proofpoint.

REPORT

Cybersecurity: The 2023 Board Perspective

Board director views on the global threat landscape, cybersecurity priorities and CISO relations

proofpoint.com

Table of Contents

Introduction

With the disruption caused by the pandemic now largely behind us, many in the boardroom could be forgiven for thinking the CISO would take on a less prominent role this year. But another bumper 12 months in cybersecurity quickly laid that notion to rest.

With most organizations now tasked with securing a much larger attack surface, cyber criminals are increasingly targeting our people. At the same time, ongoing tensions between Russia, Ukraine and NATO have once again brought state-sponsored threat actors to the fore.[1]

High-profile data breaches,[2] a rise in ransomware[3] and disruptive attacks on the supply chain[4] have also laid bare the many devastating consequences of cyber threats. With the potential damage stretching beyond revenues, the board needs a cybersecurity perspective now more than ever to safeguard company reputation, protect customers and avoid costly business disruption.

Unsurprisingly in this environment, many feel more at risk and less prepared than in past years. Overall, most board members believe their organizations are not set up to cope with an attack when—not if—it strikes.

They're more optimistic in other areas. Most board members say they understand the threat landscape and believe their data is adequately protected. Whether this translates to an effective cybersecurity strategy is another matter.

To get to the heart of these issues and more, Proofpoint commissioned a survey of more than 600 board members at organizations with over 5,000 employees across these 12 countries:

- The United Kingdom
- The United States
- Canada
- France
- Germany
- Italy
- Spain
- Australia
- Singapore
- Japan
- Brazil
- Mexico

We analyzed their responses to get a boardroom perspective of the threat landscape, the role of the CISO and the broader world of cybersecurity. We also compared the results with CISOs surveyed in our *2023 Voice of the CISO* report.[5] Pairing the surveys helps provide a more complete picture of where CISOs and their boards are on the same page—and opportunities for better alignment.

Once again, this year's report would not have been possible without the active engagement of these board members. Thank you for your continued support, valuable insights and vital feedback.

1 James Pearson (Reuters). "Russian hackers targeting Western critical infrastructure, UK says." April 2023.
2 Sergiu Gatlan (BleepingComputer). "AT&T alerts 9 million customers of data breach after vendor hack." March 2023.
3 Marnie Muñoz (Bloomberg). "Cyber Insurance Premiums Surge by 50% as Ransomware Attacks Increase." June 2023.
4 Sam Sabin (Axios). "Why organizations struggle to fend off supply chain cyberattacks." June 2023.
5 Proofpoint. "2023 Voice of the CISO Report." May 2023.

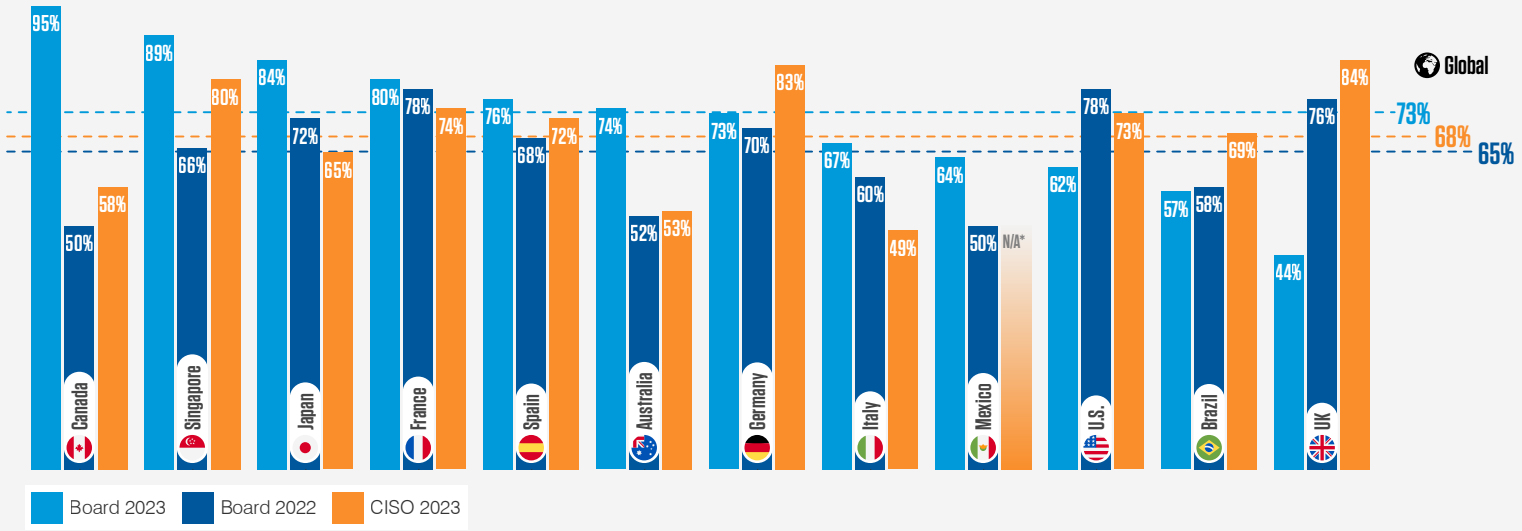
Section 1: The threat landscape–a view from the boardroom

As always, the threat landscape is a top concern of board members. But this year, impending threats are occupying their thoughts more than usual.

Almost three-quarters (**73%**) of board members believe they face a risk of a major cyber attack in the next 12 months. Not only is this high as a standalone figure, but it's also a noteworthy increase from the **65%** who agreed with the statement the previous year.

The shift echoes the year-over-year increase of CISOs who expressed the same concern in our *2023 Voice of the CISO* report. Now roughly in line with board members, **68%** of CISOs saw their organizations at risk versus just **48%** the year before.

Percentage of board members and CISOs who agree that their organization is at risk of a material cyber attack in the next 12 months

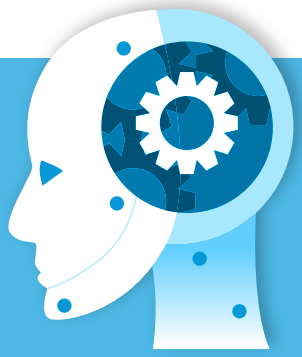


These concerns are felt most keenly among boards in the manufacturing (**80%**) and retail (**77%**) sectors, where once again, board members and CISOs are in close agreement. Each of these industries faces its unique challenges. But both handle masses of personal and financial information. And both have large frontline workforces that may lack cybersecurity understanding. All of these factors make the sector a prime target for cyber attacks.

