mimecast

THE STATE OF HUMAN RISK 2025

Security Leaders Evolve

In 2024, human risk surpassed technology gaps as the biggest cybersecurity challenge. Organizations spent billions fortifying their tech stacks, yet breaches continue unabated. That's because security isn't just a technology problem, it's a human problem. Insider threats, credential misuse and user-driven errors now account for most security incidents. Attackers don't just hack in – they are increasingly targeting the human layer with precision. They are leveraging AI-powered phishing, exploiting collaboration tools, and bypassing traditional authentication methods. The results? Bigger, costlier breaches that are harder to detect and contain.

The increase in complexity comes from efforts in protecting, detecting, and responding to external threats and attacks but the emphasis on external protection often comes at the expense of visibility into the risks from within.

Humans – workers, vendors, consultants, and contractors – are the ones with their hands on the device. And despite the best defenses up and down the tech stack, hacks occur.

Two-thirds of security decision-makers interviewed by Mimecast for this State of Human Risk report agree it is inevitable or likely that their organization will suffer a negative business impact from an attack linked to an email or collaboration tool in 2025. In fact, one of 2024's most prominent breaches, the Change Healthcare cyberattack was largely attributed to human error, specifically a low-level employee's credentials compromised through a phishing email, allowing the attackers to gain access to the network without multi-factor authentication, enabling them to exfiltrate sensitive data and deploy ransomware. United Healthcare estimates the cost of its response to this breach to be between $2.3 and $2.45 billion dollars.

Enter human risk management (HRM). This report focuses on the current state of human risk, what it means for organizations, and how they can manage and mitigate it. To gain this insight, Mimecast conducted an in-depth global survey on the current state of cybersecurity and human risk by commissioning research firm Vanson Bourne to interview 1,100 IT security and IT decision makers from the United States, United Kingdom, France, Germany, South Africa, and Australia in November and December 2024, covering a range of private and public sectors, including healthcare, retail, finance, manufacturing, and utilities, and companies that had at least 250 or more employees.

Our research sought to discover:

Organizations' approach to cybersecurity, particularly in relation to human-related security risks.

The use of collaboration tools and the associated cybersecurity implications for an organization.

How budgets are currently impacting cybersecurity and human risk management.

The impact of AI on cybersecurity, both as a threat and solution.

KEY FINDINGS FROM THE STATE OF HUMAN RISK 2025 SURVEY

85% say their organization's cybersecurity budget has increased in the last 12 months.

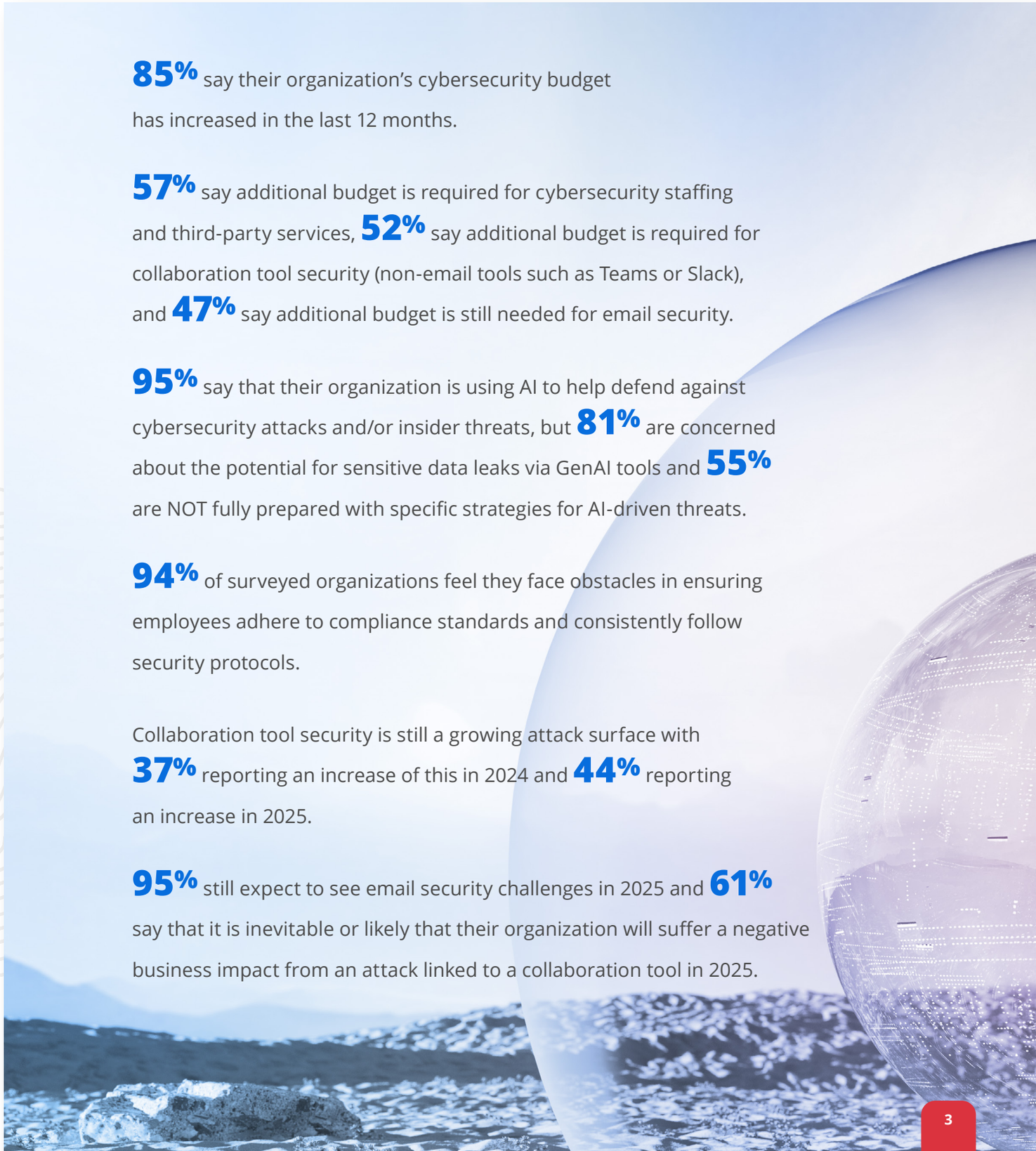
57% say additional budget is required for cybersecurity staffing and third-party services, **52%** say additional budget is required for collaboration tool security (non-email tools such as Teams or Slack), and **47%** say additional budget is still needed for email security.

