proofpoint

REPORT

2026 Voice of the CISO

Higher stakes, closer scrutiny and a more urgent CISO agenda: global insights into CISO challenges, expectations and priorities



Table of contents

Introduction 03

Chapter 1
AI has become the defining CISO mandate 04

Chapter 2
Confidence is improving as concern shifts to workplace technology 07

Chapter 3
Human risk is now a core data security challenge 11

Chapter 4
Data loss incidents are declining, but the business impact is intensifying 14

Chapter 5
Complexity is outpacing control 17

Chapter 6
Board alignment is improving, but expectations are rising 20

Conclusion 26

Methodology and appendix 27

Introduction

Over the past year, the cybersecurity conversation has changed. For several years, CISOs have been leading a landscape in which every major threat seemed to be rising at once. This year's findings suggest a more nuanced picture. Fewer security leaders expect their organisation to experience a material cyberattack in the next 12 months, and fewer report material loss of sensitive information than in 2025.

That progress is encouraging. It shows that investments in security controls, governance and response are making a difference. But it should not be mistaken for a simpler operating environment. Cyber risk is not disappearing; it is moving deeper into the systems, identities and workflows that power modern work.

AI sits at the centre of that shift. As assistants, copilots, automation and public GenAI tools become embedded in everyday business processes, CISOs are relied on to enable innovation whilst preventing sensitive data, privileged access and critical workflows from being exposed. That dual responsibility is quickly becoming one of the defining challenges of the role.

At the same time, human risk remains central to the CISO agenda. Data rarely leaves an organisation in isolation. It moves through people, permissions, applications and devices. Whether the risk comes from a careless user, a malicious insider, a compromised account or a departing employee, protecting information now requires a deeper understanding of behaviour, context and intent.

The boardroom conversation is also changing. Cybersecurity is increasingly discussed in terms of business valuation, downtime, customer trust, regulatory exposure and operational resilience. That is a positive development, but it also raises expectations. CISOs must now translate complex technical risk into business decisions whilst governing AI, protecting data and reducing human-centric risk.

This year's Voice of the CISO report captures that transition through the perspectives of 1,600 security leaders across 16 countries. It shows where resilience is improving, where pressure is intensifying and how the CISO mandate is being rewritten for a world where people, data, identity and intelligent systems are increasingly inseparable.

We thank all participants for their time, candour and insight. Their perspectives help build a clearer view of the modern CISO experience and the priorities that will shape cyber resilience in 2026 and beyond.



Patrick Joyce
Global Resident CISO,
Proofpoint

CHAPTER 1

AI has become the defining CISO mandate

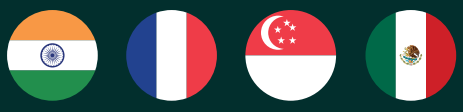
In 2025, AI was already a major concern for CISOs. In 2026, it has become the defining mandate: 78% of global CISOs say GenAI is a security risk to their organisation, up from 60% last year; 77% are concerned about losing customer data through public GenAI platforms and tools.

At the same time, AI's role in cybersecurity is becoming increasingly multifaceted: 85% say enabling the safe use of AI assistants, copilots and automation technologies is a top priority over the next two years; another 85% are looking to deploy AI-powered capabilities to help protect their organisation against human error and advanced human and AI-centric cyberthreats.

This duality is the essence of the AI challenge. Security leaders need to govern how employees use AI whilst also exploring AI as a means of improving protection. They must support innovation, productivity and competitive advantage without allowing sensitive data to be exposed through public tools, embedded assistants, autonomous agents or automations.

Many organisations are responding with restrictions: 78% of CISOs say their company blocks or restricts employee usage of GenAI tools, up from 59% in 2025. Restriction may be necessary in some contexts, but it's unlikely to be sufficient as AI becomes embedded in everyday applications. The more AI becomes part of normal work, the more governance must move from simple allow-or-block decisions to granular control, monitoring and policy enforcement.

The resourcing challenge is stark: 79% of CISOs say they're expected to manage AI-related risks without a proportional increase in resources or expertise. That finding is central to the 2026 report. AI risk is scaling faster than governance, and CISOs are being asked to manage it whilst also securing data, reducing human risk, meeting board-level requirements and maintaining operational resilience.



Regional nuance: AI governance is outpacing resources

India reports the highest GenAI risk concern and AI resource gap, both at 92%. France shows the strongest control response, with 95% blocking or restricting GenAI use and 93% making safe AI a top priority. Singapore is high on employee AI-exposure risk (91%) and GenAI restrictions (89%), whilst Mexico stands out for resourcing pressure, with 90% saying they are expected to manage AI-related risks without proportional resources or expertise.

AI risk is now widespread, but the strongest signal differs by market. In some countries, it manifests as tighter restrictions; in others, as a stronger focus on safe use, higher employee exposure or a mismatch between expectations and available resources.

Country matrix:

Country	Highest AI signal	Secondary AI signal
US	Safe AI use top priority (90%)	Blocks/restricts employee GenAI (89%)
Canada	Safe AI use top priority (91%)	Employees likely expose data via AI (83%)
France	Blocks/restricts employee GenAI (95%)	Safe AI use top priority (93%)
Germany	GenAI security risk (77%)	Blocks/restricts employee GenAI (75%)
Netherlands	Safe AI use top priority (90%)	GenAI security risk (83%)
Mexico	AI risk without more resources (90%)	Safe AI use top priority (90%)
UAE	Safe AI use top priority (86%)	AI risk without more resources (75%)
Saudi Arabia	Safe AI use top priority (72%)	AI risk without more resources (65%)
Australia	Safe AI use top priority (89%)	GenAI security risk (85%)
Singapore	Employees likely expose data via AI (91%)	Blocks/restricts employee GenAI (89%)
Japan	Safe AI use top priority (66%)	AI risk without more resources (65%)
India	AI risk without more resources (92%)	GenAI security risk (92%)
Brazil	Safe AI use top priority (87%)	Blocks/restricts employee GenAI (77%)
Italy	Safe AI use top priority (90%)	AI risk without more resources (81%)
Spain	Safe AI use top priority (93%)	Blocks/restricts employee GenAI (79%)
UK	Safe AI use top priority (80%)	AI risk without more resources (72%)