Many factors are behind this newfound alignment. Geo-political tensions are almost certainly raising perceived threat levels as hostile nations take an increasingly vested interest in disrupting Western infrastructure and organizations.

At the same time, CISOs and board members alike appear to realize that large-scale hybrid and remote work are here to stay. Like it or not, the traditional office setup is no more. That means security teams must get used to protecting disparate and dispersed workforces as a standard practice.

AI technology poses security risks



The risk of artificial intelligent (AI) tools has caught the attention of the boardroom. Almost two-thirds (**59%**) of board members believe the technology already poses a security risk to their organizations.

As it stands now, the biggest threat from tools such as ChatGPT is employees uploading sensitive content to assist with research or report writing. But bigger problems are no doubt on the horizon.

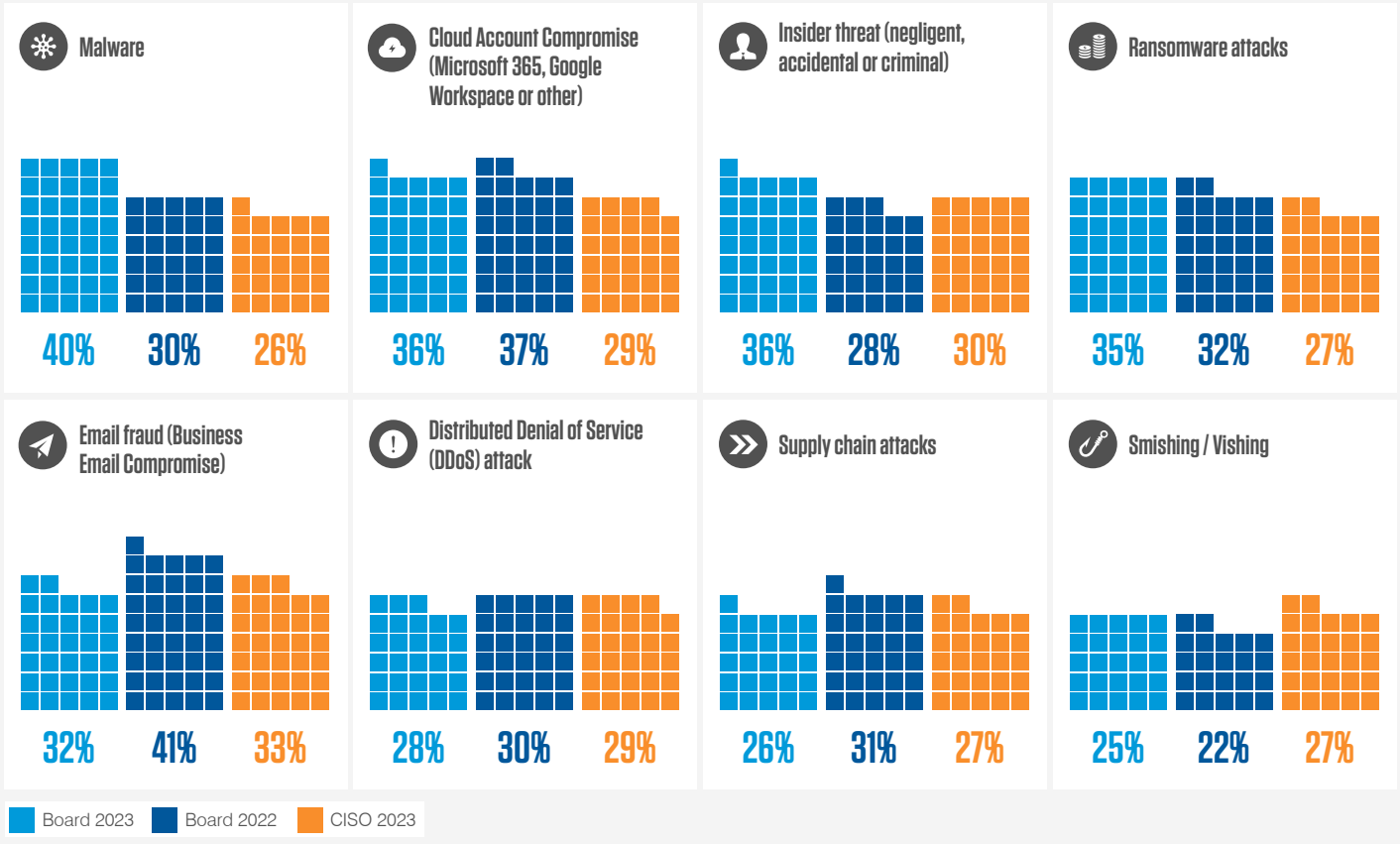
Cyber criminals already use AI to reduce the time-consuming aspects of phishing and finding and exploiting vulnerabilities. AI also allows those with limited technical chops to enhance their cyber attacks.

Japan (**79%**), Singapore (**78%**) and Australia's (**71%**) boards are the most concerned about generative AI.

Know thine enemy: What attacks are board members expecting this year?

CISOs and board members are also largely on the same page when it comes to the threats they are most likely to face. Both list cloud account compromise and insider threats as top concerns. In all, board members' top three of malware (**40%**), insider threat (**36%**) and cloud account compromise (**36%**) have changed slightly from last year's pick of email fraud/BEC (**41%**), cloud account compromise (**37%**) and ransomware (**32%**).

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



The shifting concern of boards from email fraud (business email compromise) last year to malware this year is likely driven by an increase in effective inbox security tools and high staff turnover. It takes time to train new staff on security best practices; in the meantime, new starters are much more vulnerable to malicious links and rogue attachments.

Insider threats are costing businesses upwards of $15 million a year and are still on the rise,[6] so it can only be good news that CISOs and board members are taking notice. But security teams need to act fast to effectively mitigate them.

Elsewhere, findings are somewhat more concerning. Despite a marked increase in supply-chain attacks,[7] just **26%** of board members cited the threat as a top concern. This may be partly explained by the recent finding in the *2023 Voice of the CISO* report that **64%** of CISOs believed their organization had appropriate controls in place to mitigate supply-chain risk.