95% say that their organization is using AI to help defend against cybersecurity attacks and/or insider threats, but **81%** are concerned about the potential for sensitive data leaks via GenAI tools and **55%** are NOT fully prepared with specific strategies for AI-driven threats.

94% of surveyed organizations feel they face obstacles in ensuring employees adhere to compliance standards and consistently follow security protocols.

Collaboration tool security is still a growing attack surface with **37%** reporting an increase of this in 2024 and **44%** reporting an increase in 2025.

95% still expect to see email security challenges in 2025 and **61%** say that it is inevitable or likely that their organization will suffer a negative business impact from an attack linked to a collaboration tool in 2025.



HUMAN RISK MANAGEMENT HAS ARRIVED

and Security Leaders Know It

HRM is a connected approach to cybersecurity; the business of securing an organization is a constantly evolving challenge. Security leaders are faced with difficult decisions about the tools to rely on and how best to allocate budget to minimize risk. But despite the wide array of security tools in the market today, CISOs still report struggling to get a clear picture of risk across their organization.

In fact, Gartner research shows that over 90% of employees who admitted undertaking a range of unsecure actions during work activities knew that their actions would increase risk to the organization but did so anyway. Human-centric security design is modeled with the individual – not technology, threat or location – as the focus of control, design and implementation. According to Gartner, by 2027, 50% of CISOs will formally adopt human-centric design practices into their cybersecurity programs to minimize operational friction and maximize control adoption.

As highlighted by a CIO in the insurance industry, "Technical safeguards like firewalls and intrusion detection are essential, but human behavior ultimately determines their effectiveness." This statement underscores the growing consensus that HRM is not just supportive – it's a necessity for modern cybersecurity strategies.

Executive Summary

Collaboration tools and the petabytes of data our workforce creates, accesses, changes and moves means that complexity has increased to a level never seen before.

In this report, you'll learn more about how:

- Organizations are reaching a heightened state of awareness about insider risk, as insiders have access to valuable IP that can be compromised.
- While more organizations are leveraging AI security tools to deliver increased security and team efficiency, cybercriminals are also using generative AI, which allows them to create more realistic phishing emails, collaboration tool messages, malicious web pages, and even deepfakes.
- While email and collaboration security have traditionally focused on protecting the workforce from being targeted by external attackers, the way we work has dramatically evolved, forcing organizations to understand risk from both internal and external threats.
- Despite increases in cybersecurity budgets to address human risk, email security, and collaboration tool security, organizations are still struggling to cover the cost of remaining secure.

