



proofpoint.

REPORT

2023 Voice of the CISO

Global insights into CISO challenges,
expectations and priorities

proofpoint.com

Table of Contents

Introduction	3
Chapter 1: Back to "Business as Usual".....	4
Chapter 2: Protecting People—The Cybersecurity Cornerstone.....	7
Chapter 3: Defending Data	9
Chapter 4: Building a Defence to Fight on Every Front	12
Chapter 5: Boards and CISOs—Closer to the Same Page	15
Chapter 6: Life as a CISO—In the Crosshairs, Burned Out and Under the Microscope.....	18
Conclusion.....	21
Methodology.....	22

A Reality Check for CISOs



It's no overstatement to say that the past year was a busy one in the world of cybersecurity.

Ransomware continued to wreak havoc across the globe. New and increasingly devastating attacks upended organisations of every size, across every industry and in every jurisdiction. For example, a single ransomware attack contributed to the permanent closure of Lincoln College, a 157-year-old educational bastion in rural Illinois.¹ On the other end of the spectrum, a series of attacks paralysed the government of Costa Rica, forcing officials there to declare a national emergency.²

The supply chain also found itself firmly in the sights of cyber criminals. Attackers doubled down on compromising third party, cloud and privileged identities to infiltrate networks and exfiltrate data.³

Meanwhile, critical infrastructure hung in the balance amid a backdrop of unrelenting attacks and geopolitical unease. Russian attackers targeted US airports,⁴ and Chinese-aligned threat actors exploited telecoms' vulnerabilities.⁵

The prior year, with most pandemic disruption overcome, CISOs for a brief time appeared to feel a sense of calm, composure and confidence in their security posture. Astoundingly, that feeling has already vanished, replaced by elevated concern.

As we look to 2023 and beyond, we can expect a return to a harsher reality. Ransomware looks set to wreak more disruption as data extortion becomes the rule rather than the exception. At the same time, increasing commercialisation of dark-web exploit tools, initial-access brokers and "as-a-service" attack infrastructures threaten to make cyber crime even more open to anyone with a few dollars and ill intent.

Amid growing concerns around cyber risk and organisational preparedness, navigating this threat landscape remains a matter of protecting people and defending data. Modern CISOs know that users are at the centre of cybersecurity. And they understand how critical it is to safeguard their organisation's sensitive information, especially in light of an uncertain economy and employee churn.

To gain deeper insight into the mind of the CISO during this pivotal time, Proofpoint surveyed 1,600 of them from around the world. They graciously shared their experiences over the last year and their outlook for the years ahead.

In this summary of our findings, we explore how the global recession is applying pressure to security budgets and how CISOs must remain steadfast in pressing the C-suite for critical controls to protect their organisations. We also learn how boards are increasingly becoming part of the cybersecurity conversation and the impact this is having on their understanding of security issues and their relationships with CISOs. Finally, we unpack the issue of burnout among CISOs as many struggle with the pressures of personal liability and excessive expectations.

Once again, 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 your feedback.

Lucia Milică Stacy, Global Resident CISO at Proofpoint

¹ Kris Hold ([Engadget](#)). "A US college is shutting down for good following a ransomware attack." May 2022.

² Kevin Collier ([NBC News](#)). "Costa Rica declares state of emergency over ransomware attack." May 2022.

³ Zack Whittaker ([TechCrunch](#)). "Okta says hundreds of companies impacted by security breach." March 2022.

⁴ Alyssa Blakemore ([Daily Caller](#)). "Russian Hackers Take On Major US Airports In Cyberattacks: REPORT." October 2022.

⁵ [CISA](#). "People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices." June 2022.

Chapter 1: Back to "Business as Usual"

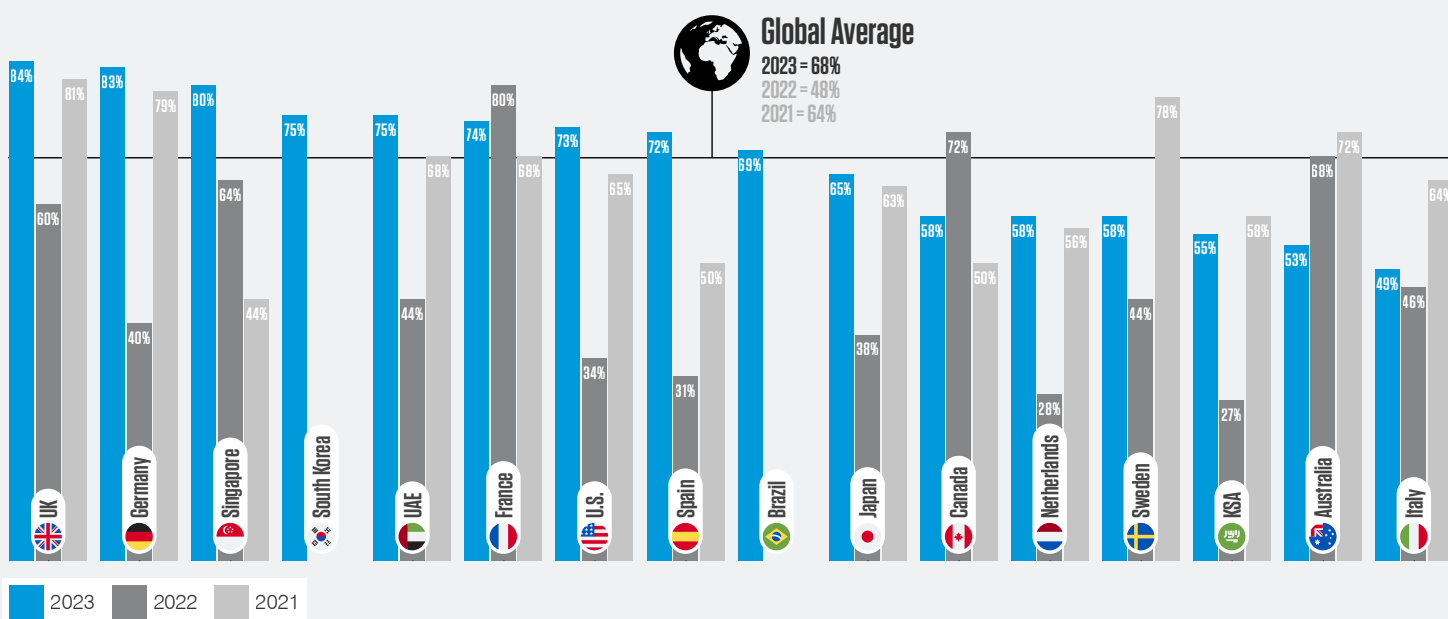
Last year's report uncovered a palpable feeling among CISOs that there was a period of calm after a once-in-a-generation crisis. With the pandemic disruption finally subsiding and hybrid work setups a mainstay for most, CISOs felt comfortable that the worst was behind them. At the time, just **48%** believed that a cyber attack was on the horizon within the coming year.

That's changing. In this year's survey, over two-thirds (**68%**) of CISOs said they feel at risk of a material cyber attack in the next 12 months. This pronounced shift suggests that security professionals see the threat landscape heating up once again, and have recalibrated their level of concern to match.

