proofpoint.

REPORT

2022 Voice of the CISO

Global Insights Into CISO Challenges, Expectations and Priorities

proofpoint.com

Table of Contents

The Year Cybersecurity Went Prime Time

As high-profile attacks disrupted supply chains, made headlines and prompted new cybersecurity legislation, 2021 proved to be another challenging time for CISOs around the world.

DarkSide's ransomware attack on Colonial Pipeline shut down fuel supplies for much of the U.S. East Coast. The Conti group brought Ireland's health service to its knees and shut down hospitals. REvil ransomware halted production at the world's largest meat processor, JBS. The REvil group also hit cloud-based managed service provider platform Kaseya.[1] That attack had a ripple effect, compromising other managed service providers that used the company's remote management software.

And those were just a few of the countless incidents that kept security professionals busy.

These high-profile breaches had profound economic and security implications. They once again showed the world just how vulnerable critical infrastructure and supply chains can be when targeted by cyber criminals. The exorbitant ransom demands in some incidents also led governments to weigh regulations banning payments to cyber crime groups.

With the impact of the pandemic on security teams gradually fading in 2021, another issue reared its head: The Great Resignation. Workers quit in droves or opted out of returning to the workforce—with considerable consequences for information protection and insider threats.[2] Finally, closing the year, the Log4j flaw[3] allowed attackers to execute code and take control of vulnerable devices, disrupting Amazon Web Services (AWS), Cisco, IBM and VMware, among others.

For 2022, we face the most unstable geopolitical landscape Europe has seen in decades, and CISOs are also left to ponder the impact of hybrid warfare on their security posture.[4]

To gauge the mindset of cybersecurity professionals during this challenging time, Proofpoint surveyed 1,400 CISOs from around the world, inviting them to share their firsthand accounts of the past 12 months and offer their insights for the future.

This second annual report explores how CISOs are adjusting in the wake of pandemic disruption, adapting strategies to support long-term hybrid work and battling an increasingly sophisticated threat landscape. We also examine how people put organisations at risk and how CISOs change priorities in response. Finally, we delve into the changing role of the CISO and how they cope with increasing and evolving demands.

This report would not have been possible without the participation of cybersecurity and information security practitioners across the globe. Thank you once again for your insights and feedback.

Lucia Milică, Global Resident CISO at Proofpoint

1 Pierluigi Paganini (Cybernews). "An in-depth analysis of the Kaseya ransomware attack: here's what you need to know." July 2021.
2 Proofpoint. "Global Cybersecurity Study: Insider Threats Cost Organizations $15.4 Million Annually, up 34 Percent from 2020." January 2022.
3 CISOMAG. "Log4j Explained: How It Is Exploited and How to Fix It." December 2021.
4 Andrew Rose (Proofpoint). "How Conflict in Ukraine Could Revolutionize the Ransomware Threat." March 2022.

Chapter 1: The Calm After the Crisis

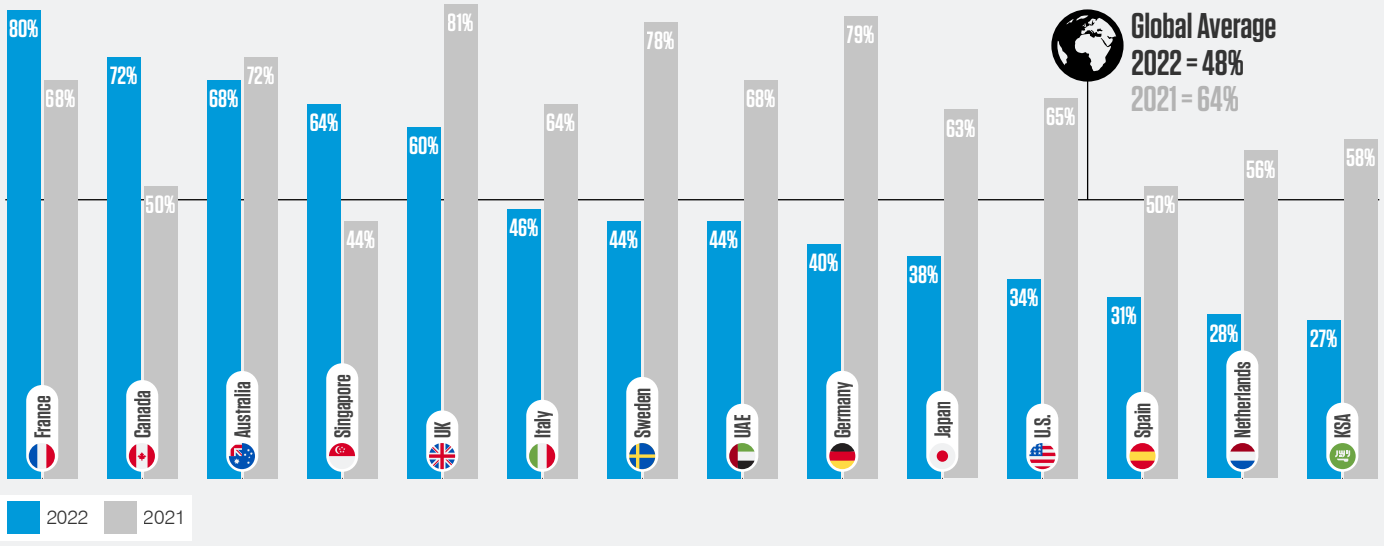
After a year of such unprecedented disruption, the world's CISOs spent 2021 coming to grips with new ways of working. But having overcome the initial rush to deploy cloud and hybrid setups and maintain business as usual, many now appear to feel more in control of their environment.

Ad hoc firefighting has been replaced by a more coherent strategy. New policies, training modules and technical controls have been introduced, all designed for today's more distributed, cloud-reliant teams.

As a result, fewer than half the CISOs surveyed (**48%**) feel that their organisation is at risk of suffering a material cyber attack in the next 12 months, compared with **64%** last year.

48% of surveyed CISOs feel their organisation is at risk of suffering a material cyber attack in the next 12 months, with one third rating the risk as very high.

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



French (**80%**), Canadian (**72%**) and Australian (**68%**) CISOs are most worried about experiencing a material cyber attack.

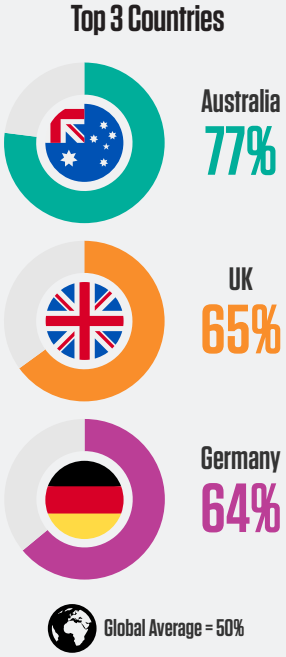
Only **28%** of Dutch CISOs and **27%** of Saudi CISOs expect to experience a material attack, making them the most optimistic of all regions surveyed.

Large organisations are more acutely aware of the risk, with **51%** of respondents from companies with over 5,000 employees considering a material cyber attack likely or very likely.

56% of CISOs from IT, technology and telecommunications companies rate the cyber attack risks on their companies as likely, the highest among all surveyed verticals, followed by manufacturing (**54%**).