MARKET ADOPTION OF HUMAN RISK MANAGEMENT

The Current Shift

Human error contributes to 95% of data breaches. Solving the challenge of human risk requires a dedicated approach to identifying, assessing, and mitigating these risks tailored to each user.

Every day, businesses face risks including accidental data leaks, unsecured collaboration channels, and poor password hygiene. In fact, Mimecast data indicates that a small fraction of employees contribute disproportionately to security incidents – just 8% of employees account for 80% of incidents. HRM solutions aim to balance innovation and productivity with better prevention strategies, rather than relying solely on post-incident remediation.

This shift recognizes that security awareness alone is not enough. In the State of Human Risk 2025, while nearly 87% of surveyed organizations train employees quarterly to identify and report threats, a significant 33% still cite employee error as their top concern, while 27% worry about lapses in vigilance caused by fatigue. The solution lies in tailoring risk management efforts to address these pain points with precision.

87% of respondents say that their organization trains its employees to spot cyberattacks at least once a quarter.

33% fear mistakes and human error in handling of email threats by employees.

27% fear employee fatigue causing lapses in vigilance.

6% say that their organization's security policies are continuously updated based on emerging trends.

While email security is still critical to securing an organization, today it's just one piece of the puzzle. Human risk management means stopping risks before they become incidents – prevention vs. remediation. Given the finding mentioned earlier – 8% of employees are responsible for 80% of security incidents – CISOs must balance productivity and innovation on the one hand with human risk on the other; and the emergence of credible AI will support in this goal.

When it comes to protecting all their email and collaboration tools, only 10% of respondents say their organization has cybersecurity systems implemented. Even more frightening is that only 6% of respondents say their organization's security policies are continuously updated based on emerging trends. In addition, respondents say their organization needs more visibility on data exfiltrated on USB devices (82%), and on files sent to personal email addresses (85%).

Survey respondents were asked to weigh in on how their organization measures the effectiveness of human risk management strategies:

44% said they look for increased employee-driven incident reporting.

44% said they monitor phishing simulation success rates.

43% said they measure employee feedback on surveys.

41% said they look to the frequency and severity of security incidents.

39% said they conduct post-training assessments or quizzes.

34% said they look to see how many employees are identified as needing extra security training.

Security professionals believe there is a high level of risk of mistakes in these areas:

Inadvertently leaking data	**84%**
Oversharing company information on social media	**82%**
Poor password hygiene	**81%**
Using unapproved cloud storage or other functionality	**80%**
Accessing files/apps through unsecured networks	**80%**
Using personal email	**79%**
Using collaboration tools	**76%**
Using a smart-phone for work-related tasks	**76%**
Browsing the web / online shopping	**76%**

Human Error

When it comes to cybersecurity failures, the financial and reputational consequences of human error are profound. Costs include breach remediation, product downtime, and potentially irreparable brand damage. Errors such as sending sensitive information to the wrong recipient or improper data disposal are surprisingly common and often catastrophic.

An insurance industry CIO succinctly explained the risks, noting, “Accidental breaches occur when employees inadvertently compromise sensitive systems through misaddressed emails or failure to follow data disposal protocols. These errors, while unintentional, carry serious consequences.”

To address these challenges, organizations are increasingly adopting connected HRM platforms. Unlike siloed solutions, these platforms provide end-to-end visibility into both external and internal risks. They can monitor collaboration tools, identify vulnerable employees, and prevent actions like unauthorized data sharing before breaches occur.

HRM Platforms

Historically, organizations have tried to address the problem of human risk via multiple, disconnected solutions. But, today it’s more important than ever to ensure that organizations can protect themselves from internal or insider risk. This leads organizations, especially smaller businesses, to ask their employees to not only identify threats that come in via email and collaboration tools, but also to properly handle organizational data.

HRM platforms deliver a comprehensive analysis of an individual’s risk profile, offering insights into behavior patterns, attack factors, and an overall risk score. The attack factor, a key metric, quantifies an individual’s risk exposure, such as the quantity of phishing emails received. While end users cannot control their attack factor, this data is invaluable to security professionals due to its direct influence on overall risk.

BUDGETS ARE INCREASING

But It's Not Enough

Cybersecurity spending is on the rise, with 85% of surveyed organizations reporting budget increases in the last year. Yet, these increases fall short of meeting growing demands. Only 3% of security leaders feel confident that their budgets are sufficient, while the majority state that additional investments are needed across areas such as staffing, collaboration tool security, and email security.

