proofpoint.

REPORT

2024 Voice of the CISO

Global Insights into CISO Challenges, Expectations and Priorities

proofpoint.com

TABLE OF CONTENTS

2024: Navigating the Cybersecurity Maelstrom

CISOs have had a lot to contend with in recent years: a global pandemic, large-scale remote work, and record levels of employee turnover. From the outside looking in, one could be forgiven for thinking the past 12 months have been serene by comparison.

But for CISOs caught in the whirlwind, this was the year the perfect storm reached its peak.

Thanks to hybrid working as standard and the growing reliance on cloud technology, the attack surface has never been larger. Cyber threats are more targeted, sophisticated, and frequent than ever before. Meanwhile, employees are increasingly mobile – often taking data with them when they change jobs.

And while generative artificial intelligence (AI) tools hold great promise, they also have lowered the bar to entry for cyber criminals. Anyone with a few pounds now has the means to launch devastating attacks.

To be sure, CISOs are enjoying closer ties with key stakeholders, board members and regulators. But this proximity also brings higher stakes, more pressure, and heightened expectations. And with flat or reduced budgets, CISOs must try to do much more with considerably less. In this environment of tight resources and rapid change, shortcuts are sometimes necessary. But they can lead to human error.

To better understand how CISOs are navigating another high-pressure year, Proofpoint surveyed 1,600 CISOs around the world. We asked them about their roles, their outlook for the next two years, and how they see their responsibilities evolving. For richer insights into complex cybersecurity practices, this year's Voice of the CISO surveyed only organisations with 1,000 or more employees.

In this summary, we explore the delicate balance between concern and confidence as many factors combine to ramp up the pressure on the CISO.

We hear how our people continue to put us at risk and what organisations are doing to bolster human-centric defences. We also delve into the mind of the CISO, tackling the challenging topics of burnout, personal liability, and boardroom relationships.

Finally, we look to the years ahead to get a better understanding of what we can expect on the cybersecurity horizon.

As always, this report would not have been possible without the insight offered by cybersecurity and information security professionals across the globe. We offer our sincere thanks for your time and feedback.

Patrick Joyce, Global Resident CISO at Proofpoint

Heightened Concerns but Growing Confidence

CISOs are struggling with a jarring mix of challenges: the waning cybersecurity spotlight as the pandemic fades from view; the ongoing struggle to secure remote and hybrid workforces; whiplash as workforces reel from the Great Resignation, tech layoffs and constant business restructuring; and the rise of hard-to-detect yet easy-to-execute threats.

Whatever the cause, one thing is clear: CISOs are nervously looking over the horizon.

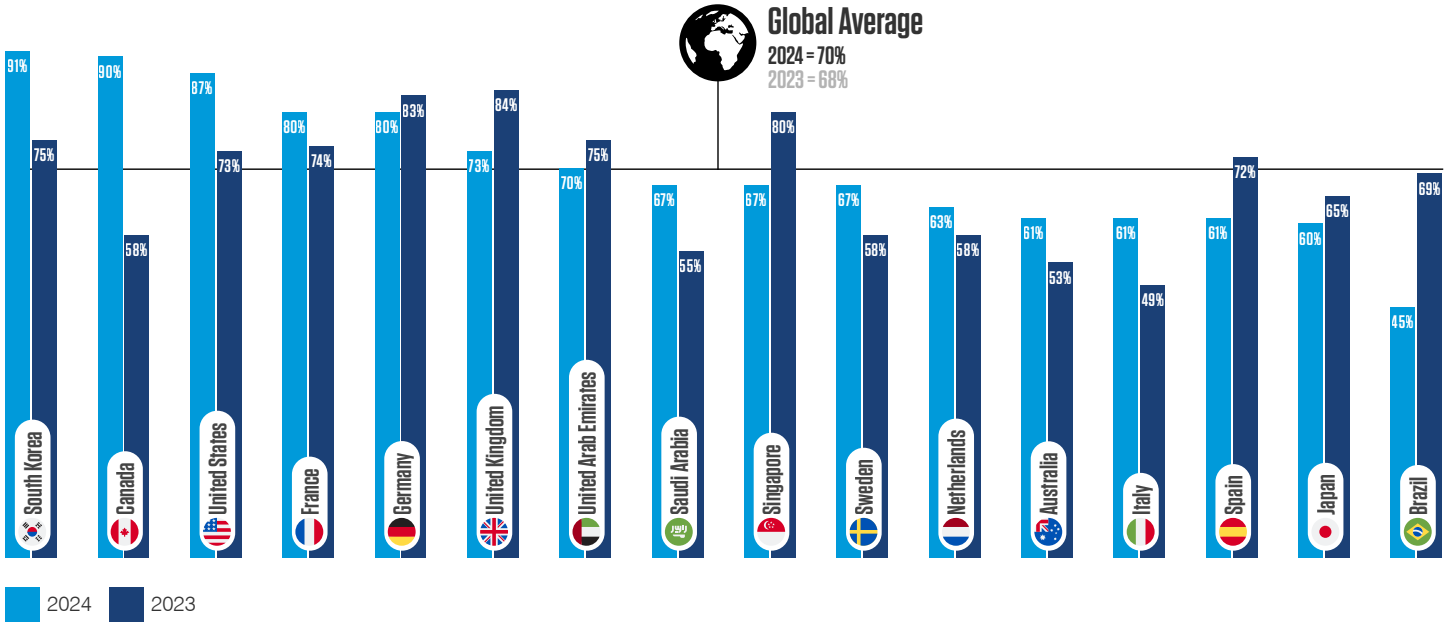
Over two-thirds (**70%**) of those surveyed feel at risk of a material cyber attack over the next 12 months. This figure is only a slight increase from **68%** last year. But compared to **48%** of respondents who felt so in 2022, today's CISOs clearly remain on high alert.

That just under a third (**31%**) feel a significant attack is "very likely" further underlines the CISO's collective anxiety, compared to **25%** in 2023.

70%

of CISOs feel at risk of experiencing a material cyber attack over the next 12 months. 31% rate the risk as very likely.

Percentage of CISOs who agree that their organisation is at risk of a material cyber attack in the next 12 months.



CISOs in South Korea (**91%**), Canada (**90%**), and the US (**87%**) are most concerned about experiencing a material cyber attack.

CISOs (**70%**) and board members (**73%**) both feel that a material cyber attack is likely in the next 12 months.

Brazil's CISOs are the most optimistic, with just **45%** fearing an attack.

Education (**86%**), transport (**77%**), and retail, healthcare and public sector (all **74%**) lead the way for cyber attack concerns across industry verticals.

Board member statistics from "**Cybersecurity: The 2023 Board Perspective report.**"

Awareness vs Preparedness

A growing concern around the likelihood of a cyber attack may seem like bad news. Still, that most CISOs are aware of the potential risks they face is heartening.

Put simply, CISOs are right to be concerned; as cyber criminals refine their tactics, target our people, and work along the attack chain for maximum impact.

There's more room for positive thinking when we look at security preparedness, too. A little under half (**43%**) of CISOs agree that their organisation is unprepared to cope with a targeted cyber attack in 2024. This is something of an improvement on 2023 (**61%**) and 2022 (**50%**).

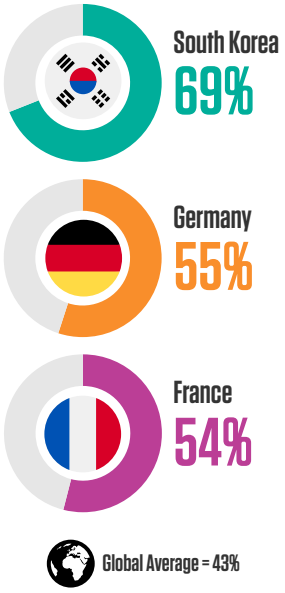
But while it's good news that more CISOs feel prepared for the challenges ahead, we can't ignore those who do not share this sentiment.

