shift in **how outbound email is secured.** To stay ahead, organizations must ensure their domains are **fully protected with DMARC**, implemented in a way that strengthens security without compromising email deliverability.

Angus Shaw
Managing Director at Brigantia Partners Limited

Trusted cybersecurity advisor

brigantia by ELOVADE

Myth vs. reality:
Email security misconceptions debunked

Myth 1:

"Anti-spam is enough to protect my emails."

Reality: Spam filters block junk mail, but they can't stop targeted impersonation attacks like CEO fraud or phishing. DMARC authenticates senders and prevents spoofed emails from ever reaching your team, partners, or customers. You need both for a layered and complete email security strategy.

Myth 2:

"I'm not responsible for the security of my outbound emails - they can't damage my business anyway."

Reality: One fake email delivered to a supplier, customer, or partner can cause devastating, and possibly irreparable, financial and reputational damage to your company. As a responsible online citizen, you are accountable for protecting your domain. Securing outbound email with DMARC ensures every message sent in your name is legitimate and trusted.

Myth 3:

"Implementing DMARC will block my legitimate emails."

Reality: When correctly set up, DMARC doesn't block your real emails - it stops impostors from abusing your domain. Misconfiguration causes delivery issues, not DMARC itself. With proper deployment, you protect stakeholders without disrupting legitimate communication. This is why it's important to leverage a trusted provider instead of doing it manually yourself, or when rolling out updates like DMARCbis.

Myth 4:

"Adopting DMARC at p=none is fine - I'm compliant."

Reality: A DMARC record at p=none may help you meet some regulations, but it only monitors; it doesn't protect. As rules tighten worldwide, real security - and compliance – will require enforcement at p=reject to block fake emails before they can cause harm.

Myth 5:

“I haven’t had any phishing attempts in my business - I don’t need DMARC.”

> **Reality:** Without DMARC, you lack visibility into phishing or other fraudulent use of your domain. Cybercriminals may already be sending fake emails without your knowledge, and these can reach the inboxes of your customers, partners, or any other stakeholders - exposing your business to serious financial and reputational damage.

Myth 6:

“I can use the DMARC reports I already get to analyze my email environment.”

> **Reality:** DMARC reports arrive as raw XML files that are difficult to read, and domain owners often receive thousands from different providers. Even skilled staff would need to spend hours decoding them manually. A proper DMARC solution consolidates this data into one clear dashboard, saving time and giving full visibility of domain activity.

Myth 7:

“We’re an SMB. Cybercriminals would rather go after bigger fish.”