The problem isn't limited to funding levels – many CISOs struggle to secure buy-in from their boards for new initiatives. Effective communication with executives is critical to justify why further investment in cybersecurity is not a luxury but a necessity. Boardrooms increasingly demand clear evidence of ROI for these tools, emphasizing measurable impacts on business continuity and security posture. Particularly in larger organizations, security leadership and IT leadership need to work closely to keep the board informed of current security threats, how their organization is addressing them, what failing to address threats could mean for the company, and what additional tools and resources they need to keep the organization secure.

At the same time, security leaders need to prioritize efficiency. Overloading teams with disconnected tools can create additional layers of intricacy, making it difficult to pinpoint actionable insights in a sea of data. A centralized, integrated HRM approach not only streamlines operations but also strengthens the case for a budget by demonstrating clear outcomes.

85% of respondents say their organization's cybersecurity budget has increased in the last 12 months.

3% say no additional budget is needed across any cybersecurity areas.

57% say additional budget is required for cybersecurity staffing and third-party services.

52% say additional budget is required for collaboration tool security (non-email tools such as Teams or Slack).

47% say additional budget is required for email security.

How CISOs Can Mitigate Budget Impacts

Security leaders will always face budget limitations – but endless spend for bringing additional security tools into the environment isn't always the answer. More tools inevitably mean more complexity, more consoles, more logs, more, more, more.

Security teams are tasked with making sense of an endless stream of data points, alerts, and incidents. With a slew of tools, separating noise from what matters is a challenge, and bringing in what data points matter from across a jumble of dashboards compounds it. Data tells a different story in isolation than it does when aggregated; for example, a click on a suspicious link is worthy of investigation, as is a suspicious login attempt from a new location, or an alert about source code exfiltration. But when all of these events occur in succession by a single user, alarm bells should sound.

Budget and security ROI conversations become more effortless when security leaders can enable their teams to correlate data quickly and accurately enough to identify incidents before they grow, and can defend these positions to their own leadership or board.

Only

3%

of security leaders feel confident that their budgets are sufficient.

EMAIL AND COLLABORATION THREAT PROTECTION

Email and Collaboration Security

Collaboration platforms like Slack, Zoom, and Microsoft Teams, along with email tools, have become cornerstones in business operations. Unfortunately, cybercriminals target these everyday interactions to compromise organizations, often turning employees into unwitting participants in their schemes – indeed, collaboration tools are still a growing attack surface, with a 7% increase in attacks over 2024. Despite the availability of advanced security tools, email remains the most exploited entry point for attackers.

This makes it critical for companies to adopt AI-powered security solutions. AI tools not only secure email and collaboration platforms but also improve staff productivity by intercepting sophisticated threats before they breach your system. These technologies are designed to adapt to attackers' evolving tactics, protecting even the most careful employees from falling victim.

The growing threat to collaboration platforms should raise alarm bells. Companies are responding to these threats, with some taking drastic measures. Marriott implemented stricter safeguards after an attack through Slack, while Disney discontinued Slack to eliminate associated risks. However, implementing bans on collaboration tools isn't sustainable for operational efficiency; it's incumbent on security teams to create integrated policies that protect users across their work surfaces.

44% of respondents have seen an increase in collaboration tool threats in the last 12 months.

60% say that their organization has a formal cybersecurity strategy that spans all key business functions, up from 48% in 2024.

96% say that the adoption of a formal cybersecurity strategy has improved their organization's cybersecurity risk level.

95% expect to see email security challenges in 2025.

61% say that it is inevitable or likely that their organization will suffer a negative business impact from an attack linked to a collaboration tool in 2025.

79% agree that the use of collaboration tools within their organization poses new threats and security loopholes that urgently need to be addressed.

67% agree that most native collaboration tool security is insufficient to meet their needs.

For example, a human risk management platform should be able to assist with collaboration tool security by integrating with Slack's API to capture a complete record of all messages, including edits and deletions, allowing for comprehensive monitoring, data loss prevention, and ediscovery capabilities by providing a searchable archive with AI-powered analysis to detect sensitive information and potential compliance violations within Slack conversations. An HRM platform acts as a centralized control point to enforce data security policies across the collaboration platform.

Sophisticated Business Email Compromise Attacks

Business email compromise (BEC) attacks are on the rise. Research shows a significant increase in frequency and sophistication of these attacks, largely due to the growing availability of AI tools that enable more personalized and convincing phishing campaigns. This makes sophisticated BEC attacks more damaging and harder to detect.

At the same time, AI is essential for combating BEC; it adapts to evolving threats, but security teams must integrate AI with proven methods. The challenge, however, is for security teams to manage and tune vast amounts of data while threat actors continuously change their techniques, requiring detections that do not rely on signatures or heuristics.