However, as MOVEit and victims of other supply chain attacks can attest, there is no room for complacency. Attacks on the supply chain are projected to cost businesses almost $46 billion by the end of 2023 and more than $80 billion by 2026—a **76%** jump.[8]

In all, **7 in 12** surveyed countries consider malware their top risk, with France (**48%**), Canada (**45%**), Singapore (**43%**) and Brazil (**43%**) leading the way.

Malware is also the most pressing concern for board members at organizations across the energy/oil/gas, education, IT, technology and telecoms, and healthcare sectors.

Insider threats are the top concern for board members in Japan (**51%**) and Canada (**45%**). Those in Australia (**53%**) and Mexico (**40%**) are more worried about email fraud.

Cloud account compromise is ranked among the top three concerns in **8 out of 12** surveyed countries, including Germany (**45%**) and the U.S. (**42%**).

The awareness-preparedness paradox

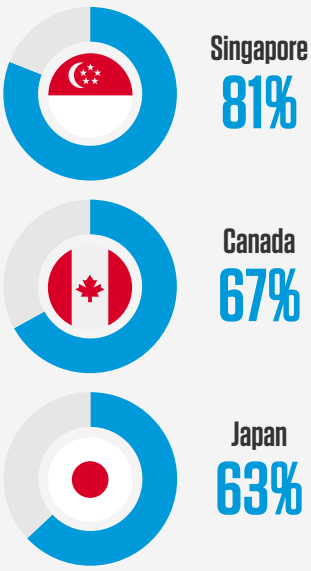
The boardroom appears to have a good understanding of risk levels and common threats. Unfortunately, this does not always mean they're prepared for them. Once again, just over half of board members believe their organization is unprepared to cope with a cyber attack in the next 12 months, a slight increase over the prior year (2023: **53%** vs 2022: **47%**). Board members in publicly owned organizations (**62%**) are much more likely to feel unprepared than privately owned organizations (**45%**).

That those closest to the action, CISOs, feel even more underprepared should be great cause for concern. Nearly two-thirds (**61%**) of CISOs now hold this belief, up from **50%** in 2020.

My organization is unprepared to cope with a targeted cyber attack in the next 12 months

Board members in Singapore (81%), Canada (67%) and Japan (63%) feel the most unprepared for cyber attack.

Top 3 Countries Least Prepared



6 Proofpoint. "2022 Cost of Insider Threats Global Report." January 2022.
7 Craig Temple (Proofpoint). "Hidden Risk: How to Recognise and Prevent Supply Chain Attacks." April 2023.
8 Juniper Research. "Juniper Research Study Reveals Staggering Cost of Vulnerable Software Supply Chains." May 2023.

It is easy to see why CISO concerns have trickled into the boardroom. After the events of recent years, cyber resilience is now a hot topic among the C-suite. Boards are therefore much more in tune with the challenge of maintaining business as usual while under cyber attack.

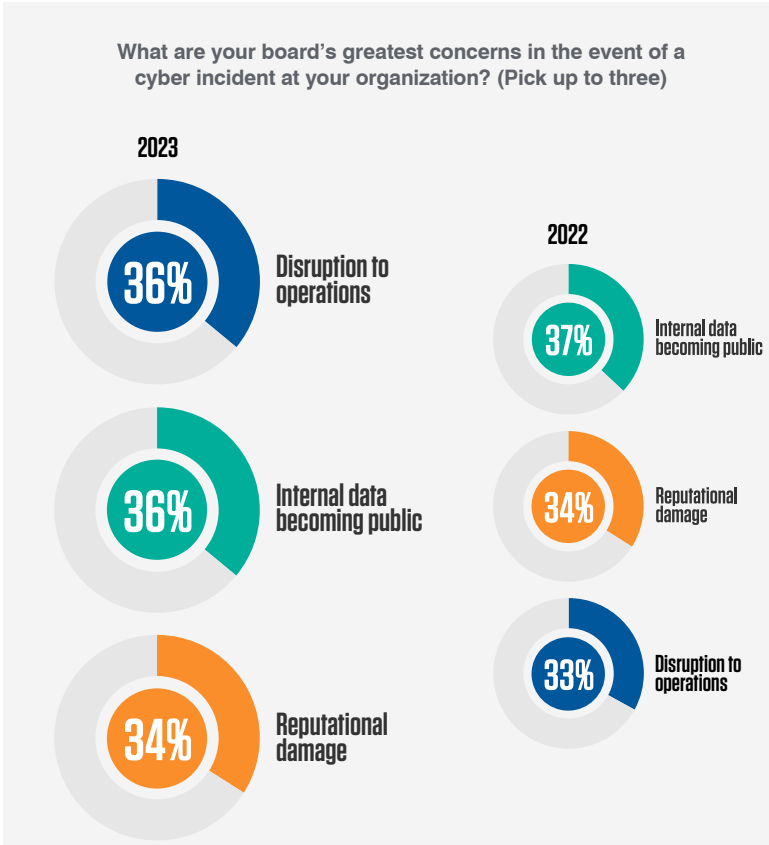
Still, that board members and CISOs feel largely unable to defend and remediate these all-but-inevitable cyber threats should ring alarm bells.

Counting the Consequences

When it comes to the potential damage caused by a cyber attack, the boardroom held steady in its outlook. As in 2022, disruption to operations (**36%**), internal data becoming public (**36%**) and reputational damage (**34%**) top the list of board members' greatest concerns. Underpinning these anxieties is the need to protect the organization from anything that could impede its long-term financial health and viability.

Around the world, Singapore, Japan, the UK and the U.S. view disruption to operations as the most pressing concern.

In Canada, Germany, Spain and Brazil, internal data becoming public is the top fear.



"It's easy for board members to take their eyes off cybersecurity when current events take precedence and raise new concerns. Even if 72% of board members feel comfortable with their understanding of cyber risk today, the modern landscape is constantly introducing new complexities and cybercriminals are not standing still. Other priorities should not overshadow cybersecurity, especially in our deeply interconnected world where systemic risk is a growing problem."