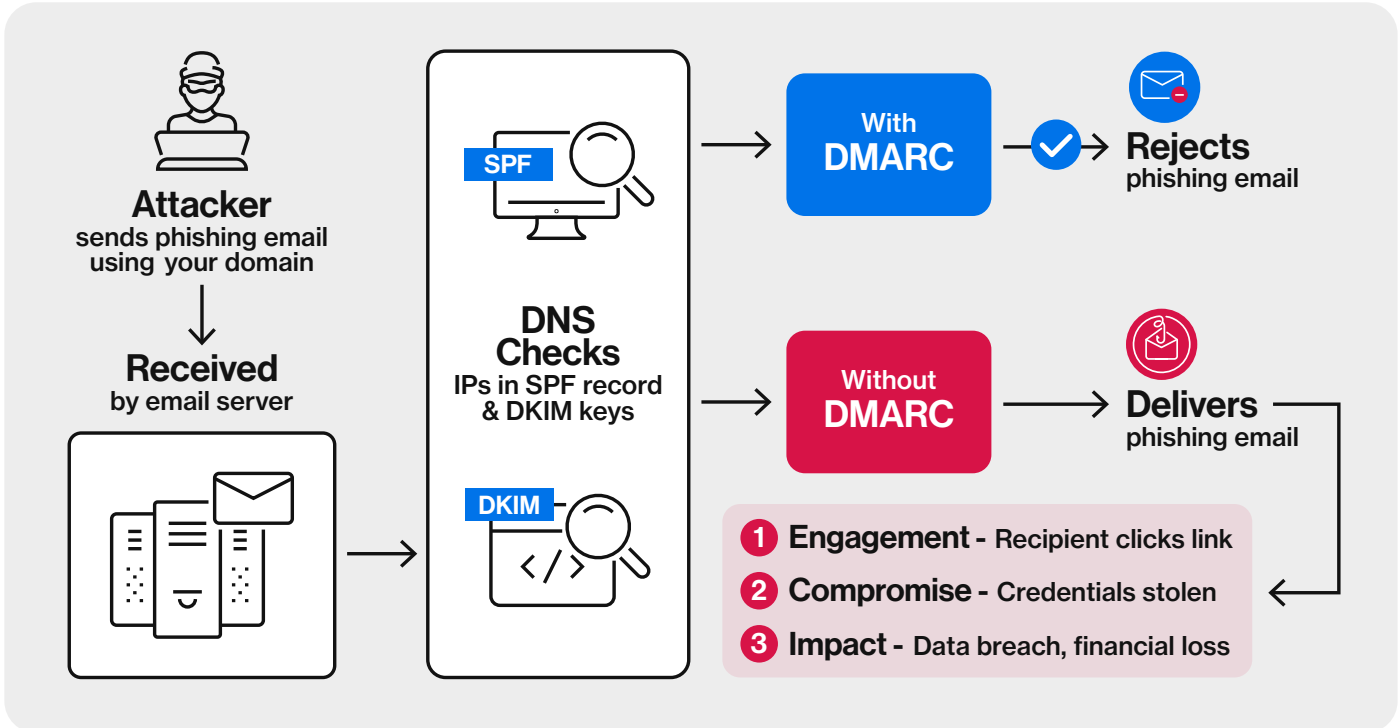
> Size doesn’t matter to cybercriminals - the opportunity does. SMBs are often attractive targets precisely because they lack the security budgets and protection of larger enterprises, making them easier to exploit. Even one spoofed email can compromise customer trust, drain funds, or shut down operations. DMARC closes this gap by protecting your domain, no matter the size of your business.