The head of IT at a retail company summed up the need for using AI, stating, "You can't stand there trying to put your finger in the hole in the dam. You've got to embrace it."

The IT director at a utilities company echoed the statement, believing that not only do organizations need to embrace AI tools, but security vendors should expect to assist with implementation. "I think [it] will evolve quickly and we'll have to embrace it quickly as well," he said. "And especially within the cyberspace, you've got to always keep one step ahead of the game. So, we're looking to vendors to help us with that."

> "I think [BEC] will evolve quickly and we'll have to embrace [AI] quickly as well"
>
> – Head of IT, Retail

Survey Results

A full 95% of respondents expect to see email security challenges in 2025. There has been an increase in collaboration tool threats and 44% of survey respondents confirm that increase over the last 12 months. These stats support what Mimecast is already seeing in our most recent threat intelligence data, including an increase in spam, impersonation attacks, and known malware, as well as an overall threat increase per user for all business sizes in the Middle East and South Africa.

Further evidence of an increase in collaboration tool threats includes the fact that 79% of respondents agree the use of collaboration tools within their organization poses new threats and security loopholes that urgently need to be addressed. Additionally, 61% say that it is inevitable or likely that their organization will suffer a negative business impact from an attack linked to a collaboration tool in 2025, and 67% agree that most native collaboration tool security is insufficient to meet their needs.

There is some good news, however, in that 60% say their organization has a formal cybersecurity strategy that spans all key business functions, up from 48% in 2024, and 96% say that the adoption of a formal cybersecurity strategy has improved their organization's risk level.

In addition, 38% of organizations stated their cybersecurity practices are completely effective in protecting employees and their supply chain, and 37% said the same of protecting their customers. Also, 48% felt their cybersecurity practices were mostly effective in protecting employees and customers, and 46% said the same for their supply chain. That leaves a minority with the belief that they are not completely or mostly effective in protecting their employees (14%), customers (15%), and supply chains (16%), respectively.

The majority of surveyed organizations already have email and collaboration tool security measures in place or are currently rolling them out:

53% are currently monitoring and protecting against data leaks or exfiltration in outbound email, and 33% are currently implementing this.

54% are monitoring and protecting against email-borne attacks like malware and malicious links in inbound email, and 34% are currently implementing this.

53% are currently monitoring and protecting against email-borne attacks or data leaks in internal-to-internal emails, and 35% are currently implementing this.

52% are currently monitoring against a collaboration-tool-based attack, and 34% are currently implementing this.

53% are identifying emails that spoof their email domains, and 29% are currently implementing this.

48% are detecting and removing malicious or unwanted emails already in employee inboxes, and 40% are currently implementing this.

66% are monitoring and protecting against email-borne attacks before they reach inboxes, and 28% are currently implementing this.

DATA LOSS AND INSIDER RISK

While external risk will not cease in importance, security teams need to be just as vigilant when it comes to addressing risk from inside the organization – both intentional and unintentional.

Whether it's a disgruntled employee exfiltrating sensitive IP or assisting external bad actors by providing access to critical systems, a negligent user who is spread too thin and fatigued, a compromised user who has inadvertently given their credentials to a bad actor, or finally, a targeted user who has fallen prey to cybercriminals using social engineering to gain access to systems through impersonation, organizations must prepare for being compromised by users from within.

43% of respondents have seen an increase in internal threats or data leaks initiated by compromised, careless, or negligent employees in the last 12 months.

66% are concerned that data loss from insiders will increase at their organization in the next 12 months.

An insider-driven data exposure, loss, leak, and theft event would cost respondents' organizations an average of **$13.9 million.**

Survey Results

When asked about negligent, compromised, and targeted users, 43% of respondents have seen an increase in internal threats or data leaks in the past 12 months, and 66% expect to see an increase in data loss at their organization in the next 12 months. Security decision-makers reported an insider-driven data exposure leak and theft event would cost an average of $13.9 million.

Artificial Intelligence

The use of AI in cybersecurity is significantly on the rise, with many organizations increasingly adopting AI-powered solutions to combat evolving cyber threats, detect anomalies, and improve overall security posture. This trend is driven by AI's ability to analyze vast amounts of data quickly and identify patterns that might otherwise go unnoticed by traditional methods. Unfortunately, AI is also increasingly a weapon used by cybercriminals. AI-powered cyberattacks leverage algorithms and techniques to automate, accelerate, or enhance various phases of cyberattacks.

Mimecast's Threat Intelligence Hub features a recent successful phishing campaign that leveraged a legitimate CMS to send fraudulent job offer emails from well-known brands.