Lucia Milică Stacy, Policy Council & Board Member for National Technology Security Coalition

Cyber Risk Concerns by Industry

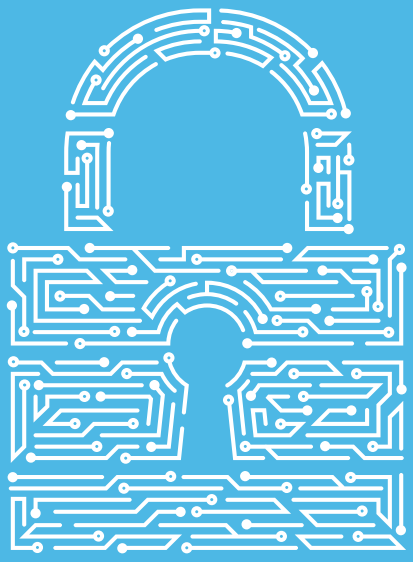
When considering the consequences of a cyber attack, concerns are relatively evenly split among sectors. Ultimately, board members share the view that service disruption, reputational damage and data loss are likely to be devastating whatever the industry.

In the worlds of IT, technology and telecoms, public sector and business and professional services, internal data being exposed topped the list of common concerns.

For the energy, oil and gas and education sectors, disruption to operations was the primary fear.

In healthcare and financial services, litigation costs and fines were top of mind.

And in more consumer-facing industries—such as media, leisure and entertainment, retail and financial services—reputational damage is, understandably, the biggest cause for concern.



Protecting people. Defending data.

The boardroom is under no illusion when it comes to the always hot topic of people risk. Just under two-thirds of board members (**63%**) and CISOs (**60%**) believe human error to be their biggest cyber risk. These figures are down a little since last year. Still, with user interaction integral to almost all successful cyber attacks, it is heartening to see this issue remains high on the agenda.

Despite an awareness of the risk posed by people, **72%** of board members believe that their users understand their role in protecting against cyber threats, a slight drop from last year's **76%**. However, CISOs are a little less confident, with only **61%** agreeing.

This slight disconnect is likely down to the CISO's more in-depth understanding of user-focused attacks. With more insight into behaviours and threat tactics, security leaders are acutely aware that even well-trained users can be duped or distracted into making a mistake.

Board members in Canada (**80%**), Japan (**75%**) and France (**72%**) feel strongest that human error is their organization's biggest cyber vulnerability.

Board members in France (**90%**), Singapore (**86%**) and Brazil (**85%**) are the most confident that the data within their organization is adequately protected.

Board members have much more confidence in their organization's ability to safeguard its data. Three-quarters believe company data is adequately protected; that's unchanged from last year.

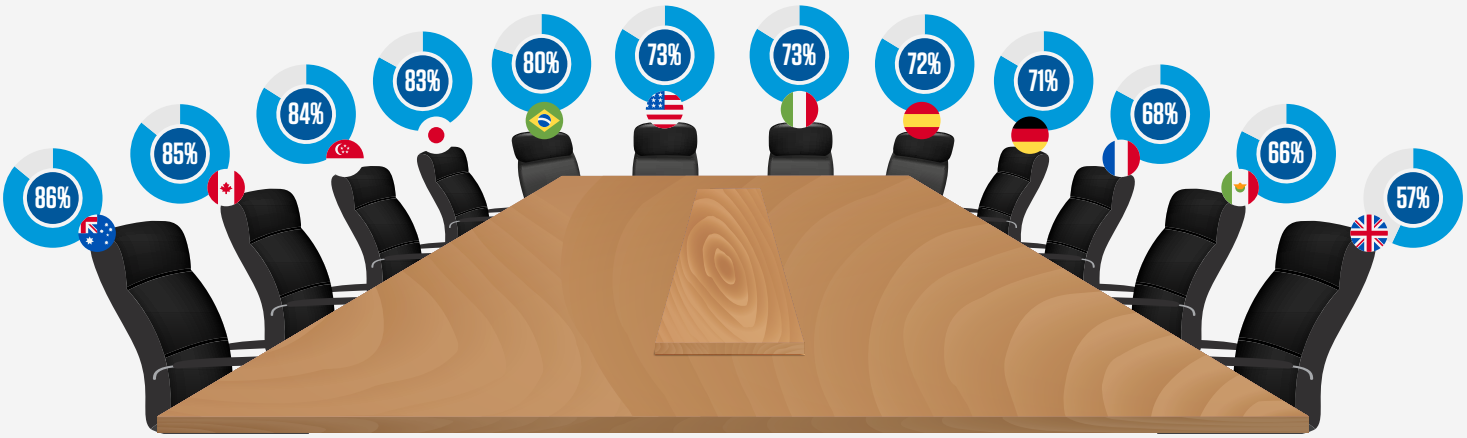
Once again, CISOs were less certain, with just **60%** in agreement. Boards may see information protection as something of a checkbox compliance exercise. CISOs are unsurprisingly much more aware of the many obstacles that stand in the way of achieving this goal.

Some CISOs may even see data loss prevention as a near-impossible task against a backdrop of staff turnover, remote working, cloud reliance, BYOD and third-party relationships.

Section 2: Cybersecurity posture and the boardroom

Overall, most board members feel positive about their cybersecurity posture. Three-fourths (**75%**) say they are comfortable making decisions on security issues affecting the business.

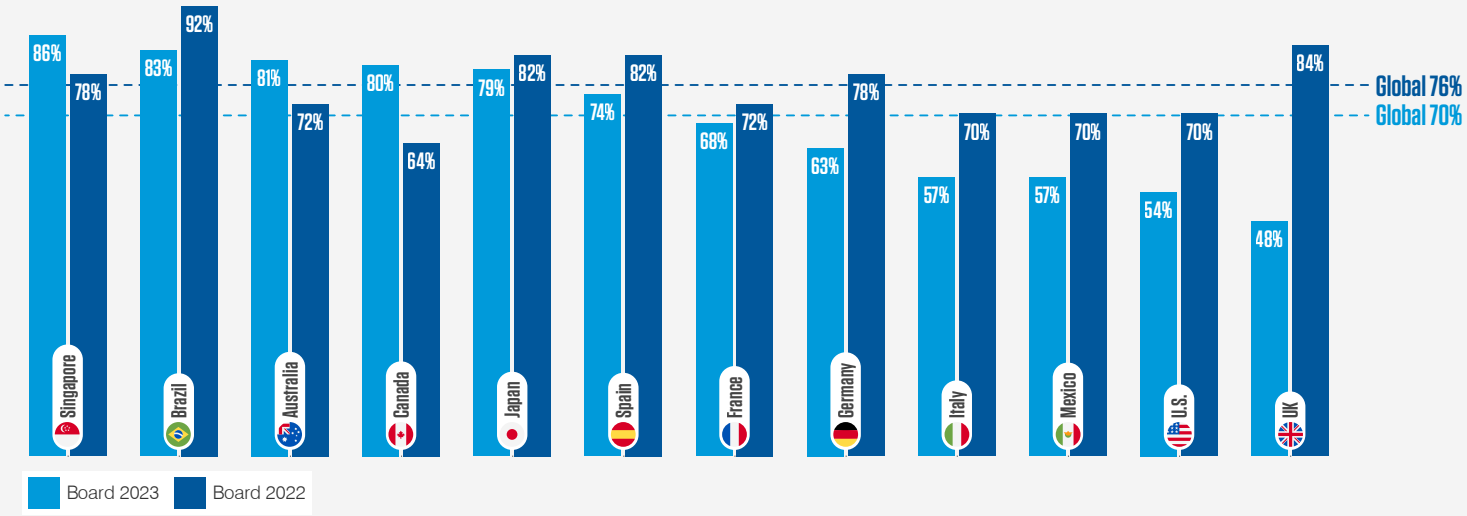
My board is comfortable making decisions about cybersecurity issues affecting the organization