What to do next:
Proactive steps for improved protection

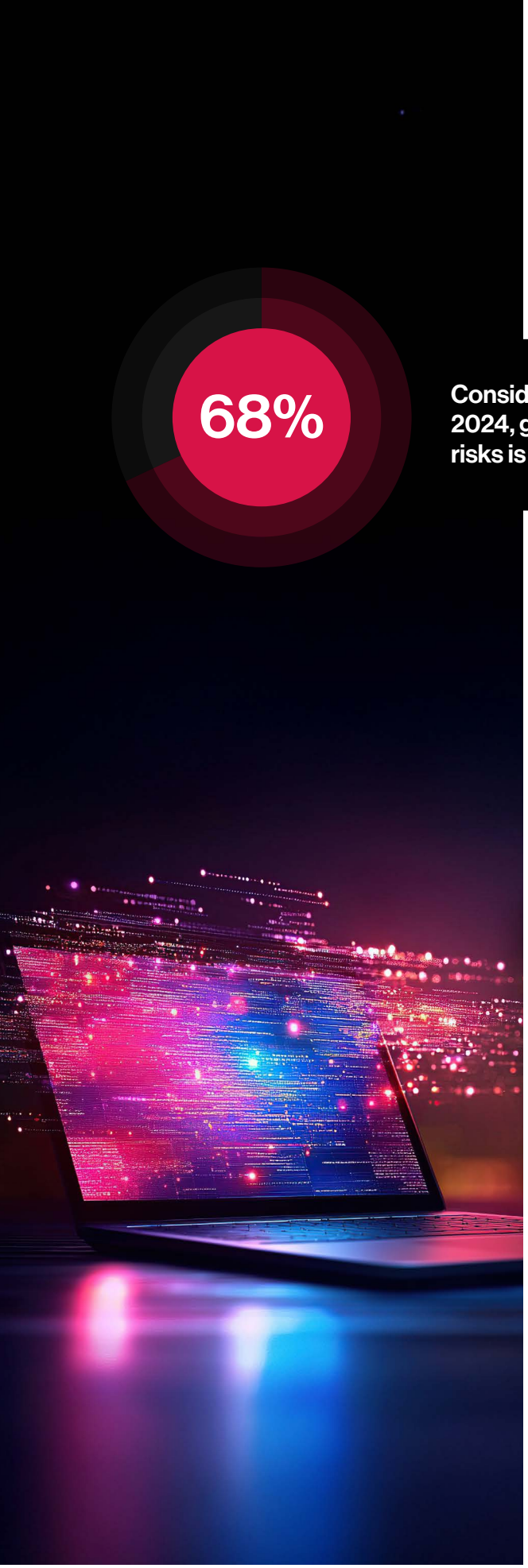
1 Implement robust email authentication

Configure SPF and DKIM, and enforce DMARC at p=reject to block fraudulent emails that appear to come from your domain. By stopping impersonation at the delivery stage, you protect customers, partners, employees, and other stakeholders before an attack can even begin.

This is where DMARC breaks the attack chain early - as shown in the threat lifecycle illustration that follows.



DMARC stops attacks at the delivery stage, breaking the chain before fake emails reach inboxes.



Considering that human error was behind 68% of breaches in 2024, giving employees the tools and training to spot these risks is just as important as the technology itself.

2 Prepare for AI-powered threats

Cybercriminals are already using AI to scale attacks. Adapt by deploying AI-driven security monitoring, anomaly detection, and incident response tools. Staying ahead means pairing defensive AI with regular training to help staff recognize the new risks posed by generative (or any other) technologies.

3 Secure third-party ecosystems

Assess and monitor the cybersecurity practices of vendors and partners. Enforce consistent standards for authentication, patching, and incident response. With supply chain and third-party breaches on the rise, strong oversight of external relationships is now essential to protecting your business and customers.

4 Govern technology use

Create clear policies on the use of unsanctioned software and AI tools. Provide secure, approved alternatives so employees don't turn to risky workarounds. Shadow IT and shadow AI can expose sensitive data and open new vulnerabilities. Strong governance helps prevent costly incidents.

5 Train and educate users – but don't rely on this alone

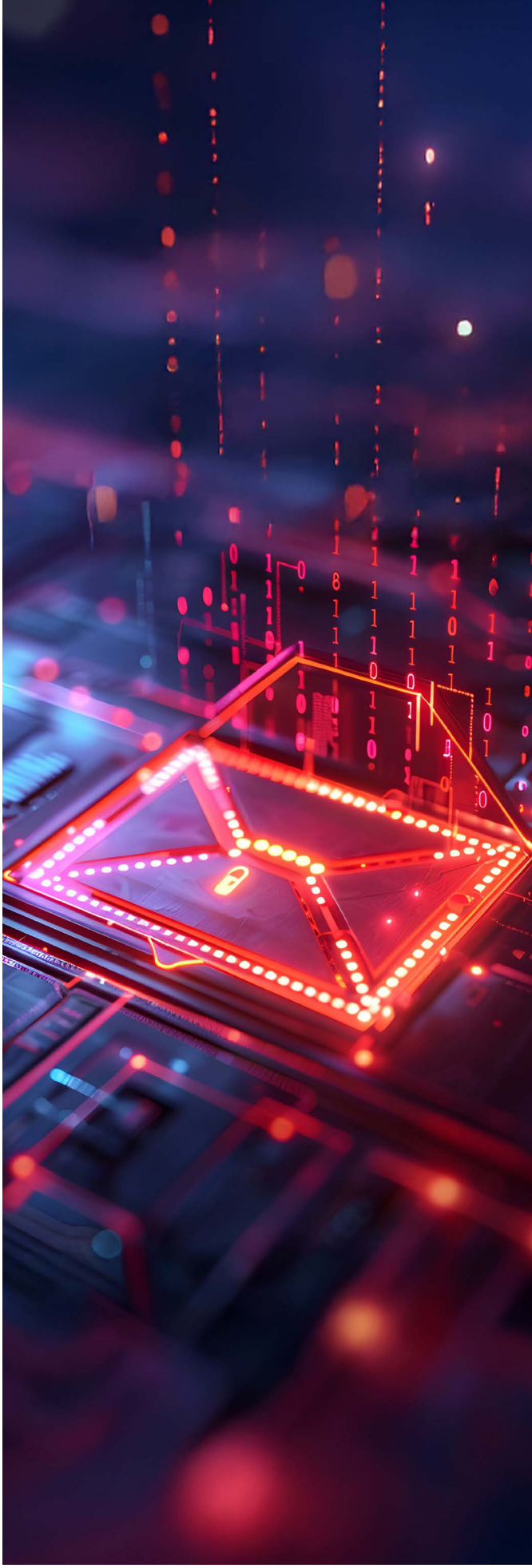
Employees play a key role in defense against phishing, BEC, and AI-driven email scams. Run awareness campaigns, send phishing simulations, and establish clear reporting processes so staff can act quickly on suspicious activity.