That **70%** feel at risk of a cyber attack yet almost half feel unprepared for its impact is concerning. It highlights again the unwavering disconnect between cybersecurity awareness and preparedness.

43%

of CISOs agree that their organisation is unprepared to cope with a targeted cyber attack in 2024.

Percentage of CISOs who agree that their organisation is unprepared to cope with a targeted cyber attack in 2024. Top three countries:



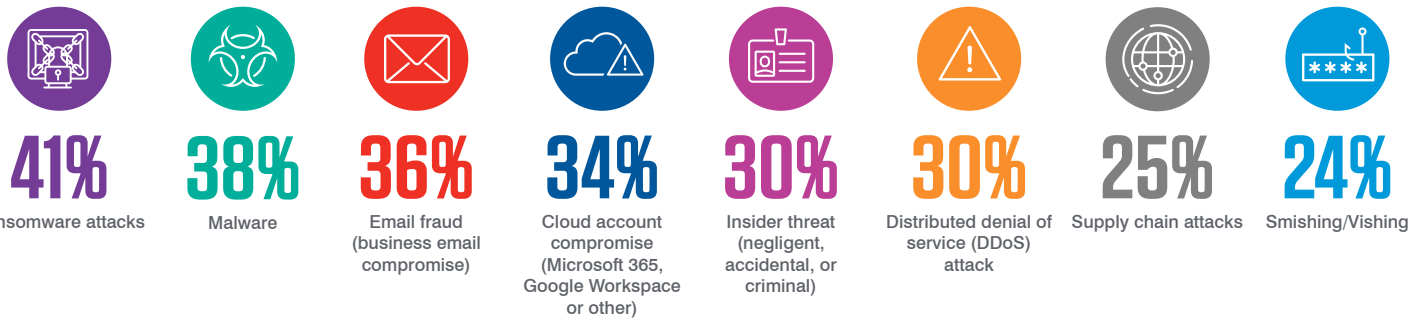
CISO's view of the threat landscape

What keeps CISOs awake at night? Not surprisingly, **41%** see ransomware as the leading threat across the next 12 months. Malware (**38%**), email fraud (**36%**), cloud account compromise (**34%**), Insider threats (**30%**), and DDoS attacks (**30%**) round out the top five concerns.

Several of these issues – email fraud, insider threats, DDoS attacks, and cloud account compromise – remain on the list from last year. Ransomware's rise to the top of the list is an interesting change, if not unsurprising given high-profile attacks in 2023 and into 2024.

Attackers have greatly raised the stakes with double and triple extortion threats and maturing ransomware ecosystems. That's why CISOs must look for opportunities to disrupt attacks at every stage of the attack chain – from initial compromise to lateral movement and privilege escalation to data exfiltration.

What, if anything, do you perceive to be the biggest cybersecurity threats within your organisation/industry in the next 12 months? (Pick up to three.)



On another positive note, boards seem increasingly receptive to the concerns of the CISO. Both appear to be closely aligned; board members see malware, insider threats, cloud account compromise, and ransomware as the biggest cybersecurity threats facing their organisations.

Ransomware is the top concern among CISOs in Japan (**64%**), UK (**51%**), Sweden (**49%**), and the Netherlands (**49%**).

Among industries, manufacturing and production (**54%**), retail (**46%**), and healthcare (**43%**) all agree that ransomware will be the biggest threat over the next 12 months.

Malware threats lead the way in Italy (**53%**), Brazil (**46%**), and Singapore (**45%**).

Email fraud remains among the top three concerns since the first Voice of the CISO report in 2021. This year, it is of the most concern among CISOs in Saudi Arabia (**50%**), Australia (**46%**), Germany (**46%**), Canada (**42%**), The Netherlands (**42%**), and Japan (**42%**).

Email fraud, however is seen as the biggest threat over the next 12 months by the following industries: public sector (**61%**), transport (**58%**), and financial services (**41%**).

"In today's evolving threat landscape, CISOs are navigating through the aftermath of the pandemic, adjusting to the new normal of hybrid work, and grappling with enormous tech industry shifts. Amid these transformative times, the emergence of sophisticated cyber threats that exploit human vulnerabilities and systems is undeniable. While the heightened probability of cyber attacks might seem alarming, it's reassuring that CISOs are acutely aware and prepared for potential risks. The concern CISOs harbour is a testament to their vigilance; recognising that cyber criminals are continuously honing their strategies to exploit every link in our security chains."

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

Human Error: The Persistent Vulnerability

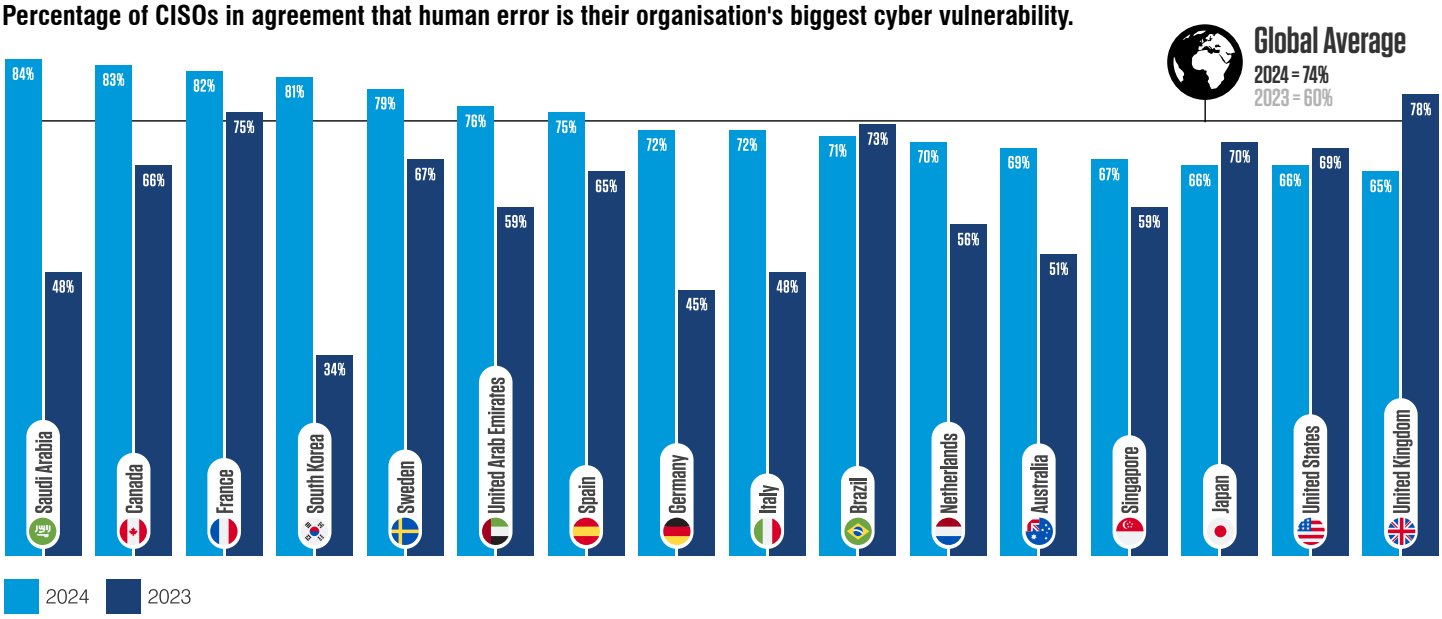
Just as concern around impending cyber attacks is growing, so too is the consensus on the top risk factor: people. In a year of growing insider threats and data loss caused by people, more CISOs than ever see human error as their biggest cyber vulnerability.

Almost three-quarters (**74%**) of surveyed CISOs feel this way, up from **60%** in 2023 and **56%** in 2022. Board members are not as convinced. A little under two-thirds (**63%**) agree that human error is the biggest vulnerability, suggesting that CISOs have more work to do to bring the boardroom up to speed.

74%

of CISOs consider human error to be their organisation's biggest cyber vulnerability.

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



An even higher number of CISOs (**80%**) see human risk, including employee negligence, as a key cybersecurity concern over the next two years. That's up from **63%** in 2023. This sentiment was most keenly felt in France (**91%**), Canada (**90%**), Spain (**86%**), South Korea (**85%**), and Singapore (**84%**).

CISOs seem to understand that, given most successful cyber attacks require human interaction, data loss is inherently a people problem. Still, **86%** believe their employees understand their role in defending their organisation; almost half (**45%**) strongly agree.

In other words, CISOs believe their people know what is being asked of them but still feel that they pose an enormous risk. The implication: users grasp what's expected of them but lack the skills, knowledge and tools required to defend their organisation's data.

CISOs in Saudi Arabia (**84%**), Canada (**83%**), and France (**82%**) are most concerned about human error being their organisation's biggest cyber vulnerability.

CISOs within these sectors: education (**89%**), media leisure and entertainment (**85%**), and public sector (**78%**) believe human error is their organisation's biggest cyber vulnerability.

Protecting against the people problem

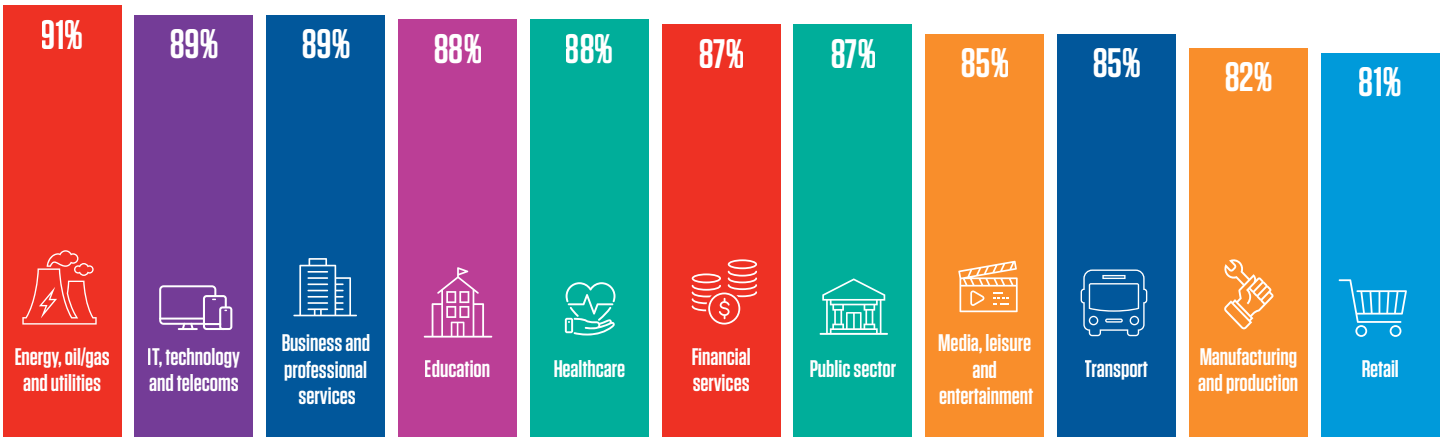
To mitigate this area of human vulnerability, many CISOs are turning to AI-powered technology. Of those surveyed, **87%** are looking to deploy such tools to protect against human error and block advanced human-centric cyber threats.

This holds true across all surveyed industries, with retail (**81%**), IT, technology and telecoms (**89%**), and education (**88%**) leading the way.

87%

of global CISOs are looking to deploy AI-powered capabilities to help protect their organisations against human error and advanced human-centric cyber threats.

Percentage of CISOs by industry who are looking at deploying AI-powered capabilities to help protect their organisations against human error and advanced human-centric cyber threats.



"As the digital landscape evolves, CISOs unanimously point to one constant in the cybersecurity equation: the human element. Despite recognising that insider threats and inadvertent data mishandling are on the rise, there's a consensus that employees are aware of their cybersecurity responsibilities. Yet, there's an acknowledgment of a critical gap – understanding doesn't always equate to capability. To bridge this divide, CISOs increasingly seek AI-driven technologies as an ally in reinforcing human defences against sophisticated cyber threats."

Martin Bally
VP & Chief Information Security Officer, Campbell Soup Company

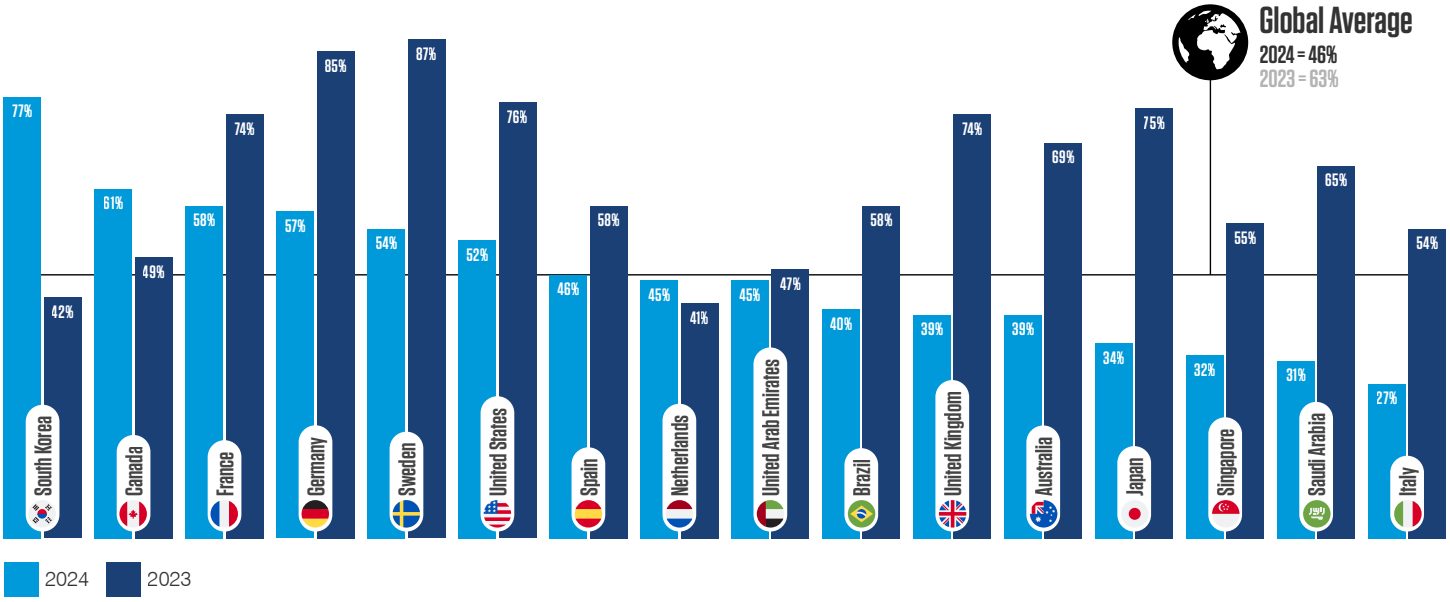
Data Protection and Insider Threats

An increasing awareness of both risk levels and risk factors looks to have translated to tighter security over the past 12 months. This year, fewer than half (**46%**) of global CISOs reported a material loss of sensitive information – down from **63%** last year.

That said, several countries came in considerably higher than this worldwide average. Over two-thirds (**77%**) of CISOs in South Korea reported the loss of sensitive data, followed by **61%** in Canada, **58%** in France, and **57%** in Germany.

77% of organisations in South Korea dealt with material data loss in the last year – the highest rate of any country surveyed.

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



Where industries are concerned, education (**68%**), financial services (**54%**), and media, leisure and entertainment (**54%**) are the most affected by sensitive data loss in this year's report.

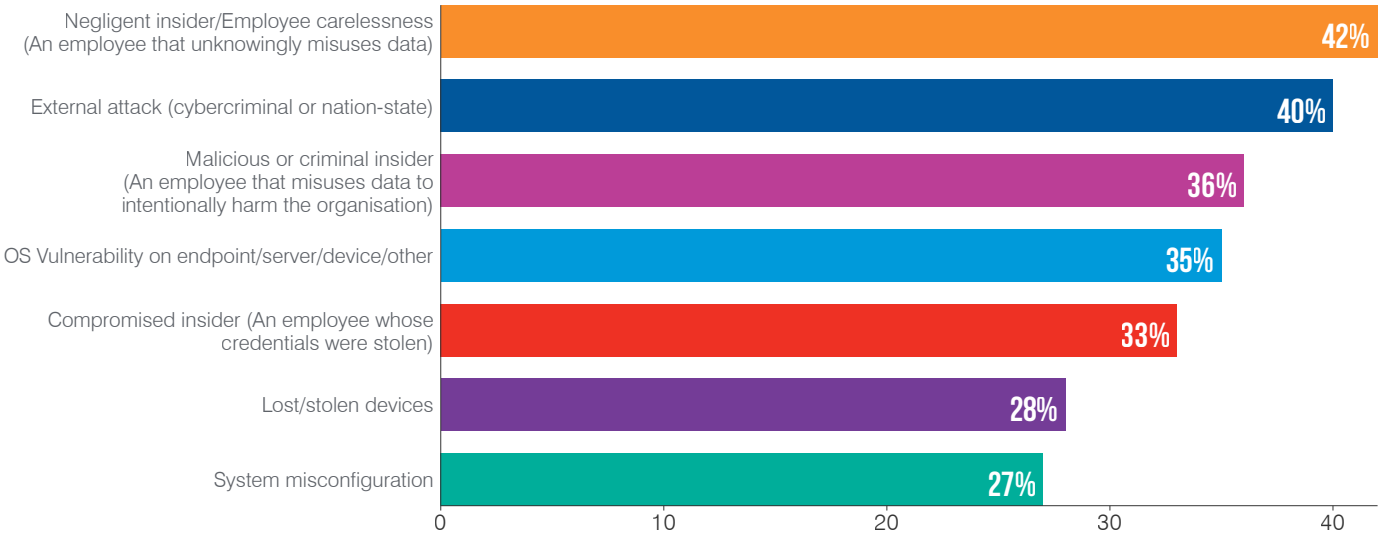
As for what's behind these events, many familiar faces are on display. Of the CISOs who experienced a sensitive data loss, **42%** lay the blame on negligent insiders/careless employees. Other common factors include external attacks (**40%**) and malicious or criminal insiders (**36%**).

Employees are also potentially responsible for many more factors on the list, from system misconfiguration (**27%**) to lost or stolen devices (**28%**).

Human factors have risen year on year, representing the leading cause of data loss. It's no wonder that people remain such a pressing concern for the world's CISOs.

Malicious or criminal insiders are the third leading cause of data loss after external attacks (cyber criminal or state-sponsored). They are the No. 1 factor in Australia (**49%**), UAE (**44%**), Germany (**44%**), and France (**38%**)

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



To further underline this point, people continue to contribute to data loss elsewhere. Almost three-quarters (**73%**) of CISOs said that employees leaving their organisation played a role in a data loss event.

As the rate of resignations fell back to pre-pandemic levels in many countries towards the end of 2023, concern around losing data to job switchers is down from **82%** last year. But there is no room for complacency. The modern workforce changes jobs more frequently than any generation in history, and data will continue to leave with them at an alarming rate.

The trend is most pronounced among industries that handle large amounts of highly sensitive information, underlining the challenge of protecting data against intentional exfiltration.

95%

of CISOs in the education sector have lost data with an employee leaving their organisation. Healthcare (89%), media, leisure and entertainment (88%), financial services (83%), and transport (80%) complete the top five.

The consequences of material data loss stretch far and wide. Most CISOs reported financial loss (**43%**), post-attack recovery costs such as operational downtime and data recovery (**41%**), and loss of critical data (**40%**).

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

New tools and changing priorities

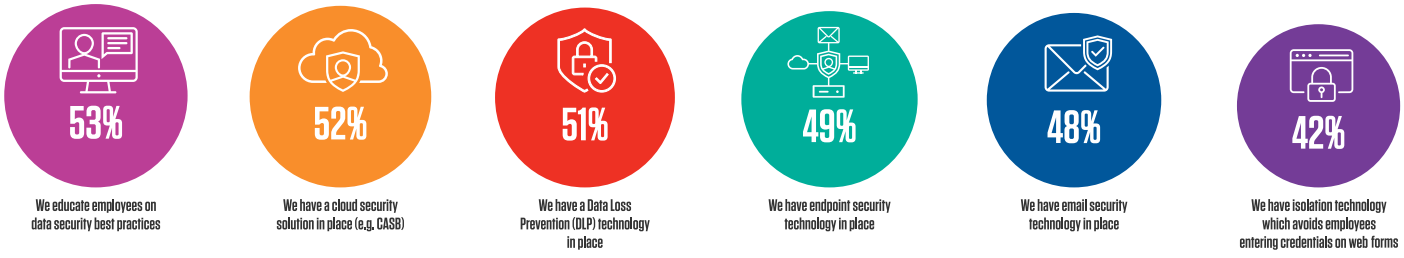
Combating data loss remains a top priority for CISOs around the world, for obvious reasons. About half educate employees about security best practices (**53%**) and use cloud security solutions (**52%**) to get a handle on the issue.

Others deploy dedicated data loss prevention (DLP) technology (**51%**), endpoint security (**49%**), email security (**48%**), or isolation technology (**42%**) to block employees from entering credentials on web forms.

As people remain our most vital line of defence right across the attack chain, CISOs are right to place user education as a pivotal part of their security strategy. But given that **80%** of CISOs also see human error and negligence as a top concern, it's not clear what fruits those efforts have borne.

Financial loss (**43%**), post-attack recovery costs (operational downtime, data recovery, legal) (**41%**), and loss of critical data (**40%**) are the biggest consequences of data loss.

What protocols do you have in place to combat organisational data loss?



Going forward, CISOs have a clear idea of how best to tackle data loss. Some **87%** agree that information protection and data governance are top priorities. This is a major uptick from previous years – **61%** in 2023 and **59%** in 2022.

The adoption of DLP technology has also surged, up to **51%** this year from **35%** in 2023. As a result, **81%** of CISOs now believe that their data is adequately protected. That's up from **60%** in 2023 and **56%** in 2022.

As outlined in Proofpoint's 2023 Board Perspective Report three-quarters of board members shared this view, putting the boardroom in closer agreement with their CISOs than in previous years.

Spotlight on: Recovery

Every CISO strives to defend the organisation from cyber attacks. But as threats grow more advanced and targeted, security teams often work from the premise that their defences will be compromised or breached at some point. And when that happens, they need to know how to recover – fast.

In a ransomware attack, **62%** of CISOs said their organisations would likely pay the attacker to restore systems or avoid the release of company data. This figure is unchanged from last year's survey.

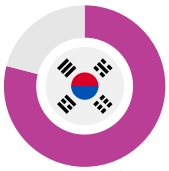
Many others plan to rely on insurance coverage. Overall, **79%** of CISOs agree that if hit by a cyber attack in the next 12 months, they would use cyber insurance to cover losses.

Investing in cyber insurance is usually a preferred option. But it's no substitute for a robust cybersecurity defence. Buying a comprehensive policy is not as straightforward as it once was. And insurers often insist on stringent protocols and protections as a condition of coverage. CISOs using insurance as a fallback should check policy documents and ensure their organisation has the right amount and type of coverage.

If impacted by ransomware within the next 12 months, my organisation is likely to pay a ransom to restore systems/ prevent the release of data. Top three countries:

Saudi Arabia
83%

Canada
82%



South Korea
79%

"CISOs worldwide continue to strengthen cyber defences, recognising that the human factor continues to be the primary driver of data loss. Even as the tidal wave of resignations stabilises, the transient nature of today's workforce signifies that the risk of data walking out the door remains more than a mere possibility – it's an alarming certainty. Particularly in sectors where sensitive information is the currency, CISOs find no reprieve from vigilance. The relentless pace of job movement ensures that protecting against data loss is not just a priority but an ongoing battle in the digital realm."

Phil Ross
Chief Information Security Officer, Air New Zealand

The Cyber Realities for a CISO in 2024

There's been no way to avoid the rise of generative AI over the past year. Whether it's a net force for good or bad will play out – and be debated – for years to come. But one thing's for sure: it's not going anywhere.

So far, CISOs are approaching the technology with a degree of caution. A little more than half (**54%**) believe the technology poses some form of a security risk to their organisation.

54%
of CISOs believe generative AI poses a risk to their organisation.

Spotlight on AI: The double-edged sword

Much is made of AI's potential to aid cyber criminals, and rightly so. With this technology, attacks could get easier to scale and simpler to carry out. Advanced techniques once out of reach for anyone but well-funded cyber criminal gangs and state-sponsored attackers are now up for grabs.

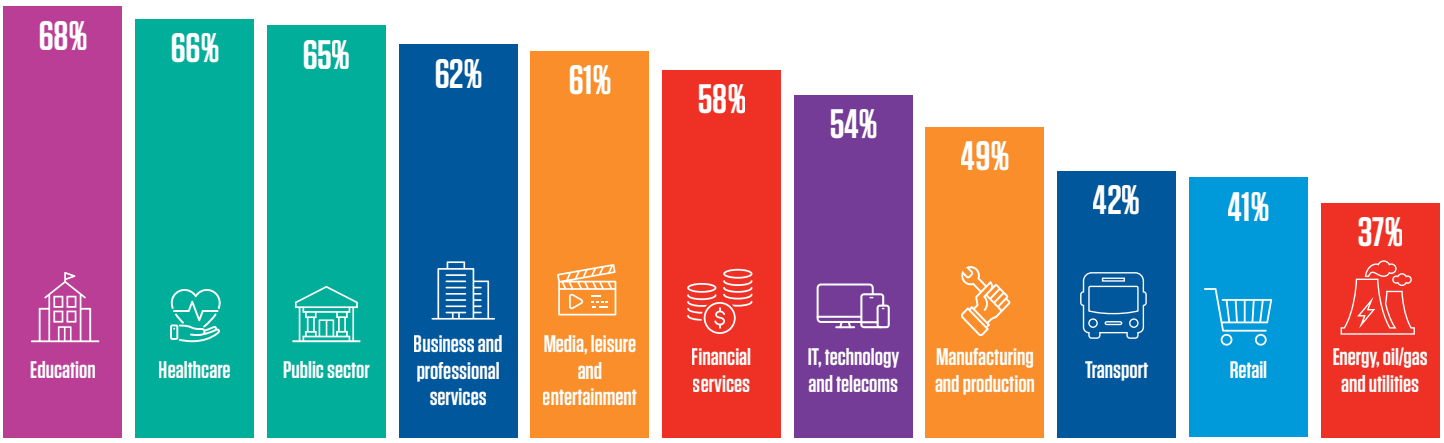
However, greater accessibility of generative AI models can only help defenders, too. Even in these early stages, we can already connect the dots between external threats, sensitive content, and anomalous behaviours or activity. That's something that has not been possible at the same speed and scale with human moderation or traditional analysis.

With this information, we can intervene in communications, focus protections where they are most needed, and stop or limit threats before they occur.

Given the hype-and-bust cycle of many technology trends, it might be tempting to dismiss AI as another fad. But it's already changing cybersecurity. And as the technology improves and security leaders learn new and better ways to apply it, AI could transform the industry.

CISOs in South Korea (**75%**), Canada (**73%**), and France (**64%**) feel most at risk from ChatGPT/generative AI.

Percentage of CISOs by industry who believe generative AI is a security risk to their organisation.



ChatGPT and other generative AI models top the list of systems introducing risk to organisations. But the CISOs also have a keen eye on other platforms such as Slack, Teams and other collaboration tools (**39%**), as well as the ubiquitous Microsoft 365 (**38%**).

Spotlight on budgets and priorities

AI is not the only major trend taking its toll on CISOs. Changing economic conditions around the world are also piling added pressure on already overstretched security teams.

Overall, **59%** of CISOs agree that economic conditions have hurt their organisation, up slightly from **58%** in the previous year.

CISOs in South Korea are being hit the hardest, with **79%** feeling the impact of the turbulent economy. Those in Canada (**72%**), France (**68%**), Germany (**68%**), and Spain (**64%**) are not far behind.

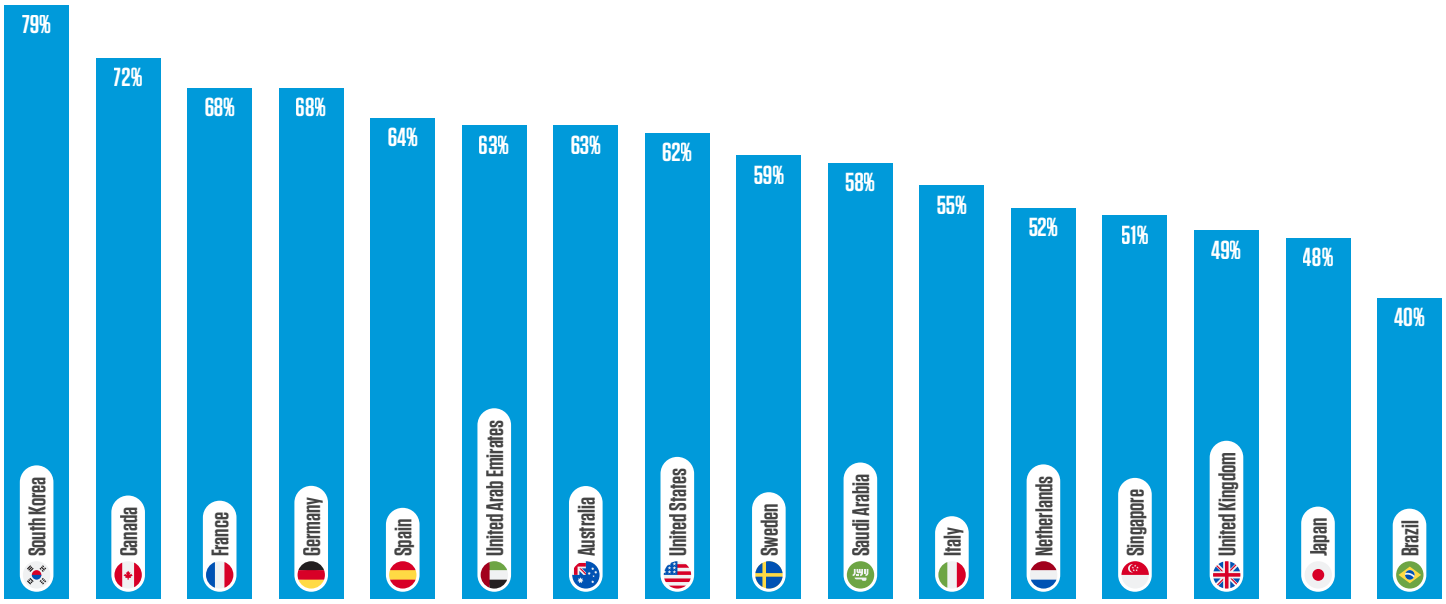
With many security budgets remaining flat at best, CISOs know they are tasked with doing more – or at least, the same – for less. Almost half (**48%**) have been asked to cut staff, delay backfills or reduce spending.

To deliver the most value in this environment, most (**58%**) plan to focus on improving information protection and enabling greater business innovation, just like we saw in 2023.

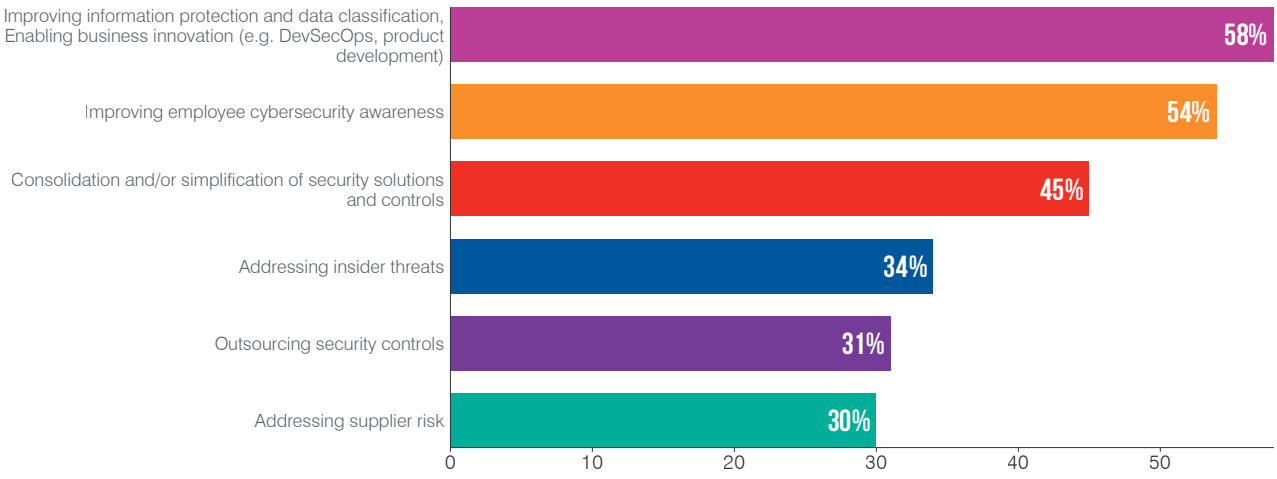
In a notable change to last year's findings, improving employee cybersecurity awareness is now the second-highest priority for the CISOs. While perhaps not surprising, the ranking gives yet another clear sign that human-centric security is now a firm fixture in most cyber strategies.

Cybersecurity budgets have been cut most severely in education (**68%**), healthcare (**68%**), financial services (**55%**), media, leisure and entertainment (**55%**), and IT, technology and telecoms (**48%**)

Percentage of CISOs who agree that the current economic downturn and business challenges have negatively impacted their organisation's ability to resource cybersecurity budgets.



What are the top priorities for your organisation's IT security department over the next two years? (Pick up to three.)



"The ascent of generative AI has been inescapable, marking a new era in cybersecurity that's here to stay, inciting debates on its ultimate impact. CISOs tread carefully, cognizant of AI's double-edged sword – its democratisation grants both cyber criminals and defenders unprecedented capabilities. Cyber attacks could become more scalable and effortless, yet this very technology equips us with real-time insights into threats, a feat unachievable by traditional means. While scepticism often greets technological revolutions, dismissing AI's potential in cybersecurity would be a misstep; it's not just reshaping the field – it's poised to revolutionise it as we adapt and harness its evolving power."

Judy Hatchett
VP, Information Security & CISO, Surescripts

Strengthening Board-CISO Relations

As a recent addition to most boardrooms – and still a worrying omission from some – the CISO has traditionally struggled to get on the same page as the rest of the board.

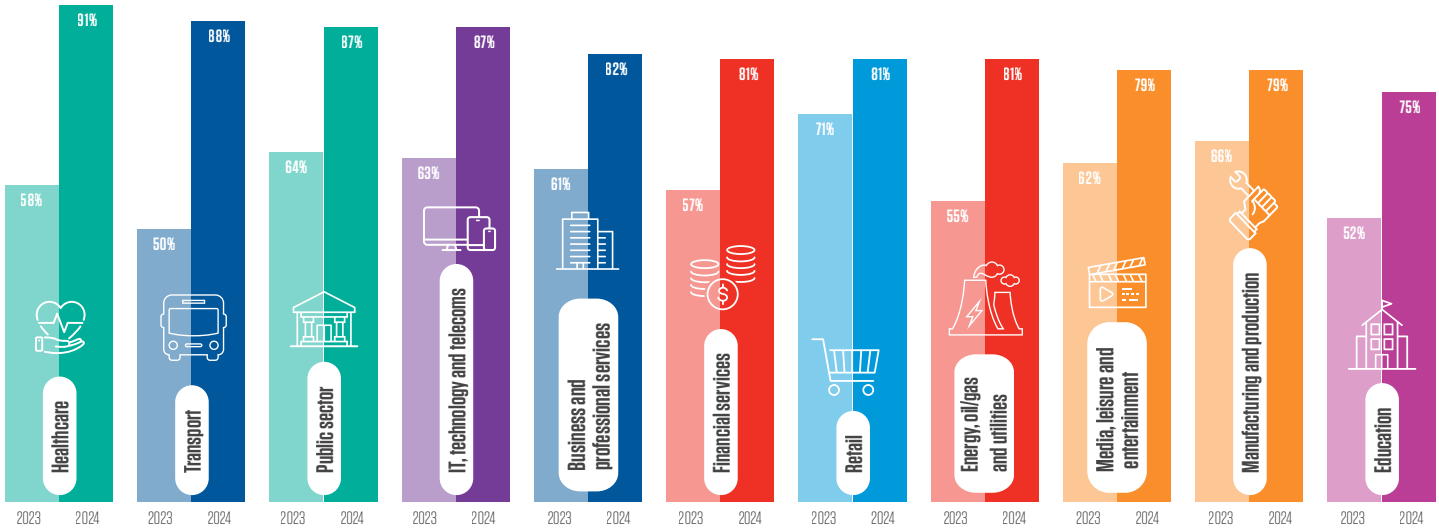
Back in 2022, only half (**51%**) of surveyed CISOs reported seeing eye to eye with their boards. This figure increased only slightly to **62%** in 2023.

This status quo looks to be changing, however. This year, **84%** of CISOs say they see eye to eye with board members on the issue of cybersecurity. The shift echoed across all industries, with healthcare (**91%**), transport (**88%**), and energy, oil/gas and utilities (**81%**) among those most in agreement.

84%

of CISOs believe cybersecurity expertise should be required at the board level.

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



Many factors are likely behind this notable change. Many CISOs have kept their place at the table post-pandemic, influencing wider business strategy as a result. For their part, they may also have taken steps to speak the language of the boardroom, successfully translating security concerns into potential business impact.

This development may have driven the marked increase in CISOs believing cybersecurity expertise to be a board-level requirement – up to **84%** from **62%** in 2023. If the CISO is to remain in the boardroom, it makes sense that they would expect other board members to better understand their remit.

Has this perceived cohesion truly led to a greater understanding? It certainly looks that way.

CISO's believe that their board's greatest concerns about a material cyber attack are: disruption to operations (**44%**), loss in revenue (**44%**) and reputational damage (**43%**).

Most CISOs in Saudi Arabia (**95%**), Brazil (**92%**), Germany (**90%**), and UAE (**90%**) report seeing eye to eye with their board.

CISOs in Singapore (**77%**), Canada (**75%**), and Italy (**70%**) are least concerned about cybersecurity expertise at board level.

Given your interaction with the board, what do you believe are their greatest concerns with regard to a material cyber attack on the business? (Pick up to three.)

	Significant downtime	Disruption to operations	Impact on business valuation	Reputational damage	Loss of current customers	Loss in revenue
Global	37%	44%	34%	43%	39%	44%
UK	32%	39%	25%	41%	27%	37%
US	41%	49%	49%	33%	47%	48%
Canada	33%	53%	38%	40%	45%	42%
France	40%	40%	32%	39%	26%	43%
Germany	49%	49%	36%	51%	41%	42%
Netherlands	32%	43%	35%	46%	25%	47%
Sweden	32%	45%	28%	42%	41%	55%
Italy	45%	41%	30%	41%	32%	41%
Spain	24%	45%	31%	54%	44%	46%
KSA	38%	41%	23%	33%	50%	53%
UAE	42%	34%	31%	51%	43%	57%
Australia	35%	50%	40%	47%	45%	43%
Singapore	49%	60%	32%	52%	29%	43%
Japan	38%	34%	39%	54%	46%	23%
South Korea	37%	42%	43%	33%	43%	43%
Brazil	23%	45%	38%	33%	42%	38%

Main Concern Second/Third Concerns

CISOs have come a long way from being on the sidelines to becoming key players in the boardroom. The recent global pandemic served to not only cement the CISOs' role but also put them front and center in shaping business strategy, speaking in language that resonates with the C-suite and relating security in terms of business outcomes. This sea change has resulted in cybersecurity becoming a board-level skill, and an important success factor for any executive to have as part of their professional portfolio. It is becoming clearer every day that Board-CISO integration is not a temporary fad, rather an enduring enhancement to business strategy that will be necessary for success in the modern digital era.

Paige Adams
Group Chief Information Security Officer, Zurich Insurance Company Ltd

The Story Continues... Unrelenting Pressure on CISOs

The CISO's journey in recent years is one of progress. Since Proofpoint began producing *Voice of the CISO* in 2021, we've seen three encouraging trends:

- An increase in cybersecurity representation at the board level
- Closer alignment between CISOs and board members
- Growing acceptance of the need for human-centric security strategies

But progress is very rarely linear. And as any protector knows, with great power comes great responsibility. The added prominence and deference to CISOs around the world has brought more pressure, higher stakes and greater scrutiny to the role – at times, perhaps too much.

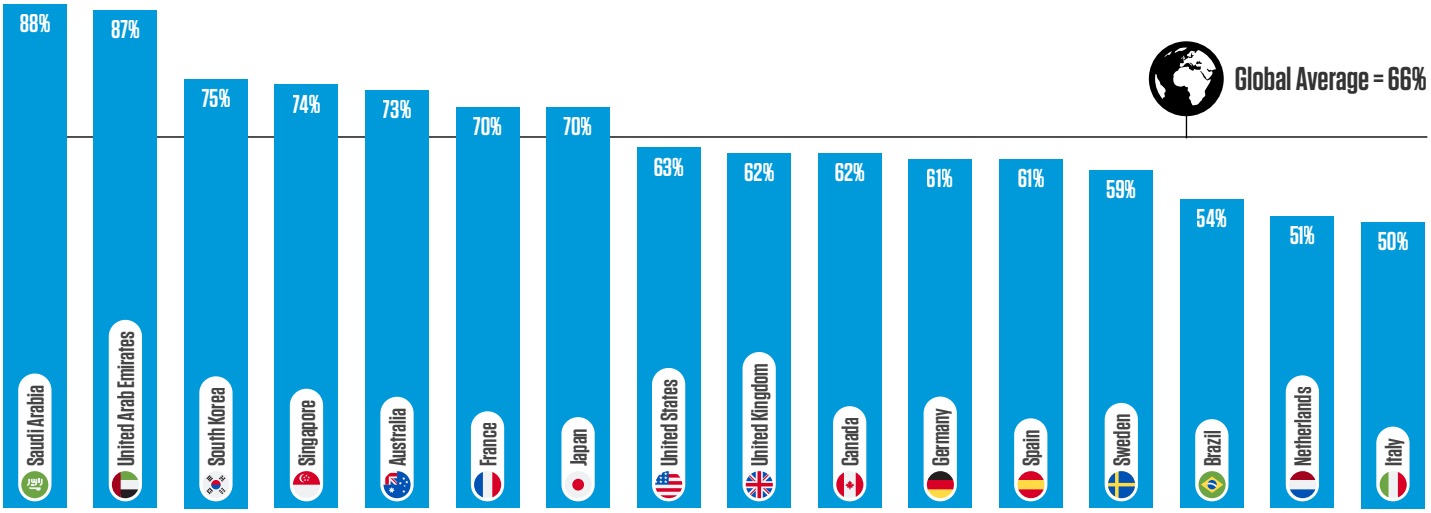
Two-thirds (**66%**) of CISOs surveyed for this year's report agree that expectations of the CISO/CSO are unrealistic.

66%

of CISOs believe there are excessive expectations on the CISO/CSO. This is a continued increase on previous years...

2023 = 61%
2022 = 49%
2021 = 21%

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



Worse, their concerns have gone unanswered. The feeling has risen – sometimes sharply – every single year of our survey.

The result of these excessive demands runs much further than overstretched resources and low job satisfaction. More than half (**53%**) of the world's CISOs have experienced or witnessed burnout in the past 12 months.

This finding is understandably concerning. But we are seeing some progress in this regard. Almost a third of CISOs (**31%**) say they haven't witnessed or faced burnout, up from just **15%** last year.

CISOs in South Korea (**72%**), Sweden (**63%**) and Australia (**62%**) are most likely to have experienced or witnessed burnout.

Personal liability remains a concern

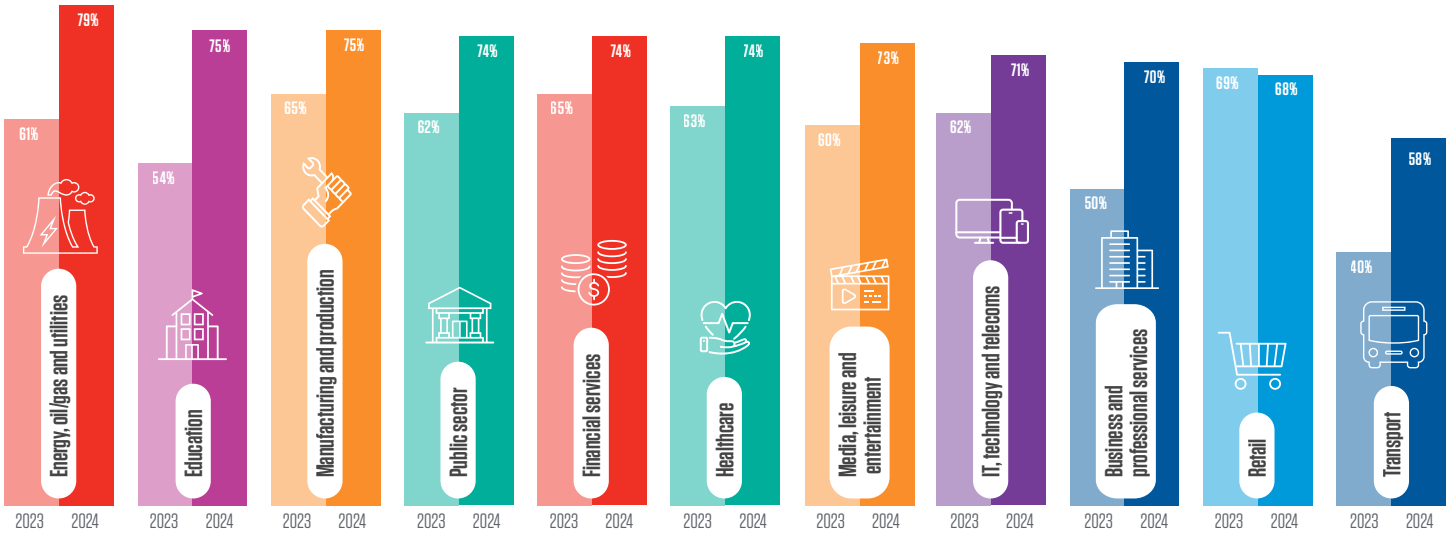
Several high-profile legal cases involving CISOs only add to the mounting pressure on the role. Most notably, the US Securities and Exchange Commission (SEC) brought landmark charges against a SolarWinds CISO last year for "fraud and internal control failures" in the lead-up to the company's 2020 supply chain attack.

With incidents like these top of mind, **66%** of global CISOs are concerned about personal, financial and legal liability in their role. That's up slightly from **62%** in 2023.

Fears over a lack of protection are causing some CISOs to think twice when making career decisions, too. This year's survey found that some **72%** would not join an organisation that doesn't offer directors & officers (D&O) insurance or similar coverage against financial liability in the event of a successful cyberattack.

Those in manufacturing and production (**75%**), financial services (**74%**), and retail (**68%**) feel most strongly about the issue.

Percentage of CISOs who agree that they would not join an organisation that does not offer directors and officers (D&O) insurance coverage (or similar personal liability insurance) to protect them from financial liability in the event of a successful cyber attack.



CISOs in Saudi Arabia (**47%**), Netherlands (**48%**), and Japan (**49%**) are least concerned about personal, financial and legal liability.

A majority of Brazil's (**85%**), Spain's (**81%**), and Germany's (**79%**) CISOs would not take a role without D&O or equivalent insurance.

CISOs in the Netherlands (**60%**), Sweden (**62%**), and Canada (**63%**) are least concerned about such cover.

Conclusion

Even after a tough year, CISOs are finding reasons to stay positive. More are concerned about a material cyber attack in the near future. But fewer feel unprepared, suggesting greater confidence in their efforts to prevent and defend against attacks.

Most also report closer relationships with key stakeholders and the boardroom. This change underscores the growing recognition of the role at the highest levels of the organisation and importance of cybersecurity.

Still, CISOs have plenty to keep them busy. Employee turnover remains a critical concern. Employee turnover has become the norm, with job leavers posing a sustained risk of data loss across all sectors. Spotting this trend, most CISOs have adopted DLP technology and invested in education.

In the meantime, the threat landscape will continue to evolve. Familiar foes like ransomware and BEC attacks remain a big cause for concern. And emerging technologies such as AI pose new challenges.

But ultimately, people and their behaviours continue to pose the greatest ongoing risk to organisations. Fortunately, many CISOs are investing more in human-centric security approaches in response. Despite its risks, AI also has the potential to help. Intelligent tools that can intervene to warn against or block risky behaviours in real time will be pivotal in the ongoing fight against human error.

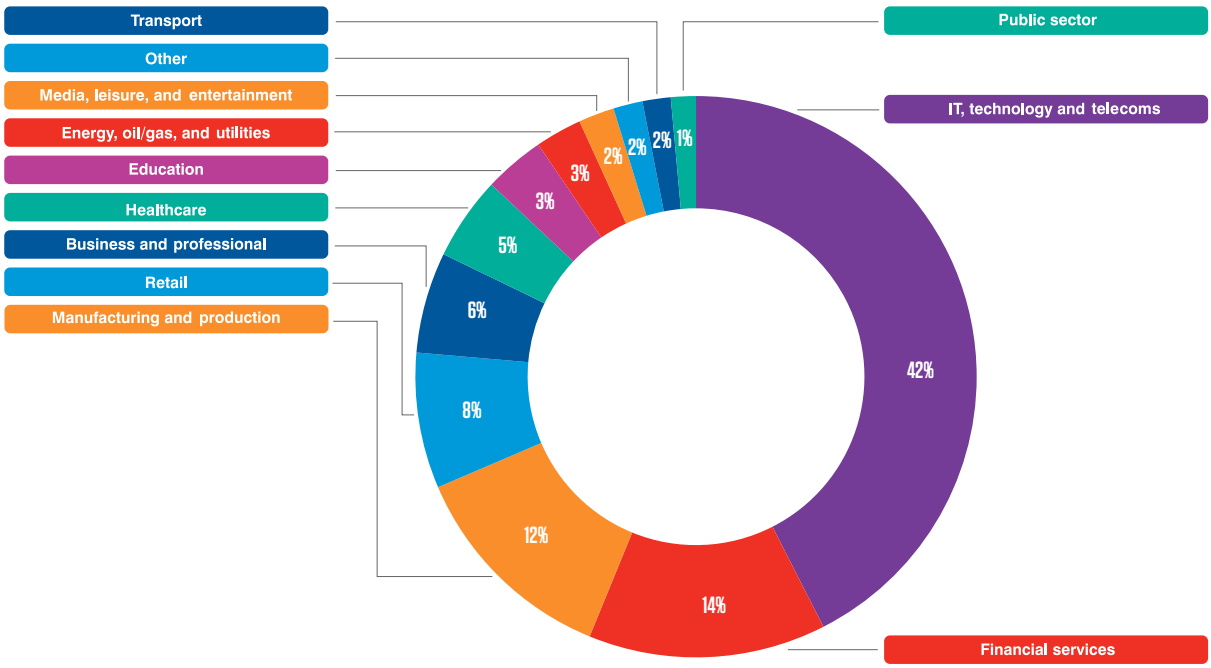
Another challenge to CISOs may well be the job itself. With growing concern around personal liability and increasing numbers reporting excessive expectations, burnout and challenging budgets, the pressure continues to mount. Solving this problem must be a top priority if we are to ensure modern CISOs are equipped for the scale of the task they continue to face now and into the future.

Methodology

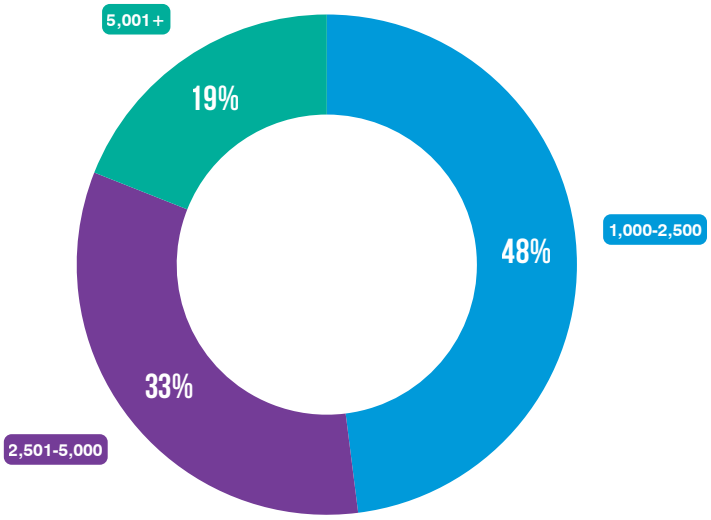
The Proofpoint 2024 Voice of the CISO survey, conducted by Research firm Censuswide between 20 January – 2 February 2024 surveyed 1,600 chief information security officers from organisations of 1,000 employees or more across different industries in 16 countries. One hundred CISOs were interviewed in each market, which includes the US, Canada, the UK, France, Germany, Italy, Spain, Sweden, the Netherlands, UAE, KSA, Australia, Japan, Singapore, South Korea, and Brazil.

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

Industry split among respondents:



Company size split among respondents:



proofpoint®

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

About Proofpoint, Inc.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' 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 organisations of all sizes, including 85 percent 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.

0400-015-02-01 05/24