REPORT

proofpoint.

2025 Voice of the CISO

Global insights into CISO challenges, expectations and priorities

Table of contents

Introduction

2025: CISOs navigate another turbulent year

Patrick Joyce,
global resident CISO
at Proofpoint

Over the years, the cybersecurity industry has witnessed the rise and fall of countless buzzwords—from “cloud computing” to “zero trust.” While these concepts often begin as trends, they quickly become deeply embedded in how organizations conduct business.

Today, the standout term dominating headlines and boardroom conversations alike is artificial intelligence (AI). Once considered an abstract concept, AI is now firmly entrenched in the daily operations of enterprises across the globe. In the cybersecurity realm, we’re seeing AI radically transform both the tactics of cyberdefenders and the techniques of malicious actors.

As a result, CISOs are faced with a dual responsibility: integrating AI technologies to enhance security posture, while also ensuring responsible and ethical use throughout the organization. Misuse or unchecked implementation can open the door to data leaks, regulatory violations, and reputational harm.

Yet, as with any major technological shift, the introduction of AI brings not only new risks but also new opportunities. CISOs are increasingly called upon to strike a balance between innovation and risk mitigation—a position that places them at the forefront of strategic business decision-making.

But AI is just one force reshaping the role of today’s CISO. As threats grow more complex and enterprise environments become more demanding, many organizations are rethinking the structure of the CISO position altogether. Some are splitting responsibilities across multiple roles, while others are expanding the scope to include broader technology leadership. What’s clear is that the role of the CISO is evolving—rapidly and continuously.

In this year’s *Voice of the CISO* report, Proofpoint surveyed 1,600 CISOs at organizations with 1,000 or more employees worldwide. We explored their priorities, challenges and expectations for the next two years—from persistent threats like data sprawl and human error to growing concerns around burnout and boardroom alignment.

This report offers a comprehensive snapshot of the modern CISO experience, shaped by the voices of global security leaders. We thank all participants for their time, candor and valuable insights.

CHAPTER 1

Confidence clashes with concern

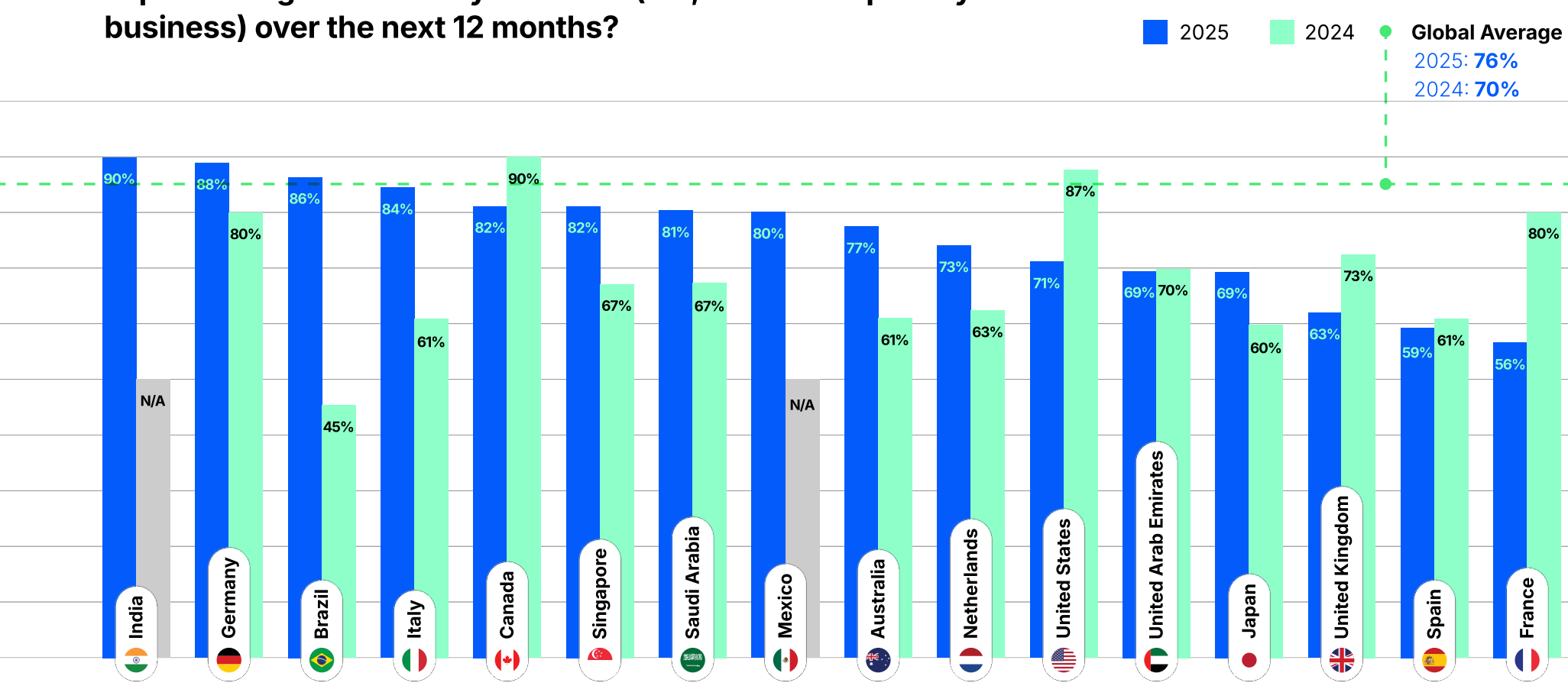
On the back of yet more high-profile breaches and increasingly sophisticated cyberattacks so far this year, it should come as little surprise that CISOs are concerned about the increasing threat landscape and its potential impact on their business.

More than three-quarters (76%) feel their company is at risk of a material cyberattack within the next 12 months, with just over a third (36%) believing it to be “highly likely“. This is a notable increase from the 70% and 31% who shared the respective sentiments last year.

76%

believe their company is at risk of experiencing a material cyberattack in the next 12 months, with 36% considering it highly likely.

How likely or unlikely do you feel your company is at risk of experiencing a material cyberattack (i.e., where it impacts your business) over the next 12 months?



India is highest at 90%

followed by Germany (88%) and Brazil (86%); the lowest is France (56%).

We do not have to look far for potential factors behind this growing concern. Of the CISOs surveyed for this year's report, two-thirds (66%) indicated that they experienced a material loss of sensitive information within the past 12 months. This is a marked increase from just 46% the previous year.

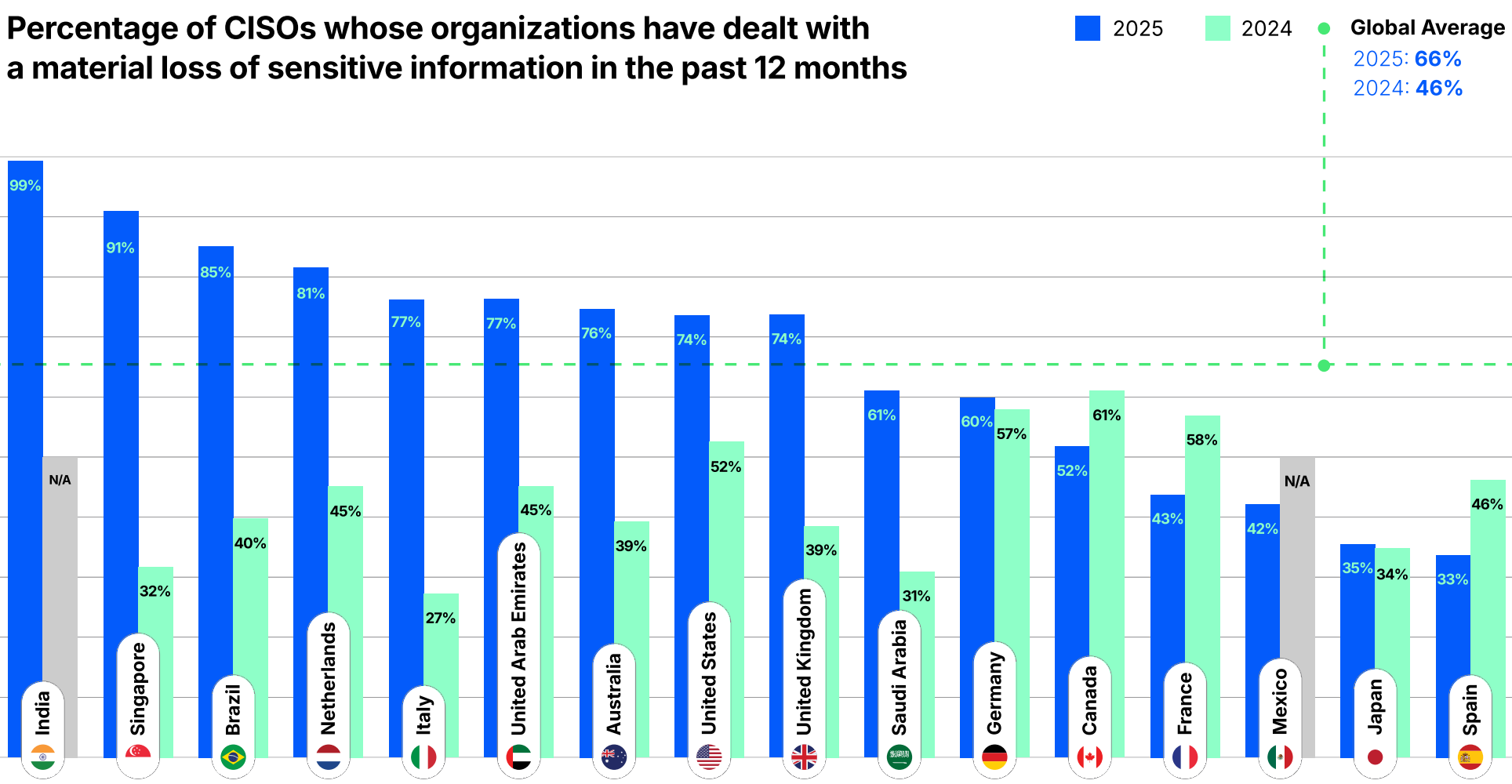
That said, several countries came in considerably higher than this worldwide average. A staggering 99% of Indian CISOs reported the loss of sensitive data, followed by Singapore (91%) and Brazil (85%), while Spain is the lowest at 33%. Across verticals, financial services was the highest at 87%, and education was the lowest at 29%.