78%

say GenAI is a security risk

85%

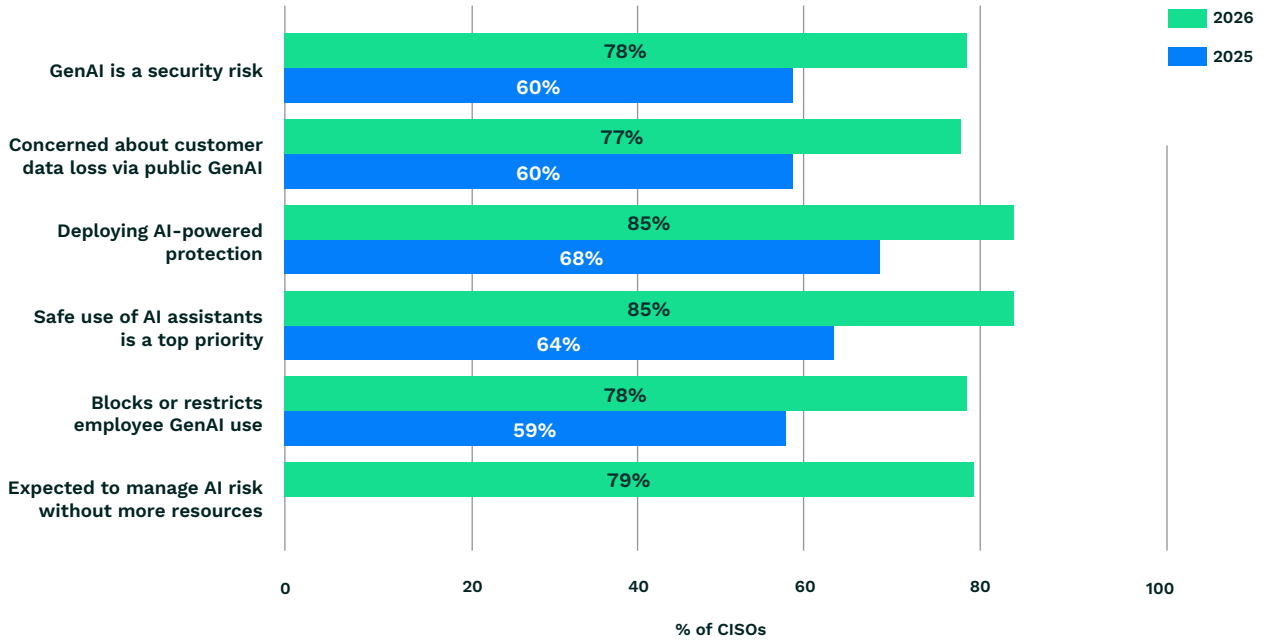
say safe AI is a top priority

79%

manage AI risk without proportional resources



The AI mandate expands faster than resources



“AI is now central to the CISO agenda. Security leaders are being asked to enable AI assistants, copilots and automation whilst preventing sensitive data from being exposed through the same tools. Blocking access may reduce immediate risk, but it will not solve the governance challenge. As AI becomes embedded in everyday work, CISOs need granular controls, stronger visibility and the resources to manage risk at the same speed the business is innovating.”



Judy Molenaar
Vice President, Information Security and Chief Information Security Officer, Surescripts, LLC.

CHAPTER 2

Confidence is improving as concern shifts to workplace technology

For several years, Voice of the CISO research has captured a profession bracing for impact. In 2026, the tone is different. Global CISOs are still concerned, but they are less likely to view a material cyberattack as imminent: 61% believe their organisation is at risk of a material cyberattack in the next 12 months, down from 76% in 2025. The proportion who say such an attack is very likely also fell, from 36% to 29%.

There is a similar signal in data loss: 53% of CISOs say their organisation dealt with a material loss of sensitive information in the past 12 months, down from 66% in 2025. This is not a declaration of safety—more than half of global CISOs still report material data loss. But it does suggest that some organisations are making measurable progress in reducing incident frequency.

That improvement sits alongside continuing concern about preparedness: 56% say their organisation is unprepared to cope with a targeted cyberattack in 2026, only slightly down from 58% last year. This is the tension at the heart of 2026 findings—fewer CISOs believe a material attack is imminent, but there is no broad sense that the challenge has been solved.

The country-level picture shows the scale of variation. India reports the highest likelihood of a material cyberattack at 94%, followed by the US at 89% and Australia at 78%. At the other end of the spectrum, Canada reports 39%, Mexico 44% and Japan 46%. Reported material data loss also varies sharply: the US is the highest at 84%, followed by India at 76% and Australia at 68%, whilst Canada and France are the lowest at 36% each.

Regional nuance: APJ leads attack expectation at 72%

APJ reports the highest regional average for material cyberattack likelihood at 72%, compared with 59% in EMEA and 57% in the Americas. It also reports the highest regional average for material data loss at 64%, compared with 53% in the Americas and 47% in EMEA. Within APJ, India stands out across several measures: 94% believe a material cyberattack is likely; 76% report material data loss; 93% identify human risk as the biggest vulnerability; and 92% say GenAI is a security risk. Japan is at the other end of the regional profile, with consistently lower concern across attack likelihood, burnout and several AI-risk indicators.

Together, these findings show why the confidence story cannot be read in isolation. Concern is shifting towards the systems and platforms CISOs are most worried about; identity, collaboration, SaaS, cloud file-sharing and AI-enabled workflows.

61%

believe a material cyberattack is likely in the next 12 months

56%

say their organisation is unprepared for a targeted cyberattack

53%

dealt with material data loss in the past 12 months

Likelihood of a material cyberattack

Highest countries

India 94%

US 89%

Australia 78%

Lowest countries

Canada 39%

Mexico 44%

Japan 46%

Material data loss experienced

Highest countries

US 84%

India 76%

Australia 68%

Lowest countries

Canada 36%

France 36%

Germany 37%

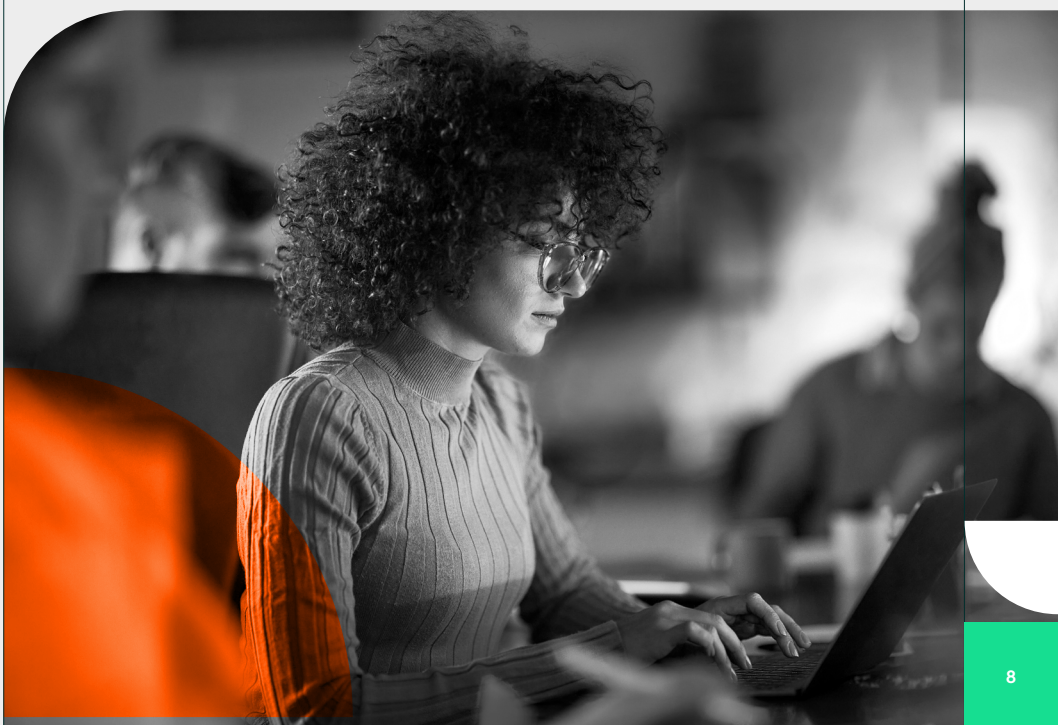
The shift is reflected in the threat inventory. Traditional threat categories are still prominent, but several have declined sharply year on year. Email fraud fell from 37% to 27%; ransomware dropped from 36% to 23%; malware fell from 33% to 19%; and insider threats declined from 37% to 30%.

The most selected threat in 2026 is cloud account takeover or compromise, cited by 33% of CISOs. This is a small change from 34% in 2025, but its position at the top of the list is significant. The leading concern is not a single payload or campaign type. It is the compromise of the accounts and environments employees rely on to work, communicate and access data.

When CISOs are asked which systems they are most worried about introducing risk, the shift becomes clearer. Collaboration platforms rank first at 34%. AI assistants, copilots or autonomous agents embedded in workflows and SaaS applications with third-party integrations follow closely at 33% each. Public GenAI tools are next at 31%, followed by cloud storage and file-sharing platforms at 30%, and APIs and automation tools at 29%.

This is a very different centre of gravity from a list led exclusively by ransomware, malware or email fraud. The systems causing concern are the same ones businesses rely on to move faster across knowledge of work, customer engagement, product development, sales, finance and operations. They also connect to identity, access and sensitive data.

For CISOs, the implication is practical. Defending the organisation increasingly requires visibility across the places where work happens and the ability to enforce policy without slowing business momentum. The security model must account for people creating and moving data across cloud platforms, collaboration environments, SaaS integrations and AI-embedded workflows.