Well-trained teams reduce the likelihood of human error, which remains a factor in most breaches. But with attackers increasingly using AI to mimic trusted domains and even launch internal attacks from compromised accounts, training alone isn't enough.

Pairing user awareness with strong authentication measures like DMARC ensures staff aren't left to fight these battles on their own.

Ignoring email security: The cost of inaction

The current threat landscape is changing at a speed never seen before as AI introduces new risks. By not securing your organization's emails, you're leaving compliance, your reputation, and indeed, continuity, on the line. In this section, we explore the potential business fallout of ignoring email protection.



Heavy financial losses

Beyond the immediate costs of containment and recovery, email-based attacks drain budgets through legal fees, regulatory fines, and ransom demands. Indirect losses add up as deals collapse, insurance premiums rise, and customers take their business elsewhere.

For many organizations, the financial fallout is long-lasting and, in severe cases, can even force a shutdown - as we saw earlier in this report.

Erosion of trust

Few things are harder to recover than credibility. A spoofed domain or leaked customer data can undo years of brand-building in days. Once clients, investors, or the public question your ability to protect sensitive information, winning back their trust becomes a slow and uncertain process.

Communication breakdown

A successful email attack can disrupt the very channel businesses rely on most. From blacklisted domains to blocked delivery of legitimate messages, once trust in your email stream is lost, the knock-on effects reach customers, suppliers, and partners.

Misinformation through phishing or impersonation campaigns compounds the damage, eroding confidence in every interaction.

Disrupted operations

Email compromise doesn't just mean downtime - it can grind core business processes to a halt. Fraudulent payment requests, hijacked supply chain communications, or ransomware-driven lockouts cause widespread operational delays.

Productivity decreases as staff shift focus from delivering value to cleaning up the fallout of a preventable attack.

Rising compliance risks

Regulators are increasingly setting strict requirements for email authentication and phishing protection. Failing to comply can lead to rejected emails, lost access to markets, or suspension of payment processing capabilities.

Inaction leaves organizations exposed not only to attackers but also to escalating legal and regulatory consequences.

The risk of ignoring email security extends far beyond IT. It threatens finances, trust, and business continuity. Acting now costs far less than recovering from the damage of inaction.

Conclusion & future forecast

For the remainder of 2025 and beyond, we expect to see GenAI continue to transform the threat landscape. Human manipulation and deception are accelerating, with AI making email attacks more targeted, more convincing, and harder to stop. In this environment, email security is no longer just a best practice - it's a necessity for business continuity.

The rise of smarter email-based threats and stricter global regulations reinforces one truth: organizations must take control of their email identities. DMARC, enforced at p=reject, is a simple but powerful step businesses can take to block impersonation and prevent fraudulent emails from ever reaching inboxes.