Education sector CISOs feel most at risk at

89%

followed by financial services (79%), media, leisure, and entertainment (79%) and healthcare (78%); the lowest is retail and business services (both 64%).

Percentage of CISOs whose organizations have dealt with a material loss of sensitive information in the past 12 months



In addition to these increased statistics, over half (58%) of global CISOs agree that their organization is unprepared for a cyberattack in 2025. Once again, this represents an increase, up from 43% last year. Canada ranked the highest (76%); Spanish CISOs showed more confidence, with only 33% agreeing they are not ready to weather a targeted attack in the year to come.

67%

of global CISOs agree that their organization's overall cybersecurity culture is strong.

However, while growing CISO concern may be easy to understand, the collective view of their own organization's cyberposture is more difficult to square away. Over two-thirds (67%) of global CISOs agree that their overall cybersecurity culture is strong, Mexico topping the chart at 82% and Spain the lowest at 43%.

The disconnect between confidence and concern suggests CISOs feel they are on the wrong side of a losing battle. If cyberculture is robust, but attacks are likely, are breaches now considered inevitable regardless of the defenses that are put in place?

"This year's findings highlight a striking duality: While many organizations report confidence in their cybersecurity culture, there remains a prevailing sense of vulnerability. The increase in CISOs expecting a material attack speaks volumes about the evolving threat landscape. It is clear that many security leaders view a breach not as a possibility, but as a near inevitability. The challenge now lies in transforming confidence into resilience, ensuring that preparedness is more than a perception."

Paige Adams,
group chief information security officer, Zurich American Insurance Company

CHAPTER 2

Attacks from all angles

After an assessment of the threat landscape, it's clear today's CISOs have plenty of reasons for concern. When asked what they perceived to be the biggest cybersecurity threat to their organization, this year's survey respondents failed to reach a consensus.

Unsurprisingly, email fraud (37%) sits atop the growing inventory of CISO concerns, as it has since our first report was published in 2021. However, insider threats (37%), ransomware (36%), cloud account takeover (34%), malware (33%) and supply chain attacks (33%) now occupy attention in almost equal measures.

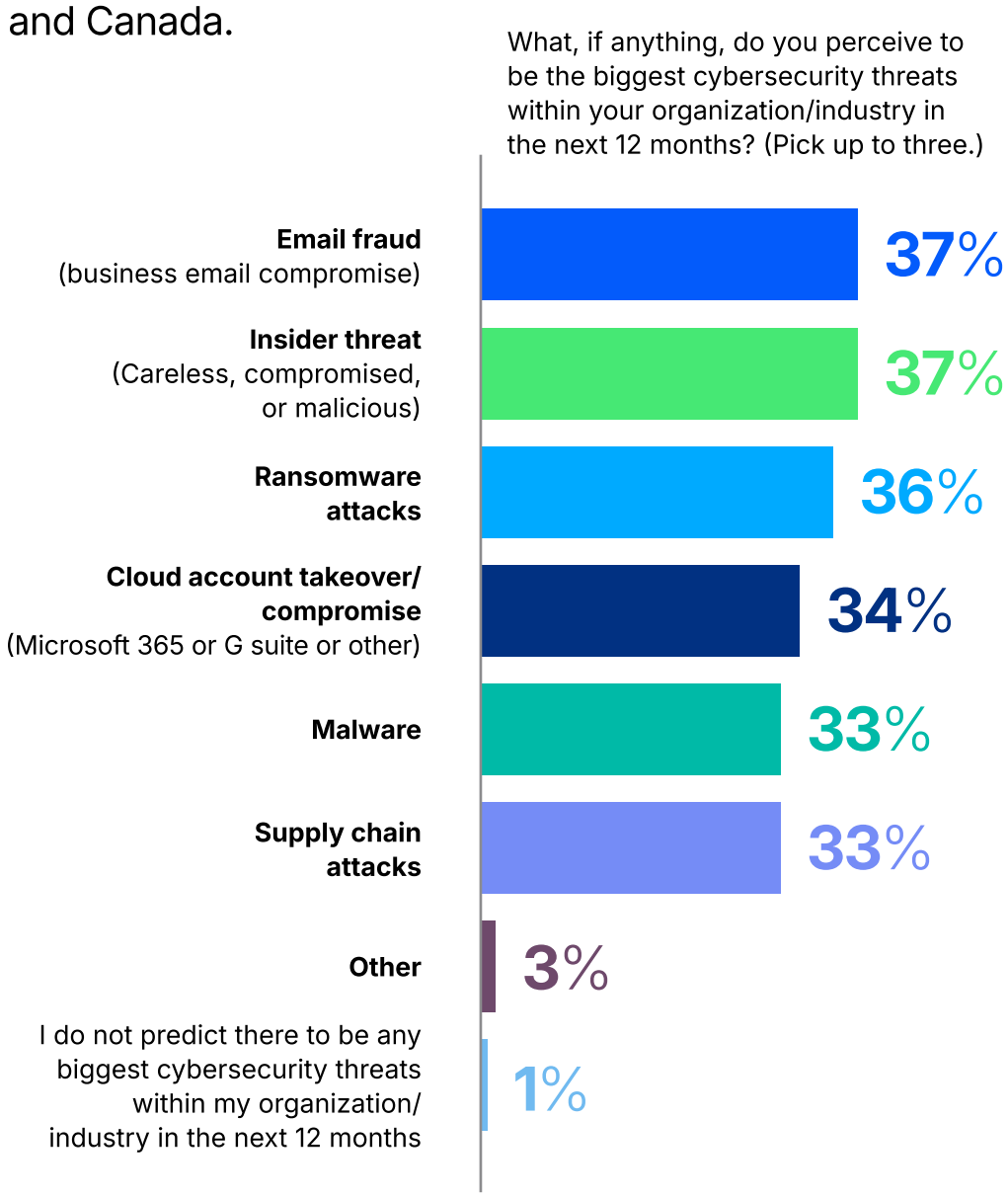
While many share similar concerns, the primary threat likely causing sleepless nights among CISOs differs around the world. Email fraud is a top concern among those in the U.S., UK, Italy and the UAE, while supply chain threats top the list in India, Singapore and Canada.

Insider threats topped the list of concerns for companies with 5,000+ employees.

Education views ransomware (63%) and malware (56%) as the highest threats and insiders as the least threatening (26%). Media/leisure is above average for insider threats (51%).

Saudi Arabia considers insider threats the biggest risk (50%),

more so than any other country surveyed. Malware is of least concern in the United States, Saudi Arabia, Australia, Singapore and the UK.



Varied attacks. Same consequence.

The wide array of threats troubling CISOs this year may differ in their tactics and procedures, but the outcome is nearly always the same. Whether caused by a careless insider, a spoofed email, malicious payload or compromised supplier, the end result is the same: data loss.

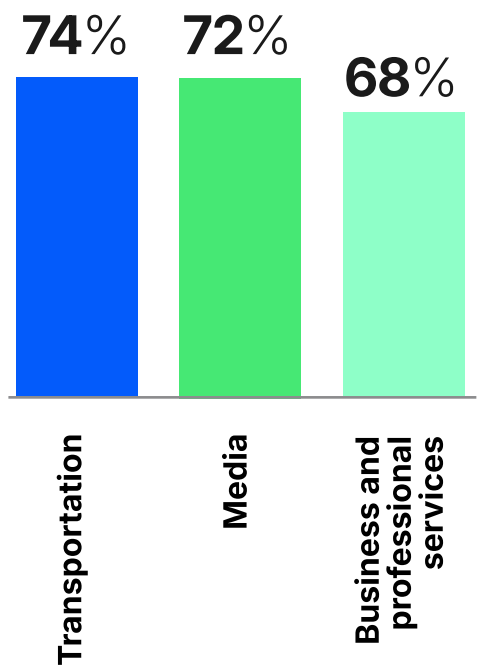
That so many threats of concern to CISOs share this same end goal demonstrates just how much pressure security teams are under to identify and keep sensitive data where it belongs.

So much so, that should it fall into the wrong hands, many are willing to engage with cybercriminals to do what it takes to get it back. Two-thirds (66%) of CISOs said their organization would be likely to pay a ransom to restore systems or prevent the release of data by an attacker.

CISOs in Canada (84%) and Mexico (84%) are among the most willing, while those in Spain (51%) are the least prepared to pay.

If impacted by ransomware within the next 12 months, my organization is likely to pay a ransom to restore systems or prevent the release of data.

Industries



Top three countries prepared to pay a ransom:
Canada (84%)
Mexico (84%)
U.S. (76%)

"The breadth of threats facing organizations today underscores the need for a holistic security strategy. No single attack vector dominates, and this diversification of risk is forcing CISOs to remain vigilant on all fronts. From insider threats and email fraud to ransomware and supply chain vulnerabilities, every entry point demands equal scrutiny. The reality is that effective cyberdefense today requires both broad visibility and rapid adaptability."

Judy (Hatchett) Molenaar,

vice president, information security and chief information security officer, Surescripts, LLC

CHAPTER 3

Data sprawl vs. data security

Data sprawl has been a mounting challenge for organizations for many years. The more data we create, move, process and store every day, the harder it is to classify, track and secure. However, recent developments have only compounded the issue.

The rise and rapid adoption of LLMs and GenAI apps, such as ChatGPT, has changed the playing field, making it much easier to create, share, save and potentially expose information in the shadows. CISOs are certainly not oblivious to this threat. Over two-thirds (67%) see information protection and governance as a top priority.

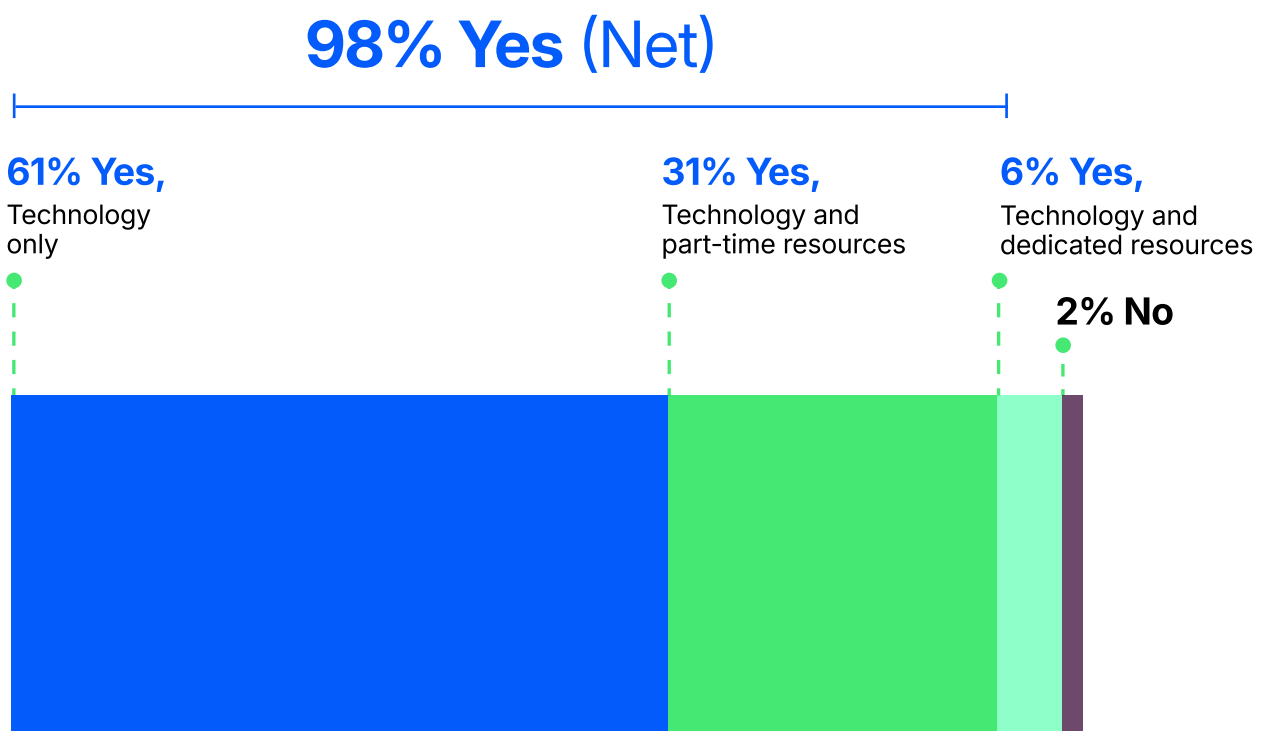
2/3

of global CISOs (67%) see information protection and governance as a top priority.

Mexico ranked the highest at 86%, followed by Australia (84%) and Canada (82%), with the UK the lowest at 53%.

Any concerns that a third of global CISOs are not prioritizing data protection to a higher degree are quickly allayed by the finding that 98% of organizations indicate that they have a data loss prevention (DLP) program in place. That said, 61% have only implemented technological protections, while 31% bolster this with part-time resources, and just 6% have dedicated DLP resources at their disposal.

Does your organization have a data loss prevention (DLP) program in place?



71%

of CISOs in the education sector said they have DLP technology in place, the highest across all industries.

Aside from DLP taking first place, other common technological solutions include cloud security (30%), data security posture management (DSPM) (29%), web security and/or browser isolation (28%) and insider risk management (28%).

Data Loss: What technologies do you have in place to combat organizational data loss? (Pick all that apply)

35%
Data loss prevention (DLP)

30%
Cloud security (e.g., Cloud DLP/CASB)

29%
Data security posture management (DSPM)

28%
Web security and/or browser isolation (e.g., Web DLP)

28%
Insider risk management

27%
Employee awareness training

26%
Endpoint security (e.g., Endpoint DLP)

26%
Email security

2%
Other

0%
We don't have any specific data loss technologies

Saudi, Germany and Mexico rank highest for DLP implementation

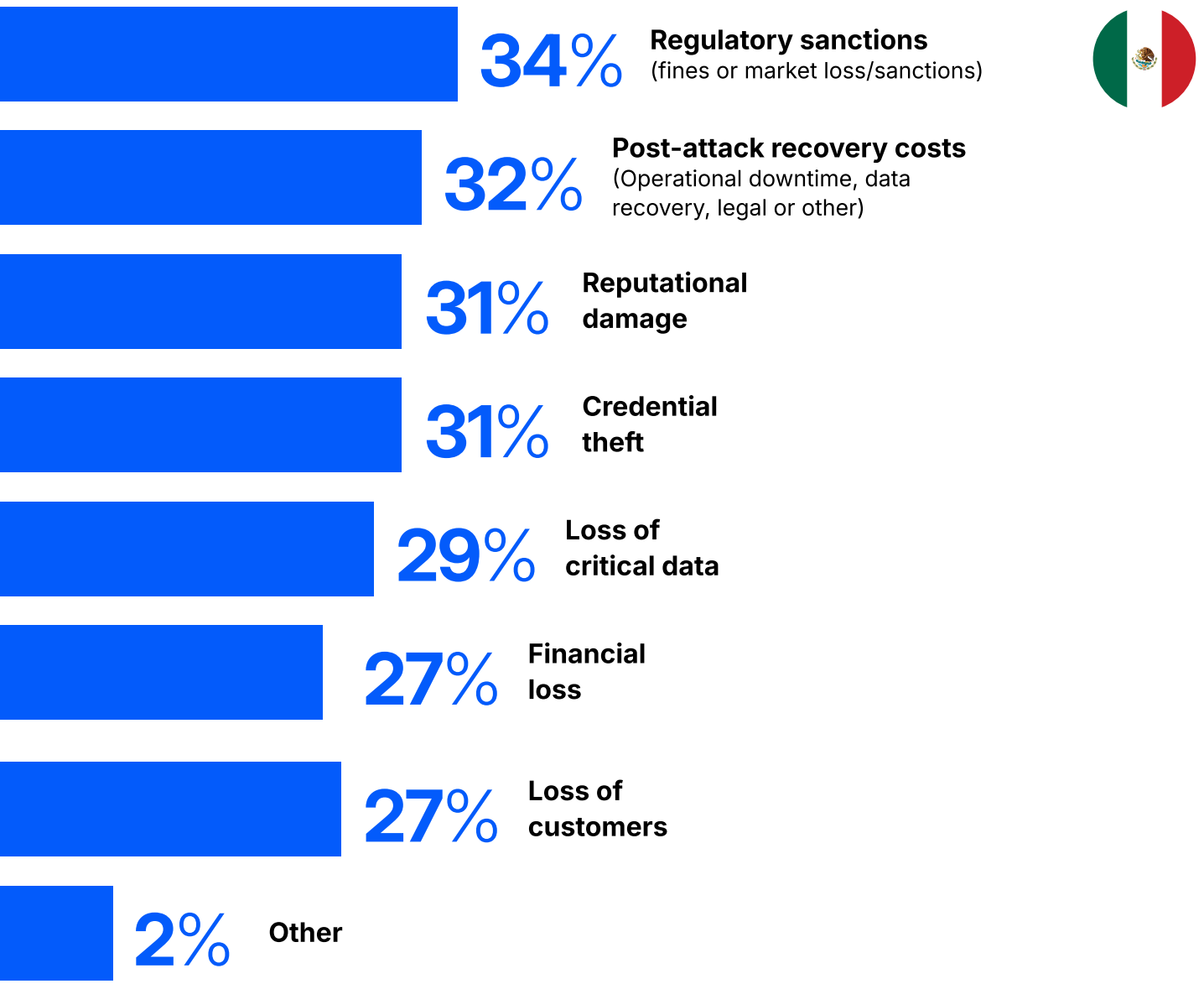
Only 23% of French CISOs said they have DLP technology in place, followed by Singapore (24%) and India (25%).

Data doesn't walk out the door by itself

As to whether data protection programs are up to muster, feelings are mixed. Just two-thirds of CISOs surveyed indicated that the data within their organization is adequately protected despite almost all having DLP technologies in place. Those in the U.S. and Mexico are most confident (81%) while Spain's CISOs express the most concern (45%).

Whatever they feel about the effectiveness of their protections, CISOs are right to be worried about the impact of data loss. Of the 66% that experienced a loss of sensitive information in the past 12 months, regulatory sanctions, post-recovery costs, reputational damage and credential theft topped the list of consequences which they experienced.

What was the end result of the event on your organization?
(Pick all that apply).(Respondents whose organization dealt with material loss of sensitive information in the past 12 months)



Only

15%

of healthcare orgs that experienced a data breach resulted in loss of critical data. Data breaches at 42% of IT firms resulted in regulatory sanctions, higher than finserv (32%), healthcare (32%) and government (38%).

Mexico was highest (50%) on post-attack recovery costs

followed by UAE (47%). Mexico (45%), the Netherlands (40%) and Japan (40%) were above global average on regulatory sanctions. Only 9% of French organizations lost customers due to data loss.

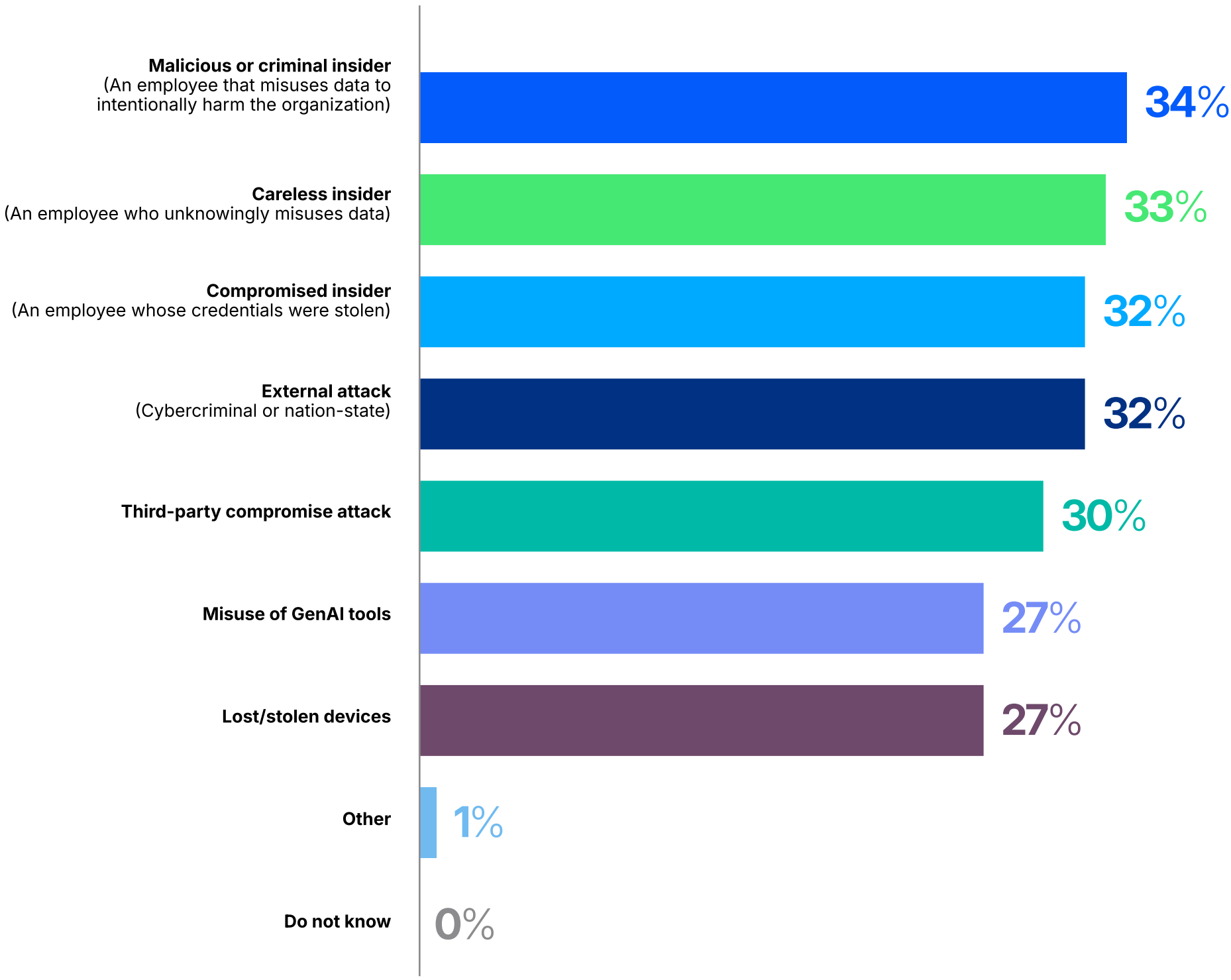
These findings raise a pressing question. If almost all organizations have some form of DLP strategy in place, why have the majority experienced data loss and other associated consequences? Once again, we do not have to look far to find an answer.

Of the primary causes of data loss events, the top three–malicious/criminal insiders, careless insiders and compromised insiders–are all people and behavioral-driven. Data doesn't lose itself. People lose it, intentionally or unintentionally.

92%

of CISOs said that employees leaving their organization played a role in a data loss event, up from 73% last year.

What was the root cause of the data loss event?
(Pick all that apply) (Respondents whose organization dealt with material loss of sensitive information in the past 12 months)



"Despite near-universal adoption of DLP programs, material data loss remains alarmingly common. As data becomes increasingly distributed and easily shared—particularly through GenAI-enabled platforms—traditional controls are struggling to keep pace. The causes of these losses, often rooted in human behavior, point to deeper issues around governance and visibility. To protect sensitive information in 2025 and beyond, organizations must evolve from static protection to dynamic, context-aware security."

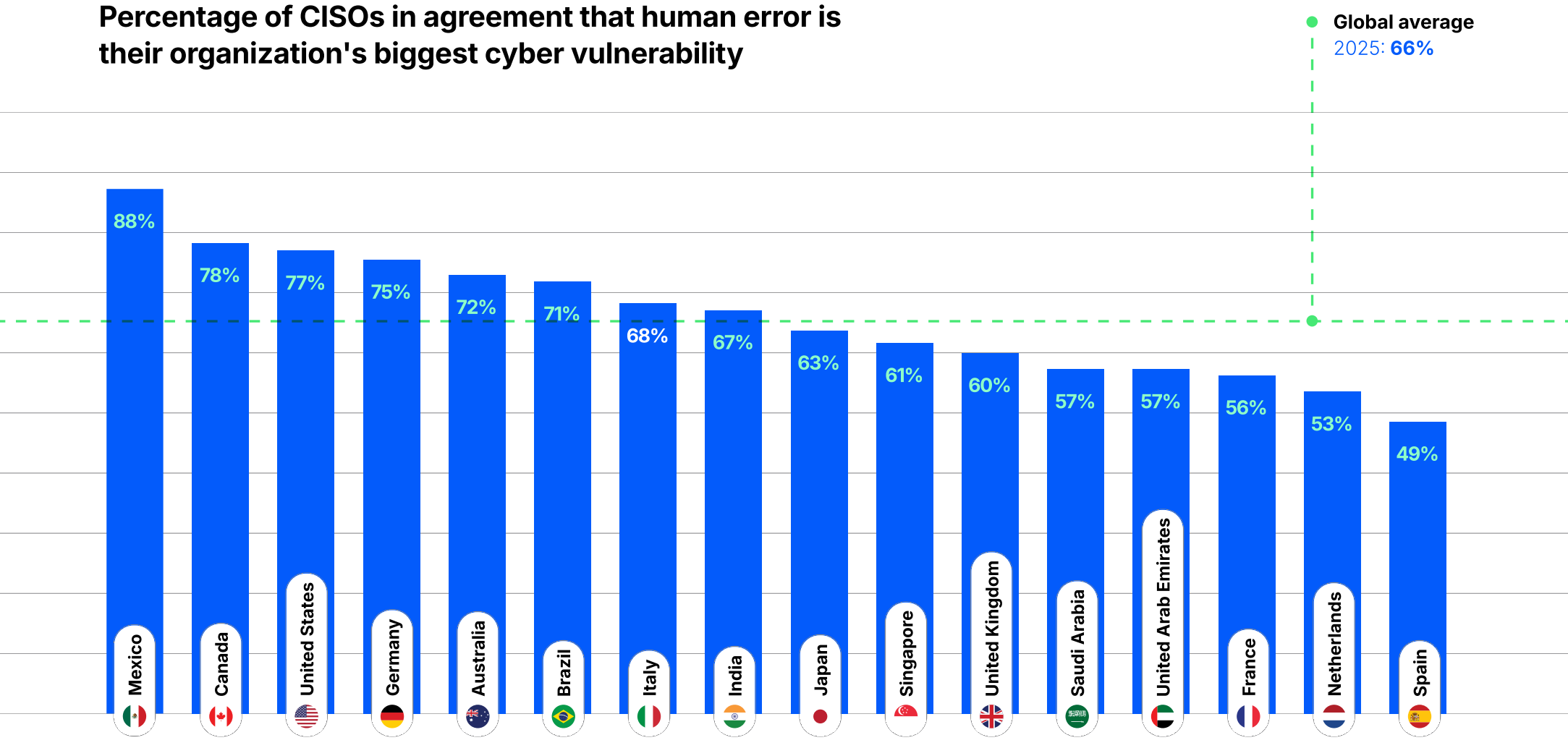
Phil Ross,
chief information security officer, Air New Zealand

CHAPTER 4

The people problem persists

As anxiety over potential cyberattacks increases, there's also growing consensus on the leading risk factor: people. With a rise in insider threats and data loss driven by human actions, CISOs around the world (66%) agree that human risk is their organization's greatest cyber vulnerability across the board.

Percentage of CISOs in agreement that human error is their organization's biggest cyber vulnerability



Of course, the people problem is nothing new. Users have been a contributing factor in most cyberattacks for many years now. That a majority of CISOs (68%) believe their employees have a strong understanding of cybersecurity best practices in spite of this, however, is altogether more surprising.

Employees who truly understand their role in protecting an organization and demonstrate that understanding through appropriate behavior, cannot also be the biggest risk their organization faces.

68%

of global CISOs believe employees have a strong understanding of data security best practices and their role in protecting the organization against cyberthreats.

When we delve deeper into how CISOs assess cybersecurity understanding, things become a bit clearer. Despite the role of people in cyberattack and data loss, employee security awareness training is way down the priority list for CISOs when asked to list technologies they have in place to combat organizational data loss.

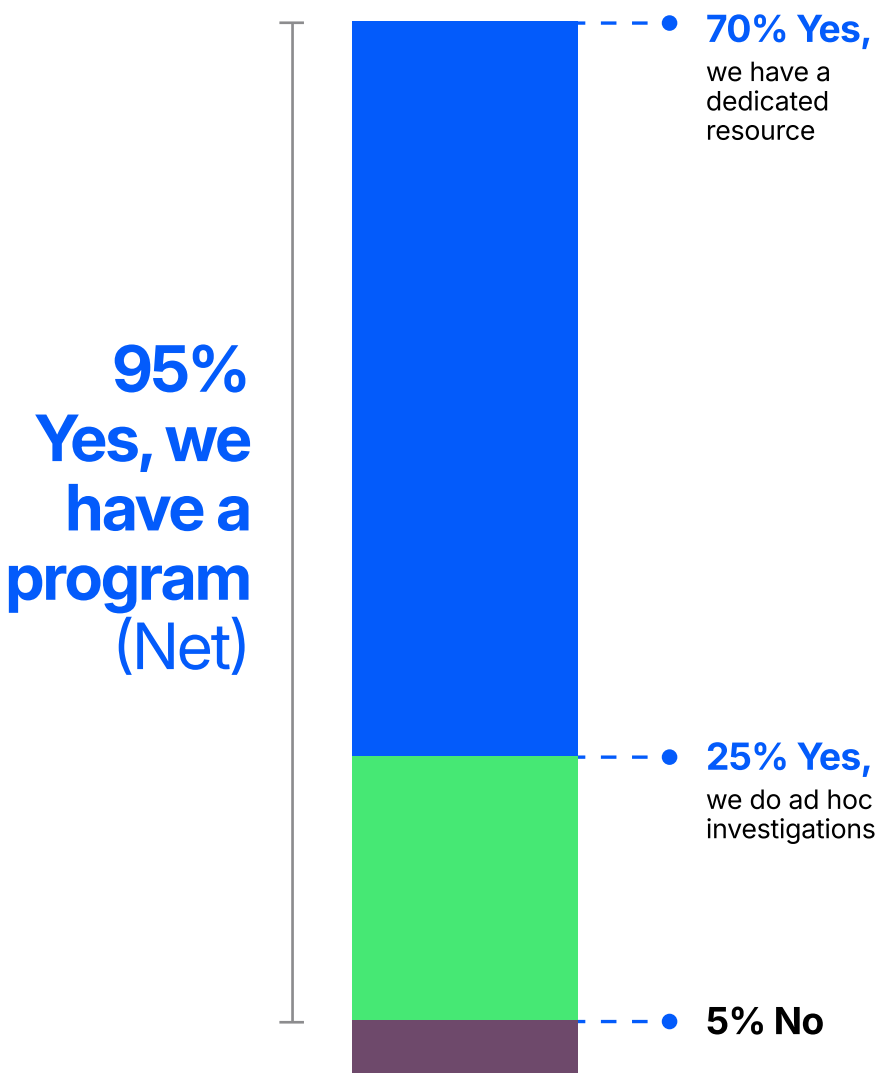
If people are not regularly trained and assessed on their understanding of —and reactions to— the types of threats they are likely to face, and when and where they are likely to face them, they cannot possibly appreciate the extent of their role in keeping attackers at bay.

To make matters worse, human-centric protections are found somewhat lacking elsewhere too. Despite insiders leading the way as the primary cause of data loss, just 70% have a dedicated resource for insider risk management, leaving almost a third of businesses exposed.

12%

of retail and healthcare organizations admitted to not having an insider risk management program, making them the most exposed industries amongst those surveyed.

Does your organization have an insider risk management program in place?



More than a quarter (26%) of French companies

do not have an insider risk management program in place, followed by Japan (15%), the UK and Canada (10%).

"Year after year, human error continues to rank as the greatest cybersecurity vulnerability—and 2025 is no exception. It is encouraging to see that many CISOs believe their employees understand their role in data protection. However, awareness alone does not equate to security. Organizations must go further by equipping users with the tools, training and support needed to act securely in an increasingly complex, AI-riddled digital environment."

Param Vig,
chief information security officer, Solventum

CHAPTER 5

AI: Friend and foe

While organizations could do more to raise employee awareness of cybersecurity threats, it is not the only factor behind human risk's near-permanent top spot on the inventory of CISO concerns.

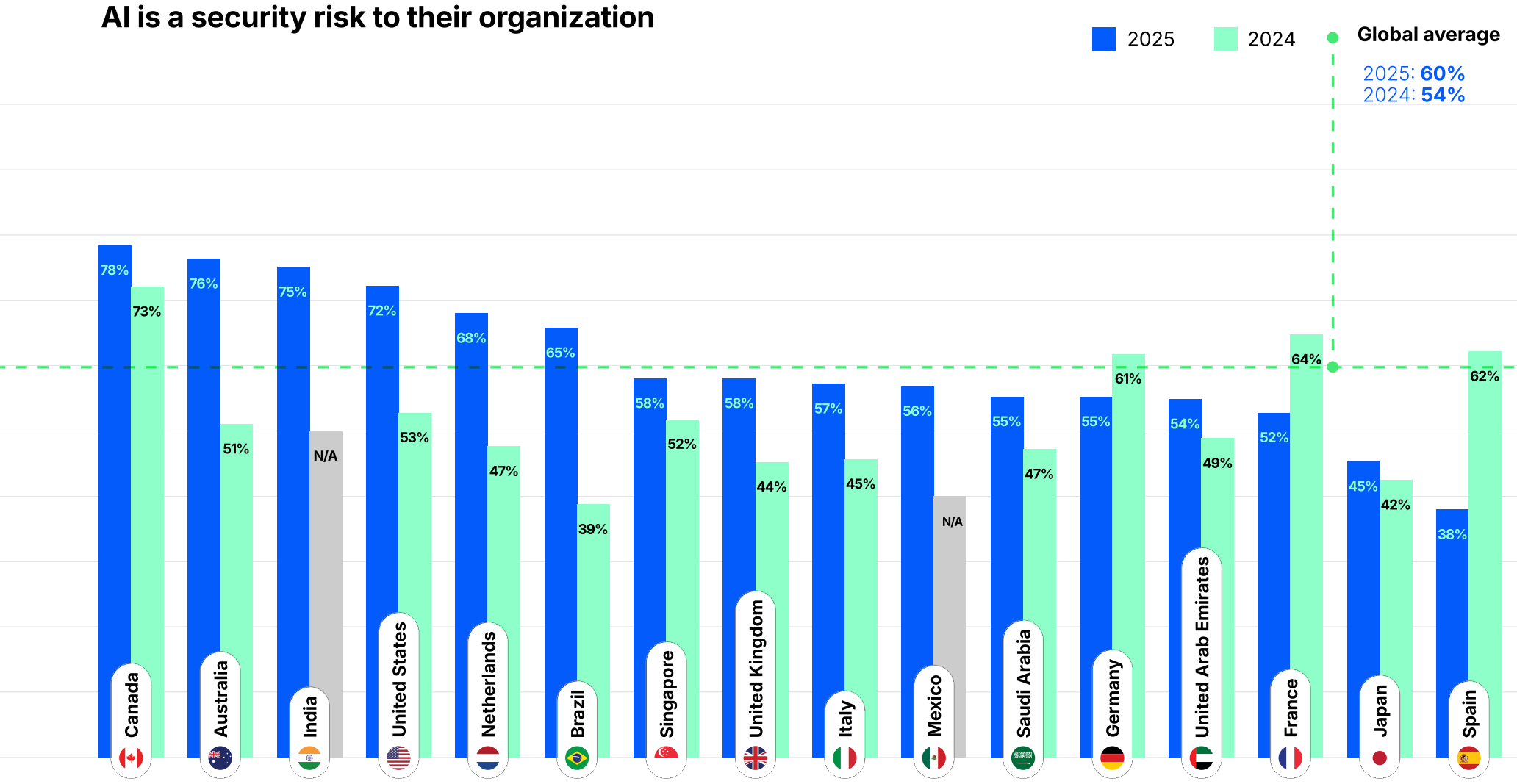
The way we work and share information has changed, bringing with it new and changing risks.

Therefore, the way we protect our people and data in this environment must also change. The rapid accessibility and adoption of GenAI has all but opened an invisible back door into many organizations, allowing people to share and create data outside traditional protections.

60%

of global CISOs believe generative AI poses a risk to their organization, up from 54% in 2024.

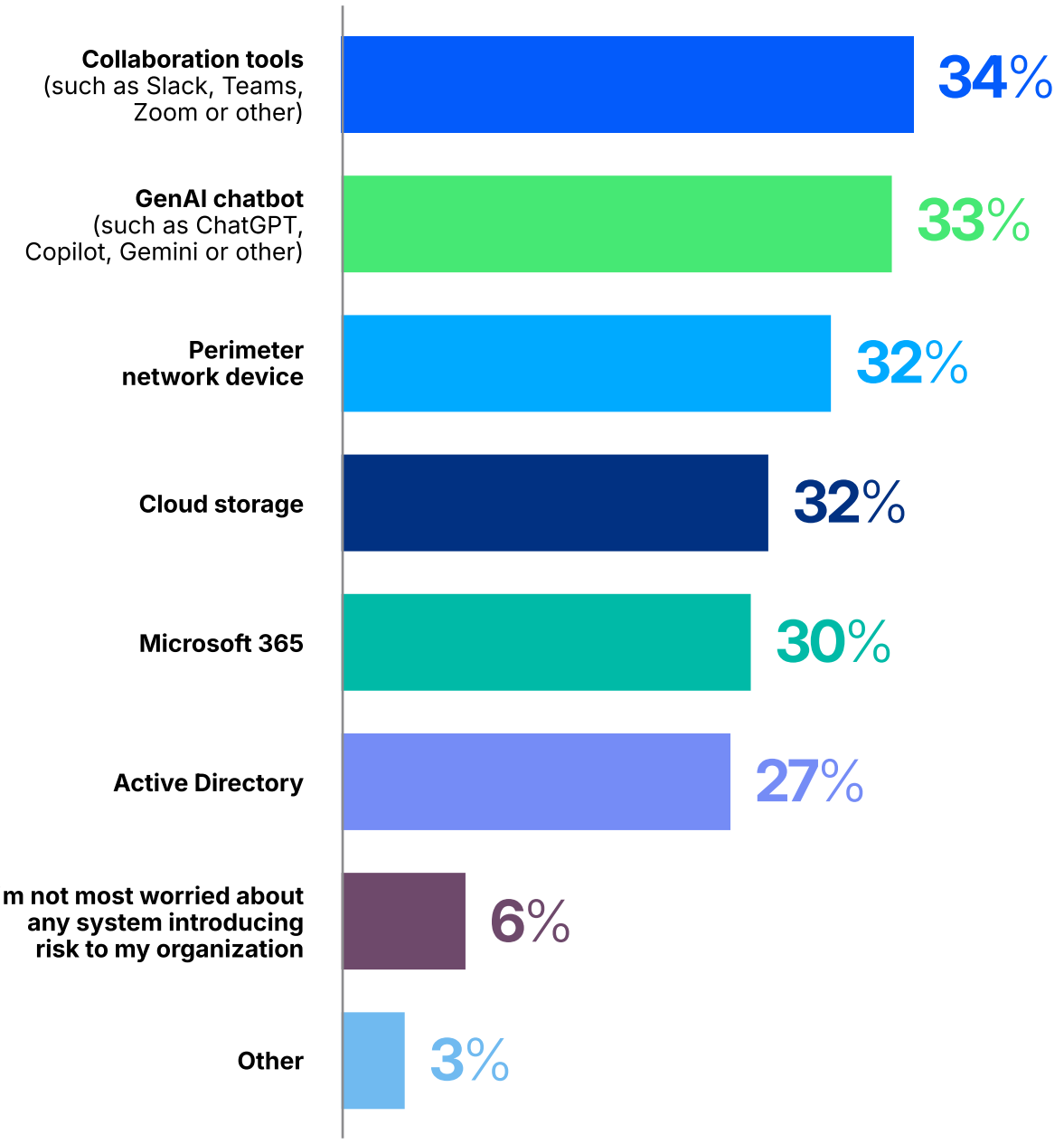
Percentage of CISOs who believe generative AI is a security risk to their organization



The same amount, three in five global CISOs, are concerned about losing customer data through the use of public GenAI platforms and tools. CISOs in the U.S. are the most concerned (80%), with their counterparts in Spain the least concerned (39%). Across industries, retail (70%), IT, technology and telecom (70%) and transport (69%) were most concerned, with education the least concerned at 34%.

CISOs are naturally alert to these developments in AI-powered applications. When asked which systems they were most worried about introducing risk to their organization, collaboration tools and GenAI chatbots like ChatGPT, Copilot and Gemini topped the list.

What system, if any, are you most worried about introducing risk to your organization?
(Pick up to 3)



Embracing AI: balancing risk and reward

Many are taking action in response to AI's increased ubiquity. Over half (59%) of global CISOs say their company blocks or restricts employee usage of GenAI tools. This is more prevalent in India (74%), Canada (73%) and the US (72%).

However, despite growing concern, most understand that the availability and potential benefits of such tools require care management and governance rather than restriction. Of the CISOs surveyed, 64% say enabling the use of AI tools is a top priority over the next two years. This is felt most strongly in Mexico (81%), Australia (74%) and Japan (73%).

More than two-thirds (67%) of global CISOs say their organization has already implemented guidelines to enable employees to use AI tools within the limits of company data protection policies. Top of the chart was Canada and Mexico (84%), Australia (83%) and the U.S. (82%).

Enabling the safe use of AI tools and automation technologies is a top priority over the next 2 years for 64% of global CISOs.

Others (68%) are focused on using AI as an advantage and are considering deploying AI-powered capabilities to help protect their organization against human error and advanced human-centric cyberthreats. While a significant figure, this is down from 87% last year, suggesting the hype around AI as a cybersecurity "silver bullet" is at least beginning to subside.

59%

of global CISOs say their company blocks or restricts employee usage of generative AI tools.

68%

of global CISOs are looking at deploying AI-powered capabilities to help protect their organization against human error and advanced human-centered cyberthreats.

67%

of global CISOs say their organization has guidelines in place to ensure employees can use AI while adhering to our organization's data protection policies.

"AI presents both tremendous promise and considerable risk for today's security leaders. While many CISOs are rightly concerned about data leakage and misuse through generative AI tools, they also recognize AI's potential to enhance cyber defenses. Striking the right balance—one that fosters innovation while maintaining strict controls—will be critical. As AI becomes further embedded in business processes, governance and transparency will be non-negotiable."

John Driggers,
CISO and
cybersecurity director,
SLB

CHAPTER 6

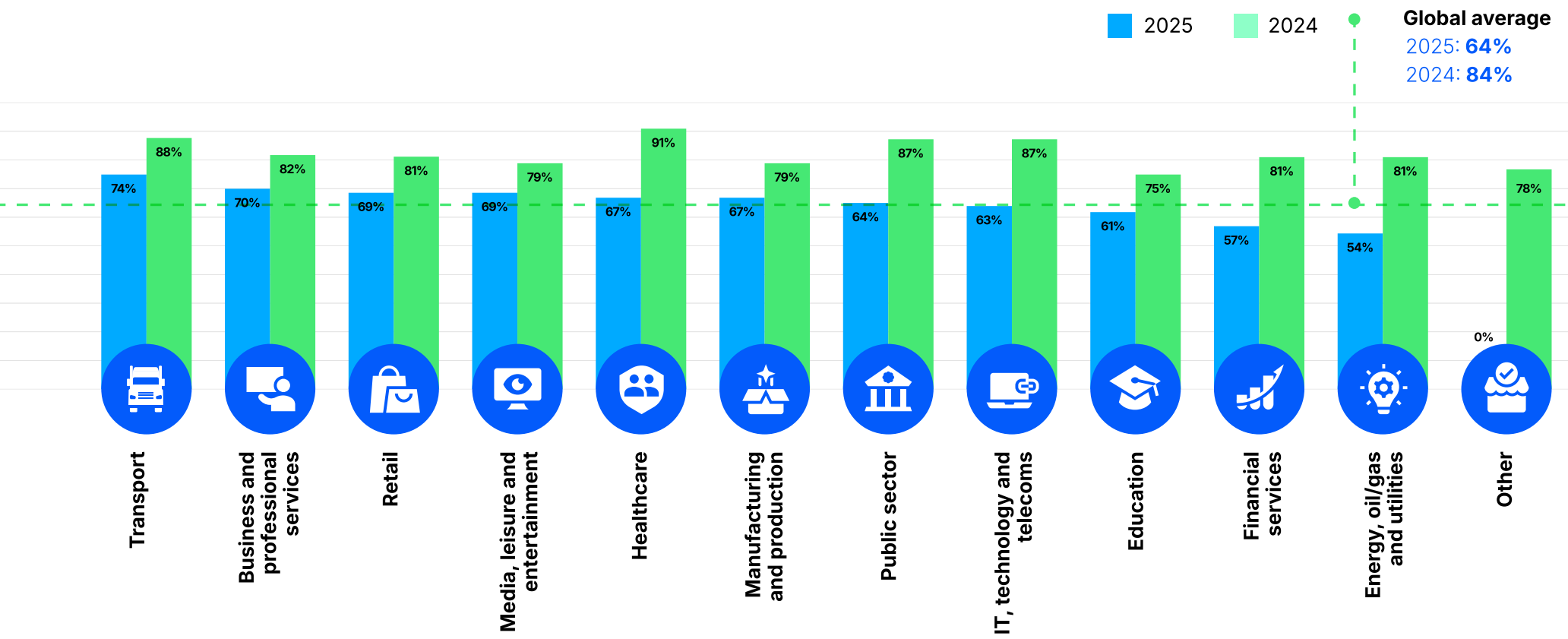
The CISO's seat in the boardroom

As a relatively recent introduction to most boardrooms, relations between the CISO and the wider executive suite are not always as strong as many would like.

Looking back to 2022, just 51% of global CISOs said they saw eye to eye with their board on the issue of cybersecurity. This figure increased to 62% in 2023, all the way to 84% in 2024. Unfortunately, it is not a trajectory that has continued.

Of this year's surveyed CISOs, just under two-thirds (64%) agree that their board sees eye to eye with them on the issue of cybersecurity. There is strong board alignment in Australia (82%), Mexico (79%), and Canada (78%). Least aligned are Spain (47%), Singapore (51%) and Japan (54%).

Percentage of CISOs by industry who agree their board sees eye to eye with them on the issue of cybersecurity, by industry



As for what is behind this downturn, there are likely many factors at play. For one, the CISO is no longer such a rarity in presenting at the boardroom table, potentially leading to complacency around the importance of the role and the continued need for their expertise.

The demand for cybersecurity knowledge at the board level is also viewed as less imperative by CISOs themselves. Only 66% now believe cybersecurity expertise should be required by board directors, down from 84% in 2024. This may be due to increased confidence in the CISO's ability to speak the language of the boardroom and explain cyber issues to those with less understanding of the industry and the current threat landscape.

There is further evidence of the growing confidence CISOs have in their boards elsewhere, too. Last year, CISOs cited the impact on business valuation as the least pressing concern when it comes to the consequences of a material cyberattack. This year, it tops the list, demonstrating that communication and discussion of cyber issues at the board level is making a difference in overall risk management strategy. The C-suite and their boards likely have a much more realistic view of the potential impact of attacks on their organizational reputation and the bottom line.

66%

of global CISOs agree that cybersecurity expertise should be required at the board director level.

Board cybersecurity concerns: Given your interactions with the board, what do you believe are their greatest concerns with regard to a material cyberattack on the business? (Pick top three)

Secondary Concern Primary Concern

	Loss of sensitive information	Significant downtime	Disruption to operations	Impact on business valuation	Reputational damage	Loss of current customers	Loss in revenue	Other	I don't believe they have a particular concern with regard to a material cyberattack on the business
GLOBAL	**32%**	**31%**	**31%**	**35%**	**31%**	**31%**	**26%**	**2%**	**1%**
U.S.	29%	31%	**38%**	**44%**	**44%**	28%	29%	0%	0%
Canada	31%	18%	29%	**32%**	**38%**	30%	24%	0%	0%
France	21%	22%	23%	**32%**	16%	**33%**	15%	14%	1%
Germany	**38%**	27%	23%	30%	35%	**39%**	29%	0%	0%
Netherlands	34%	**40%**	**36%**	35%	24%	**36%**	30%	0%	0%
Mexico	**39%**	**39%**	**35%**	**39%**	**39%**	31%	29%	0%	2%
U.A.E.	**36%**	19%	25%	**40%**	25%	31%	24%	0%	0%
Saudi Arabia	36%	29%	**44%**	28%	29%	**40%**	39%	5%	0%
Australia	27%	**36%**	**30%**	29%	29%	21%	19%	0%	0%
Singapore	**37%**	35%	**37%**	35%	**44%**	29%	20%	0%	0%
Japan	36%	**44%**	21%	**37%**	32%	36%	26%	1%	1%
India	23%	32%	**43%**	35%	**37%**	28%	29%	0%	1%
Brazil	29%	34%	**36%**	**40%**	26%	**40%**	33%	0%	0%
Italy	**37%**	**41%**	29%	36%	25%	24%	22%	4%	2%
Spain	**31%**	26%	24%	28%	22%	25%	**29%**	14%	1%
U.K.	**31%**	28%	24%	**41%**	24%	26%	15%	1%	0%

"CISO-board relationships are improving, but many boards still undervalue cybersecurity as a strategic business priority. CISOs must actively shape board understanding of cybersecurity as a strategic, risk-based function. They can build trust by co-defining risk appetite aligned with regulatory, financial, and reputational stakes. By presenting a clear, risk-oriented view of the organization's cyberposture and offering a governance framework, CISOs can enable informed investment decisions. Crucially, they must shift the board's focus from compliance to resilience—framing cybersecurity as a core enabler of business continuity and long-term value."

Ben McLaughlin,
chief information security officer, Proofpoint

CHAPTER 7

Different year. Same CISO pressures.

The role of the CISO has evolved significantly in recent years. Since Proofpoint has been conducting this global annual survey, we have seen greater representation of the role in the C-suite and at the board level, with a closer alignment between cybersecurity and business strategy.

However, with greater prominence comes increased pressure. For the second year running, two-thirds of CISOs (66%) feel they are subject to excessive expectations. This is felt most keenly by those in Mexico (87%).

66%

of global CISOs agree that there are excessive expectations levied on them.

Percentage of CISOs who agree that there are excessive expectations on the CISO/CSO

CISOs in the spotlight

With expectations remaining consistent yet burnout increasing, it appears CISOs need more support to cope with an increasingly demanding and changing role. With only 67% believing that their organization offers adequate budgets, staff and tools to meet their cybersecurity goals, there is clearly more work to be done in dealing with the psychological pressures and stress of the job.

Exposure to risk and mounting responsibility are undoubtedly factors behind CISO stress levels. Over two-thirds (67%) feel they are personally held accountable when a cybersecurity incident occurs. This figure has remained steady in recent years, up slightly from 62% in 2023 and 66% in 2024. This accountability in the role was felt the most by CISOs in the U.S (85%), Mexico (82%), Canada (81%), and Australia (80%).

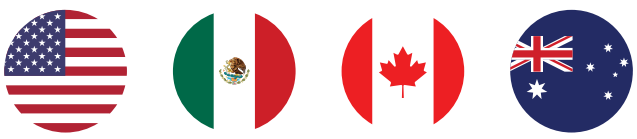
However, there are reasons for optimism on this front at least. With 65% of CISOs reporting that their organization has taken steps to protect them from personal liability related to cybersecurity, we can hope to see the pressure on CISOs ease at least slightly in the years ahead.

Over

2/3

of global CISOs (67%) feel they are personally held accountable when a cybersecurity incident occurs.

Across industries, CISOs in transportation (77%) and retail (75%) felt most protected, whereas CISOs in financial services (53%) and public sector (59%) felt the least protected.



CISOs in the U.S, Mexico, Canada and Australia felt most protected from personal liability by their company.

"The pressure on CISOs remains unrelenting, with high expectations and increasing personal accountability defining the role. While there are encouraging signs—such as greater board support and organizational steps to mitigate liability—the rate of reported burnout continues to rise. This highlights a disconnect between the recognition of the CISO's burden and the support structures available. Sustainable security leadership requires not only technical investment but also a focus on the wellbeing of those charged with protecting the enterprise."

Brian Cox,
vice president and chief information security officer, Cox Enterprises

Conclusion

CISOs could be forgiven for thinking life is on repeat in recent years. Once again, most believe a cyberattack is imminent, that they are unprepared to deal with its consequences and feel their people are their greatest areas of risk.

In 2025, however, there are several new developments in the mix. The widespread adoption of AI into the way we work with generative AI tools and LLMs brings a new world of both risk as well as opportunity for the cyberdefender. Many are using these powerful technologies to bolster defenses and improve ways of working.

All of this only adds to the pressure on CISOs to secure their organizations in the face of a rapidly changing threat and technological landscape. As a result, expectations remain high and increasing numbers are feeling the pressure and are experiencing burnout.

With little room to give, this adds greater credence to the notion that the CISO role will continue to evolve. Could 2026 be the year that we see a greater divergence of responsibilities between those focused on threat defense and incident response on one hand and others aligning their focus on cyber governance, risk and compliance on the other?

That remains to be seen. But there's one thing we can be sure of, CISOs are sure to have a full array of opportunities and challenges in protecting people, safeguarding data and keeping organizations safe from harm.

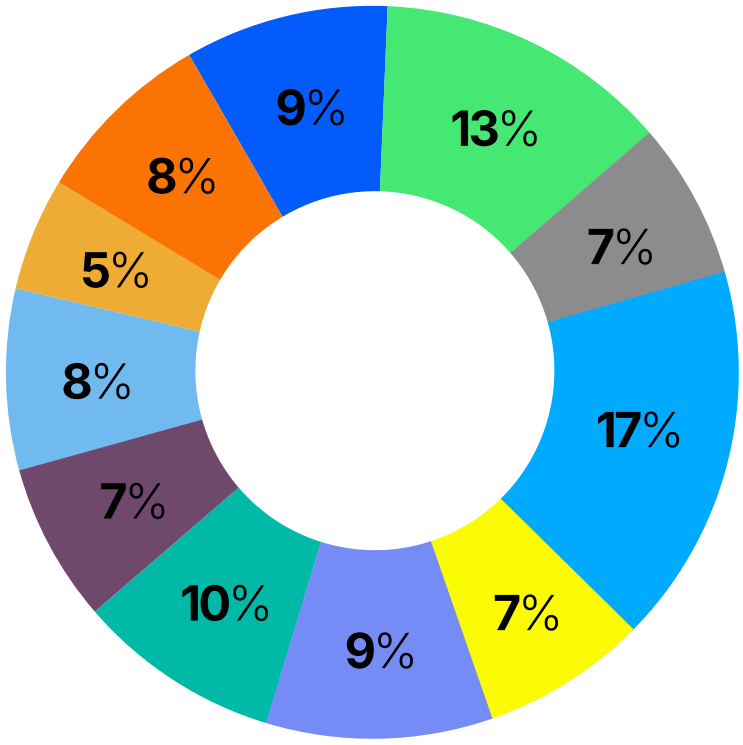
Methodology

The Proofpoint 2025 Voice of the CISO survey, conducted by Research firm Censuswide between 4 March–14 March 2025, surveyed 1,600 chief information security officers from organizations of 1,000 employees or more across different industries in 16 countries.

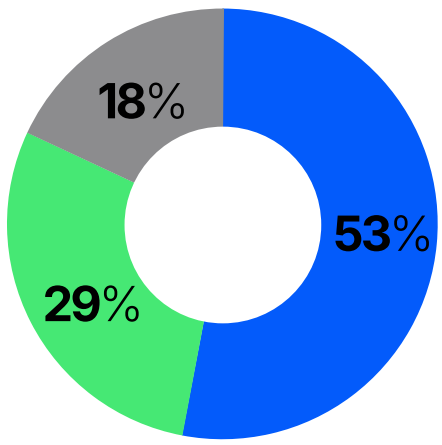
One hundred CISOs were interviewed in each market, which includes the U.S., Canada, Brazil, Mexico, the UK, France, Germany, Italy, Spain, the Netherlands, UAE, KSA, Australia, Japan, Singapore and India.

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

Industry split among respondents



Business and professional services	151
Education	200
Energy, oil/gas and utilities	113
Financial services	275
Healthcare	107
IT, technology and telecoms	148
Manufacturing and production	156
Media, leisure and entertainment	111
Public sector	122
Retail	88
Transport	127
Other	2



Company size split among respondents

1,000-2,500 employees	850
2,501-5,000 employees	464
5,001+ employees	286

Contact us

at info@proofpoint.com
to better protect your business.

proofpoint.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM

0400-015-02-01 08/25