More broadly, the industry has experienced other well-known, insider-risk-driven cyberattacks: Data exposure at Pegasus Airlines due to employee negligence, the Mailchimp triple data breach caused by social engineering, the theft of Slack's code repositories due to a compromised vendor, intellectual property theft by a malicious insider at Yahoo, and a massive data breach by former Tesla employees.

How the Good Guys Use AI

Organizations use AI in cybersecurity primarily to improve threat detection by analyzing vast amounts of data to identify patterns and anomalies that may indicate malicious activity, enabling faster response times and proactive threat mitigation. This includes features like automated incident response, behavioral analysis of user activity, vulnerability scanning, and predictive analytics to anticipate potential attacks, all while minimizing human intervention in routine tasks like log analysis and system monitoring.

95%

of respondents say that their organization is using AI to help defend against cybersecurity attacks and/or insider threats.

81%

are concerned about the potential for sensitive data leaks via GenAI tools.

55%

are NOT fully prepared with specific strategies for AI-driven threats.

How Cybercriminals Use AI

Cybercriminals are also using generative AI, which allows them to create more realistic phishing emails and malicious web pages, and more easily trick employees into clicking on links, downloading malicious attachments, and visiting malicious websites. Bad actors are also using AI to automate tasks, generate more realistic deepfakes, target specific victims with personalized attacks, and even to develop more sophisticated malware that is harder to detect. Another way threat actors leverage AI is to scan code for vulnerabilities, greatly decreasing the time it takes them to discover potential exploits.

Most organizations are using AI tools to minimize insider risk:

46%
Threat detection and real-time monitoring

46%
Analysis and response to phishing attacks

43%
Endpoint protection and anti-malware tools

43%
Behavioral or sentiment analysis and insider threat detection

43%
Automated incident response systems

Governance and Compliance

Governance and compliance establishes a robust framework to identify and manage cyber risks, keeping operations legally sound and in line with industry standards and internal policies. With a focus on securing sensitive data, ensuring business continuity, and dodging damaging legal fallout from data breaches or security incidents, governance and compliance is an organization's proactive defense against the invisible enemy.

But let's take it a step further with AI. When skillfully deployed, AI supercharges compliance efforts, working tirelessly to analyze mind-boggling volumes of data, spot potential threats, identify real-time anomalies, automate tedious security work, predict incoming attacks, and prioritize responses. It enables proactive threat mitigation and ensures adherence to relevant security standards and regulations, and maximizes efficiencies to streamline ediscovery efforts.

AI not only boosts organizations' compliance and security levels but also turbocharges staff efficiency across organizations of every size, industry, and location worldwide. The future of cybersecurity isn't in locks and keys – it's in security tools that leverage AI strategically, and it's arguably the only way to outsmart and outpace the ever-evolving world of cybercrime

Survey Results

When it comes to survey respondents and AI, 95% say that their organization is using AI to help defend against cybersecurity attacks and/or insider threats, 81% are concerned about the potential for sensitive data leaks via GenAI tools, and 55% are not fully prepared with specific strategies for AI-driven threats.

What organizations are doing to address the potential for AI to exploit human behavior and mistakes in cybersecurity:

44% are implementing AI-powered monitoring and protection tools

44% are developing internal AI tools to protect against AI-driven attacks

42% are training on how to use AI to avoid exploitation

40% are creating policies on AI usage

38% are updating or introducing code of conduct for AI-driven risks

36% are collaborating/sharing relevant information with partners

35% are conducting simulated AI-driven phishing attacks

SECURITY AWARENESS EVOLVES

Security awareness is a cornerstone of modern cybersecurity, equipping employees to identify and respond to cyber threats while minimizing risks like data breaches. By addressing the human element – the most significant vulnerability – effective training empowers employees to safeguard their organization's digital assets through a clear understanding of security protocols and by recognizing malicious activity.

But to avoid the pitfalls of broadly training all users, without focusing on those who face higher risk, a more innovative approach is needed. Interactive, engaging modules that cover critical topics such as phishing recognition, password hygiene, and data protection are foundational. Leveraging personalized risk insights, such as tailoring content for individuals identified as high-risk based on data-driven testing, enhances the effectiveness and relevance of the training.

HRM platforms represent the next evolution in security awareness. These platforms provide real-time insights into employee behavior and risk levels, allowing organizations to target training where it's most needed. HRM tools can quantify effectiveness by showing measurable improvements in behavior and identifying areas where gaps remain, guaranteeing actual impact.

It's essential to recognize that a one-size-fits-all approach fails in the context of security awareness. Adaptive learning solutions are critical, focusing resources on employees whose behavior suggests the highest risk. Equally important is the ability of HRM platforms to provide continuous feedback loops, demonstrating progress and pinpointing weaknesses, which helps build a culture of proactive cybersecurity.

Survey Results

In looking at what the survey can tell us about the current state of security awareness training, 87% of respondents say that their organization trains its employees to spot cyberattacks at least once a quarter. And while that might spell good news for awareness, 33% of respondents fear mistakes and human error in handling of email threats by employees, 27% fear employee fatigue is causing lapses in vigilance, and 43% have seen an increase in internal threats or data leaks initiated by compromised, careless, or negligent employees in the last 12 months. In addition, two-thirds are concerned that data loss from insiders will increase at their organization in the next 12 months.

The potential frustration with a continued lack of security awareness is reflected in a statement from an IT director in the utilities industry when he said, "I wish everyone was at the same level of awareness. [We're] trying to embed it as a cultural thing. So, we spend a lot of time publicizing stuff on the intranet and through training and materials and communication and try and bring it to the front of mind." Continued awareness training, coupled with support from an HRM platform to identify the riskiest users, can help organizations get there.

87% of respondents say that their organization trains its employees to spot cyberattacks at least once a quarter.

33% fear mistakes and human error in handling of email threats by employees.

27% fear employee fatigue is causing lapses in vigilance.

43% have seen an increase in internal threats or data leaks initiated by compromised, careless, or negligent employees in the last 12 months.

66% are concerned that data loss from insiders will increase at their organization in the next 12 months.

> "[We're] trying to embed it as a cultural thing."
>
> – IT Director, Utilities

KEY TAKEAWAYS AND RECOMMENDATIONS

For each of the past nine years, Mimecast has conducted its annual survey to uncover the current state of cybersecurity. To date our focus has been trained on email and collaboration security, shifting this year with the evolving security landscape to human risk. The details provided in this year's report are intended to give readers insight into the ways fellow cybersecurity professionals are securing their organizations, as well as the challenges they are facing on a wide range of topics.

It is our hope readers will use this report and its data as a guide for creating plans to secure their organizations in the coming year.

1. Assess Your Organization's Human Risk and Implement Human Risk Management Tools

Evaluate your human risk management (HRM) maturity level. Identify factors contributing to human risk, such as complex processes, employee workload, and stress levels. Develop a strategy aligned with your organization's risk tolerance. Explore comprehensive HRM platforms that fit your budget and resources. Use these tools to monitor, manage, and reduce human error-driven risks effectively.

2. Boost Insider Threat Visibility

Conduct assessments to understand your organization's intentional and unintentional insider risk potential. Pay close attention to employees leaving the organization or those who may be most likely targeted by cybercriminals. Deploy tools, ideally within an HRM platform, to monitor employee behaviors, detect suspicious activities, and mitigate the risk of data loss or compromise from inside threats.

3. Maximize the Impact of Artificial Intelligence

Regularly evaluate the AI tools your team uses. Ensure they are fully integrated and aligned with organizational needs. Stay updated on emerging AI tools and understand the tactics used by cybercriminals to counteract evolving threats.

4. Strengthen Email and Collaboration Tool Security

Assess and update your email security tools. Consider adopting comprehensive email security and collaboration platforms. Train users to spot sophisticated phishing and BEC attacks while supporting them with advanced AI-based security technologies.

5. Mitigate Collaboration Tool Risks

Recognize that collaboration platforms are growing as attack surfaces. Secure these tools by implementing safeguards similar to those used for email security, ensuring minimal exposure to threats.

6. Optimize Security Budgets for HRM Platforms

Work toward gaining executive buy-in for implementing a comprehensive HRM platform. Carefully evaluate if it will be managed in-house or requires external vendor support. Allocate funds wisely to cover the most critical aspects of security.

7. Pinpoint High-Risk Users; Monitor and Measure Training Effectiveness

Use HRM platforms to identify employees who are most susceptible to cyberattacks, focusing additional training and security measures on these individuals to minimize overall risk. Continuously track the success of your security awareness initiatives.

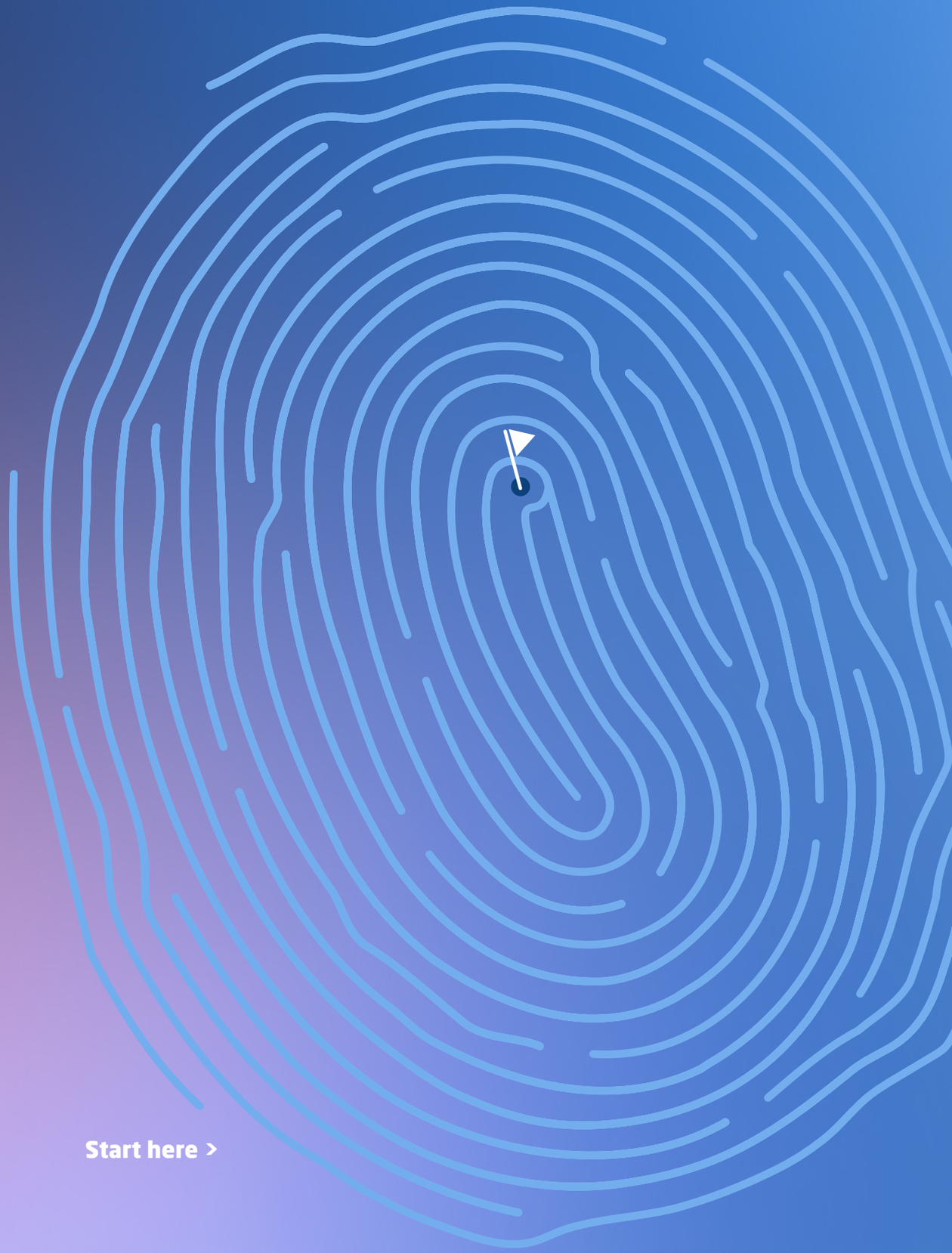
8. Evolve Protections for Business Email Compromise

Evaluate the likelihood of falling victim to BEC attacks and ensure all employees are well-trained to recognize these threats. Pair education with robust technology to defend against sophisticated email schemes

METHODOLOGY

This is the ninth year in a row that Mimecast has conducted an in-depth global survey on the current state of cybersecurity. For our 2025 report, we commissioned research firm Vanson Bourne to interview 1,100 IT security and IT decision makers in November-December 2024 from the United States, United Kingdom, France, Germany, South Africa, and Australia. A range of private and public sectors were covered, including healthcare, retail, finance, manufacturing, and utilities. Respondents had to be from organizations with 250 or more employees. Vanson Bourne also conducted qualitative interviews with UK-based security leaders.

Survey participants worked at organizations ranging between 250 to 500 employees (5% of the total) and more than 10,000 employees (20% of the total). These companies were spread across 11 industrial sectors, including financial services (12%), technology and telecommunications (13%), retail (15%), healthcare (10%), manufacturing (11%) and the public sector (5%).



Start here >

About Mimecast

Mimecast is a leading cybersecurity company transforming the way businesses manage and mitigate human risk. Its AI-powered, API-enabled connected Human Risk Management platform is purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.