Keith Thompson
Sendmarc Co-Founder and CTO

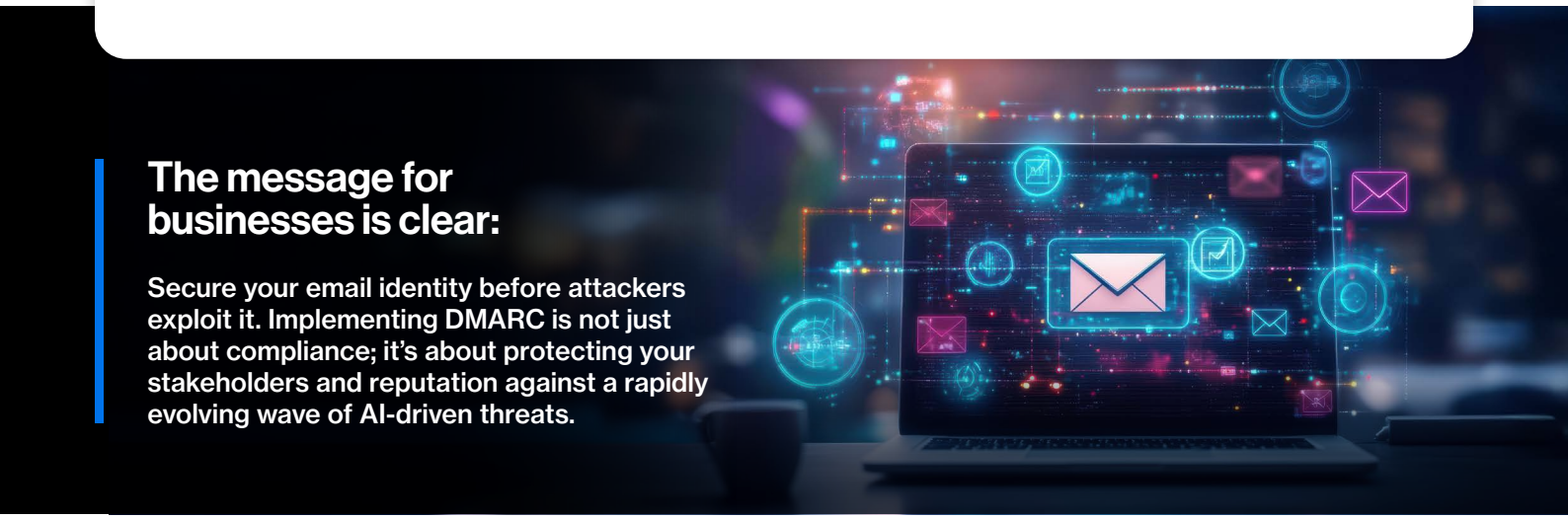
"In the last year, we've seen attackers **using AI to weaponize leaked corporate emails and credentials** to generate BEC attacks that perfectly mimic employee behavior. When an AI can analyze six months of email metadata to identify your CFO's habits and communication style, we're no longer defending against phishing - we're **defending against precision profiling at scale.**

This shift means the traditional 'human firewall' is obsolete. **Even trained security professionals can't distinguish AI-generated attacks** from legitimate communications when adversaries deploy LLMs trained on actual corporate data. The uncomfortable truth is that expecting employees to spot these threats is now organizational malpractice.

The future of email security requires resilient, open standards that assume both human judgment and automated defenses will fail. We need authentication frameworks that don't just verify where emails claim to originate, but preserve that verification across the complex routing, forwarding, and mailing list infrastructure that modern business demands. This is exactly why **evolving standards like DMARCbis are critical** because static defenses can't match threats that evolve at machine speed."

The message for businesses is clear:

Secure your email identity before attackers exploit it. Implementing DMARC is not just about compliance; it's about protecting your stakeholders and reputation against a rapidly evolving wave of AI-driven threats.



Simple & future-ready email protection

In partnership with leading DMARC provider Sendmarc, we help businesses protect against phishing, spoofing, and impersonation - threats that are only accelerating in the age of AI. Together, we make it simple to secure your organization's most critical communication channel: email.

Sendmarc's DMARC solution empowers you to safeguard any number of domains with confidence. By enforcing DKIM, SPF, and DMARC, you protect your brand, maximize deliverability, and comply with growing global regulations - all while safeguarding your reputation and building trust with your customers.

Sendmarc is also aligning its platform with DMARCbis (DMARC 2.0) as soon as the protocol is finalized, so you can seamlessly benefit from its new features without added complexity.

> **The goal is to make adoption straightforward and effective, giving you full protection without the burden of manual management.**

That's why automation matters. While manual DMARC implementation and management require time and effort, Sendmarc makes it effortless.

Why automation matters

Manual DMARC setup is time-consuming and complex. Sendmarc simplifies the process, making management effortless. Here's how **automated DMARC compares** to doing it manually: