mimecast

THE STATE OF

HUMAN RISK

2026

EXECUTIVE SUMMARY

In 2024, human risk surpassed technology gaps as the biggest cybersecurity challenge. Organizations spent billions fortifying their tech stacks, yet breaches continue unabated. The problem isn't that humans are the weakest link, it's that security strategies haven't evolved to protect the ways people actually work.

Insider threats, credential misuse, and user-driven errors now account for most security incidents. Attackers don't just hack in anymore; they're increasingly targeting the human layer with precision. They leverage AI-powered phishing, exploit collaboration tools, and bypass traditional authentication methods. The results? Bigger, costlier breaches that are harder to detect and contain.

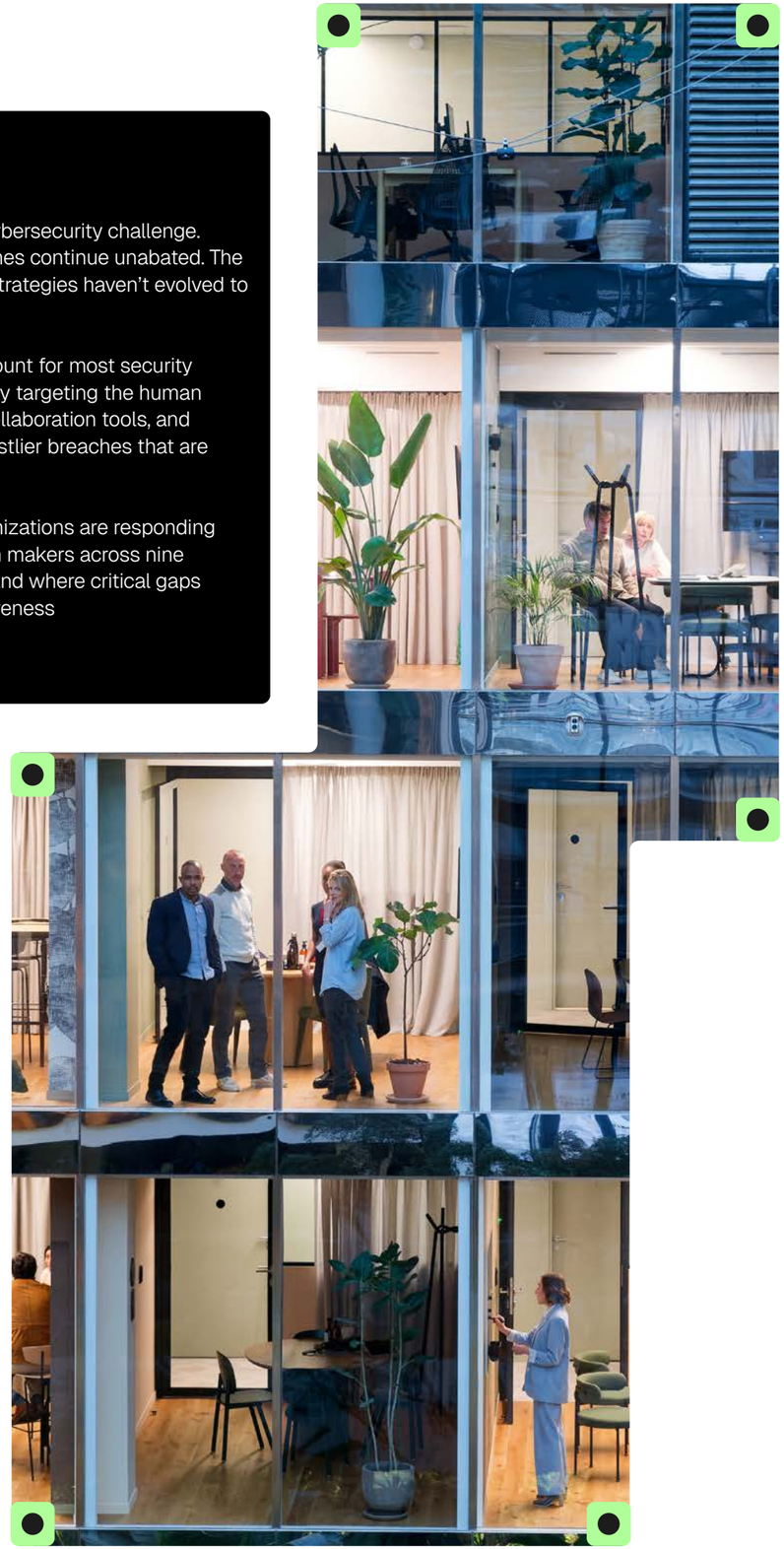
This tenth annual State of Human Risk report examines how organizations are responding to this shift. Based on a survey of 2,500 IT security and IT decision makers across nine countries, we reveal where security leaders are making progress and where critical gaps remain. The message is clear: 2026 is the year to move from awareness to action.

The Human Risk Imperative: Why 2026 Demands Action

The evidence is overwhelming: insider threats, credential misuse, and user-driven errors account for most security incidents. Respondents estimate that a single insider-driven data exposure, loss, leak, or theft event would cost their organization an average of $13.1M. With organizations experiencing an average of six such incidents per month, this equates to a projected $78.6M in monthly exposure or approximately $943.2M annually.

The Recognition-Action Gap

Our research reveals universal awareness but fragmented execution. While 91% of organizations face obstacles ensuring employee compliance, and 96% acknowledge incomplete protection, only 28% of organizations combine both regular security awareness training and continuous monitoring for policy violations—two foundational actions that any organization serious about human risk management should have in place. This disconnect creates dangerous exposure: 71% expect collaboration tool attacks will cause business impact in 2026, yet 38% still only rely solely on native security controls—despite 64% agreeing native collaboration tools are insufficient.



Five Critical Gaps Defining 2026

In 2026, organizations face five interconnected security gaps—from fragmented communication channels to AI-powered threats—that traditional defenses struggle to address. The core problem isn't awareness but execution: translating recognized vulnerabilities into coordinated action before the gap between knowing and doing becomes catastrophic.

1. The Attack Surface Explosion
Threats now span email, collaboration platforms, and internal communications and 38% still rely solely on native security controls for collaboration tools.

2. The Insider Risk Crisis
Just 8% of employees account for 80% of security incidents[1]. Organizations recognize three distinct risk profiles (negligent, compromised, and malicious) but fail to coordinate prevention strategies, with only 28% combining both regular security awareness training and continuous monitoring.

3. The Integration Paradox
While 65% of organizations surveyed find security tool integration too complicated, those who succeed achieve 40% faster threat remediation and comprehensive visibility. Ironically, at organizations that are unsuccessful at integration, tool sprawl ends up creating the exact fragmentation that integration is meant to solve.

4. The Governance Breakdown
Despite universal recognition that governance matters, 59% of respondents lack confidence that they can quickly locate communications data for regulatory requirements. Organizations relying on manual processes (36% for monitoring and 23% for policy management) face inevitable bottlenecks as data volumes surge across fragmented systems.

5. The AI Readiness Gap
While 69% of respondents see AI-driven attacks as inevitable within 12 months, only 55% report using AI-powered tools for threat detection and real-time monitoring. Organizations are more likely to report implementing AI-powered monitoring and protection tools (48%) than training employees to recognize AI exploitation (44%) or creating specific AI usage policies (41%).

[1]This 8%/80% stat is from the Mimecast whitepaper The Size and Shape of Workforce Risk.

The Path Forward: Integrated Human Risk Management

Success requires abandoning siloed approaches in favor of integrated platforms that coordinate people-focused initiatives, technology-focused controls, and governance frameworks while continuously adapting to evolving threats. The organizations winning this battle share common characteristics: they identify high-risk users through behavioral analytics, tailor controls based on individual risk profiles, deploy unified protection across all communication channels, automate compliance enforcement, and prepare for AI-driven threats with both defensive AI and governance.

The Business Case Is Clear

Organizations must prevent incidents before they occur, reduce detection and response time, improve compliance posture, increase security team efficiency, and demonstrate measurable risk reduction to boards and executives. Factor in regulatory fines, legal exposure, and reputational damage on top of the $943.2M annual insider risk exposure quantified above, and the ROI of spending on human risk management instead of costly breach remediation becomes undeniable.

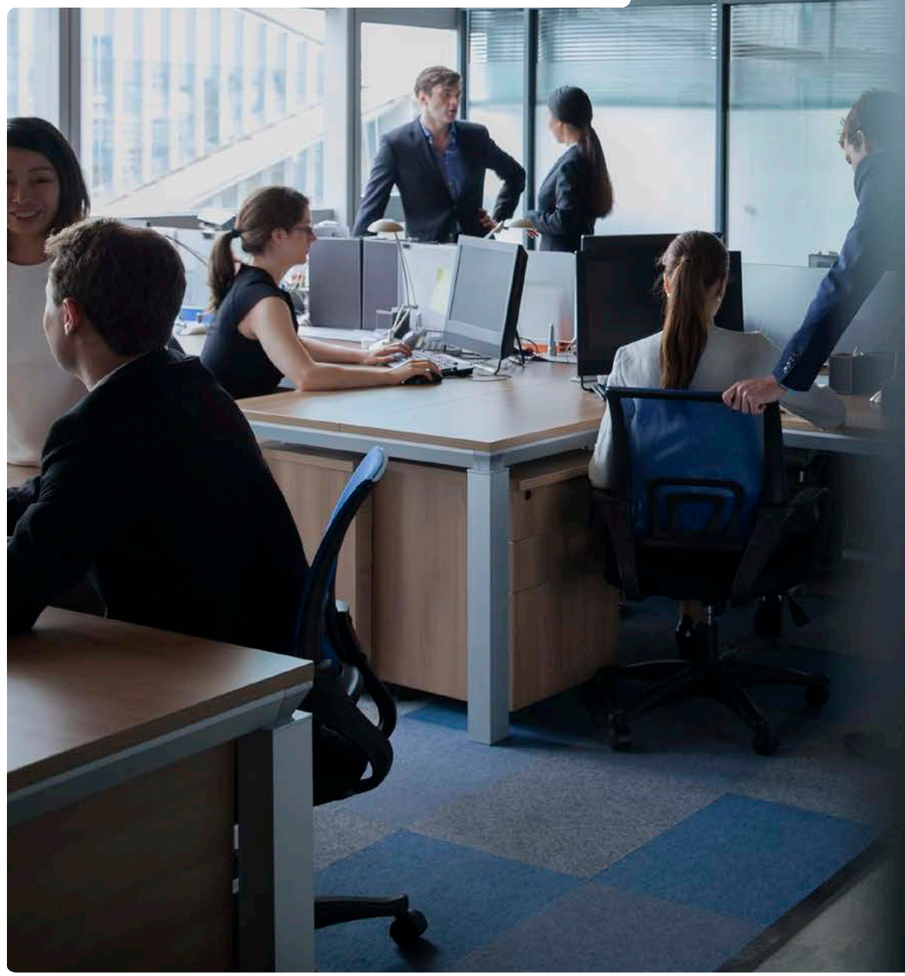
The Choice for 2026

The question is no longer about whether to invest in human risk management, it's whether organizations will act before the next potentially very costly incident. Those who treat human risk management as an integrated strategic priority will thrive. Those who continue piecemeal approaches will struggle.

METHODOLOGY: We surveyed 2,500 respondents (1,922 IT decision makers, 578 IT security decision makers) across nine countries in November and December 2025. All organizations had over 250 employees and over 250 email users. Organization sizes ranged from 250 to over 10,000 employees.

GEOGRAPHIC COVERAGE: US (500), UK (300), Germany (300), France (300), Spain (200), Italy (200), South Africa (200), Singapore (250), Australia (250)

SECTORS COVERED: Financial services, healthcare (public and private), IT/technology/telecoms, manufacturing, retail, public sector, energy/utilities, business services, construction, consumer services, media/entertainment



KEY FINDINGS

- 2,500 organizations with 250 to over 10,000 employees surveyed
- Across 9 countries
- In 10 industry sectors
- 1,922 IT decision makers / 578 IT security decision makers

$13.1M

average estimated cost per insider-driven incident × 6 incidents/month = $943.2M annual exposure

Only **28%**

combine both regular security awareness training (53%) and continuous monitoring (52%)

69%

agree AI will be used in attacks against their organization in next 12 months

71%

expect negative business impact from collaboration tool attacks in 2026

65%

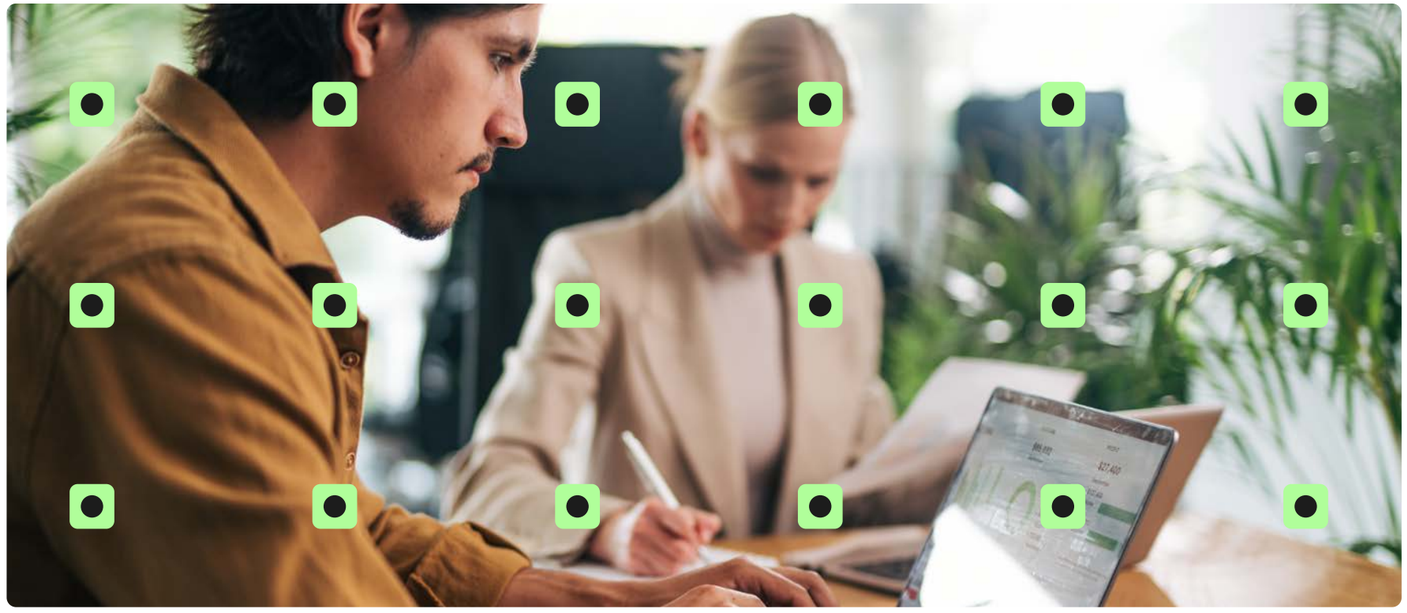
find integrating cybersecurity tools and solutions complicated

59%

lack confidence in quickly locating data for regulatory/ legal requirements

91%

face governance and compliance challenges



THE ATTACK SURFACE EXPLOSION

From Email-Only to Omni-Channel Risk

The traditional security perimeter no longer exists. Modern organizations face threats across email, Slack, Microsoft Teams, Zoom, and dozens of other collaboration platforms, each representing a potential entry point for sophisticated threat actors. Native security controls built into these platforms are proving inadequate against today's attacks. Security teams must shift their focus from detecting rare zero-day vulnerabilities to defending against attackers who systematically exploit human trust at scale.

What began as primarily an email security challenge has evolved into a complex omni-channel threat landscape. While 96% of organizations anticipate email security challenges throughout 2026, a striking 71% now specifically expect negative business impact from attacks targeting collaboration tools. This expansion shows no signs of slowing.

External threats exploit the fact that 8% of employees account for 80% of incidents.[1] Can you identify your 8% before attackers do?

AI can create highly realistic emails, messages, and voice deepfakes that are harder for users to recognize.

Techniques like ClickFix show how attackers convince users to execute malicious commands directly bypassing technical controls entirely.

"Employees often click malicious links despite training, which increases the risk of corporate phishing and credential compromise."

(South Africa, Healthcare)

Multi-Channel Threat Growth

Threats are accelerating across every channel. Email remains a primary attack target with 53% reporting increased phishing volume featuring malicious links or attachments and 48% seeing a rise in business email compromise. Collaboration tools face equal pressure, with 45% experiencing increased cyberattacks. Internal risks grow simultaneously: 42% report more data leaks from compromised employees, while another 42% see increases from malicious insiders.

The Native Security Gap

A dangerous disconnect exists between what organizations know about their security posture and what they're doing about it. While only 38% rely solely on native collaboration tool security, 71% expect attacks targeting these tools will cause negative business impact in 2026. In 2025, 67% agreed that native collaboration tool security was insufficient, a prediction that has proven accurate.

Native security tools were not architected to defend against sophisticated attacks targeting human psychology and trust. They lack the context-aware detection capabilities needed to identify when legitimate-looking communications are carefully crafted social engineering attempts. For organizations relying solely on these controls, every collaboration platform represents an undefended attack vector.

Business Impact Reality

When security incidents successfully penetrate organizational defenses, the financial consequences are devastating. Most organizations (71%) experience one to 10 insider-driven data exposure events monthly making breaches routine, not exceptional.

Real-world breaches underscore these findings. The 2024 Change Healthcare cyberattack demonstrates how human error can cascade into catastrophic costs. A low-level employee's credentials were compromised through a phishing email, granting attackers network access to systems that lacked multi-factor authentication. United Healthcare estimates the total response cost at $2.3 to $2.45 billion for this single incident.

The Scale of Modern Threats

Mimecast's threat detection identified 9.13 billion threats over the first nine months of 2025 illustrating the sheer volume of attacks organizations face daily.

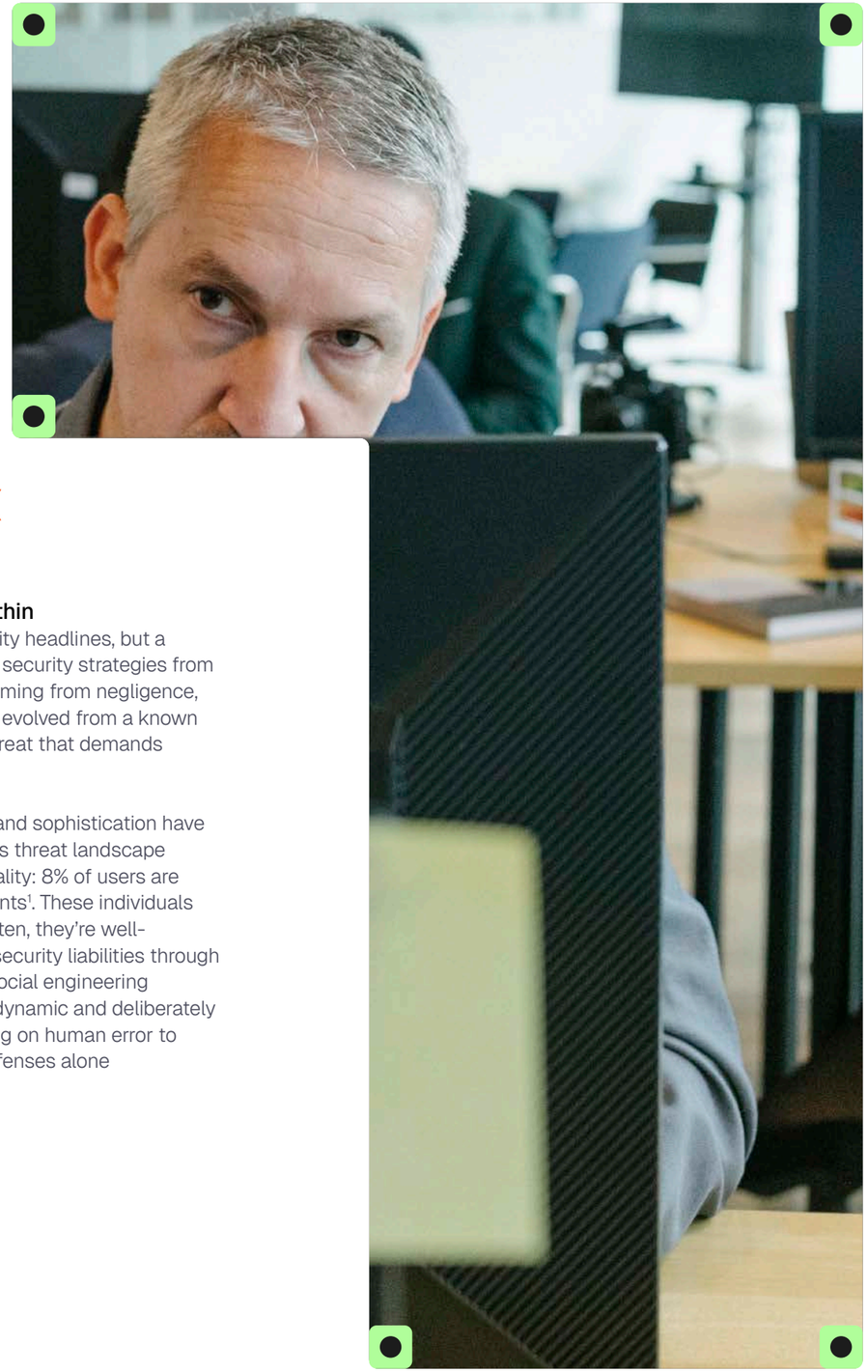
Attackers have evolved sophisticated tactics that exploit the trust inherent in business communications. They now deploy automated business email compromise conversation chains that can sustain believable exchanges over time. They deliberately switch communication channels—starting with email, moving to phone calls, then shifting to Microsoft Teams—specifically to bypass security controls that don't monitor across platforms. They weaponize trusted enterprise services like DocuSign and SharePoint, knowing that native security controls are configured to automatically trust these widely used platforms.

Organizations can no longer afford to treat email and collaboration platform security as separate concerns, nor can they continue relying on native controls that were never designed to stop human-targeted attacks at scale.

[1] This 8%/80% stat is from the Mimecast whitepaper The Size and Shape of Workforce Risk.

"Human risk is one of our most complex problems, as it stems from social engineering, which is difficult to mitigate. Therefore, we conduct active training and propose tools to block, control, and monitor humans, including AI tools for pattern detection."

(Spain, Financial Services)



THE INSIDER RISK IMPERATIVE

When the Threat Comes from Within

External threats dominate cybersecurity headlines, but a more insidious danger is undermining security strategies from the inside. Insider risk—whether stemming from negligence, compromise, or malicious intent—has evolved from a known vulnerability into a critical business threat that demands immediate strategic attention.

The challenge isn't new, but its scale and sophistication have reached unprecedented levels. Today's threat landscape is defined by a stark mathematical reality: 8% of users are responsible for 80% of security incidents[1]. These individuals aren't necessarily bad actors. More often, they're well-intentioned employees who become security liabilities through fatigue, distraction, or sophisticated social engineering attacks. Adversaries understand this dynamic and deliberately target these vulnerable users, counting on human error to provide entry points that technical defenses alone cannot prevent.

Three Distinct User Risk Profiles

Security teams must recognize and address three fundamentally different user risk categories, each requiring tailored prevention strategies:

The Distracted: The Unintentional Threat

These employees pose risks through careless behavior rather than malicious intent. Organizations are deploying multiple approaches to address this challenge. More than half conduct regular security training and awareness campaigns (53%) and continuously monitor for policy or data handling violations (52%). Nearly half (48%) deploy role-based access controls and data permissions. Just 37% provide contextual prompts or "nudges" to prevent risky actions in real time.

The Exploited: The Compromise Risk

Even security-conscious employees can become liabilities when adversaries specifically target them. To prevent targeted users from becoming compromised, nearly half use automated blocking or isolation of suspected account compromise (47%) and deploy AI-driven detection of targeted or unusual user activity (46%). Additionally, 46% provide real-time alerts and guided responses for high-risk users.

The Malicious: The Intentional Threat

Some users deliberately abuse access for personal gain, revenge, or external coercion—and this threat is accelerating at the exact same rate as unintentional risk. Over the past year, 42% of organizations report increased threats from malicious insiders, identical to the 42% seeing rises in negligent employee incidents. This parity reveals a critical reality: organizations cannot train their way out of insider risk. Organizations need technical controls that detect and prevent both careless mistakes and calculated exploitation.

The Critical Coordination Gap

The most alarming finding from our research isn't what organizations are doing, it's how they're doing it. While security teams deploy extensive controls across both people-focused and technology-focused domains, only 28% combine security awareness training (53%) and continuous monitoring (52%). This means organizations could be operating with fragmented defenses where preventive measures work in isolation rather than as an integrated system.
The consequences are severe: user risk profiles fail to inform technical control

"We try to educate our employees and familiarize them with the topic of risk. Education has become very important in this day and age."

(Germany, Financial Services)

[1]This 8%/80% stat is from the Mimecast whitepaper The Size and Shape of Workforce Risk.

deployment, behavioral analytics don't automatically trigger technical blocks, and technical alerts don't prompt targeted training interventions. Each security layer operates essentially blind to the others, creating exploitable vulnerabilities that sophisticated adversaries are increasingly prepared to leverage.

As one security leader in Italy's financial services sector demonstrated, coordination is achievable: "Every employee is a sensor: suspicious clicks trigger immediate micro-training; after two errors in the quarter, the privileged account is blocked until a video interview with the CISO." This approach illustrates what the 28% who coordinate successfully accomplish—behavioral detection triggers immediate response, pattern recognition escalates to access controls, and human verification occurs before restoration. Without that coordination, even well-resourced organizations risk deploying the right controls in the wrong isolation—security that exists but doesn't connect.

> "Human error is one of the main risks; users must be trained and made fully aware of the risks."
>
> (France, IT/Technology/Telecoms)

The Acceleration of Active Monitoring

Organizations are dramatically increasing their monitoring of internal activities to detect insider threats before they materialize. Monitoring adoption is accelerating: 59% now use integrated behavioral analytics (up from 50% in 2025), 56% analyze sentiment, and 48% manually review flagged communications. Yet the mix of manual and automated approaches reveals most programs remain immature.

The Path Forward

Insider risk has evolved from a periodic concern into a persistent operational reality that demands coordinated, intelligence-driven responses. Looking forward, 66% express concern that data loss from insiders will increase at their organization in the next 12 months, and an equal 66% worry that employees struggle to use data safely while complying with regulatory requirements.

The organizations succeeding in this environment aren't necessarily deploying more tools or conducting more training. Instead, they're connecting their people-focused initiatives with their technical controls, ensuring that behavioral insights inform access decisions and that security events trigger appropriate human interventions.

THE INTEGRATION PARADOX: WHEN MORE TOOLS BECOME A PROBLEM

The Attacker Advantage

While security teams struggle to connect their own systems, attackers face no such constraints. Modern attack chains seamlessly combine CAPTCHA-protected phishing pages, SVG-embedded JavaScript, and legitimate remote management tools in coordinated sequences that exploit the gaps between disconnected security controls.

The irony is brutal: organizations that successfully integrate their tools are more likely to report faster threat remediation (40%), comprehensive visibility (40%), and simplified security operations (37%). Yet most remain trapped in tool sprawl, unable to connect the systems meant to protect them.

The Coordination Crisis

The fragmentation extends beyond tools to strategy itself. Only 28% of organizations combine both regular security awareness training and continuous monitoring. Behavioral insights fail to inform technical controls. Technical detections don't trigger targeted user interventions. Security operates in functional silos rather than as a unified strategy. These are exactly the things attackers exploit.

Breaking the Cycle

The paradox: organizations need integration to manage complexity, but integration itself proves too complex to implement. Skills gaps, legacy constraints, vendor limitations, and organizational silos create barriers most teams cannot overcome alone.

Those who succeed see dramatic benefits. Those who fail remain trapped in tool sprawl—watching dashboards while attackers exploit the gaps between their disconnected defenses. The path forward requires platforms that integrate by design, not point solutions that promise eventual integration.

65% find cybersecurity tool integration complicated, yet for those that succeed, five major benefits can be felt:

- Better threat sharing to improve security posture
- A more comprehensive view of security environment
- Faster threat remediation
- Improved compliance and audit readiness
- Better event investigation capabilities

THE GOVERNANCE CRISIS

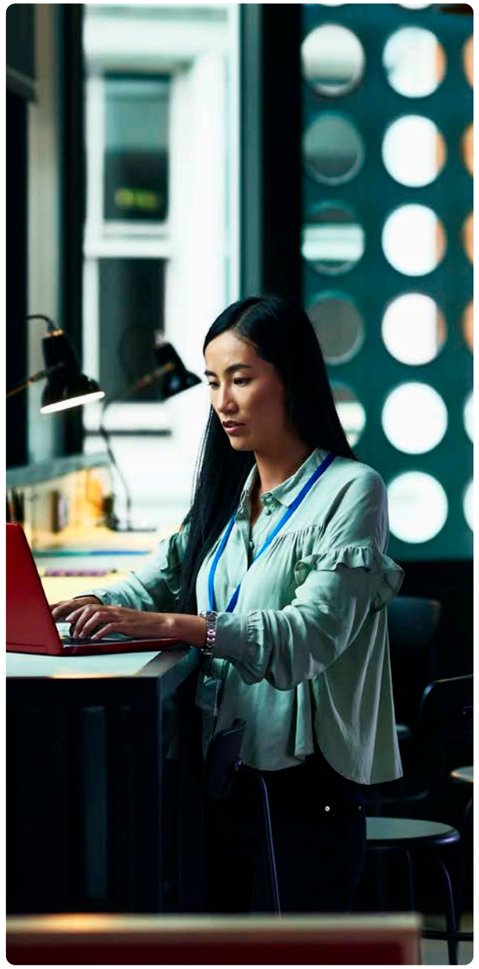
When Compliance Confidence Crumbles

As regulations multiply and data proliferates, security teams have become digital archaeologists, racing to locate data before regulatory deadlines expire or fines arrive. Despite massive investments in SIEM platforms, DLP solutions, and managed security services at scale, 59% of organizations lack confidence they can quickly locate and retrieve communications data when regulators demand it. When 91% face governance challenges, this isn't isolated implementation failure, it's systemic breakdown.

The Human Risk Dimension

Beyond location challenges, organizations grapple with human factors and emerging risks. A full 66% express concern that employees struggle to use data safely while complying with related regulations. The rise of generative AI tools has introduced new anxiety, with 80% worried about potential sensitive data leaks through these platforms.

The implications extend beyond inconvenience. Regulatory investigations, litigation holds, and audit requests all demand rapid data retrieval. Organizations that cannot deliver face financial penalties, legal exposure, and reputational damage. In an environment where attackers exploit ungoverned collaboration channels, shadow IT repositories, and misconfigured cloud storage during post-compromise exfiltration, governance failures create security vulnerabilities.



The Persistence of Manual Processes

Despite the availability of sophisticated automation technology, many organizations continue to rely on manual processes that cannot scale.

For compliance and data retention: only 37% have automated compliance tools across multiple channels, 23% manage policies manually via IT or compliance teams, 21% rely on built-in capabilities of communication platforms, and 18% have automated compliance tools for email only.

As one healthcare security practitioner in Spain observed, "Security policies should not be static and, therefore, should be reviewed and updated periodically, taking into account both the constantly evolving threat landscape and current laws and regulations." Manual processes make this continuous adaptation nearly impossible.

59% lack confidence in data retrieval + 36% rely on manual monitoring = Compliance crisis

"We've been using AI to minimize the major impact of human risk however [...] we're still attempting to determine whether we'd be better off without AI and continuing our practices manually."

(UK, Retail/Distribution/Transport – illustrating automation hesitation)

Converging Compliance Pressures

Multiple pressures are converging simultaneously. A total of 80% express concern about data leaks via GenAI tools, and 91% face obstacles ensuring employees adhere to compliance standards consistently.

These concerns exist alongside limited success in achieving governance goals through technology integration. Only 40% report benefiting from improved compliance and audit readiness as a result of integrating security tools. For the remaining 60%, compliance goals through integration have yet to be fully realized.

The Accelerating Challenge

If governance systems are breaking down under current threat volumes and data growth rates, AI-driven attacks will shatter what remains. The path forward requires more than deploying additional tools—it demands a fundamental rethinking of how organizations approach data governance, with emphasis on automation, centralization, and unified policy frameworks that can scale. Without this transformation, the governance crisis will evolve from a compliance problem into an existential business risk.

Four Pillars of Governance Failure

Governance challenges cluster around interconnected failures:

1. LIMITED ENFORCEMENT AUTOMATION:
Half of all organizations rely on manual compliance processes that cannot scale, resulting in inconsistent policy application, delayed responses to violations, and heavy reliance on human judgment.

2. INCONSISTENT RETENTION POLICIES ACROSS SYSTEMS:
Different policies governing email collaboration tools and cloud storage, with no unified retention schedule. Data may be kept too long (expanding discovery risk) or deleted too soon (creating compliance violations). Shadow IT compounds the problem by creating ungoverned repositories outside official policy frameworks.

3. AUDIT AND INVESTIGATION DIFFICULTY:
Data scatters across multiple platforms with no centralized search capability. Incomplete metadata and indexing force teams to manually reconstruct communication threads.

4. FRAGMENTED OVERSIGHT:
No single owner exists for communications governance. Responsibilities fragment across IT, legal, compliance, and security teams.

AI'S DOUBLE-EDGED SWORD

Racing to Deploy, Struggling to Defend

Organizations face a stark contradiction: AI represents both their most promising defense and their most concerning threat. While billions flow into AI-powered security tools, a dangerous preparation gap persists.

The numbers reveal the scope: 82% of security leaders express concern about AI being weaponized as an attack vector, with a similar proportion (71%) worried employees will fall victim to AI-enhanced social engineering. Data leakage through generative AI tools compounds these concerns, with 80% expressing worry about sensitive information exposure. Most striking, 69% consider it inevitable that AI will be used in an attack against their organization within the next 12 months.

Yet only 40% report being fully prepared with specific strategies for AI-driven threats. This 29-point gap between recognition and readiness represents a critical vulnerability window that sophisticated attackers are already exploiting.

Fragmented Defensive Deployment

AI defensive tool adoption shows progress but remains incomplete. Just over half of organizations (55%) now use AI for threat detection and real-time monitoring, up from 46% the previous year. Exactly half deploy AI for phishing analysis and response, endpoint protection, and automated incident response systems. Behavioral analysis and insider threat detection using AI also increases to 49%, up from 43% the prior year.

The inverse is equally telling: nearly half have not yet implemented AI for basic threat detection, half lack AI-powered phishing defenses, and 51% have no AI systems monitoring for insider threats or analyzing behavioral patterns. This creates two distinct cohorts: those racing ahead with comprehensive AI defenses, and those hesitating while threats accelerate.

The Tool-Training Imbalance

Investment patterns reveal a critical misalignment. Nearly half of responding organizations (48%) are implementing AI-powered monitoring and protection tools (the highest investment category). Yet training employees to recognize AI exploitation lags at just 44%, while only 41% have created specific AI usage policies or conduct simulated AI-driven phishing attacks (40%). Organizations prioritize technology acquisition over human capability development and governance frameworks. This imbalance creates strategic blind spots—deploying smarter systems while leaving personnel vulnerable to AI-enhanced social engineering.

69% say AI attacks are inevitable, yet only **40%** are fully prepared, resulting in a **29%** awareness-action gap.

"Uncontrolled AI poses a very high security risk."
(Spain, Energy/Oil/Gas/Utilities)

"We are constantly using AI to monitor human risks."
(US, IT/Technology/Telecoms)

Three Factors Driving Hesitation

Despite recognizing the inevitability of AI attacks, many organizations delay defensive AI deployment for three primary reasons:

1. Governance Concerns:
Organizations struggle with AI's rapid evolution, unsure how to implement controls that remain relevant. Regulatory ambiguity, particularly in regions like the European Union implementing the AI Act, creates friction that slows adoption.

2. Security Risks:
Leaders fear introducing new vulnerabilities through the very systems meant to protect them. Concerns span data exposure through generative AI tools, model poisoning, and adversarial attacks.

3. Proof of Value Requirements (Unclear ROI):
Organizations struggle to quantify AI effectiveness, contributing to delays. These hesitations carry legitimate concerns but impose real costs. Governance frameworks require time to mature, but 69% face inevitable AI attacks during that maturation period. Manual analysis cannot scale to match AI attack volumes. And the financial stakes are clear: a single major breach can cost billions.

"We do not use AI to any degree."
(UK, Public Sector)

"Attackers increase the risk of unintentional data leaks by using AI to create highly personalized emails that more easily trick employees."
(France, Financial Services)

The Current Threat Reality

Real-world attacks already demonstrate AI's offensive capabilities: automated BEC conversation chains that sustain believable exchanges for weeks, AI-generated voice phishing that mimics executives, and CAPTCHA-protected phishing pages that defeat automated analysis.

Traditional indicators of phishing—poor grammar, generic greetings, obvious formatting errors—disappear when AI generates content. AI lowers barriers to convincing attacks, enabling threat actors with limited technical skills to execute sophisticated campaigns at scale.

Strategic Imperatives

The AI arms race has arrived. Organizations deploying defensive AI now, with appropriate governance frameworks, position themselves to detect and respond to emerging threats Those awaiting perfect solutions face sophisticated attacks without adequate defenses.

The path forward requires balanced investment: sophisticated tools paired with comprehensive training, technical capabilities matched with clear policies, and rapid adoption tempered by appropriate governance. The threat landscape demands action.

HOW HUMAN RISK VARIES ACROSS GLOBAL MARKETS

Global Patters, Local Nuances

While human risk is universal, regional approaches vary dramatically based on regulatory environments, threat landscapes, cultural norms, and resource availability. This snapshot highlights key findings from nine major markets. For detailed country-by-country analysis, visit our regional insights page.

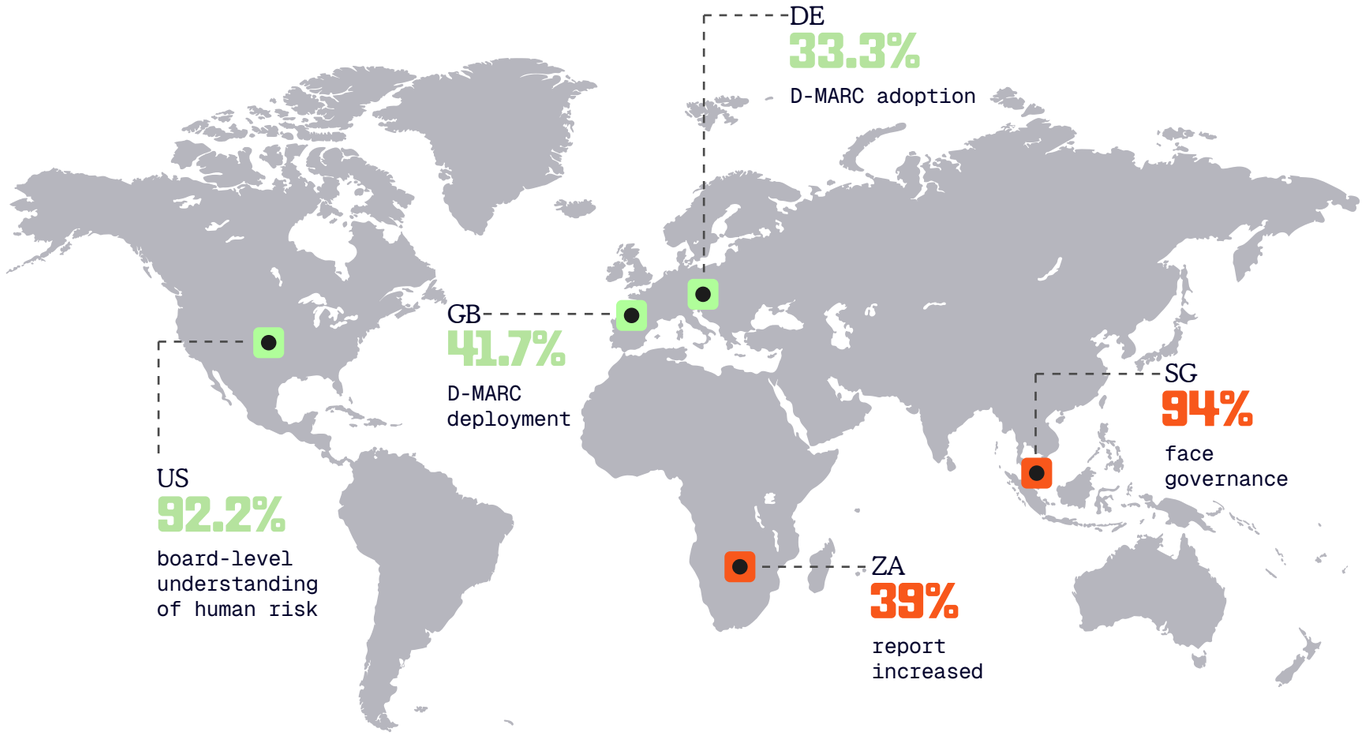
Three Tiers of Maturity

There are three levels of maturity when it comes to how organizations across the globe have implemented human risk management strategies:

AI Adopters (US, Singapore): High awareness + high adoption + seeing ROI. Leading in defensive AI deployment, strong people-technology integration, board-level engagement, willing to experiment and iterate.

Cautious Pragmatists (UK, Germany, France): High awareness + measured adoption + compliance focus. Privacy and governance considerations influence pace, strong security fundamentals, preference for proven technologies, and methodical evaluation before deployment.

Emerging Leaders (Spain, South Africa, Australia): Growing awareness + selective adoption + resource focus. Rapid maturity development, innovation balanced with constraints, ROI-focused decision making, learning from mature markets while adapting to local context.



Regional Highlights

US - United States: 92.2% board-level understanding of human risk (highest globally), 38.4% DMARC adoption, 85.4% AI concern (highest globally), leading in coordinated people + technology approaches. Challenge: Tool sprawl despite bigger budgets. Lesson: Early AI adoption doesn't require perfection.

GB - United Kingdom: 41.7% DMARC deployment (highest in Europe), 83% AI concern but slower adoption, strong GDPR-driven compliance foundations. Challenge: Awareness-action gap on AI defenses. Lesson: Privacy-by-design creates sustainable programs.

DE - Germany: 33.3% DMARC adoption, 81% see increased attack sophistication, methodical "study-test-deploy" approach, strong data sovereignty focus. Challenge: Systematic testing delays deployment. Lesson: Rigorous testing creates durable security programs.

FR - France: Strong financial services driving standards, sophisticated AI threat understanding, selective adoption with privacy guardrails. Challenge: Balancing innovation with privacy protection. Lesson: Thoughtful adoption based on clear threat understanding works.

ES - Spain: Rapid security maturity, "prove it first" approach to AI, emphasis on continuous policy updates, active experimentation with governance awareness. Challenge: Demonstrating value before widespread deployment. Lesson: Continuous policy adaptation creates agile programs.

ZA - South Africa: 39% report increased account takeover, high concern about training effectiveness gaps, focus on maximizing ROI under resource constraints. Challenge: Skilled personnel shortages in competitive global market. Lesson: Resource constraints drive efficiency innovation.

SG - Singapore: One of only two markets globally classified as an "AI Adopter", Singapore leads in defensive AI deployment and people-technology coordination, outperforming APAC peers amid a region where 94% face governance challenges. Challenge: Maintaining leadership as peers close the gap. Lesson: Government-industry collaboration accelerates maturity.

AU - Australia: Strong email security fundamentals, critical infrastructure requirements driving investment, government-led frameworks (Essential Eight) providing clear guidance. Challenge: Remote operations creating unique security challenges. Lesson: Clear regulatory requirements accelerate maturity.

Universal Challenges Despite Regional Differences: All regions face 91-93% governance challenges, 65%+ integration complexity, 69%+ AI attack inevitability, with only 28% combining both regular security awareness training and continuous monitoring.

STRATEGIC TAKEAWAY: While tactics vary by region, the strategic imperative is universal. Human risk management requires integrated platforms coordinating people-focused initiatives, technology-focused controls, governance frameworks, and continuous adaptation. Point solutions and siloed initiatives fail regardless of geography. See more detailed regional analysis.

KEY TAKEAWAYS & RECOMMENDATIONS

What are your next steps?
This year's survey data reveals five critical action areas where forward-thinking security leaders are making measurable progress. Here's how to translate research insights into organizational action, aligned with proven solution approaches:

1. Secure Email and Collaboration Channels

The Challenge: 71% expect negative impacts from a collaboration attack, 96% expect email challenges, and 64% agree that most native security tools are insufficient.

Actions: Unify attack surface protection. Stop treating email and collaboration security as separate problems. Deploy unified threat protection across email AND collaboration platforms, implement AI-powered adaptive detection (55% of survey respondents are already using this), extend email security to Teams/Slack/Zoom, and monitor for BEC and impersonation across all channels.

What to Look For: Unified platforms protecting both email and collaboration tools. AI-powered detection that adapts to emerging threats in real time. Security awareness at the moment of risk, not quarterly training. Integrated compliance reporting across all communication channels.

Success Metrics: Reduction in successful attacks, time to detect/remediate across channels, coverage percentage, and user reporting rates.

2. Implement Human Risk Management

The Challenge: Only 28% combine both regular security awareness training and continuous monitoring, 8% of employees cause 80% of incidents[1], and insider incidents have the potential to cost $13.1M with six monthly occurrences.

Actions: Identify and score risky users through behavioral analytics, create three user risk profiles (negligent, compromised, targeted), deploy continuous monitoring across communication platforms, balance productivity with risk through adaptive policies, and focus resources on your highest-risk 8% of users.

What to Look For: Platforms correlating behavior across channels, real-time risk scoring, training platform integration, incident response automation, and user risk visibility.

Success Metrics: Reduction in insider incidents, user risk score and time to detect improvements, training effectiveness (behavior change), and prevention costing less than security incidents.

3. Strengthen Data Loss Prevention and Compliance

The Challenge: 59% lack data retrieval confidence, 91% face governance challenges, 66% are concerned about insider data loss, and 80% are concerned about GenAI leaks.

Actions: Implement automated compliance enforcement, create consistent retention policies across systems, deploy integrated DLP solutions (only 47% currently using dedicated DLP), enable rapid data location for audits, and address GenAI data leaks through monitoring and approved alternatives.

What to Look For: Unified governance across platforms, automated compliance workflows, insider risk detection, audit-ready reporting, GDPR/CCPA support, and SIEM/SOAR integration.

Success Metrics: Data retrieval time improvement, increased percentage governed by automation, reduction in data leaks, audit findings reduction, and confidence improvement.

4. Consolidate and Integrate Security Tools

The Challenge: 65% find integration too complicated, tool sprawl hindering response, and only 28% combine both regular security awareness training and continuous monitoring.

Actions: Audit stack for redundancies and gaps, prioritize platforms with multiple capabilities over point solutions, seek vendors with open APIs for SIEM/SOAR/IAM integration, establish centralized visibility, and coordinate people and technology initiatives (connect training with threat detection, link risk scores with access controls).

What to Look For: Platforms with multiple capabilities, proven API ecosystems, SIEM/SOAR integration, unified visibility, and customer references demonstrating successful consolidation.

Success Metrics: The ROI is clear, but most organizations remain trapped in fragmentation preventing unified response to attacks spanning email, collaboration tools, and data repositories. Benefits of this undertaking are tool count reduction, integration completeness percentage, detection time across environment, security team efficiency (alerts to incidents ratio), and reduced total cost of ownership.

[1] This 8%/80% stat is from the Mimecast whitepaper The Size and Shape of Workforce Risk.

5. Prepare for AI-Driven Threats

The Challenge: 69% see AI attacks as inevitable, only 40% are fully prepared, 80% are concerned about AI vectors and social engineering, and investment favors monitoring and protection tools (48%) over training employees to avoid exploitation (44%) and creating policies on AI usage (41%).

Actions: Deploy AI-powered detection (55% already using for threats, 50% for phishing), create AI usage policies and governance (currently only 41% have policies), train employees on AI-driven social engineering (only 44% currently training), develop internal AI tools to counter threats (46% developing), and balance AI deployment with human judgment training.

What to Look For: AI detecting AI-generated content, behavioral models spotting AI social engineering, governance frameworks for GenAI usage, and training for AI exploitation techniques, explainability, and transparency.

Success Metrics: Detection of AI-generated attacks, employee reporting of suspected AI attacks, policy compliance rates, training completion and behavior change, and incident prevention.

The Business Case

If you need help getting the resources required to accomplish your human risk management goals, here are clear numbers that help make the business case for an investment in HRM solutions:

- Expected $13.1M average cost per insider incident
- 6 incidents per month on average
- $943.2M annual insider risk exposure
- 71% expect business impact from collaboration tool attacks in 2026
- $2.3-2.45B Change Healthcare breach cost from a single compromised employee credential

The cost of inaction exceeds the investment in human risk management solutions.

CONCLUSION: THE HUMAN RISK RECKONING

The data from 2,500 organizations across nine countries delivers an unequivocal message: human risk has become cybersecurity's defining challenge, demanding immediate coordinated action.

The Stats are Clear Evidence

This report is designed to deliver insight into human risk and help provide security leaders with guidance on next steps. This year's stats are clear evidence that the time to act is now.

The Execution Gap

The crisis lies not in recognition but in translation. Organizations know what threatens them, yet only 28% combine both regular security awareness training and continuous monitoring. This awareness-action gap is where the breach occurs.

Consider the contradiction: 91% of organizations acknowledge obstacles to employee compliance and 96% recognize incomplete protection—yet nearly three-quarters still operate with fragmented defenses where people-focused and technology-focused controls never communicate. Attackers don't exploit what organizations fail to see. They exploit what organizations see but fail to connect.

Five Interconnected Priorities for 2026

The critical gaps identified in this report are not isolated problems requiring separate solutions. They are interconnected vulnerabilities stemming from a fundamental failure to treat human risk as an integrated strategic priority:

1. Secure all communication channels with unified protection.

2. Manage human risk through behavioral analytics and user-centric controls.

3. Govern data with automated compliance and rapid retrieval.

4. Integrate security tools into unified platforms.

5. Prepare for inevitable AI-driven threats with defensive AI and governance.

These five priorities are mutually reinforcing. Unified channel protection feeds behavioral analytics with richer data. Better human risk scoring informs governance policies. Integrated platforms make all of it operationally feasible. And AI readiness underpins every layer. Organizations that treat these as five separate line items will replicate the very fragmentation this report warns against.

Organizations Must Move from Awareness to Execution

Organizations that treat human risk management as an integrated strategic priority will prevent breaches, protect their reputations, and demonstrate genuine security maturity. Those that continue with piecemeal approaches will struggle to contain costs, maintain compliance, and defend against attackers who exploit the gaps between disconnected systems.

2026 is the year to move from awareness to execution. Not because the data suggests it. Because the data demands it. The organizations that close the gap between knowing and doing will define the next era of cybersecurity resilience. The rest will become case studies in what happens when awareness alone is mistaken for defense. The question facing every security leader is simple: Will you act before the next incident, or after?

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.

mimecast.com