68%

of CISOs feel their organisation is at risk of experiencing a material cyber attack in the next 12 months, with 25% rating 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 the UK (**84%**), Germany (**83%**) and Singapore (**80%**) are most concerned about experiencing a material cyber attack.



Italy's CISOs are the most optimistic, with just **49%** fearing an attack.



CISOs (**68%**) and board members (**65%**) both feel that a material cyber attack is likely in the next 12 months.



Retail (**77%**), manufacturing (**76%**) and finance (**71%**) lead the way for cyber attack concerns across industry verticals.

Awareness vs Preparedness

Increased awareness among CISOs of the danger of a potential cyber attack can be viewed as a positive. But we found a concerning disconnect between the perceived likelihood of such an event and how prepared organisations are to deal with one.

Nearly two-thirds (**61%**) agree that their organisation is unprepared to cope with a targeted cyber attack. Once again, this is above 2022's figure of **50%** and more in line with 2021's finding of **66%**. This is further evidence that CISOs are returning to the "new normal"—though it's a normal that offers little comfort.

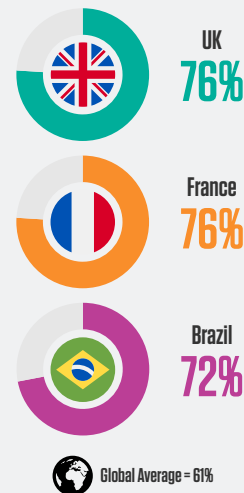
61%

of CISOs agreed that their organisation is unprepared to cope with a targeted cyber attack in 2023.

For their part, board members are much more confident in their organisation's ability to deter cyber threats. In our survey of board members last year, just **47%** believed they were unprepared for such an eventuality.⁶ But with CISOs having a better read of security posture and understanding of the threat landscape, this board-level optimism is likely based on an incomplete picture of the current situation.

Percentage of CISOs who agree that their organisation is unprepared to cope with a targeted cyber attack in 2023

Top 3 Countries



A CISO's eye view of the threat landscape

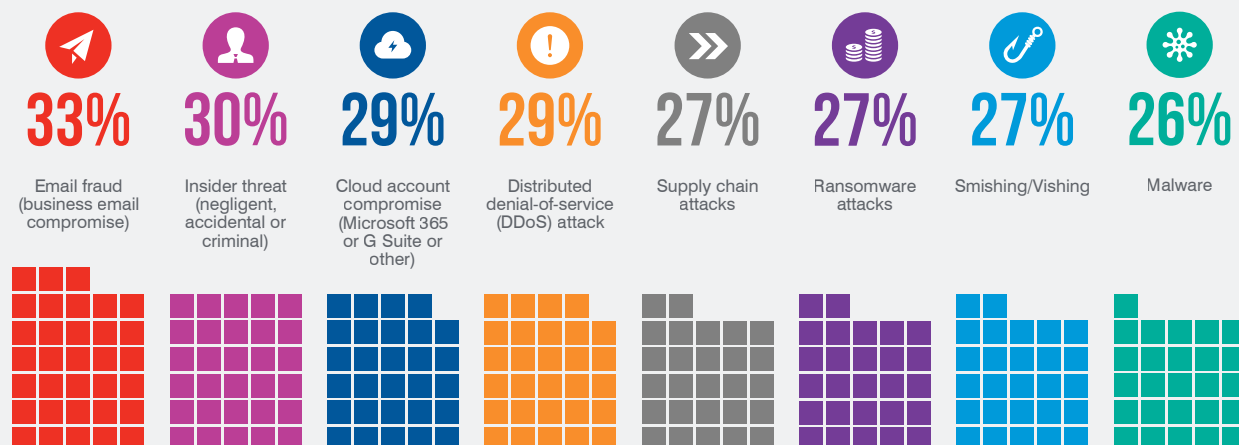
When it comes to the kinds of threats occupying the minds of the world's CISOs, four major categories lead the way:

- Email fraud (**33%**)
- Insider threats (**30%**)
- Cloud account compromise (**29%**)
- DDoS attacks (**29%**)

This list is almost unchanged from the previous year (though email fraud and insider threats swapped places in the top two spots.) CISOs are right to remain concerned about these threats. Their continued prominence as a top priority reflects the challenge they continue to pose.

On a more positive note, CISO concerns seem to be filtering through to the rest of the C-suite; board members agree that email fraud poses the most pressing threat.

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.)



6 Board member statistics from "Cybersecurity: The 2022 Board Perspective Report."



Email fraud is the top concern among CISOs in Japan (45%), UAE (45%), France (35%) the UK (34%) and Germany (31%).



Insider threats lead the way in Spain (38%), Singapore (35%) and Canada (32%).



Among industries, business and professional (39%), public sector (38%), retail (35%) and IT, technology and telecoms (33%) all agree that email fraud will be the biggest threat over the next 12 months.

“

Organisations are finally back to 'business as usual' following years of coping with the pandemic and its aftermath. CISOs fully understand how critical their supply chains are and the significant impact of cyber-attacks and ransomware on those supply chains. There is a need for a continuous and constantly evolving partnership between companies and their suppliers on the topic of cybersecurity that results in stronger requirements and cyber controls. Working collaboratively across sectors to raise the level of security yields benefits for all and creates greater deterrence for the adversaries.



**Deborah Wheeler, SVP & CISO,
Delta Air Lines**

”

Chapter 2: Protecting People—The Cybersecurity Cornerstone

Just as CISOs remain largely unchanged in their view of the threat landscape, they also hold their organisation's employees in a similar light to previous years.

Almost two-thirds (**60%**) consider human error to be their organisation's biggest cyber vulnerability. This is consistent with our findings in 2022 and 2021. In those studies, **56%** and **58%**, respectively, agreed with the statement.

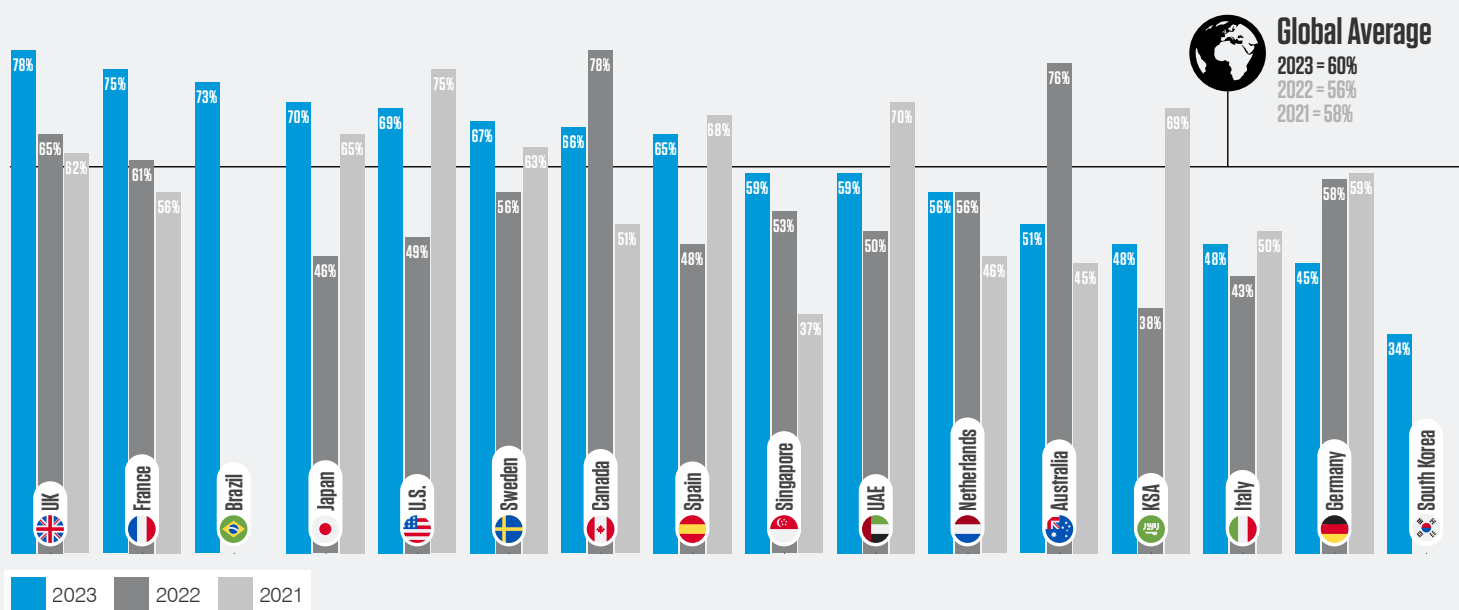
An even higher percentage of board directors (**67%**) shared this view. The finding suggests that the C-suite now, if belatedly, recognises the threat that CISOs have witnessed firsthand. This newfound awareness can only be good news.

Still, CISOs have expressed similar concerns about human vulnerability for several years now. Clearly, improving confidence in workers' cybersecurity savviness remains a challenge.

60%

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.



Even more CISOs (**63%**) agree that human risk more broadly—including malicious and negligent employees—is a key cybersecurity concern in the next two years. This is most keenly felt in the UK, where **78%** of CISOs agree, followed by:

- Japan (**75%**)
- Brazil (**72%**)
- Singapore (**72%**)
- US (**68%**)
- Spain (**68%**)

The people problem

It is hardly surprising that people risk remains such a prominent concern among CISOs when just **61%** believe that employees understand their role in protecting their employer. This leaves **2 in 5** CISOs ill at ease about whether their users are equipped to detect and deter cyber threats.

Once again, this number is consistent with previous findings (**60%** in 2022 and **58%** in 2021). The trend suggests little progress in building a culture of security awareness.

Countries with the highest percentage of CISOs who agree that “employees understand their role in protecting their organisation against cyber threats,” include:

- France (**79%**)
- Japan (**75%**)
- UK (**75%**)
- Spain (**73%**)

In our earlier survey, board members reported a greater level of confidence. More than **75%** agreed that employees understand their role—a concerning disconnect about the perceived security posture of their people.

This is likely because board directors can be sheltered from employees’ day-to-day actions, in many cases interacting only with higher-ranking, well-informed and top-performing workers. By contrast, the CISO rightly has a closer ear to the ground—and a more realistic grasp of cybersecurity awareness and abilities throughout the organisation.

61%

of CISOs believe that their employees understand their role in protecting their organisation against cyber threats, with 25% strongly agreeing.



CISOs in France (**79%**) have the most confidence that employees understand their role in protecting their organisations.



The belief that people are the biggest security vulnerability decreases as company size increases: **61%** in those with 200-499 employees and **47%** in those with 5,000+.



CISOs in retail (**76%**), transport (**67%**), IT, technology and telecoms (**67%**) and finance (**67%**) are most concerned about people risk over the next two years.

“

Research consistently finds that human error is one of the key contributors to successful cyber attacks. As long as this vulnerability remains, CISOs will struggle to protect their data and systems. Although human error is inevitable, having guardrails, as well as strong policies and procedures in place, can go a long way in mitigating this risk and hardening your people perimeter.



Paige H. Adams, Global Chief Information Security Officer, Zurich Insurance

”

Chapter 3: Defending Data

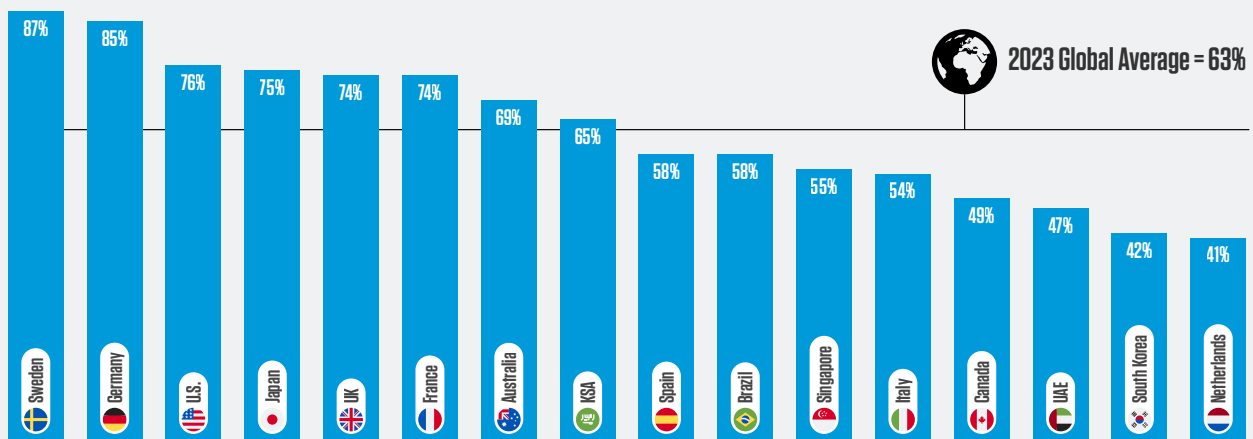
Protect people, defend data: these are the keys tenets of any effective cybersecurity strategy. But unfortunately, organisations appear to struggle with both.

Almost two-thirds—**63%**—of global CISOs say they have had to deal with the loss of sensitive information in the past year. Bearing the brunt of data loss incidents are organisations in energy (**71%**), business and professional services (**68%**) and retail (**68%**).

63%

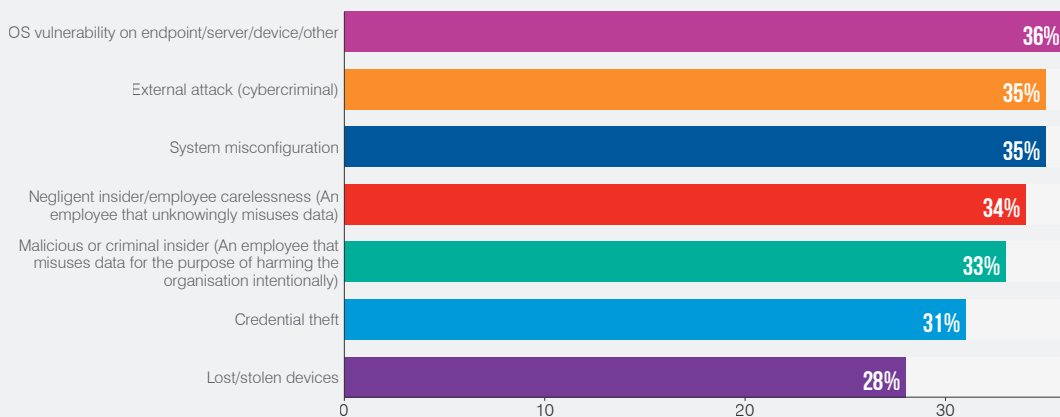
of global CISOs say their organisation has dealt with a material loss of sensitive information in the past 12 months.

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



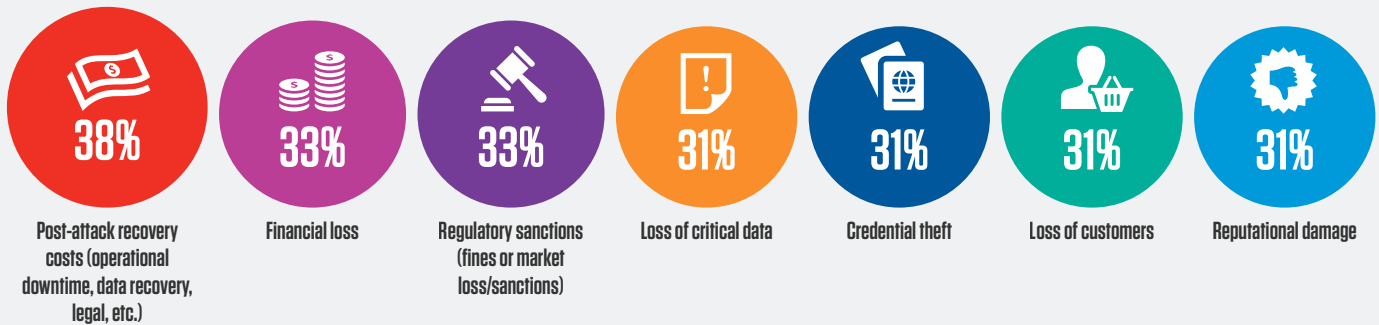
For most, data loss came about as a result of an operating system (OS) vulnerability on endpoint, server or device (**36%**), an external attack (**35%**), system misconfiguration (**35%**) or negligent insider (**34%**).

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)



And the consequences of data loss are as far reaching as the causes. Most CISOs report post-attack recovery costs such as operational downtime and data recovery (38%), financial loss (33%) and regulatory sanctions (33%).

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



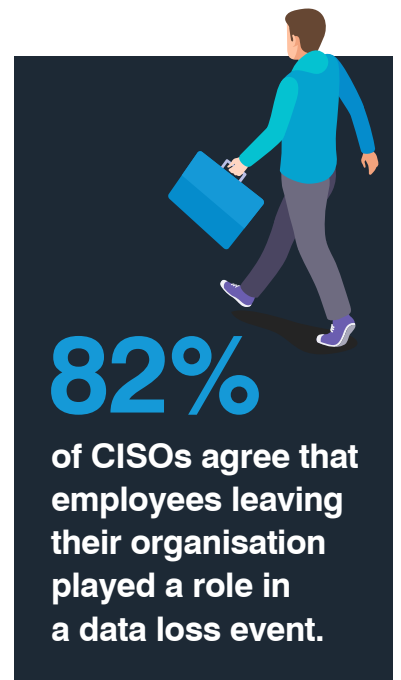
Spotlight on malicious insiders

Although insider negligence edged out malicious and compromised users as the leading cause of data loss events last year, CISOs expect a reversal in the year ahead. Malicious (43%) and compromised (40%) insiders are deemed more likely to cause a data breach or exposure in the next 12 months. The finding suggests that CISOs increasingly believe that more employees are exposing data on purpose. The continuing impact of the Great Resignation—and more recently, mass layoffs—undoubtedly loom large in this assertion.

Many industries saw a significant increase in post-pandemic staff turnover. Some 82% of CISOs report that employees leaving their organisation has contributed to a data loss event. The two sectors affected the most were retail (90%) and IT, technology and telecoms (88%).

These trends leave security teams with a near-impossible challenge. When people leave, stopping them from taking data is difficult.

Some organisations require written guarantees from former employees that they will delete all company data. Others threaten the new employer of potential liability if the employee shares any data from the old job. But neither is close to being a satisfactory solution.



Organisations typically deploy a variety of security solutions and mitigating controls to protect against the loss of sensitive data, but they often overlook one factor—employees who leave for greener pastures often take the data with them. CISOs can't solve this problem with technical controls alone, and this is where a strong security culture comes in. Educating employees, setting the expectations, garnering senior business leadership support—and then adding procedures and controls around it—can mitigate and eliminate some of the most common data leak problems.



Patrick Joyce, VP, Chief Global Security Officer (CISO & CSO), Medtronic



Dealing with data loss

Against a backdrop of constant data loss across industries and countries, **60%** of CISOs still contend that they have adequate data protections in place.

Board members are even more confident, with **75%** believing this to be the case. However, this may be due to CISOs sharing with them a well-presented picture of events rather than the unfiltered reality.

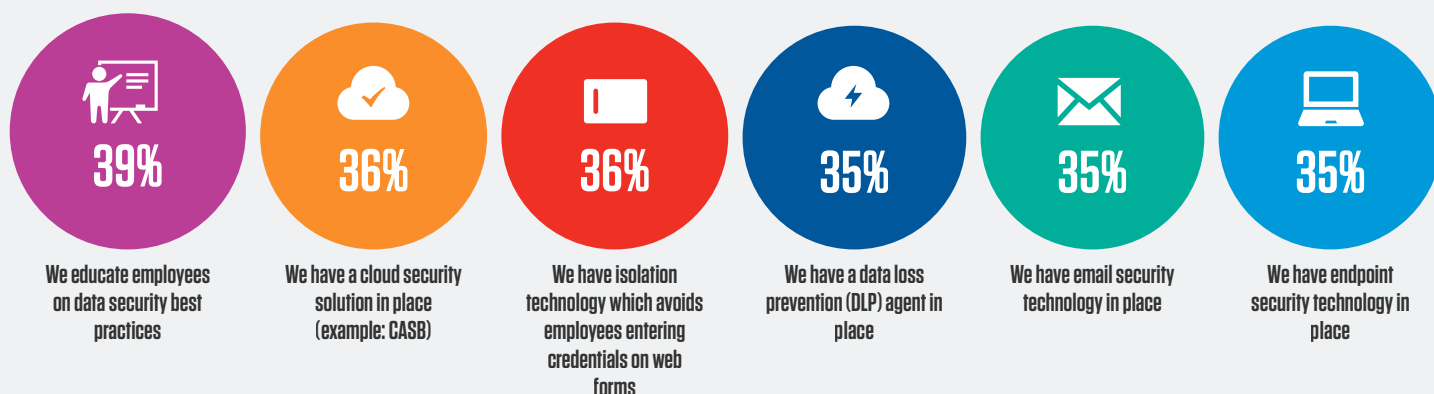
Despite confidence in their current abilities, information protection and data governance remain a top priority going forward for **61%** of the world's CISOs. That's a slight increase from **59%** last year.

Once again, board members feel more strongly, with **75%** in agreement. Again, this is likely because of their limited view—board members focus on top-line concerns rather than the numerous security issues CISOs deal with throughout the year.

When it comes to the tools and protocols making up cyber defence, most CISOs report a broad and varied arsenal.

60%
of CISOs agree
that the data within
their organisation is
adequately protected.

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



With people a major contributor to data loss, it is heartening to see that user education leads the way as a defence. But as effective as awareness training can be, it does little to combat malicious or compromised insiders.



87% of organisations in Sweden dealt with material data loss in the last year—the highest rate of any country surveyed.



Insider negligence is the leading cause of data loss in Brazil (**54%**), Japan (**48%**) and Singapore (**40%**).



Loss of critical data (**36%**) and reputational damage (**36%**) are the biggest consequences of data loss for large organisations (5,000+ employees).



Smaller organisations (200-499 employees) are most impacted by post-attack recovery costs (**46%**).

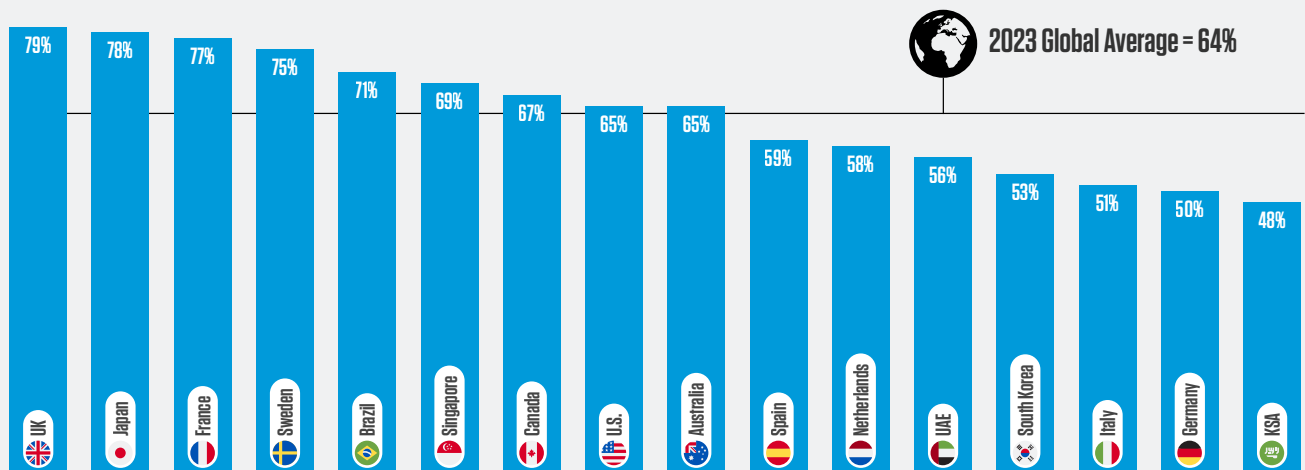
Chapter 4: Building a Defence to Fight on Every Front

Today's CISOs face a fight on multiple fronts. They must combat external threats such as ransomware and supply chain risk to malicious, negligent and compromised insiders. For the most part, CISOs feel they have adequate resources to wage such a war. But many remain woefully overexposed.

As supply chains grow larger and more complex, protecting these increasingly opaque networks is more difficult than ever.

In spite of this, most CISOs say they have the issue under control. Some **64%** believe they have appropriate controls in place to mitigate supply chain risk. This represents a modest increase from 2022 (**59%**), demonstrating that the issue remains a top priority.

Percentage of CISOs who agree their organisation has appropriate controls in place to mitigate supply chain risk.



When it comes to more direct attacks on their organisation, CISOs are increasingly prepared to rely on insurers to limit the damage. Almost two-thirds (**61%**) said they would place a claim on cyber insurance policies to recover losses incurred. Retail (**75%**) and IT, technology and telecoms (**65%**) are most likely to mitigate financial losses in this way.

The World Economic Forum reports that **71%** of organisations have cyber insurance in place,⁷ so this finding is no surprise. But relying on such policies alone is growing more complicated.

For one, a recent increase in claims has led many insurers to raise premiums; some are withdrawing coverage for common threats like ransomware altogether.⁸ What's more, while insurance can offer some financial compensation in the event of a data breach, it does little to rebuild customer trust or company reputation.

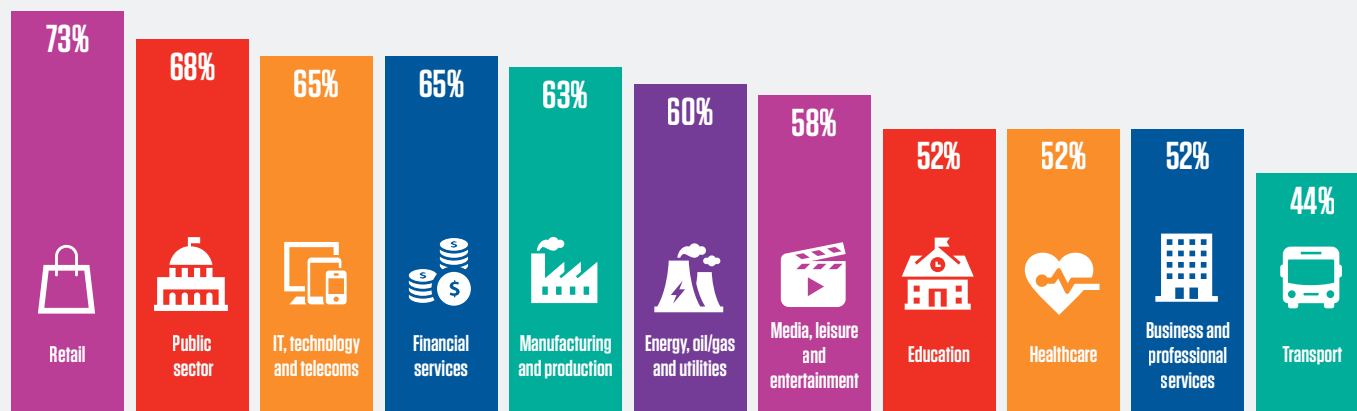
This, along with an increase in more sophisticated and devastating ransomware attacks, may be why CISOs are increasingly open to paying ransoms to cyber criminals.

Just **14%** disagree that their organisation is likely to pay a ransom to restore systems or prevent the release of data in the next 12 months; **62%** say the opposite.

⁷ [World Economic Forum](#). "Global Cybersecurity Outlook 2022." January 2022.

⁸ [Euronews](#). "Cybercrime: Insurance giant Axa to stop covering ransomware payments in France." July 2021.

Percentage of CISOs by industry who agree that if impacted by ransomware within the next 12 months, their organisation is likely to pay a ransom to restore systems/prevent the release of data.



Most CISOs (**62%**) are confident that their organisation can detect and remove a threat actor using stolen or compromised credentials before any material damage occurs. Just **14%** disagree.

This confidence is likely misplaced. While most organisations may have adequate endpoint detection and response technology, such tools will not alert on compromised credentials.

Spotlight on budgets and priorities

With a look to the future, CISOs' priorities for the next two years are largely unchanged from last year's report. The desire to innovate (**39%**), consolidate (**37%**) and outsource (**35%**) aspects of cybersecurity remain strong. The numbers underline a commitment to these transformational long-term projects.

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



But a global economic downturn could make it more challenging for many organisations to achieve these aims. Over half (**58%**) of CISOs agree that recent economic events have hit their cybersecurity budget. The two sectors most affected are the public sector and IT, technology and telecoms (**65%** of CISOs in both reporting budget cuts).

No one can control global market forces. Still, organisations must not make rash budgetary decisions when concerns about cybersecurity preparedness are on the rise. CISOs must have a seat at the table when boards set spending priorities.

58%

of global CISOs say the current economic downturn has negatively impacted their organisation's cybersecurity budget.



CISOs in retail (**76%**) are most confident that their organisation has appropriate controls in place to mitigate supply chain risk.



CISOs in the UK (**79%**), France (**73%**) and Sweden (**73%**) are most likely to rely on cyber insurance to cover losses.



Ransoms are most likely to be paid by CISOs in the UK (**75%**), Japan (**73%**) and Brazil (**73%**).



UK (**73%**), Brazil (**73%**) and US (**67%**) CISOs believe their budgets have been most negatively impacted by the economic downturn.



CISOs in retail (**69%**), public sector (**65%**) and IT, technology and telecoms (**65%**) are the industries most impacted by the economic downturn.



It is imperative to have alignment with leadership on the need to provide resources that maintain a robust cybersecurity programme, even when dealing with a difficult business climate. Our adversaries do not stop in an economic downturn—on the contrary, they step up their efforts knowing that organisations may put fewer resources into their defences. Maintaining solid cybersecurity protections is always paramount because the threat landscape will only continue to expand.



Juan Gomez-Sanchez, Global Chief Information Security Officer, Whirlpool Corporation



Chapter 5: Boards and CISOs—Closer to the Same Page

The issue of CISO and board member alignment is not new. But as the CISO role takes on greater influence, board-level interactions are more frequent—and relations appear to be improving as a result.

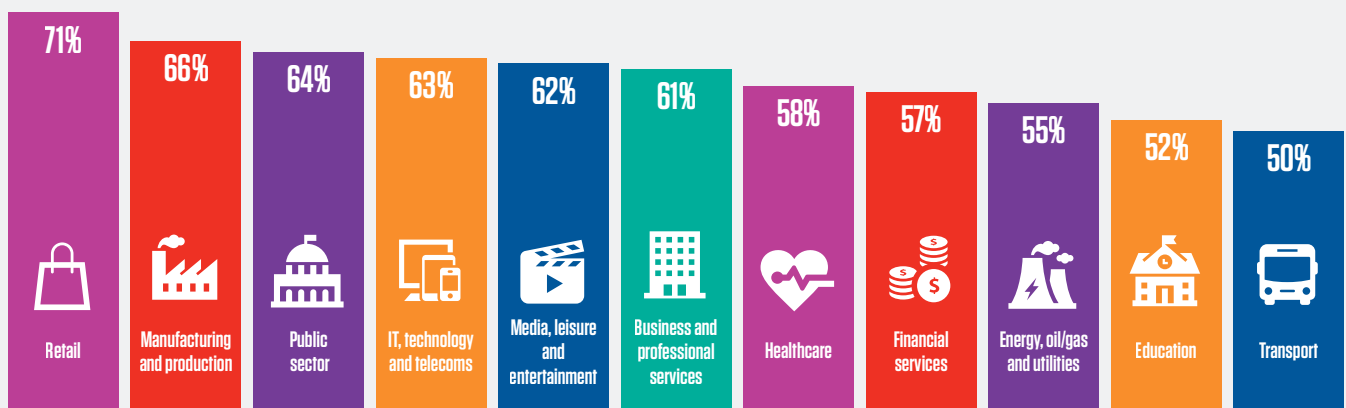
A little under two-thirds (**62%**) of CISOs agree that their board sees eye to eye with them on cybersecurity issues. That's up from **59%** in 2021 and **51%** in 2022. For their part, board members are even more positive about the relationship, with **69%** feeling the same way.

As CISOs feel more at risk of a cyber attack and less prepared to cope with the consequences, they are beginning to feel more in tune with their boards—an encouraging sign. Both, no doubt, hope this trend can continue. And perhaps the slight drop in perceived positive relations in 2022 was little more than late-pandemic stress and strain.

62%

of CISOs say their board sees eye-to-eye with them on the issue of cybersecurity.

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



Even though relations are burgeoning, a slight disconnect remains around the consequences of a cyber attack. Based on their interactions, CISOs believe their boards' greatest concerns to be:


















- Reputational damage (**36%**)
- Impact on business valuation (**36%**)
- Loss of current customers (**36%**)



While all of these concerns are valid, they are slightly out of step with the top real-world impacts of data loss:

- Operational downtime and data recovery (**38%**)
- Financial loss (**33%**)
- Regulatory sanctions (**33%**)

That said, many of the concerns held by CISOs and board members are interlinked. Operational downtime leads to reputational damage, impact on business valuation and loss of customers.

Given your interactions 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.)

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

 Main Concern  Second/Third Concerns

Room for improvement

Good feelings between CISOs and board members remains high, but it is still not quite a perfect marriage. Some **62%** of CISOs believe cybersecurity expertise should be a board-level requirement, suggesting that many believe technical knowledge is lacking in the boardroom.

CISOs in retail (**73%**), IT, technology and telecoms (**69%**) and education (**67%**) believe in this view most strongly, while healthcare (**50%**) and transport (**44%**) are least likely to agree.

In the US, **70%** of CISOs share this view. Perhaps not surprisingly, the Securities and Exchange Commission (SEC) has proposed requiring publicly traded companies to disclose whether any of their board directors have cybersecurity experience.

62%

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

“

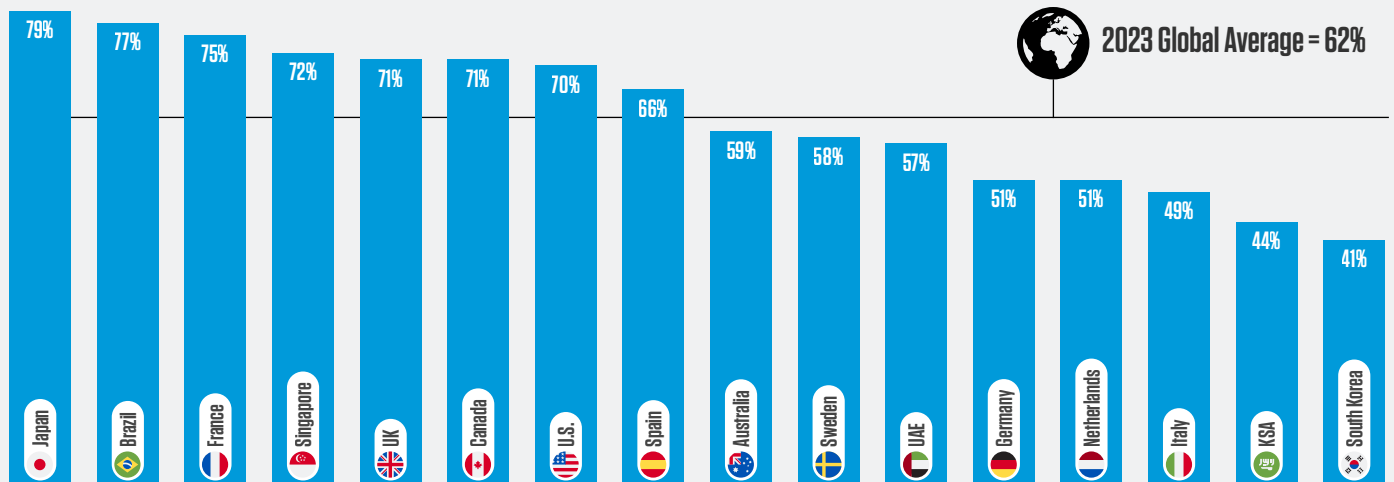
As regulatory scrutiny increases, board members are recognising the crucial role played by their Chief Information Security Officer (CISO) in managing the mounting demands of cyber governance and oversight. By forging closer partnerships and aligning with their security experts, boards can effectively implement and oversee strategies that enhance their organisation's cybersecurity and fortitude, positioning them to overcome emerging threats, challenges and ensuring shareholder value.

”



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

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



Whether such a rule will close the knowledge gap between CISOs and other board members remains to be seen. But many security professionals around the world will be keeping a close eye on it. An increased cybersecurity capability in the boardroom benefits all. And if existing board members can't fulfil this role, that might mean greater career prospects for security professionals who can.



CISOs in Brazil (80%), Japan (80%) and the UK (74%) are most likely to agree that their board sees eye to eye with them.



CISOs in South Korea (45%), KSA (45%) and Germany (39%) are least likely to agree that their board sees eye to eye with them.



CISOs in transport (42%) and media, leisure and entertainment (41%) feel significant downtime is the primary concern of their boards.

Chapter 6: Life as a CISO—In the Crosshairs, Burned Out and Under the Microscope

Cybersecurity's role in helping to navigate the pandemic has undoubtedly brought with it some positives. CISOs now have more of a voice in the boardroom. And more than ever, they have been able to demonstrate the importance of effective security in driving business strategy.

But it's not all good news. Having enabled home and hybrid working suddenly and at scale in a time of crisis, many feel that the continued pressure on the role is unsustainable.

Almost two-thirds, **61%**, of CISOs agree that they face excessive expectations. That's up from **49%** in 2022 and **57%** in 2021. A return to business as usual could be behind this growing concern. With the panic to secure home and hybrid setups behind them, many organisations are now tightening cybersecurity budgets. The shift leaves CISOs with the same objectives but fewer resources to achieve them.

Across industries, those in retail (**69%**) and IT, technology and telecoms (**69%**) feel the heaviest expectations. Transport (**48%**) and healthcare (**42%**) CISOs feel the least pressure. The divergence suggests that the burden of security is spread more widely throughout safety-critical industries.

61%

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

“

CISOs have always had a stressful job, but the additional pressures—like board expectations to deliver risk reduction faster and challenges in influencing middle management on delivering it, budget challenges and shortages of skilled talent—are creating an untenable situation for many. That's why more CISOs are changing roles or leaving the cybersecurity field altogether. Finding a better balance may sound impossible, given the 24/7 nature of the role, but it's absolutely necessary for maintaining resilience in the face of burnout.



**Celeste Lowe, Group Director,
IT Security, Nine**

”

The burden of personal liability

Another significant contributor to the pressure felt by the world's CISOs is the ever-present possibility of personal liability—**62%** expressed concern about the subject. Just **15%** said it was not a worry in their current role.

The increased responsibility of the CISO has brought increased scrutiny from regulators. The failure of Uber's former CISO to report a data breach resulted in a felony conviction. CISOs are well aware of what this verdict and others like it could mean for them, and they are seeking reassurance.

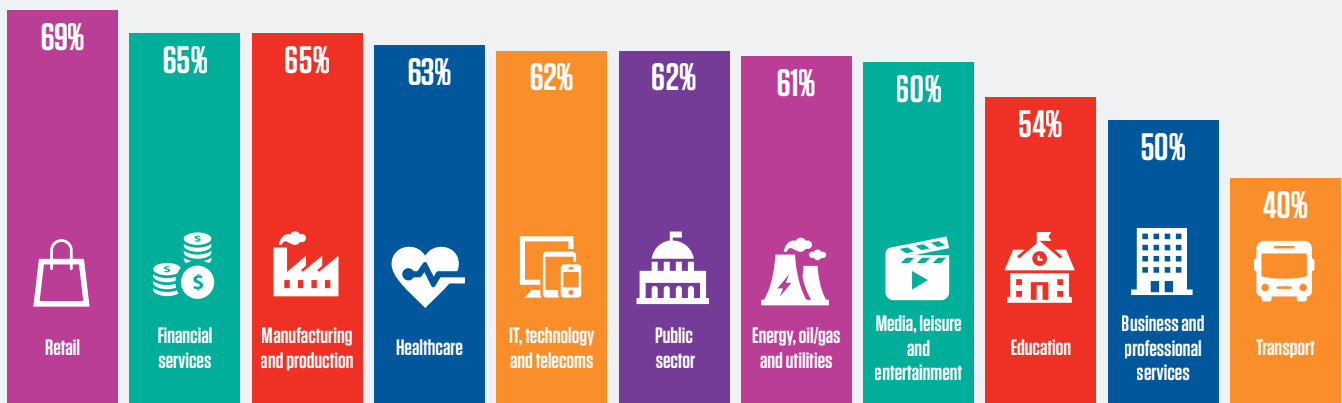
Most CISOs (**61%**) say they would not join an organisation that does not offer directors and officers (D&O) insurance or something similar to protect them from financial liability stemming from a successful cyber attack. Just **14%** disagree.

Understandably, CISOs in industries with high volumes of sensitive data or heavy regulation such as retail (**69%**), financial services (**65%**) and manufacturing (65%) are most likely to demand insurance coverage.

62%

of CISOs are concerned about personal liability in their role.

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 retail (**72%**) and IT, technology and telecoms (**68%**) are most concerned about personal liability.



CISOs are most likely to experience burnout in the retail (**72%**) and IT, technology and telecoms (**66%**) industries.

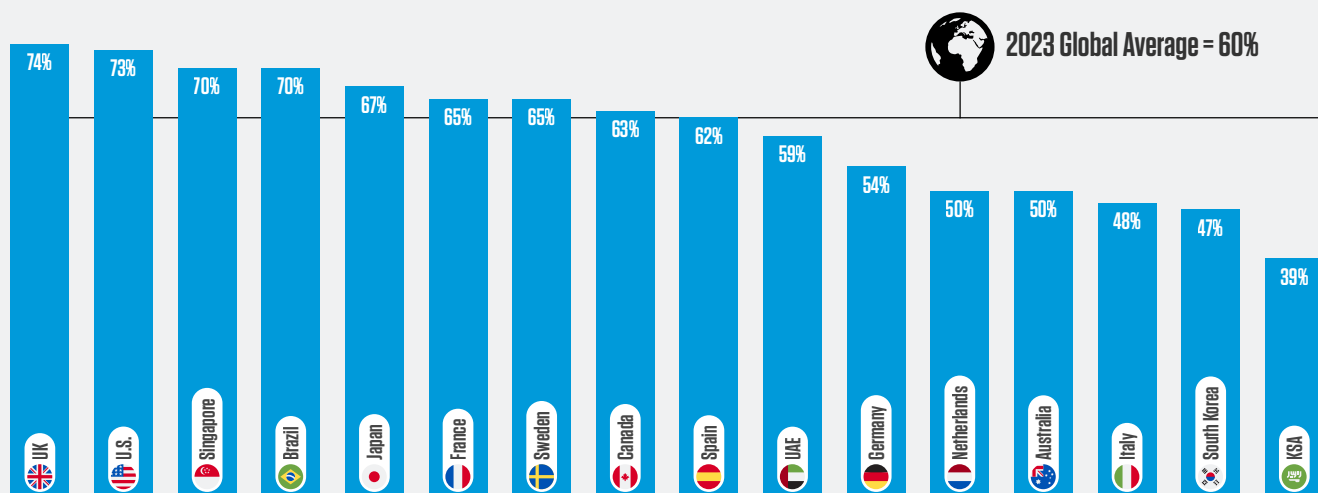


CISOs in France (**75%**), Japan (**75%**) and UK (**74%**) are most likely to agree that they face excessive expectations.



Those in Italy (**51%**), Saudi Arabia (**51%**) and South Korea (**36%**) are least likely to agree that they face excessive expectations.

Percentage of CISOs who agree that they have experienced burnout within the past 12 months



Unfortunately, the result of increased pressure, scrutiny and personal liability is all too inevitable. High-stress environments, shrinking budgets and mounting expectations are hurting global CISOs' quality of life. A full **60%** say they have experienced burnout in the past 12 months. Just **15%** disagree.

At the end of another blockbuster year for cybersecurity professionals, this is a critical finding. Once again, it underscores the need to stay grounded, both professionally and personally.

The scale of the issue can't be overstated. Forrester recently predicted that a Global 500 firm will be exposed for unsafe working conditions of its cybersecurity employees in 2023.⁹

The onus is on cybersecurity leaders to ensure that this does not happen on their watch. But this is possible only when CISOs are given the space to express concerns and the time to recharge and build resilience.

60%

of CISOs agree that they have experienced burnout within the past 12 months.

⁹ [Forrester](#). "Predictions 2023: Cybersecurity, Risk, And Privacy." October 2022.

Conclusion

After the chaos and disruption of the first pandemic year, CISOs found themselves in a period of transition. Confidence in remote setups and understanding of the post-pandemic threat landscape grew. So did belief in their ability to protect their organisations in this “new normal.”

But for CISOs, there’s no longer anything new about what has become a normal way of working. With the initial scramble behind them and two more years of remote work under their belts, it is back to reality. And with that comes a familiar state of elevated concern.

CISOs are under no illusions about the risks posed by their people. But some are misplacing their confidence when it comes to protecting data. Insider threats are a growing problem. And as staff turnover shows no signs of slowing across many industries, it is likely to be an issue for some time.

On top of this, security budgets are feeling the pinch of the economic downturn. Existing controls may be enough to mitigate supply chain risk, detect and remove threat actors, and cover potential losses from ransomware. But how long they will remain so is impossible to guess.

This return to a harsh reality culminates in CISOs feeling the strain. It’s no wonder that most are feeling the pressure of rising expectations, personal liability and burnout.

But signs of hope remain. That CISOs are voicing these concerns is a huge step in the right direction. And with most feeling more aligned with board members, they have a solid foundation upon which to build and deliver change.

The question is, with shrinking budgets and long-term talent shortages, will CISOs have the resources they need to do so?

“

CISOs are no strangers to challenges such as tight budgets, people-driven risks and a growing threat landscape—most have been there before. But the positive shift we are seeing in board-CISO relationships means security leaders now have new allies in their corner. Together, boards and CISOs have a solid opportunity to bolster their risk-based cybersecurity strategies and drive meaningful changes. CISOs and their board allies may find it necessary to lend their support and provide sponsorship for business segments which may be struggling to find the capacity and prioritisation necessary to implement these changes. In the dynamic cybersecurity environment, new challenges will always arise, and it is much easier to solve them when the two sides are working together in tandem toward a common goal.



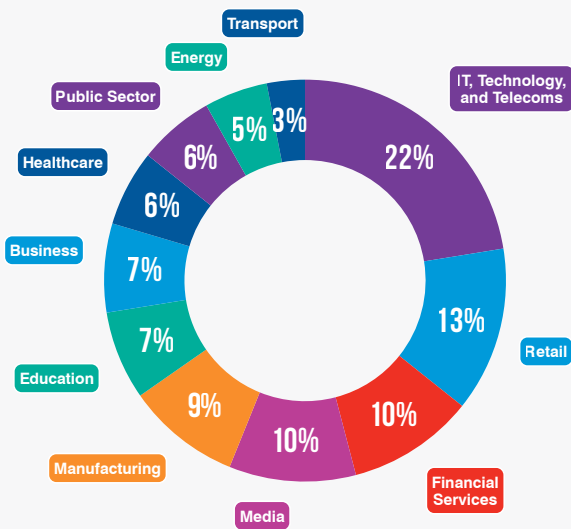
**David McLeod, VP, Information Security Officer,
The Walt Disney Studios**

”

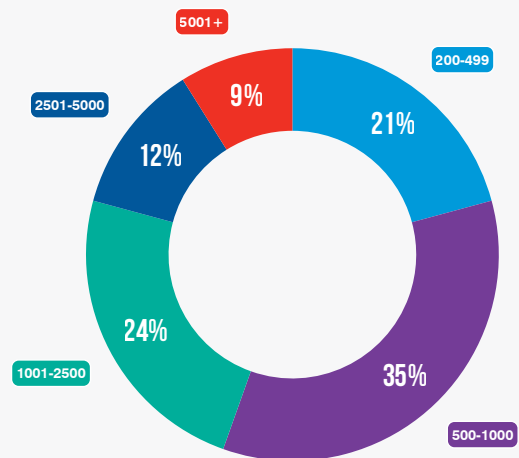
Methodology

The Proofpoint 2023 Voice of the CISO survey, conducted by research firm Censuswide between 30 January and 7 February, 2023, surveyed 1,600 chief information security officers from organisations of 200 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.

Industry split among respondents:



Company size split among respondents:



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



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

ABOUT PROOFPOINT

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 75 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.