Regional nuance: Workplace technology risk fragments by market

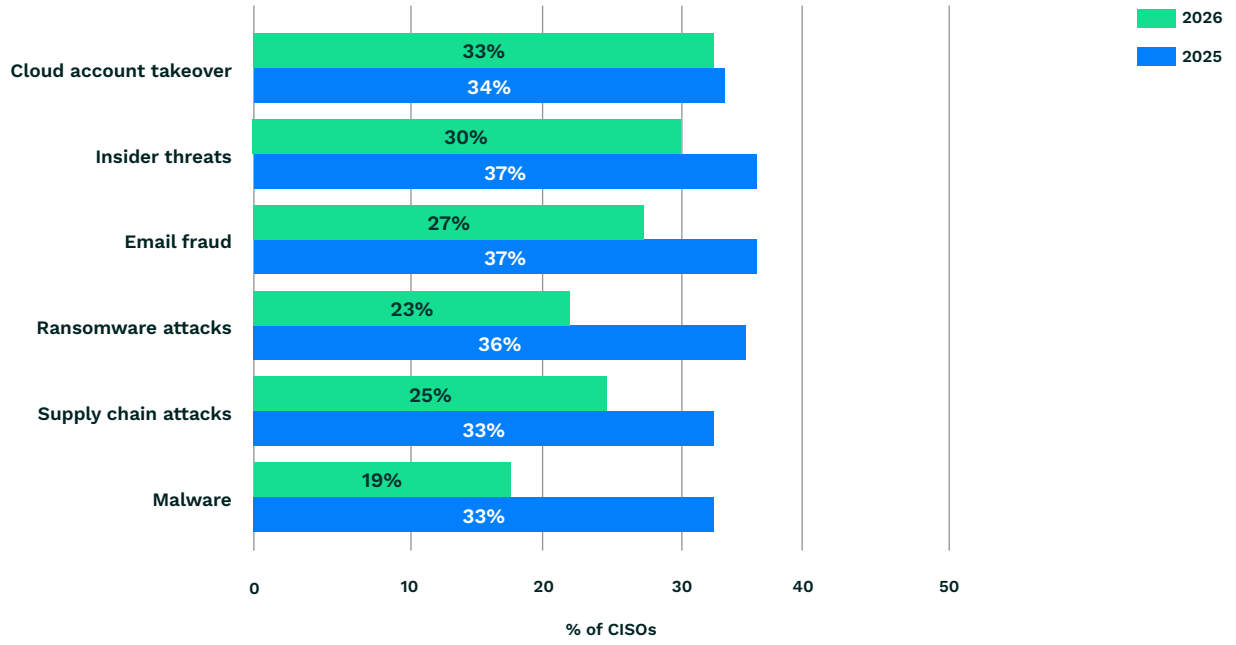
The systems introducing risk differ sharply by geography. Japan leads concern around collaboration platforms (44%); Brazil leads on AI assistants and autonomous agents (46%); Canada leads on SaaS and third-party integrations (44%); and Australia and Japan are highest on public GenAI tools (41%). Saudi Arabia is the only market where APIs and automation tools lead (39%), underscoring how integrated workflows are reshaping the attack surface differently by region.

The risk has not moved to one new platform. It has moved into the everyday work fabric, with different primary and secondary concerns by market.

Country matrix:

Country	Primary signal	Secondary signal
US	AI assistants/agents (41%)	APIs/automation (32%)
Canada	SaaS/third-party integrations (44%)	AI assistants/agents (41%)
France	Collaboration platforms (37%)	Public GenAI tools (35%)
Germany	Cloud storage/file sharing (32%)	Collaboration platforms (30%); SaaS/ third-party integrations (30%)
Netherlands	Collaboration platforms (35%)	SaaS/third-party integrations (31%)
Mexico	Collaboration platforms (38%)	SaaS/third-party integrations (37%)
UAE	Microsoft 365 (36%); Public GenAI tools (36%)	AD/identity infrastructure (35%)
Saudi Arabia	APIs/automation (39%)	AD/identity infrastructure (36%)
Australia	Public GenAI tools (41%)	SaaS/third-party integrations (37%)
Singapore	APIs/automation (32%); Cloud storage/file sharing (32%); Collaboration platforms (32%)	Public GenAI tools (31%)
Japan	Collaboration platforms (44%)	Public GenAI tools (41%)
India	AI assistants/agents (42%)	AD/identity infrastructure (34%); Collaboration platforms (34%)
Brazil	AI assistants/agents (46%)	Collaboration platforms (40%)
Italy	SaaS/third-party integrations (41%)	Cloud storage/file sharing (39%)
Spain	Public GenAI tools (38%)	AI assistants/agents (34%)
UK	SaaS/third-party integrations (33%)	AD/identity infrastructure (32%); Collaboration platforms (32%); Perimeter devices (32%)

Traditional threat concern falls year on year



“This year’s findings point to progress, but not certainty. Fewer CISOs expect a material cyberattack and fewer report material data loss, yet more than half still feel unprepared for a targeted attack. The centre of concern is shifting from familiar threat categories to the workplace technologies people use every day. The priority now is turning improved confidence into practical resilience across identities, collaboration platforms, cloud environments, SaaS and AI-enabled workflows.”



Phil Ross
Chief Information Security Officer, Air New Zealand

CHAPTER 3

Human risk is now a core data security challenge

Human risk is no longer a peripheral concern in the CISO's risk register. In 2026, it is central to how organisations understand data security: 79% of CISOs say human risk is their organisation's biggest cyber vulnerability, up from 66% in 2025. This is one of the largest year-on-year shifts in the report.

The data loss findings explain why. Among organisations that dealt with material loss of sensitive information, the leading root cause was malicious or criminal insiders, cited by 46% of CISOs. Careless insiders and compromised insiders were each cited by 38%. Misuse or misconfiguration of AI tools followed closely at 37%, alongside external attacks and third-party compromise attacks at 36%.

These findings show how data loss is increasingly shaped by a combination of behaviour, identity and tooling. The traditional distinction between insider and outsider risk is less useful when credentials can be stolen, permissions can be misused, AI tools can be misconfigured and departing employees can take sensitive information with them. The risk often sits at the intersection of people, identities, permissions and systems rather than in either category alone.

Departing employees remain a particularly acute challenge: 93% of CISOs whose organisations experienced material data loss say employees leaving the business played a role. This finding reinforces the importance of protecting data across the full employee lifecycle, from onboarding and access provisioning to monitoring, offboarding and post-departure controls.

Among organisations that experienced material data loss, 97% say they have visibility into how many data repositories and/or GenAI tools their organisation has in use. But visibility is only a starting point. The greater challenge is turning that visibility into real-time, context-aware controls that understand user intent, data sensitivity, permissions and movement across modern work environments.



Regional nuance: Human risk peaks in France, India and Singapore

Human risk is highest in France (95%), followed by India (93%) and Singapore (92%). Japan is lowest at 62%. Among organisations that experienced material data loss, the root-cause pattern is more varied—Brazil is highest for malicious or criminal insiders (66%), the UAE is highest for careless-insider risk and lost or stolen devices (52% each) and Australia is highest for compromised insiders (50%).

The global root-cause story is human-centric, but the local shape of that risk varies. Some markets skew towards malicious insiders, others towards careless behaviours, compromised identities, AI misconfiguration or lost devices.

Country matrix:

Country	Primary root cause	Secondary root cause
US	Compromised insider (45%); Malicious/ criminal insider (45%)	External attack (39%)
Canada	Malicious/criminal insider (47%)	AI misuse/misconfiguration (44%)
France	Careless insider (47%)	Malicious/criminal insider (39%)
Germany	Careless insider (46%)	External attack (41%); Third-party compromise (41%)
Netherlands	Compromised insider (42%); Malicious/ criminal insider (42%)	AI misuse/misconfiguration (34%); Third-party compromise (34%)
Mexico	Malicious/criminal insider (56%)	Careless insider (44%)
UAE	Careless insider (52%); Lost/stolen devices (52%); Malicious/criminal insider (52%)	AI misuse/misconfiguration (46%)
Saudi Arabia	External attack (38%)	Compromised insider (36%)
Australia	Compromised insider (50%)	Careless insider (47%)
Singapore	Malicious/criminal insider (44%)	Compromised insider (43%)
Japan	Malicious/criminal insider (53%)	Compromised insider (49%)
India	Malicious/criminal insider (47%)	External attack (42%)
Brazil	Malicious/criminal insider (66%)	AI misuse/misconfiguration (53%)
Italy	Malicious/criminal insider (41%)	Careless insider (39%); External attack (39%)
Spain	Malicious/criminal insider (40%)	Third-party compromise (38%)
UK	Compromised insider (48%)	Malicious/criminal insider (44%)

79%

say human risk is the biggest cyber vulnerability

93%

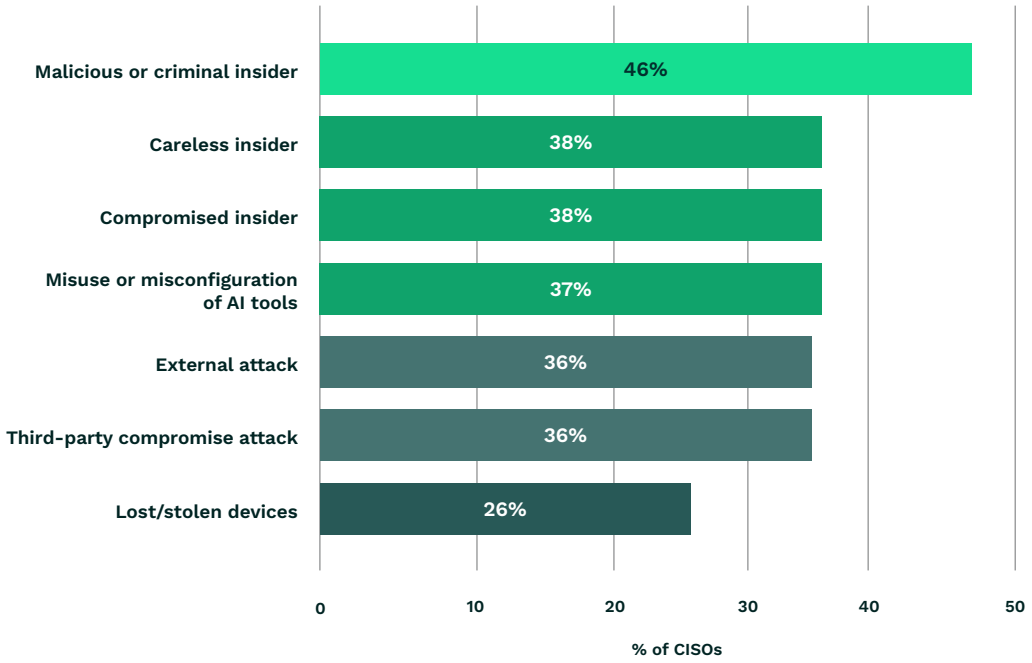
say departing employees played a role in data loss

37%

cite misuse or misconfiguration of AI tools as a data loss root cause



Root causes of material data loss in 2026



> Human risk has become inseparable from data security. The leading causes of data loss now sit at the intersection of people, identity, access and intent—whether the user is malicious, careless or compromised. That means organisations cannot rely on technology controls alone. They need a human-centric security model that follows sensitive data across the employee lifecycle, especially when people change roles, access new tools or leave the business.



Param Vig
Chief Information Security Officer, Solventum

CHAPTER 4

Data loss incidents are declining, but the business impact is intensifying

On the surface, the data loss picture appears to be improving. The proportion of CISOs reporting material data loss has fallen year on year. But for the organisations that do experience it, the consequences are becoming more severe.

Among those organisations, regulatory sanctions rose from 34% to 40%. Financial loss increased from 27% to 38%. Post-attack recovery costs climbed from 32% to 38%. Reputational damage rose from 31% to 37%, and credential theft also reached 37%. Loss of critical data increased to 36%, whilst loss of customers remained comparatively lower at 28%.

The story, therefore, is not simply fewer incidents; it is fewer incidents with sharper business consequences. Data loss is increasingly viewed through the same lens boards use for broader cyber risk: financial exposure, operating disruption, regulatory pressure, customer trust and long-term reputation.

This shift helps explain why data protection, identity security and AI governance are becoming strategic priorities: 85% of CISOs say these areas are strategic priorities for their organisation; 86% say they have continuous visibility and control over sensitive data across cloud, collaboration tools, endpoints and AI systems. The same proportion say their current controls effectively mitigate risks introduced by AI, SaaS and modern work patterns.

These are strong signals of maturity. But they sit alongside the persistent human risk and data movement challenges outlined in the previous chapter. Control may be improving, yet the environments they protect are expanding. Sensitive information now moves across more employees, applications, repositories, AI tools and automated workflows than ever before. The business impact of getting that wrong is rising.



Regional nuance: Fewer incidents, sharper consequences

The impact of data loss is not uniform. Regulatory sanctions are highest in France (47%), followed by Australia and Singapore (46% each). Post-attack recovery costs are most acute in Brazil (55%). Japan leads on loss of critical data (55%), the UAE leads on loss of customers (52%) and the UK is highest for reputational damage (45%).

The regional story is not only where data loss happens, but how it affects the business. The dominant consequence differs by market, from sanctions and recovery costs to customer loss and reputation.

Country matrix:

Country	Primary consequence	Secondary consequence
US	Financial loss (44%)	Reputational damage (39%)
Canada	Credential theft (42%); Regulatory sanctions (42%)	Financial loss (33%)
France	Regulatory sanctions (47%)	Loss of critical data (44%)
Germany	Recovery costs (43%)	Financial loss (41%)
Netherlands	Loss of critical data (45%)	Financial loss (37%); Reputational damage (37%)
Mexico	Recovery costs (54%)	Loss of critical data (46%)
UAE	Loss of customers (52%)	Reputational damage (50%)
Saudi Arabia	Regulatory sanctions (38%)	Recovery costs (36%)
Australia	Financial loss (49%)	Regulatory sanctions (46%)
Singapore	Regulatory sanctions (46%)	Recovery costs (44%)
Japan	Loss of critical data (55%)	Credential theft (45%)
India	Recovery costs (45%); Regulatory sanctions (45%)	Financial loss (43%)
Brazil	Recovery costs (55%)	Loss of critical data (43%); Regulatory sanctions (43%)
Italy	Loss of critical data (43%)	Credential theft (39%)
Spain	Credential theft (38%); Regulatory sanctions (38%)	Loss of critical data (33%); Recovery costs (33%)
UK	Reputational damage (45%)	Credential theft (40%); Financial loss (40%)

40%

experienced regulatory sanctions after data loss

38%

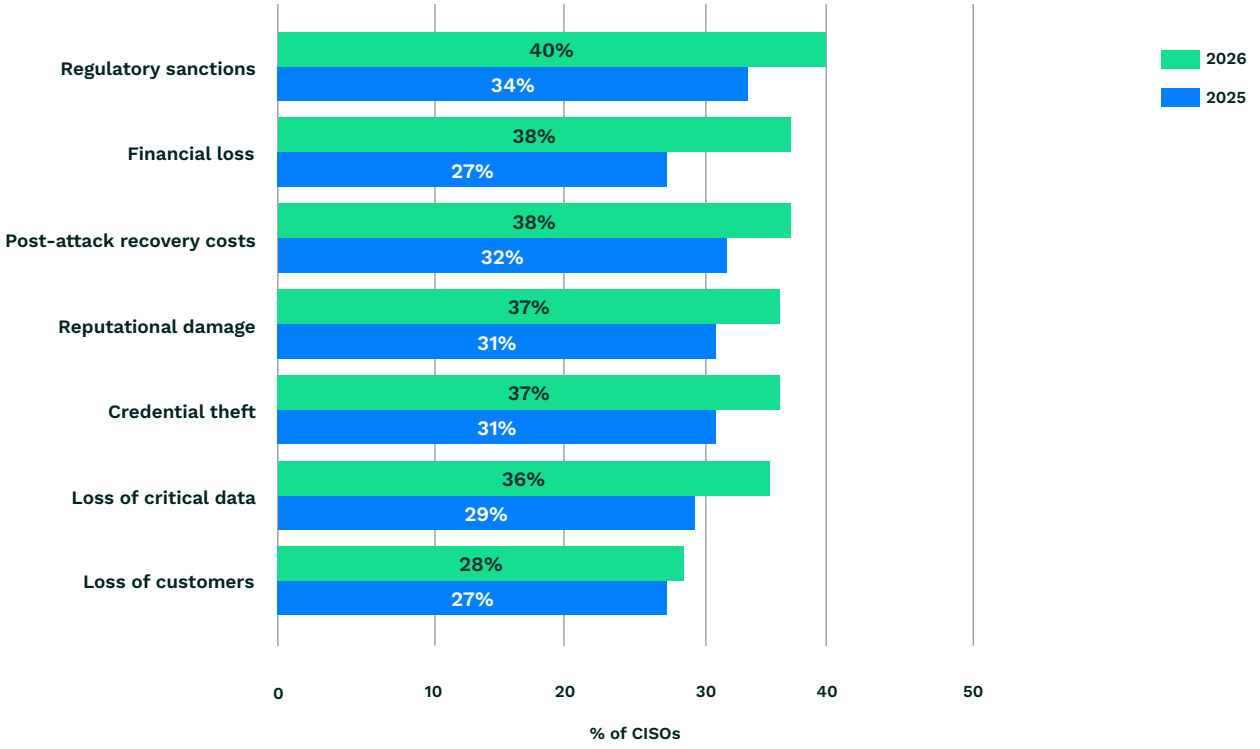
experienced financial loss

86%

say they have continuous visibility and control over sensitive data



Consequences of data loss become more severe



"The fall in reported data loss is encouraging, but the business impact of each incident is growing. Regulatory sanctions, financial loss, recovery costs and reputational damage show that data protection is now a board-level resilience issue. CISOs must be able to protect information wherever it moves, across cloud, collaboration tools, endpoints, SaaS and AI systems whilst making the business case for why data governance is essential to trust, continuity and enterprise value."



Brian Cox
Vice President & Chief Information Security Officer,
Cox Enterprises

CHAPTER 5

Complexity is outpacing control



When it comes to AI, CISOs are not reporting a lack of controls; they are reporting a control model under pressure. In 2026, 86% say they have continuous visibility and control over sensitive data across cloud, collaboration tools, endpoints and AI systems. The same proportion say their current controls effectively mitigate risks introduced by AI, SaaS and modern work patterns.

Yet the pressure signals are clear: 79% are expected to manage AI-related risks without a proportional increase in resources or expertise; 76% say employees are likely to use AI in ways that could expose sensitive data; 77% are concerned about customer data loss through public GenAI tools; and 78% block or restrict employee GenAI use.

The implication is that controls are in place, but the model is under increasing strain. AI is scaling faster than governance, widening the gap between what CISOs can see, enforce and protect. This is not a contradiction; visibility can improve whilst control becomes harder to apply at the pace of modern work. The challenge is shifting from whether security teams can see the environment to whether they can keep up with how quickly data, identities, permissions, automations and AI-enabled workflows change.

That makes complexity a governance problem as much as a technology problem. The next phase of control will depend on policy orchestration across the platforms where work happens, backed by the resources and authority CISOs need to act on risk in real time.



Regional nuance: Controls are in place, but the pressure point differs

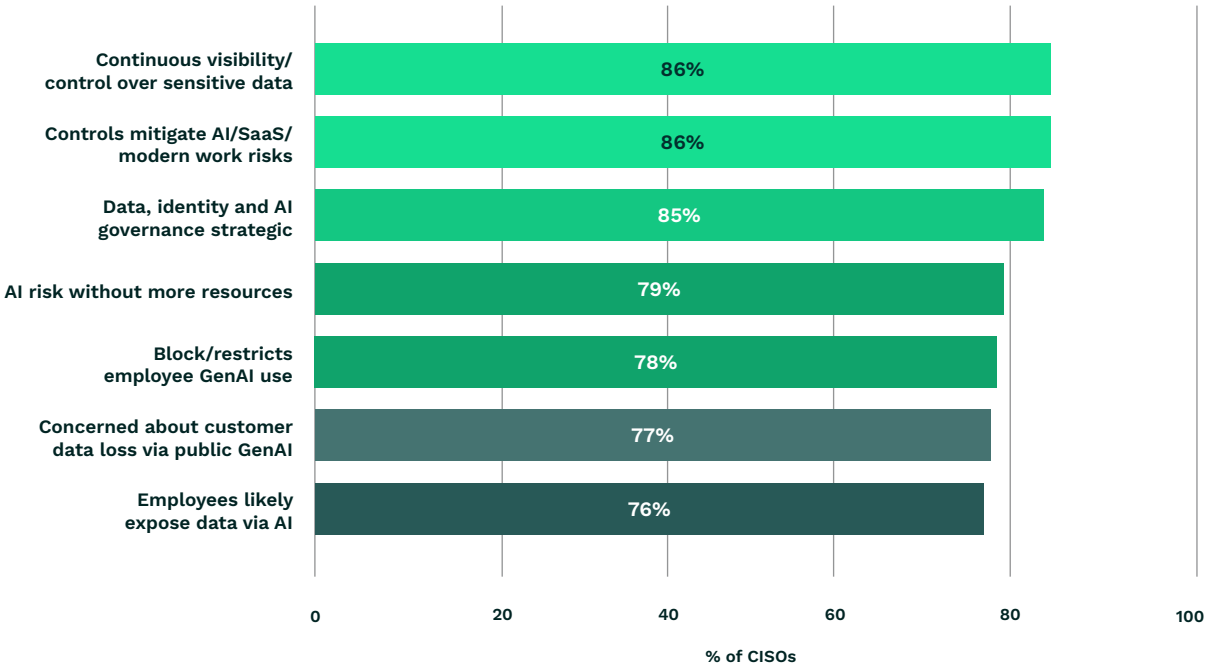
Most markets report high confidence in controls, but the pressure point differs. Spain reports the highest continuous visibility and control (97%); India is highest on controls mitigating AI, SaaS and modern-work risk (94%). France is highest on data, identity and AI governance as a strategic priority (95%) whilst also high on employee AI-exposure risk (92%) and AI resourcing pressure (91%).

Country matrix:

Country	Highest control/complexity signal	Secondary signal
US	Continuous visibility/control (93%)	Controls mitigate AI/SaaS/ modern work risk (90%)
Canada	Continuous visibility/control (91%)	Data/identity/AI governance strategic (90%)
France	Data/identity/AI governance strategic (95%)	Employees likely expose data via AI (92%)
Germany	Continuous visibility/control (76%)	Controls mitigate AI/SaaS/ modern work risk (76%)
Netherlands	Controls mitigate AI/SaaS/ modern work risk (92%)	Data/identity/AI governance strategic (92%)
Mexico	Continuous visibility/control (93%)	Controls mitigate AI/SaaS/ modern work risk (93%)
UAE	Continuous visibility/control (84%)	Data/identity/AI governance strategic (84%)
Saudi Arabia	Controls mitigate AI/SaaS/ modern work risk (77%)	Continuous visibility/control (74%)
Australia	Data/identity/AI governance strategic (89%)	Continuous visibility/control (88%)
Singapore	Employees likely expose data via AI (91%)	Controls mitigate AI/SaaS/ modern work risk (90%)
Japan	AI risk without more resources (65%)	Data/identity/AI governance strategic (65%)
India	Controls mitigate AI/SaaS/ modern work risk (94%)	Data/identity/AI governance strategic (94%)
Brazil	Data/identity/AI governance strategic (82%)	Controls mitigate AI/SaaS/ modern work risk (81%)
Italy	Continuous visibility/control (91%)	Controls mitigate AI/SaaS/ modern work risk (87%)
Spain	Continuous visibility/control (97%)	Data/identity/AI governance strategic (92%)
UK	Continuous visibility/control (88%)	Controls mitigate AI/SaaS/ modern work risk (87%)



Controls are in place, but the model is under strain



“CISOs are not saying controls are absent; they are saying the control model is under strain. Visibility may be improving, but AI, SaaS, automation and modern work patterns are changing faster than traditional governance can adapt. The next phase of security will depend on context-aware controls that understand data sensitivity, identity, permissions and behaviour in real time, backed by the expertise and authority needed to act before risk becomes loss.”



Ben McLaughlin
Chief Information Security Officer, Proofpoint

CHAPTER 6

Board alignment is improving, but expectations are rising

Cybersecurity has become more visible and commercially significant in the boardroom. In 2026, 85% of the CISOs say their board sees eye to eye with them on the issue of cybersecurity, up from 64% in 2025.

But the longer-term trend is not a straight line. Last year's report noted that board alignment stood at 51% in 2022, rose to 62% in 2023 and reached 84% in 2024. It then fell to 64% in 2025 before rebounding to 85% this year.

That seesaw pattern matters. It suggests that board engagement is becoming more visible, but not necessarily more settled. Cybersecurity may now have a firmer place on the board agenda, but alignment still depends on how effectively CISOs can translate technical risk into commercial risk, operational resilience, regulatory exposure and customer trust.

CISOs also place greater emphasis on cyber expertise at board level: 86% say cybersecurity expertise should be required at the board director level, up from 66% last year and slightly above the 84% recorded in 2024. This reinforces the same pattern: board alignment and board expertise are rebounding, but they remain dynamic rather than fixed.



The increase suggests that board alignment is not reducing the need for specialist understanding. Instead, as cyber risk becomes more intertwined with business performance, boards need deeper capability to challenge, support and govern security decisions.

The issues boards are perceived to care about reinforce this commercial framing. CISOs say their boards are most concerned about the impact on business valuation at 42%. Significant downtime and reputational damage follow at 38% each. Loss of sensitive information and disruption to operations are each cited by 37%, followed by loss of current customers at 35% and loss in revenue at 31%.

This list reads less like a technical risk register and more like a board agenda. Boards are evaluating cyber resilience in terms of enterprise value, operational continuity, customer trust, regulatory impact and reputation. That creates an opportunity for CISOs but also raises expectations. Security leaders must be able to translate threats, controls and incidents into business implications that directors can act on.

That visibility is valuable, but it also raises the bar for the CISO. Better board alignment and stronger resource signals do not remove pressure; they broaden what the business expects security leaders to deliver. In 2026, 77% of CISOs say there are excessive expectations placed on the CISO or CSO, up from 66% in 2025.

There are positive signs: 86% say their organisation provides adequate resources—budget, staffing and tools—to meet cybersecurity goals, up from 67% last year; 82% say their organisation has taken steps to help protect them from personal liability whilst ensuring compliance with regulations, up from 65%.

These findings suggest organisations increasingly recognise the importance of supporting security leaders. But support is not evenly matched to every new responsibility. The clearest example is AI. As noted earlier, 79% of CISOs say they are expected to manage AI-related risks without a proportional increase in resources or expertise. This creates a gap between general cybersecurity support and the specialised capability required for AI governance.

Burnout appears to have eased somewhat, falling from 66% in 2024 to 63% in 2025 and now to 57% in 2026 among CISOs who have experienced or witnessed it in the past 12 months. This decline is encouraging, but the figure remains high. More than half of CISOs still report burnout exposure in a role that is increasingly accountable for business continuity, innovation, data protection, identity, regulatory compliance and board communication.

The broader conclusion is that the CISO mandate is becoming both more strategic and more operationally complex. The role now requires fluency in technology, risk, people, data, AI, regulation, stakeholder perception and business impact. Success will depend on whether organisations pair expanding expectations with the authority, budget, expertise and cross-functional support required to meet them.



Regional nuance: Board alignment rebounds, but commercial concern varies

Board alignment is strongest in France (94%), with India, Mexico, the US and the Netherlands all at 93%. But board concern varies by market. India places business valuation first (49%); Saudi Arabia leads on revenue loss (47%) and operational disruption (46%). The UAE is highest on sensitive information loss (46%); Italy is highest on reputational damage (47%); the UK leads on customer loss (44%); and the US leads on significant downtime (45%).



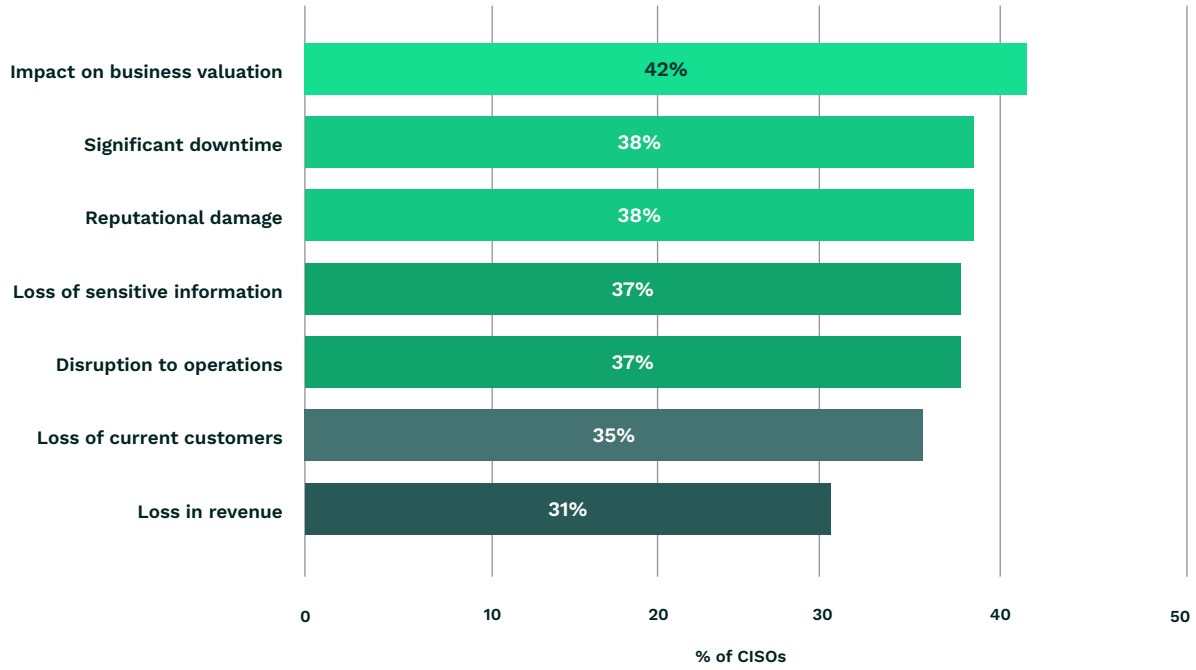
Country matrix:

Country	Primary board concern	Secondary board concern
US	Significant downtime (45%)	Reputational damage (43%)
Canada	Customer loss (44%)	Business valuation (40%); Significant downtime (40%)
France	Significant downtime (42%)	Customer loss (41%)
Germany	Business valuation (38%); Sensitive information loss (38%)	Operational disruption (31%)
Netherlands	Sensitive information loss (40%)	Customer loss (39%)
Mexico	Business valuation (43%); Sensitive information loss (43%)	Customer loss (42%)
UAE	Sensitive information loss (46%)	Revenue loss (44%)
Saudi Arabia	Revenue loss (47%)	Operational disruption (46%)
Australia	Business valuation (44%)	Significant downtime (42%)
Singapore	Business valuation (46%)	Reputational damage (38%); Significant downtime (38%)
Japan	Business valuation (47%)	Operational disruption (46%); Significant downtime (46%)
India	Business valuation (49%)	Operational disruption (45%)
Brazil	Revenue loss (43%); Significant downtime (43%)	Business valuation (42%); Operational disruption (42%)
Italy	Reputational damage (47%)	Operational disruption (43%)
Spain	Business valuation (43%)	Operational disruption (42%)
UK	Customer loss (44%)	Business valuation (41%); Reputational damage (41%)

Board alignment rebounds sharply



Board concerns about a material cyberattack





Regional nuance: Expectations rise where the mandate is broadening fastest

Pressure does not rise in a straight line from board alignment. It is shaped by the breadth of the CISO mandate and the maturity of support around it. Singapore and France report the highest excessive expectations (both 89%), followed by India (87%). AI resourcing pressure is highest in India (92%), France (91%) and Mexico (90%). At the same time, these are not simply low-support markets—resource confidence is strongest in France and Mexico (both 93%) and Canada (92%), whilst personal-liability protections are strongest in India (94%) and Australia (93%), followed by the US and France (both 91%).

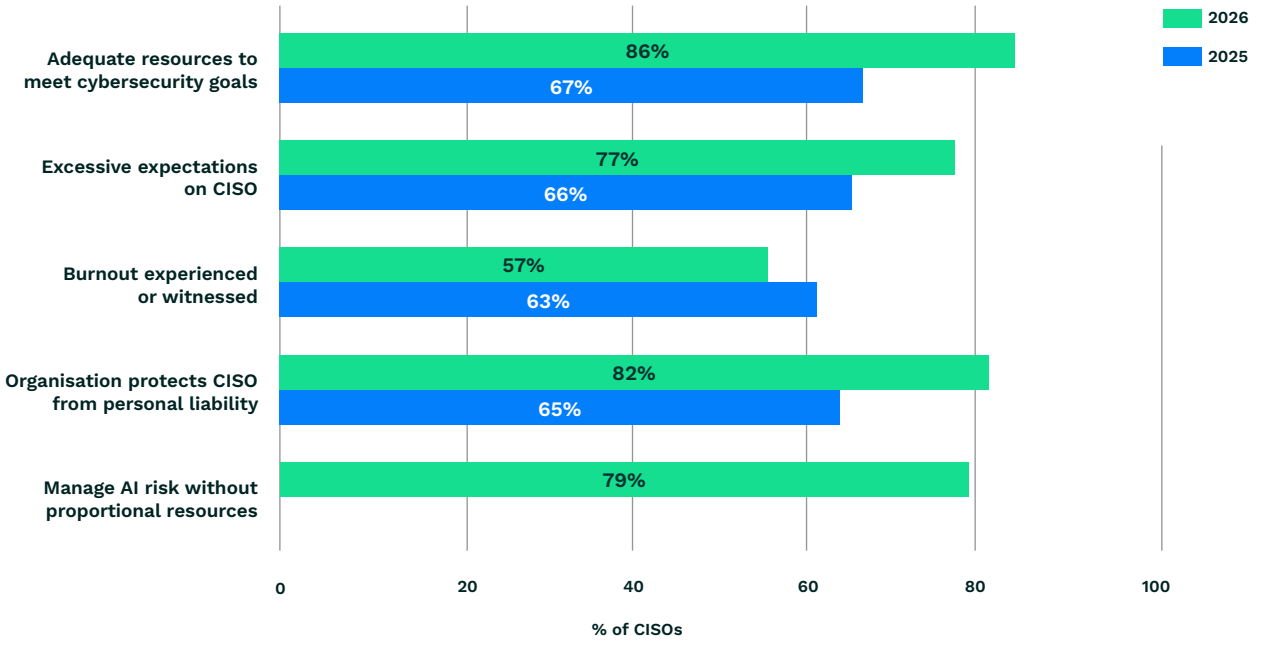
That combination is the point. Greater alignment and stronger support are helping CISOs, but they are also expanding the remit. The pressure now comes from translating cyber risk into business risk whilst governing AI, data movement and human-centric security at the same time.

Country matrix:

Country	Highest pressure signal	Strongest support signal
US	AI risk without more resources (83%)	Adequate resources (91%)
Canada	AI risk without more resources (82%)	Adequate resources (92%)
France	AI risk without more resources (91%)	Adequate resources (93%)
Germany	Excessive expectations (73%)	Adequate resources (76%)
Netherlands	AI risk without more resources (81%)	Adequate resources (88%)
Mexico	AI risk without more resources (90%)	Adequate resources (93%)
UAE	AI risk without more resources (75%)	Adequate resources (85%)
Saudi Arabia	Excessive expectations (66%)	Adequate resources (76%)
Australia	Excessive expectations (83%)	Personal liability protection (93%)
Singapore	Excessive expectations (89%)	Adequate resources (89%)
Japan	AI risk without more resources (65%)	Personal liability protection (65%)
India	AI risk without more resources (92%)	Personal liability protection (94%)
Brazil	AI risk without more resources (76%)	Adequate resources (84%)
Italy	AI risk without more resources (81%)	Adequate resources (89%)
Spain	AI risk without more resources (76%)	Personal liability protection (89%)
UK	Excessive expectations (74%)	Adequate resources (88%)



The CISO mandate broadens despite stronger support



> Stronger board alignment is a positive sign, but it also raises expectations. Cybersecurity is now discussed in terms of valuation, downtime, reputation, customer trust and operational disruption. That is the right conversation, but CISOs need more than attention from the boardroom; they need clear authority, specialist expertise and sustained support. The goal is not simply to report cyber risk more effectively, but to turn board-level understanding into better business decisions.



Patrick Joyce
Global Resident CISO,
Proofpoint



Conclusion

The 2026 Voice of the CISO findings point to a cybersecurity landscape in transition, rather than one defined by unchecked escalation. They tell a sharper story; security programmes are making progress, but the centre of risk is moving. The survey indicates that fewer CISOs expect a material cyberattack; fewer report material data loss; and traditional threat concerns, such as ransomware, malware and email fraud, have declined somewhat. To be certain, the enterprise is not less exposed, but exposure is becoming more concentrated in the systems, identities and workflows that now power the business.

AI and human risk sit at the centre of that shift: 78% of CISOs now say GenAI is a security risk, whilst 79% say human risk is their organisation's biggest cyber vulnerability. Cloud account takeover or compromise is now the most-cited cyberthreat, and among organisations that experienced material data loss, 93% say departing employees played a role. Together, these findings point to a new centre of gravity: the everyday work environment, where people, identities, applications, automation and AI increasingly shape exposure.

That makes the CISO mandate more strategic and harder to execute. Security leaders must enable AI adoption, govern human risk, protect sensitive information and explain cyber exposure in commercial terms, even as 79% say they are expected to manage AI-related risks without a proportional increase in resources or expertise.

The organisations best positioned for 2026 and beyond will be those pairing innovation with appropriate control. They will secure work as it happens, govern AI as it scales and provide CISOs the authority, expertise and resources to protect a business where people, data, identity and intelligent systems are now inseparable.

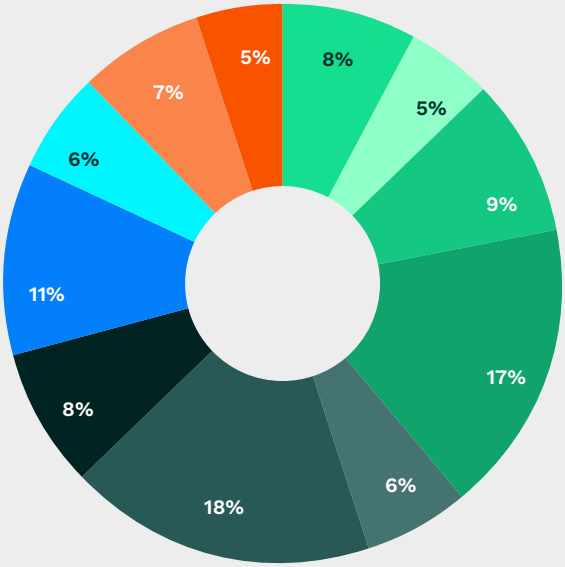
Methodology

The Proofpoint 2026 Voice of the CISO report is based on a global survey conducted by Censuswide between 11 May and 18 May 2026. The survey included 1,600 chief information security officers from organisations of 1,000 employees or more across 16 global markets.

One hundred CISOs were surveyed in each market: the US, Canada, Brazil, Mexico, the UK, France, Germany, Italy, Spain, the Netherlands, the UAE, Saudi Arabia, Australia, Japan, Singapore and India.

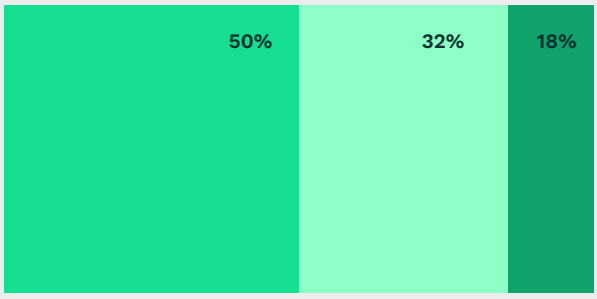
Censuswide complies with the MRS Code of Conduct and ESOMAR principles.

Industry split among respondents



Business and professional services	130
Education	84
Energy, oil/gas and utilities	148
Financial services	265
Healthcare	99
IT, technology and telecoms	285
Manufacturing and production	126
Media, leisure and entertainment	175
Public sector	93
Retail	109
Transport	86
Other	0
Total	**1,600**

Company size split among respondents



1,000–2,500 employees	803
2,501–5,000 employees	507
5,001+ employees	290
Total	**1,600**

Appendix

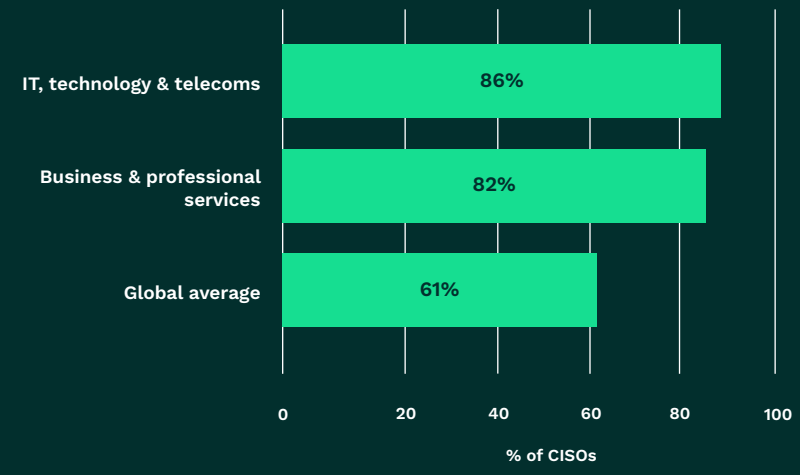
Sector signals

Global averages provide a useful benchmark, but the sector view shows how differently the 2026 cyber landscape is being experienced across industries. The same forces are shaping every CISO agenda—AI adoption, human risk, data movement and board-level scrutiny, but they are not landing evenly.

Material cyberattack expectations by sector

Attack expectations are highest in sectors built around digital platforms, connected services and customer-facing infrastructure. IT, technology and telecoms lead at 86%, followed by business and professional services at 82%, both well above the global average of 61%.

Expect a material cyberattack in the next 12 months

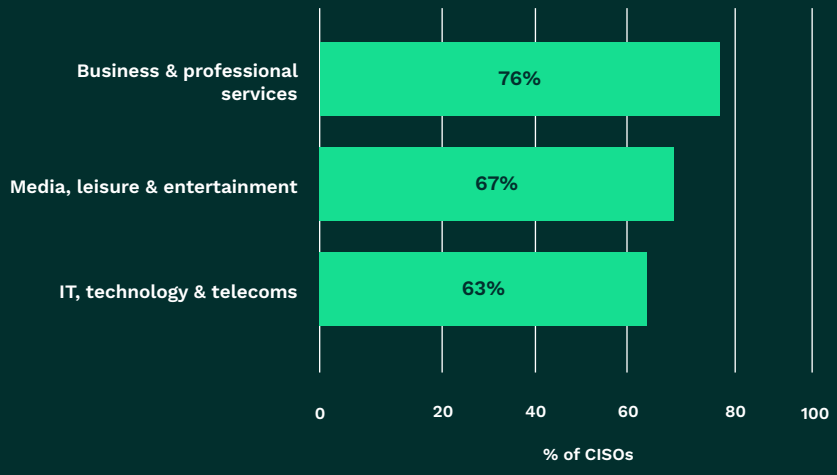


Material data loss by sector

Data loss tells a different story. Business and professional services is most likely to report a material loss of sensitive information in the past 12 months, at 76%, followed by media, leisure and entertainment at 67%, and IT, technology and telecoms at 63%.

The gap matters: the sectors most concerned about attacks are not always the sectors reporting the highest levels of data loss. For CISOs, this reinforces the need to look beyond the external threat landscape and examine how employees, partners, platforms and AI tools handle sensitive information day to day.

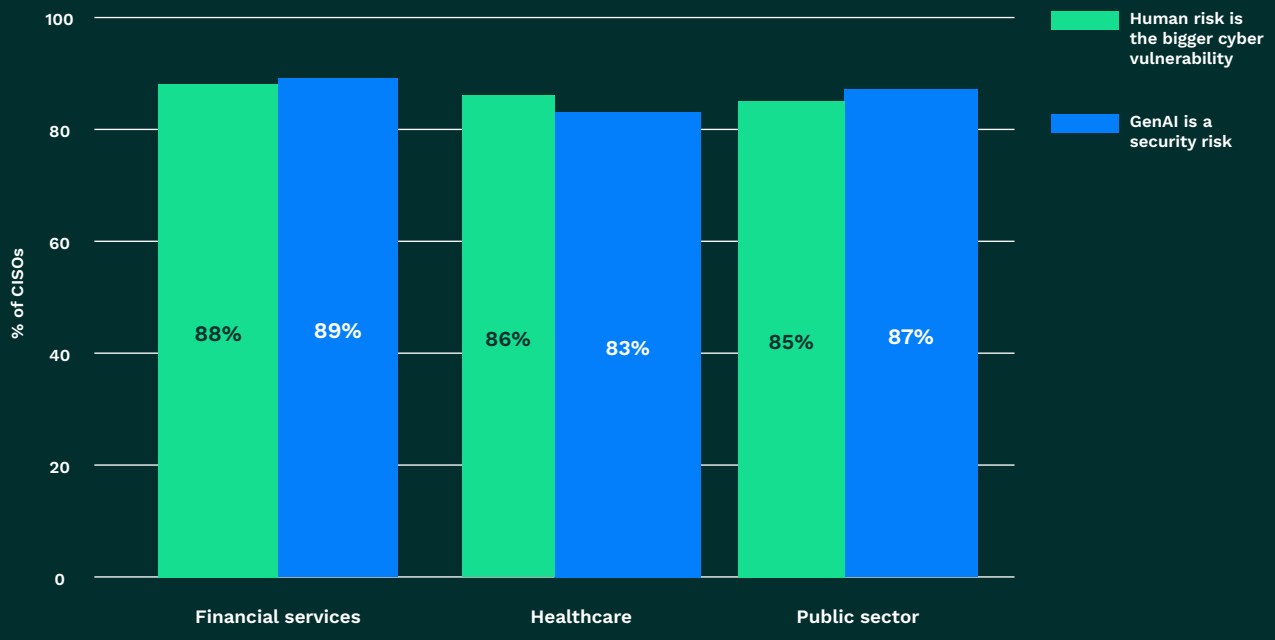
Report material data loss of sensitive information in the past 12 months



Human risk and GenAI risk by sector

Human risk and GenAI risk converge most clearly in financial services, where 88% of CISOs identify human risk as their biggest cyber vulnerability, and 89% say GenAI is a security risk. Healthcare and the public sector also report elevated concern across both measures.

Together, these sector signals point to one conclusion: security strategy in 2026 needs to be more context-specific whilst still protecting the shared foundations of modern work—people, data, identity and AI-enabled systems.





proofpoint.

About Proofpoint, Inc.
Proofpoint, Inc. is a global leader in human and agent cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 14,000 large enterprises and millions of smaller organisations in stopping threats, preventing data loss and building resilience across people and AI workflows. Proofpoint's collaboration, data and AI security platform helps organisations of all sizes protect their people and adopt AI securely and confidently. Learn more at **www.proofpoint.com/uk**.

Connect with Proofpoint on **LinkedIn**.

Proofpoint is a registered trademark or trade name of Proofpoint, Inc. in the US and/or other countries. All other trademarks contained herein are the property of their respective owners.

DISCOVER THE PROOFPOINT PLATFORM