The increasingly prominent role of the CISO looks to be behind this growing confidence. Almost three-quarters of board members say they sit on boards with at least one member who has some cybersecurity background. It should be noted that experience levels can range from CTO or CIO to those who have held senior positions in technology companies.

Sound budgets also look to have bolstered the boardroom's assessment of its cybersecurity posture. Most (**70%**) say their organization has invested enough in cybersecurity over the past 12 months. But this is down from **76%** last year, suggesting that a growing number of CISOs feel they need more resources in a fast-changing landscape.

Percentage of board members who agree that their organization has adequately invested in cybersecurity



Fortunately, for most, additional resources appear to be on their way. **Eighty-four percent** of board members believe that their cybersecurity budget will increase over the next 12 months. This is a promising indication that boards recognize the perpetual nature of cybersecurity. While most see budgets as adequate this year, they are still actively requesting and allocating more resources to keep pace with new threats and future-proof their defenses.

Elsewhere, boardroom confidence may not be reflective of the bigger picture. Most board members (**71%**) believe they understand the systemic impact of cyber risk, which, given the complex interdependencies that exist in most organizations, is rather unlikely. That said, board-level recognition that their organizations rely on many other systems, services and businesses can only be a good thing.

Cybersecurity budget increases are anticipated the most in Singapore (**97%**), Canada (**92%**), France (**92%**) and Spain (**92%**).

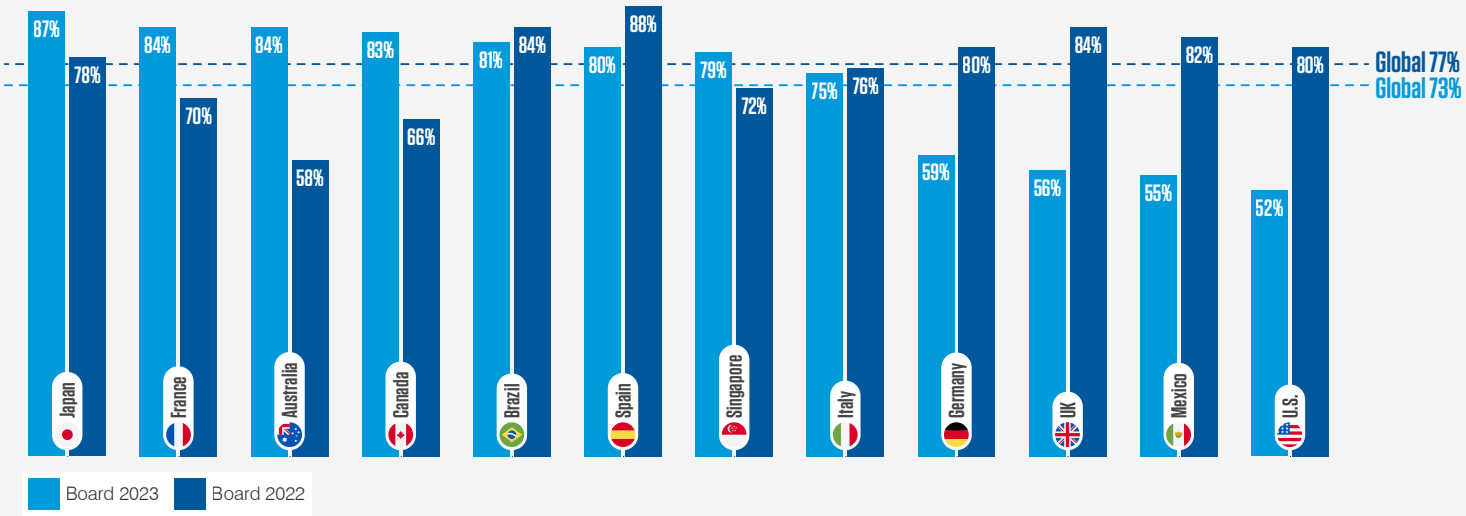
Board members in the business and professional services (**89%**), media, leisure and entertainment (**89%**), healthcare (**85%**), energy, oil and gas (**85%**) sectors are most likely to expect an increase in their cybersecurity budgets.

Board members in Singapore (**86%**), Brazil (**83%**) and Australia (**81%**) are most confident their organizations have adequately invested in cybersecurity.

A boardroom view of risk

Board members appear similarly comfortable on the topic of risk. Overall, **73%** agree that cybersecurity is a priority for their board. This is down slightly from **77%** last year, perhaps due to other concerns, such as economic uncertainty, taking precedence. Alternatively, cybersecurity may now be seen as less of a day-to-day priority as the impact of the pandemic continues to subside.

Percentage of board members who agree that cybersecurity is a priority for their board



Risk remains highest on the agenda in boardrooms in Japan (**87%**), France (**84%**) and Australia (**84%**). In the U.S., where the cybersecurity market is considered more mature, just **52%** of board members consider it a top priority. Perhaps board members have simply deemed security an integral part of "business as usual."

Most board members (**73%**) also feel that they monitor cyber risk levels well enough. They are comfortable that they have a named leader in place, see the relevant metrics and get an update from the CISO every quarter—similar to their interactions with the CFO. But whether this is adequate when up against a fast-moving and unforgiving threat landscape is debatable.

Likewise, most boards (**71%**) say they have a unique committee tasked with overseeing technology risks. Once again, this may not entirely match with reality. In most cases, such committees are overseen by finance professionals. In other words, an accountant is in charge of critical business decisions from a cyber risk perspective. Without a dedicated cyber committee, these decisions are often based on auditing and compliance expertise with a lack of operational insight.

A similar disconnect appears when it comes to prevalent threats. Again, most board members (**72%**) believe their board clearly understands the cyber risks they face. More likely, they have a firm understanding of their 5x5 risk matrix—and little grasp of the many complexities and nuances of modern cyber attacks. Still, with the right cybersecurity representation and guidance in the boardroom, this level of knowledge may suffice.

Cybersecurity: Boardroom Wish List

We asked board members what, if anything, would most improve cybersecurity at their organization. Most (**37%**) identified budget as the top factor that would improve cybersecurity. In the same vein, **35%** said they would like more cyber resources.

The same number of board members also suggested that better threat intelligence could help equip their teams to detect and deter cyber threats.

Around the world, board members in Japan (**49%**), the U.S. (**38%**) and the UK (**33%**) believe better technical controls would most improve cybersecurity. Board members in Italy (**45%**) and Singapore (**44%**) identified improved security awareness and culture among employees. And Canadian board members (**42%**) feel a more experienced CISO would lead to the biggest cybersecurity improvement.

We found a similar split across industries. Board members in the traditionally resource-starved education (**58%**) and public sectors (**46%**) requested a bigger cybersecurity budget. In comparison, those in transport (**54%**), media, leisure and entertainment (**40%**), financial services (**39%**) and manufacturing and production (**38%**) would prefer more cyber resources.

> *"Boards might have thought they were beginning to understand cybersecurity risk, but with the new SEC disclosure rules focusing on materiality as the incident disclosure trigger, a new and much deeper understanding of how the digital business creates value, and the unique cyber risks to that value, will need to emerge. The SEC is also requiring material disclosure of third-party incidents and risks, fast forwarding the issue of systemic cyber risk into governance and C-suite discussions. Disclosure will force boards and management teams to mature their processes, systems and understanding of risk impact in some fundamental new ways. We know SEC rulemaking tends to mature practices in the private sector and worldwide, so these new standards will have a global impact."*

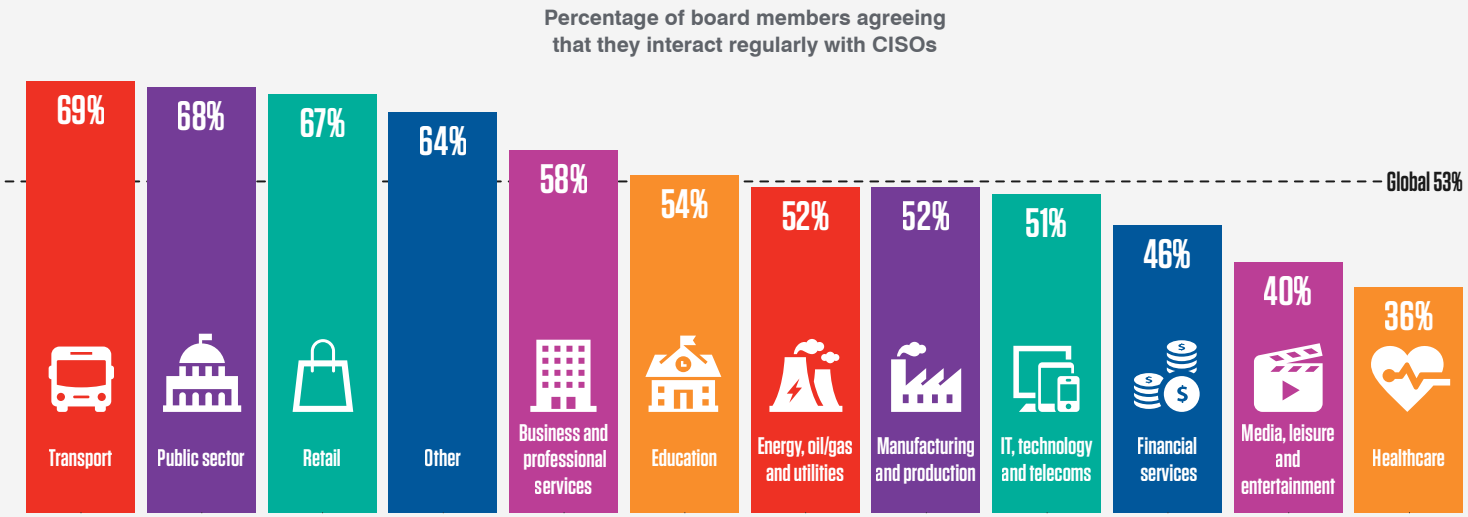
Bob Zukis, CEO & Founder, Digital Directors Network

Section 3: Communication, collaboration and CISOs in the boardroom

Increased cybersecurity representation at the board level must be seen as a huge step forward. But it counts for little if CISO voices are not being heard or, more importantly, understood. Fortunately, for most organizations, this does not appear to be an issue. But there is still much room for improvement.

Nearly a third of board members say they see the CISO only as part of a specific report or presentation. And just **53%** of board members say they regularly interact with their cybersecurity counterparts.

Though the latter figure is up slightly from **47%** last year, it still leaves around half of all boardrooms without strong CISO-C-suite relationships. That's a major detriment to a strong security posture. Regular interactions are vital to building trust and rapport because it helps ensure that cybersecurity voices are met by a receptive audience.

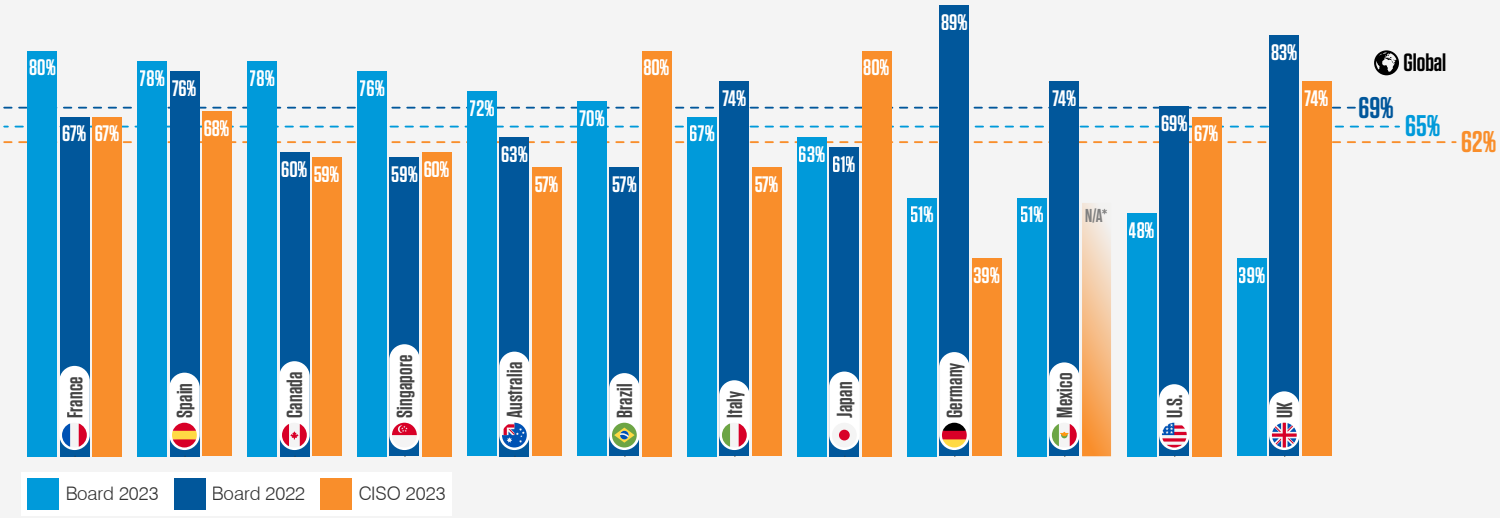


CISO presentations do appear commonplace in most organizations. Over two-thirds of board members (**69%**) say they regularly have such briefings, down slightly from **73%** last year.

But we saw signs of a fractured relationship in other areas. Just **64%** of board members say they understand cybersecurity matters well enough to have an informed discussion with the CISO. Given the volume and severity of cyber threats in recent years, this must be cause for concern. An in-depth knowledge of our industry cannot be expected from other executives. Therefore, the onus is on the CISO to ensure they are speaking the same language, delivering the right insight and always receptive to cross-boardroom conversations.

On a more positive note, when interactions do take place, they are largely good-natured. Just under two-thirds (**65%**) of board members say they see eye-to-eye and often agree with the recommendations of their CISO. A similar number (**62%**) of CISOs agree.

Percentage of board members and CISOs who agree that they see eye-to-eye with each other



Likewise, **67%** of board members feel that the CISO adequately supports them in cybersecurity matters.

Of course, it is promising that most CISOs and board members are aligned. But to ensure those on the front line of cybersecurity get the right support by those in control of the purse strings, they need a greater level of harmony. And bridging this gap is not just a task for the CISO. To ingrain a security culture from the boardroom to the rest of the company, CIOs and wider teams must fill in the gaps when CISOs are engaged in operational matters,

On the subject of improvement, board members believe the most effective steps CISOs can take to foster stronger boardroom relationships include:

- Explaining risk in business terms (**43%**)
- Tying security initiatives to business value (**43%**)
- Offering greater insight into threats (**42%**)

Board members in France (**80%**), Canada (**78%**) and Spain (**78%**) see eye-to-eye with their CISOs the most. The UK is lowest at **39%**.

CISO support is felt most strongly in Singapore (**81%**), Australia (**78%**) and Spain (**78%**).

The U.S. (**48%**) and Germany (**41%**) feel least supported by their CISO.

CISOs are comfortable raising concerns

Since Uber's former chief security officer was found guilty and sentenced to probation for his role in covering up a 2022 data breach,[9] personal liability has risen to the top of the CISO's mind. This year, **62%** cited the issue as a top concern in our *Voice of the CISO* survey.

They are not the only ones feeling the weight of this burden. A higher percentage of board members (**72%**) also expressed concern about personal liability in the wake of a cybersecurity incident at their own organization.

The issue is so high on the agenda that most board members report having conversations with their CISOs (**75%**) and CEOs (**73%**) about their exposure to personal liability. Naturally, CISOs and other board members are looking for assurances that they will be protected by insurance in the wake of a cybersecurity incident.

For the most part, CISOs are comfortable raising other important personal issues at the board level, too. Just over half of board members (**52%**) say CISO burnout has been raised as a concern. This awareness goes some way to highlighting the scale of the issue. But with **60%** of CISOs experiencing burnout in the past year, it appears some board members are not fully aware of their struggles.

CISO personal liability issues were raised with board members most often in Singapore (**86%**), Canada (**85%**) and Australia (**83%**).

CISO personal liability was most frequently raised before boards in the transport (**85%**) and media and leisure and entertainment (**82%**) sectors.

The issue of CISO burnout was raised with boards most frequently in Canada (**68%**), Germany (**61%**) and Japan (**57%**).

The leisure and entertainment (**64%**), public sector (**59%**) and education (**58%**) sectors also raised the issue of CISO burnout with boards more than most.

> *We are finally overcoming one of the biggest barriers to better organizational preparedness: the long-standing disconnect between board members and their CISOs. The two sides are warming to each other and are increasingly aligned on cybersecurity. This growing alliance is essential to driving real change, and it is encouraging to see that both directors and CISOs are committed to building stronger relationships.*

Zafar Chaudry, SVP – Chief Digital Officer, CIO & Board Director, Seattle Children's Hospital

9 U.S. Department of Justice. "Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records." October 2022.

Conclusion: Much progress–but no time for complacency

Overall, CISOs and board members are working much more closely than ever before. This progress offers hope that boardroom perspectives on cybersecurity are shifting from a necessary compliance task to an enabler that can help to shape business strategy.

The strengthening of this relationship also appears to be boosting boardroom confidence around cybersecurity. Despite concerns about impending attacks and lack of preparedness, board members say they feel comfortable and in control of their security posture.

On the surface, at least.

Most say they understand the risks they face, are happy with investment levels and have good relationships with their CISOs. This may be because board members are more comfortable with the day-to-day presence of cybersecurity and feel more in tune with security struggles following the disruption caused by the pandemic.

But boards cannot afford to get complacent. While it's natural that board members feel reassured by the presence of a C-level security professional, they must be sure that any assurances are warranted. This is only possible by undertaking an honest assessment of the cybersecurity capabilities in the boardroom and beyond.

The reality is most will be found lacking. So rather than falling into a false sense of cybersecurity, board members must actively take steps to plug gaps in their knowledge and company defenses. Here are just a few steps that can help improve your cyber strategy and security posture:

- Ensure that cybersecurity is high on the agenda every time the board meets. This will give the function regular visibility and underline its importance in the day-to-day running of your business.
- Prioritize regular interaction between the board, CISOs and other security leaders. The stronger and more open these relationships, the easier it is to align cybersecurity planning and decision-making.
- Make sure everyone understands their cybersecurity responsibilities. This means mandated, companywide security awareness initiatives and regular reviews of security budgets, resources and technology.

Ultimately, security leaders and their fellow board members are united by a shared objective—ensuring the long-term success and stability of their organization. But to achieve this aim, the board must be willing to support CISOs as they deliver the business-focused strategy and insight needed to respond to the cyber challenges of today—and tomorrow.

> *"Boards are demonstrating their commitment to their fiduciary duty to ensure their organizations are cyber resilient. They feel good about the time and resources they are investing into their understanding and managing of cyber risk. However, their struggle to translate this awareness into stronger security posture indicates directors still have much work to do. The strengthened relationships with CISOs can serve as a catalyst for improving their organization's resilience, now that the two sides are speaking the same language. With even greater challenges ahead, maintaining a laser-sharp focus on cybersecurity remains critical."*

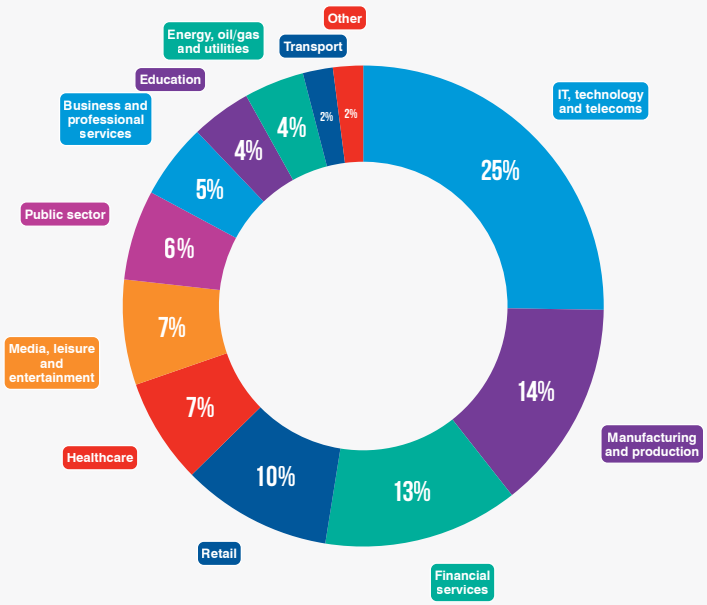
Hon Clare O'Neil MP, Minister for Home Affairs, Minister for Cyber Security, Member for Hotham—Australia

Methodology

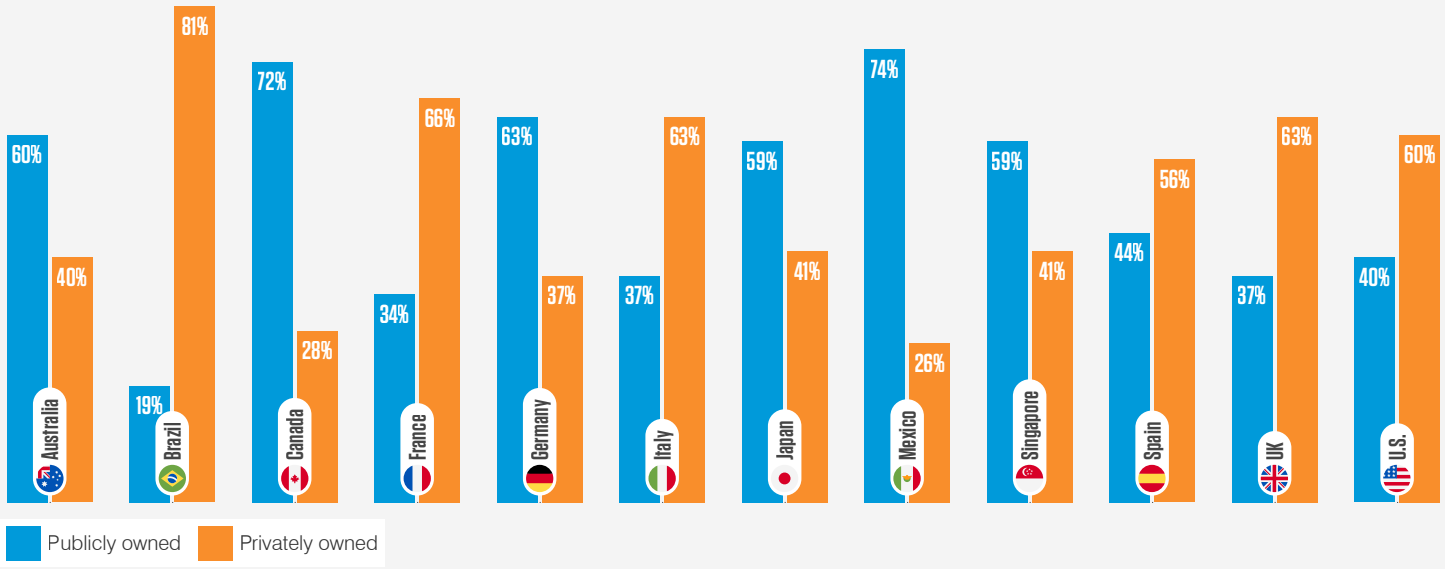
The Proofpoint Cybersecurity: The 2023 Board Perspective survey, conducted by research firm Censuswide between June 9 and June 19, 2023, surveyed 659 board directors from organizations of 5,000 employees or more across different industries in 12 countries. More than 50 board directors were interviewed in each market, which includes the U.S., Canada, UK, France, Germany, Italy, Spain, Australia, Singapore, Japan, Brazil and Mexico.

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

Within which primary sector is your organization?



Is your organization publicly or privately owned?



LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 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**.

proofpoint.

0401-003-01-01 09/23