The retail sector is most optimistic of all surveyed verticals: **33%** of respondents believe it is unlikely that attacks on their organisations will cause material damage—compared to only **5%** last year.

Percentage of CISOs who agree that their organisation is unprepared to cope with a targeted cyberattack in 2022



Increasing familiarity with the post-pandemic work environment has also left CISOs feeling more equipped to deal with cyber threats. While **66%** believed they were unprepared for a targeted attack in 2021, this is down to **50%** this year.

But feeling prepared for or at risk of a cyber attack is entirely different than being prepared. In most cases, this growing confidence of CISOs is likely a result of successfully overcoming a seismic event rather than any tangible change in risk levels or preparedness.

What's more, the fact remains that half of global CISOs do not believe their organisation is ready to detect, deter and recover from a cyber attack. In the UK and Germany, this figure climbs to around two-thirds. And in Australia, more than three-quarters say that their organisation is unprepared.

There is also a troubling disconnect between perceived risk and preparedness. Many CISOs are seemingly aware of the issue but are unable or unwilling to implement an effective solution as they struggle to identify which of the many common threats is likely to strike.

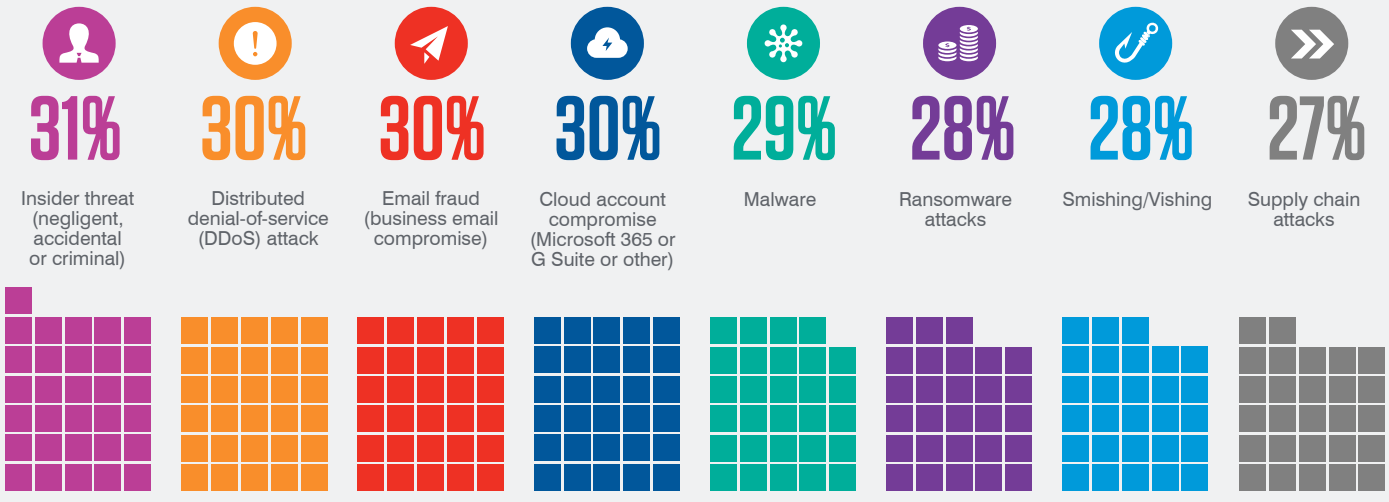
Attacks from all angles

As the threat landscape continues to grow and evolve, we once again asked CISOs about the methods of cyber attack that keep them up at night. Much like last year, the results demonstrate a worrying lack of visibility into the threats they face.

Negligent, accidental or criminal insider threats (**31%**), business email compromise (BEC) (**30%**), cloud account compromise (**30%**) and distributed denial-of-service attacks (DDoS) (**30%**) all lead the way. Meanwhile, concern about ransomware inched up just 1 percentage point since last year, despite several incredibly high-profile attacks in the last 12 months.

Of course, there is nothing wrong with a general wariness of a range of threats. But when security teams are unsure where the next attack is coming from, it is almost impossible to target protections and training where they are needed most.

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.



10 out of 14 surveyed countries consider insider threats one of the biggest three risks, with Japan (**39%**), Australia (**36%**) and Italy (**34%**) leading the way.

Ransomware is considered the No. 1 risk in Germany, the Netherlands and Spain.

8 out of 14 surveyed countries consider BEC one of the top three risks, with French (**43%**) and Emirati CISOs (**35%**) rating it the highest.

Supply chain attacks are the top concern for CISOs in Canada, Spain and Saudi Arabia (KSA).

Cloud account compromise attacks make the top three across eight geographies, with Sweden (**38%**) rating it the highest and the Netherlands (**19%**) the lowest.

Distributed denial-of-service (DDoS) attacks are a top concern for CISOs in the U.S., UK and Singapore.

CISOs can be forgiven for this lack of clarity after such recent uncertainty. Rapid adjustment to new ways of working, increased cloud reliance, and changing behaviour patterns have made it incredibly difficult to rank threats and build adequate defences.

While a lack of clarity is a concern, it is not an insurmountable issue. More than **90%** of cyber attacks start with email. Whether it is ransomware, BEC or cloud account compromise, protecting the inbox is always the best place to start.

"Leading a cybersecurity function is like walking up a down escalator. If you stand still, you will soon end up in a mess at the bottom. Even if you take one step at a time you won't advance. To make progress, you must run and keep running. You've got to be fit to be a CISO."

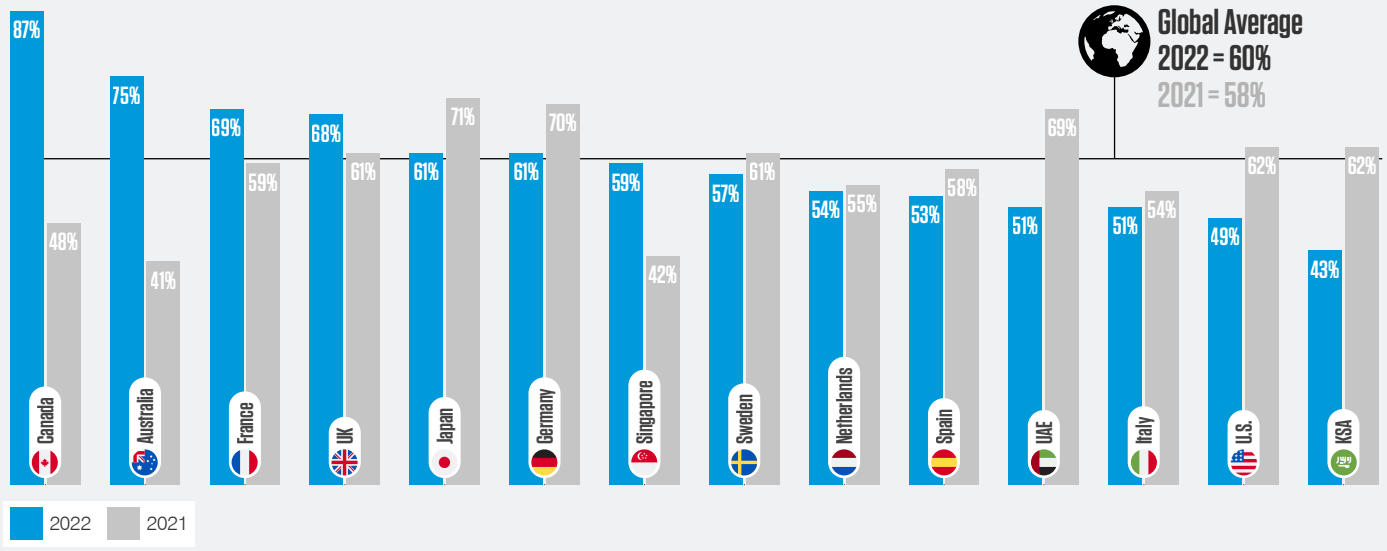
Malcolm Norman, CISO, Wood Plc

Chapter 2: People as the New Perimeter

With two years of remote work under their belt, most CISOs believe that employees understand the role they play in protecting their organisations against cyber threats. Overall, 3 in 5 respondents (**60%**) agree with this statement, up from **58%** last year. About a quarter, **24%**, strongly agree.

The trend is most pronounced in Canada and Australia, where belief in employee understanding has increased 39 and 34 percentage points, respectively, to **87%** and **75%**.

Percentage of CISOs who believe employees understand their role in protecting the organisation against cyber threats



We can attribute much of this increase in employee understanding to measures put in place to support long-term remote and hybrid setups. Many organisations spent the past two years investing in cybersecurity training and protections that focused on people.

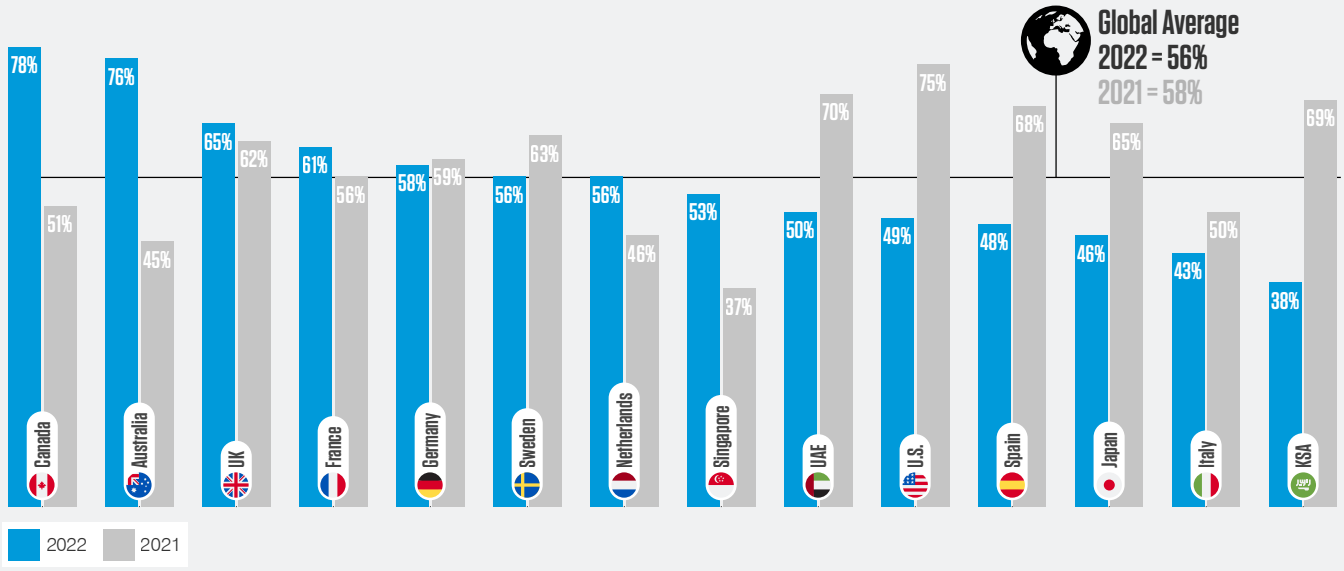
With teams working from anywhere, there is less emphasis on protecting the data centre or the office network. CISOs now realise that the perimeter is the user and are taking steps to equip them to defend it accordingly.

56% of CISOs consider human error to be their organisation's biggest cyber vulnerability.

At the other end of the scale, countries with more formal or rigid corporate environments may have struggled to make this adjustment. For example, in Saudi Arabia and UAE, belief in employee understanding fell most sharply, down 19 and 18 percentage points, respectively, to **51%** and **43%**.

The increased belief in employee savviness around security is also reflected elsewhere. This year, fewer CISOs believe that human error is their organisation's biggest cyber vulnerability, with just **56%** in agreement.

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



The notion that **60%** of CISOs believe users understand their security responsibilities, yet **56%** believe they are the number one cyber threat, raises several red flags. It suggests that many CISOs understand that most users are not adequately skilled for the role of cyber defence.

The World Economic Forum reports that **95%** of cybersecurity issues are traced to human error,[5] which highlights that many CISOs still significantly underestimate the degree of risk posed by their users. Only **38%** of Saudi CISOs consider their employees their biggest cyber vulnerability, followed by Italy (**43%**) and Japan (**46%**).

This is also the case in the education sector, where just **47%** believe users to be their most significant risk. At the other end of the spectrum, CISOs in business and professional services and manufacturing led the way with **61%** and **60%**, respectively, in agreement.

Elsewhere, attitudes have shifted among healthcare CISOs over the past 12 months. Just over half (**52%**) believe their people put their business at risk this year compared with **48%** in 2021. The reverse is true in financial services, where **52%** now believe their people are the biggest cyber risk, down from **61%** last year.

"As threat actors become increasingly sophisticated and as systems and data become more elastic and proliferate across a seemingly barrier-less landscape, it's critical for security and business leaders to focus on those priorities and partners that will help them simplify, reduce, manage and control the expanse of the attack surface and the morphing threat environment."

Patrick Joyce, Vice President and Chief Security Officer (CISO & CSO), Medtronic

5 World Economic Forum. "The Global Risks Report 2022 17th Edition Insight Report." January 2022.

Chapter 3: Risk, Remote Work and The Great Resignation

The forced migration to remote and hybrid setups in recent years has served as an enormous test case. Some 24 months into this new way of working, organisations see what it can offer in terms of flexibility, cost-savings and productivity.

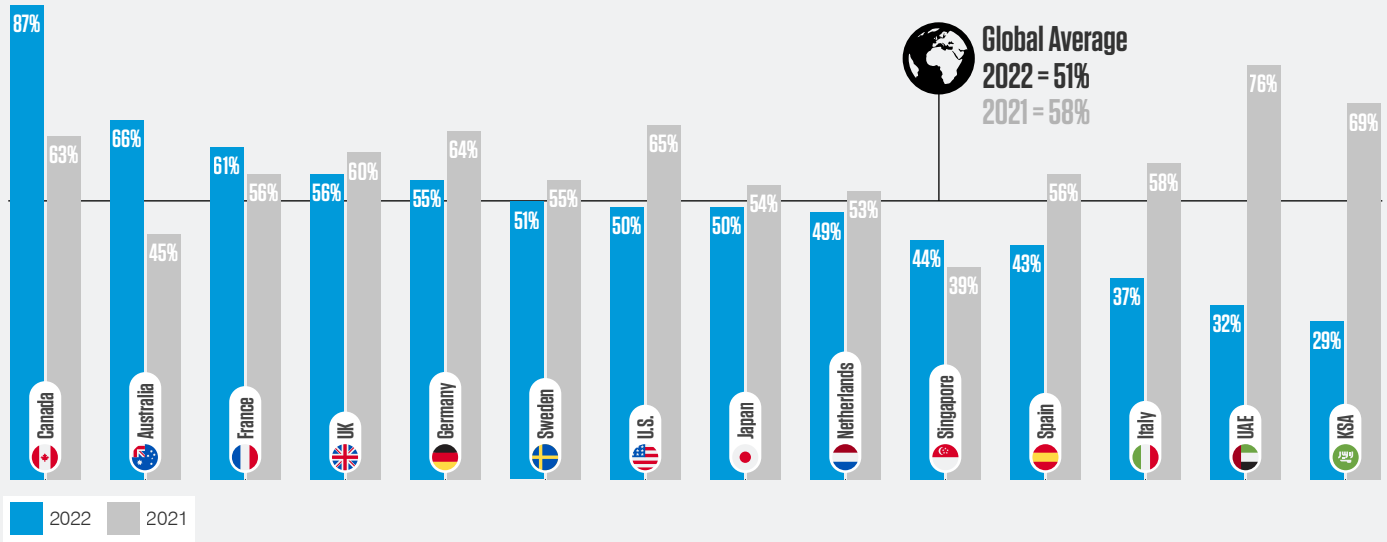
It is also popular among employees—and likely here to stay. With people now forming the defensive perimeter wherever they work, organisations need a new strategy.

51% of CISOs have seen more targeted attacks since enabling widespread remote working.

As many are discovering, hybrid and remote working make users more vulnerable to attack. At the very least, they represent a much more attractive target for cyber criminals.

Over half of CISOs across all regions agree that targeted attacks on their organisations have increased since adopting mass hybrid working. With many now much more comfortable in this environment, it should come as no surprise that this figure is down from **58%** this time last year. Even so, that's a small change; most CISOs still face a heightened cyber threat landscape. And this risk factor is far from the only issue that has arisen since hybrid working became the norm.

Percentage of CISOs saying their business has seen more targeted attacks since enabling widespread remote working



Small organisations seem more affected, with **59%** of companies with 500 employees or less saying their workforce has been targeted more since they implemented hybrid working. At the other end of the scale, only **48%** of large organisations (5,000 employees and above) agree.

The most affected industry is manufacturing (**65%**); retail and transport were the least affected at **43%**.

87% of CISOs in Canada and **66%** in Australia report an increase in targeted attacks since switching to widespread remote working, the largest percentages in our study.

In Saudi Arabia, on the other hand, only **29%** of CISOs report more targeted attacks. The U.S. is on par with the global average at **50%**.

The Great Resignation: a new challenge for security teams

Employees are leaving their jobs in record numbers for reasons ranging from post-pandemic burnout to childcare issues to changing work-life priorities. But whatever the cause, the cybersecurity implications are not up for debate.

When an employee leaves, their data often leaves with them. Sometimes, it is unintentional, such as when saved credentials reside on a personal device. But in many cases, it is deliberate. Former employees may feel ownership over data they worked on or take it with them to help in their new job.

The Great Resignation: 50% of global CISOs agree that protecting data has become an increased challenge.

Whatever the reason, the trend has left many CISOs finding it harder to protect their data. This is felt more keenly within smaller organisations that may have fewer controls in place: **55%** of respondents from companies under 500 employees agree that protecting data has become an increased challenge compared with only **47%** from CISOs of larger enterprises (5,000 or more employees).

Percentage of CISOs in agreement that protecting data has become an increased challenge (by company size)

"The dramatic change in the way we work over the last two years has brought numerous challenges, but also opportunities. Chief among them is a shift in focus toward comprehensive information protection strategies, not just defending networks and other IT assets."

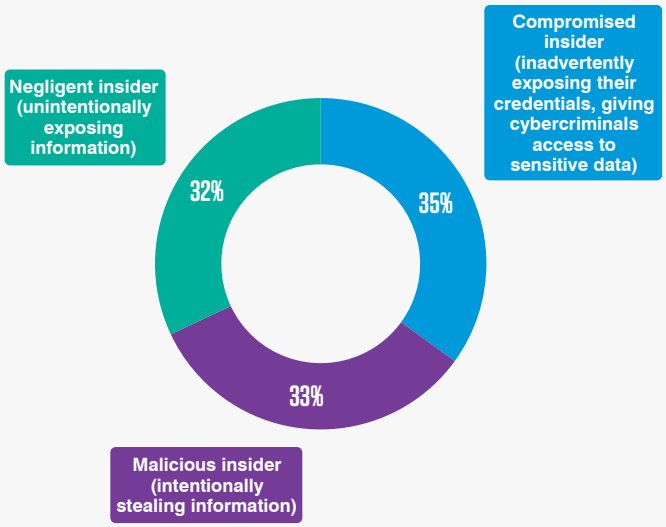
Paige Adams, Global Chief Information Security Office, Zurich Insurance

Data doesn't walk away...

Employees move it, and not always intentionally. People leaving a job present another data protection problem. Employees distracted by the prospect of greener pastures are often more prone to the types of actions seized upon by cyber criminals; behaviours such as password mismanagement, security workarounds and using business devices for personal use.

This type of behaviour is the most common cause of insider threats, with recent research showing **56%** of incidents are driven by negligence.[6] Despite this, with more staff outside the office with greater autonomy over their security hygiene, compromised, negligent and malicious insiders are of equal concern to the world's CISOs.

Data loss: in what way do you think your employees are most likely to cause a data breach or exposure in your organisation in the next 12 months, if at all?



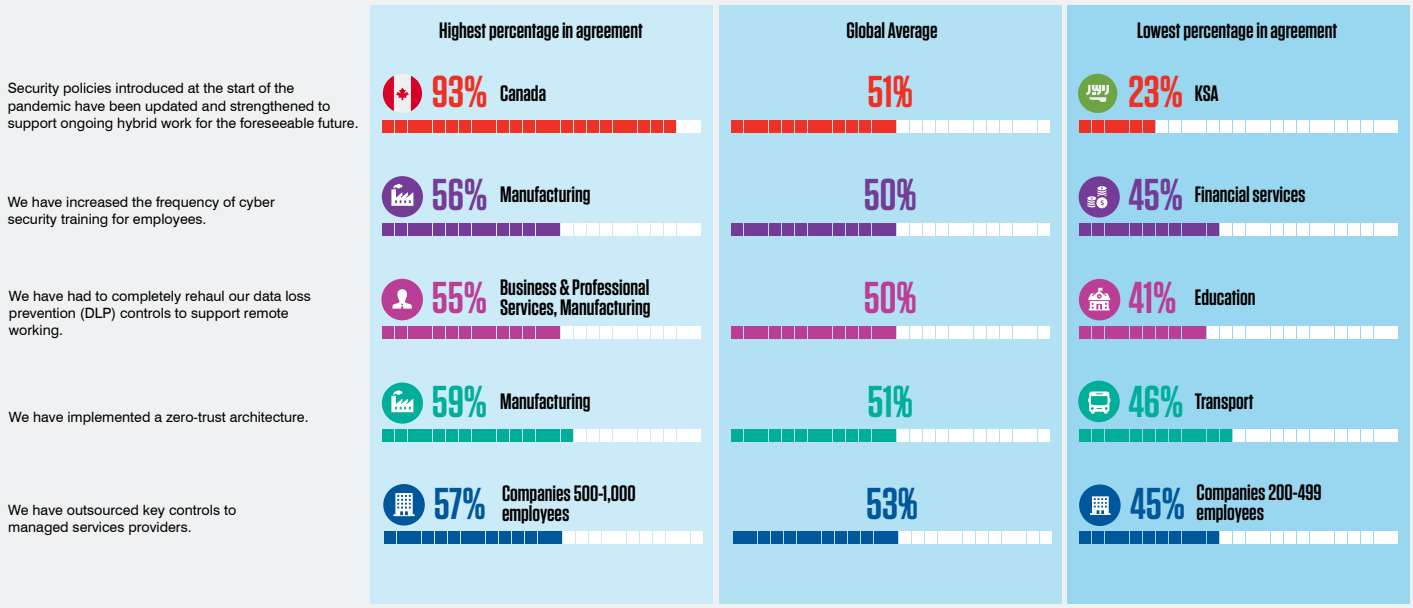
How organisations are responding to hybrid working challenges

The response to this rising threat has been mixed. While CISOs in countries such as Canada have strengthened COVID-era policies to support ongoing hybrid work, only around half (**51%**) of global CISOs have done the same.

Half of the global CISOs surveyed have increased the frequency of cybersecurity training for employees. While encouraging, this leaves **50%** at risk against increasing levels of targeted attacks. Mitigating strategies focused on deploying zero trust architecture and overhauling data loss protection solutions were a priority for half of respondents.

Finally, the outsourcing of key controls to managed services providers was most prevalent among companies with 500 to 1,000 employees.

To what extent do you agree or disagree with the following statements regarding the "work from anywhere" trend?



6 Proofpoint. "Global Cybersecurity Study: Insider Threats Cost Organizations $15.4 Million Annually, up 34 Percent from 2020." January 2022.

Chapter 4: Reigning in Ransomware

Ransomware is the oldest trick in the threat actors' playbook, but 2021 proved just how pervasive it has become. Among attacks that provide an ample supply of targets, big paydays and fast payment, ransomware is hard to beat.

56% of global CISOs agree that highly publicised ransomware attacks of the last two years have increased awareness of cyber risk among C-level executives.

The frequency and complexity of these attacks increased by over **150%** last year,[7] making this old threat one of the biggest facing modern businesses. Several high-profile incidents in recent years have also moved ransomware higher up on the CISO's agenda.

In May 2021, an attack shut down one of the largest fuel pipelines[8] in the U.S., while the world's biggest meat processor paid an $11 million ransom to restore its services.

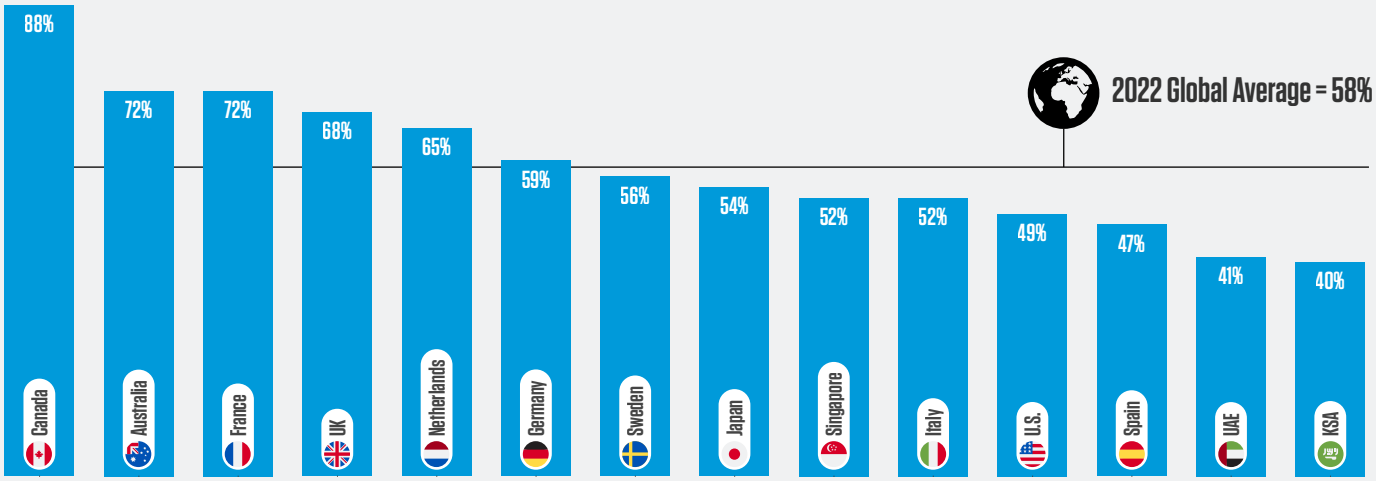
The size of this payout may seem an outlier, but experts fear that it is fast becoming the norm. The group behind the pipeline hack is estimated to have made at least $90 million last year.[9] At the same time, both the average ransom amount and the highest demand made by cyber criminals doubled year over year in 2021.[10] To make matters worse, paying ransoms is not always the end of the matter; half of victims that pay up are likely to suffer repeat attacks.[11]

Despite the rising stakes, many organisations appear unprepared for demands of any size or scale. A concerning **42%** of global CISOs admit that they do not even have a ransom policy in place.

58% of global CISOs said their organisation has set a policy on whether or not they would pay to regain their data.

These exorbitant sums are causing governments and industry bodies to debate the legality of making any ransom payments. But with strong sentiment on both sides of the "to pay or not to pay" argument, regulation will be slow—if it arrives at all.

Percentage of CISOs saying their organisation has purchased cyber insurance and is confident it will be there when needed



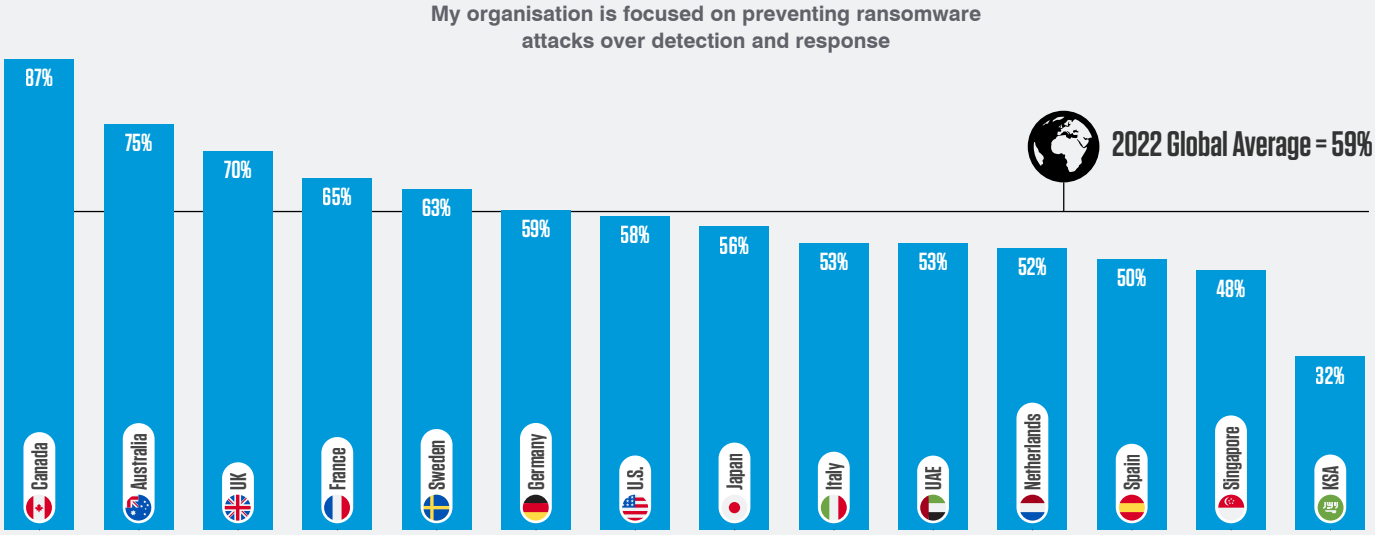
7 ENISA. "ENISA Threat Landscape 2021." October 2021.
8 Proofpoint. "Threat Briefing: Ransomware." July 2021.
9 Joe Tidy (BBC News). "Ransomware: Should paying hacker ransoms be illegal?" May 2021.
10 ENISA. "ENISA Threat Landscape 2021." October 2021.
11 Proofpoint. "What is Ransomware?"

In the meantime, many organisations look to cyber insurers for peace of mind. Over half (**58%**) of global CISOs are confident that their policy will pay out when it matters most. Canadian CISOs are the most assured, with **88%** confident that insurers will pay. That's a stark contrast to Saudi Arabia's CISOs, only **40%** of whom have confidence in their insurer.

CISOs are right to be skeptical. Many insurers now drastically limit their coverage for ransomware. Some are removing it from policies altogether.[12] This is yet another reason why organisations should look away from response and recovery and focus more on prevention.

3 in 5 global CISOs (59%) say their organisation is focused on preventing ransomware over detection and response.

Ransomware is not the simple brute-force attack of old. Instead of breaking in, encrypting files and demanding payment, today's cyber criminals often sneak in and lie in wait for maximum impact. Ransomware now crawls through networks infecting systems, deleting backups and siphoning data, making traditional response strategies obsolete.



As a result, some CISOs are changing their tactics. Nearly **60%** now prioritise prevention over response. Others, however, are woefully underprepared: 4 in 10 CISOs do not have a blueprint in the case of a ransomware incident.

"Despite its prevalence over the course of the last 18 months, ransomware and related extortion events continue to be our most significant cybersecurity concern. The sheer volume of attacks and the evolution of ransomware models indicate that the problem is getting worse, not better, and the specific targeting of operational technologies and supply chains makes defending the threat even more challenging."

Simon Strickland, Chief Information Security Officer, Johnson Matthey

12 Carolyn Cohn (Reuters). "Insurers run from ransomware cover as losses mount." November 2021.

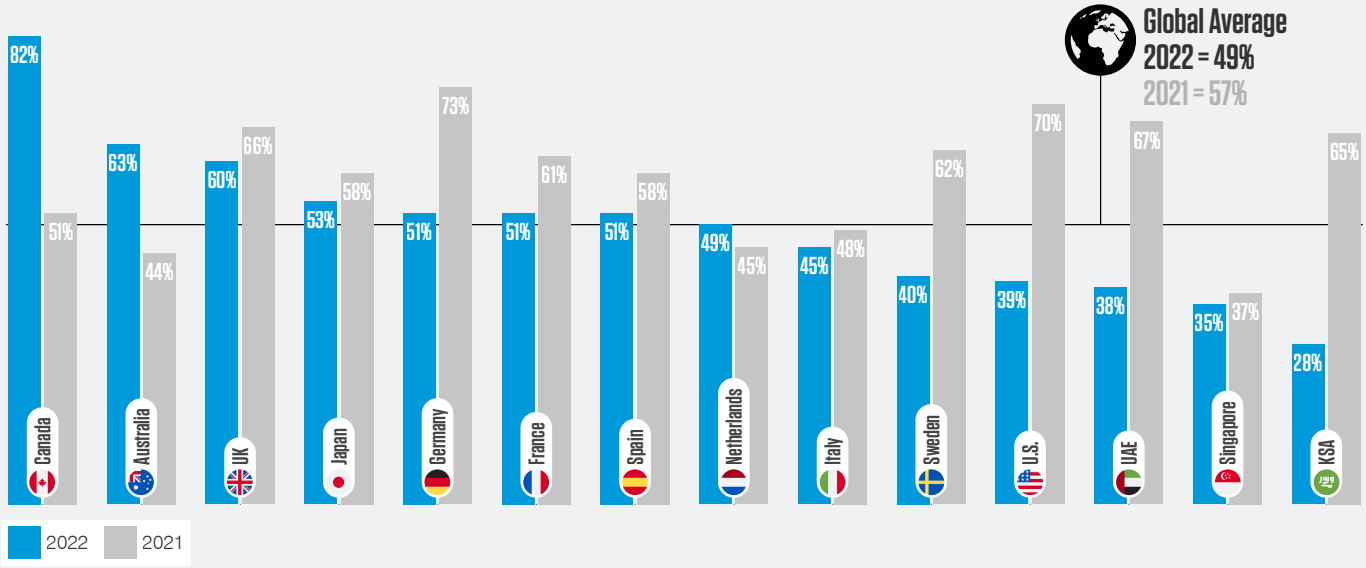
Chapter 5: Boards, Buy-In and the Bottom Line—How CISOs Are Feeling

Given the lasting impact of cybersecurity during a global pandemic, the CISO's job has never been more challenging—or more critical. The incredible demands of the past two years have pushed the role further in the spotlight and encouraged CISOs to make their voices heard, loud and clear.

Overall, CISOs across all regions believe that the expectations of their superiors and colleagues are excessive. That said, CISOs' views vary widely by country and have shifted a great deal in the last year. Still, 1 in 2 CISOs feel they face an impossible task.

Half of surveyed CISOs agree that expectations on their role are excessive, down from 57% last year.

Percentage of CISOs agreeing that expectations on their role are excessive



While German CISOs were the most likely to agree that expectations on their role were excessive last year, Canadian CISOs felt the most pressure in 2021.

Belief that perceived expectation is excessive is lowest in Saudi Arabia (**28%**), Singapore (**35%**) and the UAE (**38%**).

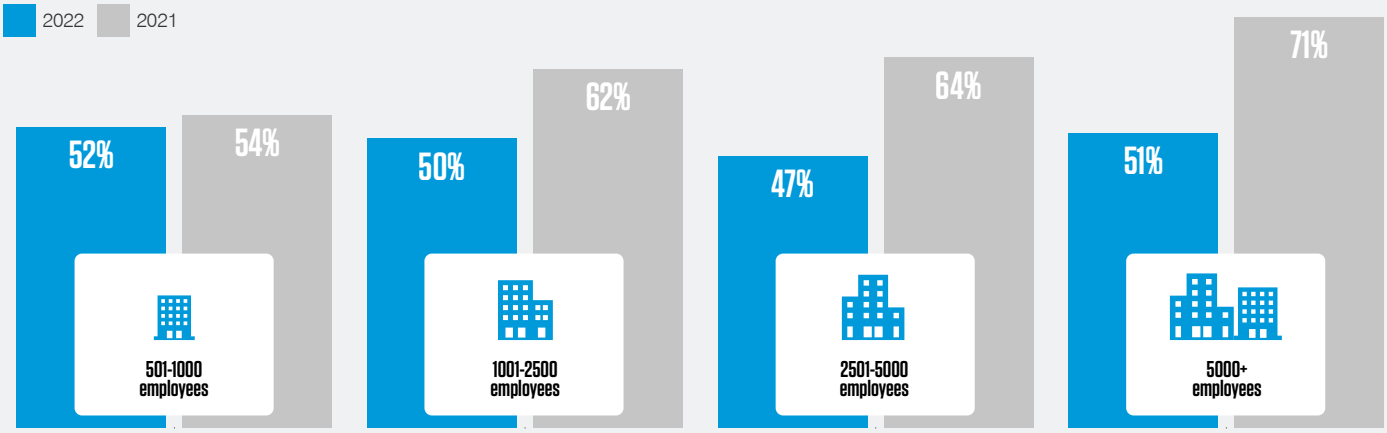
Almost a third (**31%**) more Canadian CISOs believe they face excessive expectations this year than in 2021. The opposite is true in the U.S.

Across verticals, CISOs from business and professional services companies (**57%**) feel the pressure of excessive expectations the most among their peers. Least pressured are education sector CISOs (**39%**), followed by those in retail (**42%**).

Adding to the demanding and often thankless workload of the CISO is a perceived lack of support from the boardroom, which has increased since 2021. Just over half (**51%**) of global CISOs agreed that they saw eye to eye with the board on cybersecurity matters in 2022. That's a sharp drop from **59%** the year before.

This change falls in tandem with company headcount, underlining the difficulties faced by CISOs at smaller organisations. Still, the drop in perceived board support is felt most by CISOs in charge of large organisations (5,000 employees and above), who went from **71%** agreement last year to only **51%** this year.

Percentage of CISOs in agreement that their board sees eye-to-eye with them on the issue of cybersecurity (by company size)



Average Agreement = 51%

This lack of support and agreement does not just affect buy-in and budgets. Many CISOs also report that their superiors directly affect their ability to perform their roles.

Over half (**51%**) of global CISOs agree that their reporting line can hamper their job effectiveness. This view is most prominent in the world of business services (**58%**) and technology (**54%**). But it is much less of an issue in the financial services, media and education sectors, where just **46%** agreed with the sentiment.

Only half of global CISOs surveyed (50%) believe that their organisation positions them to succeed.

Relations are strained between the CISO and the C-suite in other areas too. Only half of global CISOs surveyed now believe their organisation positions them to succeed, compared to **60%** a year ago.

Healthcare and education CISOs felt the least backed by their organisation, while those in manufacturing and technology feel most supported to successfully carry out their responsibilities.

"Excessive expectations are a result of poor risk management practices. Every CISO should ensure there is an appropriate risk management methodology that helps focus the business on what's most important. CISOs can't be expected to protect the organisation continuously from all threats. If the business fails to mitigate risk, the board will need to step in and accept the greater risk of doing nothing."

Christian Toon, CISO, Pinsent Masons LLP

Spotlight on CISO priorities and board concerns

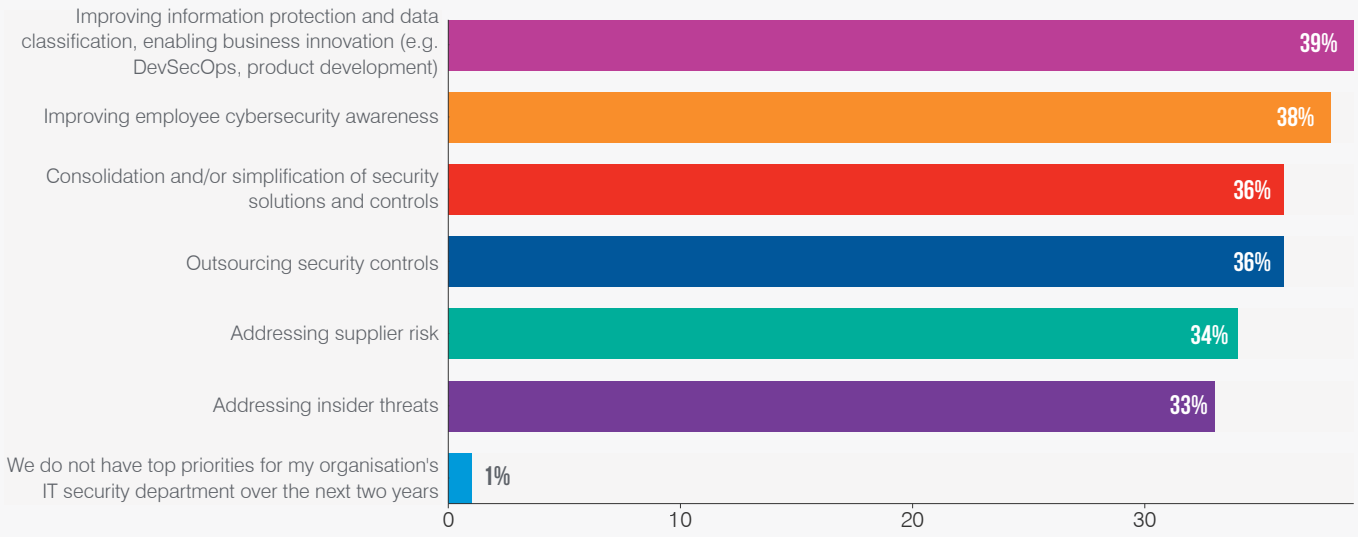
When it comes to IT security priorities over the next two years, CISOs globally rated their top three as:

- Improving information protection (**39%**)
- Improving cybersecurity awareness (**38%**)
- Consolidating and outsourcing security solutions and controls (**36%**)

While the first two categories are always high on the CISO's agenda, the latter is almost certainly driven by the events since 2020. With employees working from home, at the office and everywhere in between, IT setups are increasingly complex. That means they require new skills and more resources to secure.

The Great Resignation will play a part here too. As employees transition jobs in large numbers, organisations must ensure they always have the expertise and knowledge to implement their cyber strategy. Outsourcing can be an affordable and straightforward way to do just that.

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



Naturally, priorities differ between industries and organisations. For large companies with more than 5,000 employees, which likely have the most complex setups, outsourcing is the primary priority at **41%**. This is well above the percentage among all other company sizes.

Among industries, improving information protection is the most pressing initiative for those in IT, technology, telecoms, financial services, manufacturing and the public sector.

Priorities vary from country to country, too. In the UK, educating users is top of the agenda, while **46%** say security awareness is vital, a slight increase over last year. Education is viewed as critical elsewhere, too, topping the list in the U.S., Canada, the Netherlands, Spain and Australia. In Italy, supplier risk remains a primary concern, with **38%** of CISOs listing it as one of their top three priorities over the next two years.

Efficiency is the biggest priority for CISOs in Germany, Sweden and Japan, who view consolidation and simplification of security solutions and controls as their top priority.

Board concerns

There is no doubt that cybersecurity headlines over the last two years have awakened boardrooms worldwide to today's cyber risks.

We asked global CISOs about their top concerns when considering the impact of a cyber attack on their business based on their interactions with their board. They listed significant downtime (**37%**), disruption to operations (**36%**) and impact on business valuation (**36%**) as top of mind for board members.

Conversely, loss of revenue came last, perhaps viewed by some as a consequence of the top concerns rather than a direct impact. That said, larger organisations (with over 5,000 employees) were the most concerned.

Board cybersecurity concerns: 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.

	Significant downtime	Disruption to operations	Impact on business valuation	Reputational damage	Loss of current customers	Loss in revenue	No greatest concern
GLOBAL	37%	36%	36%	35%	35%	33%	1%
U.S.	34%	40%	47%	36%	37%	39%	1%
Canada	39%	33%	40%	39%	41%	34%	3%
UK	42%	33%	48%	37%	35%	29%	0%
France	44%	45%	48%	45%	47%	46%	0%
Germany	42%	26%	40%	30%	38%	29%	5%
Netherlands	29%	31%	21%	39%	31%	23%	0%
Sweden	36%	41%	38%	31%	31%	29%	2%
Italy	35%	33%	26%	36%	36%	28%	0%
Spain	28%	34%	26%	37%	28%	33%	0%
KSA	29%	39%	35%	27%	37%	38%	4%
UAE	45%	33%	39%	31%	30%	39%	2%
Australia	49%	42%	34%	29%	32%	33%	0%
Singapore	36%	33%	29%	31%	33%	32%	1%
Japan	34%	44%	34%	42%	36%	31%	2%

Main Concern Second/Third Concerns

Around the world, U.S., UK, and French boards view the impact of a material cyber attack on business valuation as the most pressing concern. In the Netherlands, Italy and Spain, reputation damage is the primary worry. Significant downtime is top of mind for those in Germany, UAE, Australia and Singapore.

For retail CISOs, reputational damage is the biggest risk. Brand impact was also high on the agenda for IT, technology and telecoms boards.

Significant downtime is of most concern to education, manufacturing and business services boards, while disruption to operations worries the healthcare C-suite.

Impact on business valuation is perceived as the biggest potential repercussion for energy, oil/gas and utilities—as well as IT, technology and telecoms and the media and entertainment sectors.

Conclusion

As CISOs have adapted over the past two years, many of them feel more comfortable with the level of risk they face. Patchwork systems and ad hoc policies have been replaced with more strategic cyber defences. At the same time, employees are now well-versed in working away from the office. As a result, global CISOs now believe that employees better understand their security responsibilities—and that their organisations are more equipped to cope with a cyber attack.

However, many may be falling into a false sense of security. Targeted attacks, ransomware and insider threats are all on the rise. And with most cyber attacks requiring human interaction, people remain the biggest risk factor. That relatively few CISOs have bolstered defences to protect the people perimeter in light of hybrid working is a major cause for concern.

But once again, it may be the case that they are unable—not unwilling—to empower their people. Just like last year, many CISOs do not see eye to eye with their board on matters of cybersecurity. And more than half believe that their reporting line hampers job effectiveness.

The good news: CISOs around the world know where things need to improve. Many are taking steps to enhance information protection solutions and security awareness training, both of which will be vital in long-term hybrid environments. Skill and resources shortages are being acknowledged, too, with many CISOs planning to outsource security solutions in the coming years.

Overall, CISOs appear to have embraced 2022 as the calm after the storm. But with rising geopolitical tensions and increasing people-focused attacks, the same gaps of user awareness, preparation and prevention must be plugged before the cybersecurity seas grow rough once more.

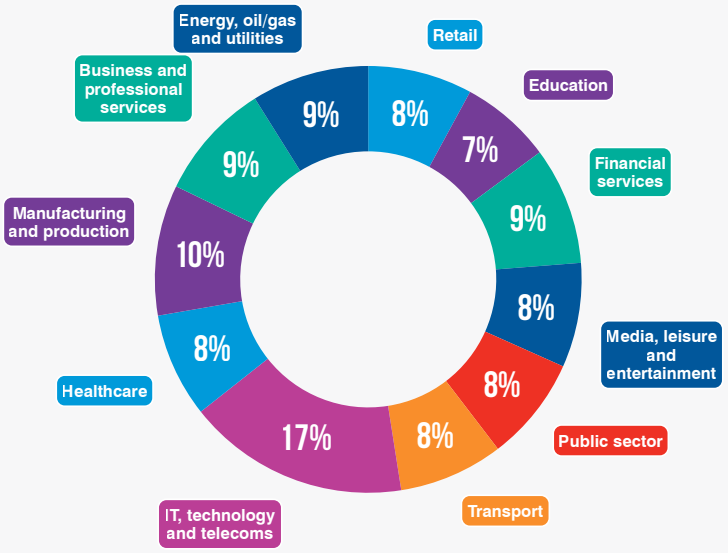
"The problems facing CISOs today are as much, if not more, business-related as they are technology-related. Cyber incidents impact the business across multiple facets, from reputational risks impacting trust and revenue to potential liabilities imposed by state and federal legislators. This has created a need for the CISO to engage the board, not only to provide the metrics surrounding the cyber posture of the business, but also to be able to tell the story from a risk-based perspective in a way that can easily be understood by its members."

Patrick Gaul, Executive Director, National Technology Security Coalition

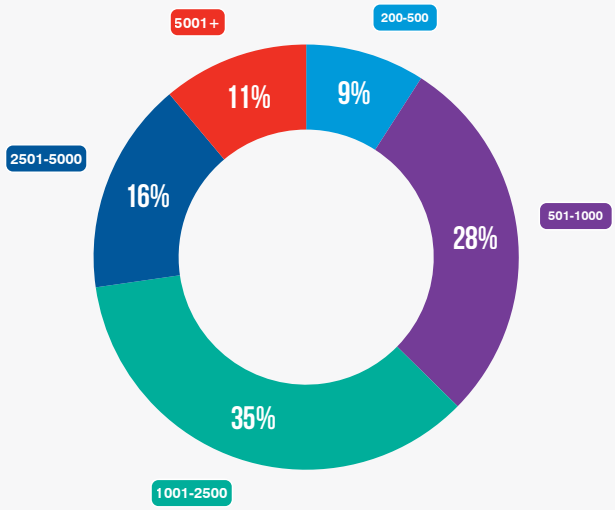
Methodology

The Proofpoint 2022 Voice of the CISO survey, conducted by research firm Censuswide between 22 February and 8 March 2022, surveyed 1,400 chief information security officers from organisations of 200 employees or more across different industries in 14 countries. One hundred CISOs were interviewed in each market, which included the U.S., Canada, the UK, France, Germany, Italy, Spain, Sweden, the Netherlands, UAE, KSA, Australia, Japan and Singapore.

Industry split among respondents:



Company size split among respondents:



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

proofpoint®

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 more than half of the Fortune 1000, 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.

0400-008-0101 05/22