proofpoint.

Cybersecurity at MIT Sloan

REPORT

Cybersecurity: The 2022 Board Perspective

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

proofpoint.com

Table of Contents

Cybersecurity From the Top: The Board Perspective 4
Section 1: A boards-eye view of the threat landscape 5
Section 2: Cybersecurity posture and the boardroom 10
Section 3: Examining the CISO's relationship with the boardroom 13
Conclusion: Actionable Insights for Board Members 16
Methodology 17

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 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.

Cybersecurity at MIT Sloan (CAMS)

Cybersecurity at MIT Sloan (CAMS) is an interdisciplinary research consortium headquartered in the Sloan School of Management at MIT. In collaboration with researchers from departments around MIT and beyond, CAMS addresses the important need to improve the cybersecurity of all organisations through an interdisciplinary research approach focused on the strategic, managerial and operational issues related to cybersecurity. CAMS brings together thought leaders from industry and government with MIT faculty, researchers and students. The research consortium delivers its findings and actionable insights through published research papers, high-impact managerial outlets and a variety of meetings, workshops, conferences and educational activities. Find CAMS research in Harvard Business Review, Sloan Management Review, The Wall Street Journal, The New York Times and many other publications. Members of CAMS, whose support funds the research and who have first access to the findings, include companies from many different industries including financial services, energy, chemicals, healthcare, industrial automation, manufacturing, information services, natural gas, utilities and more. Please visit us at https://cams.mit.edu.

Cybersecurity From the Top: The Board Perspective

Not long ago, few boards of directors knew much about cybersecurity risks, let alone took an active interest in the topic. That mindset has changed dramatically in recent years. But as this report shows, we still have some way to go.

Overall, board members are confident they understand the threat landscape, prioritise cybersecurity appropriately and have invested enough to keep their organisations safe. Still, in light of rising rates of cyber attacks and differing and sometimes conflicting opinions among CISOs, this optimism may be misplaced.

Bridging the disconnect is vital. CISOs and the wider board need open lines of communication. But often, boards are relentlessly focused on the bottom line and CISOs mired in technical language. Over time, effective business-first communication gives way to muddled perceptions and misaligned priorities.

At a time when we are more connected and digitally reliant than ever, this board-CISO relationship has never been more important. It has also never been more challenging. To protect people, defend data and ensure continued organisational success, CISOs must communicate effectively with their boards. That means putting threats in perspective, fostering collaboration and driving accountability. At the same time, board members need to work to understand how cybersecurity risks can affect their organisations' business goals.

To explore the situation further, Proofpoint commissioned a survey of 600 board members at organisations with 5,000 or more employees across 12 countries: the U.K., the U.S., Canada, France, Germany, Italy, Spain, Australia, Singapore, Japan, Brazil and Mexico. Working with researchers at MIT Sloan's research consortium, Cybersecurity at MIT Sloan (CAMS)[1], we analysed the responses and summarised the insights. We also compared some of the results to corresponding findings from our recent Voice of the CISO Report. We hope these insights help shine a light on how well CISOs and the wider board understand each other.

This report would not have been possible without the participation of board members around the globe as well as our coauthors and research partners at CAMS. Thank you for your valuable support, insights and feedback.

Lucia Milică, Global Resident CISO at Proofpoint

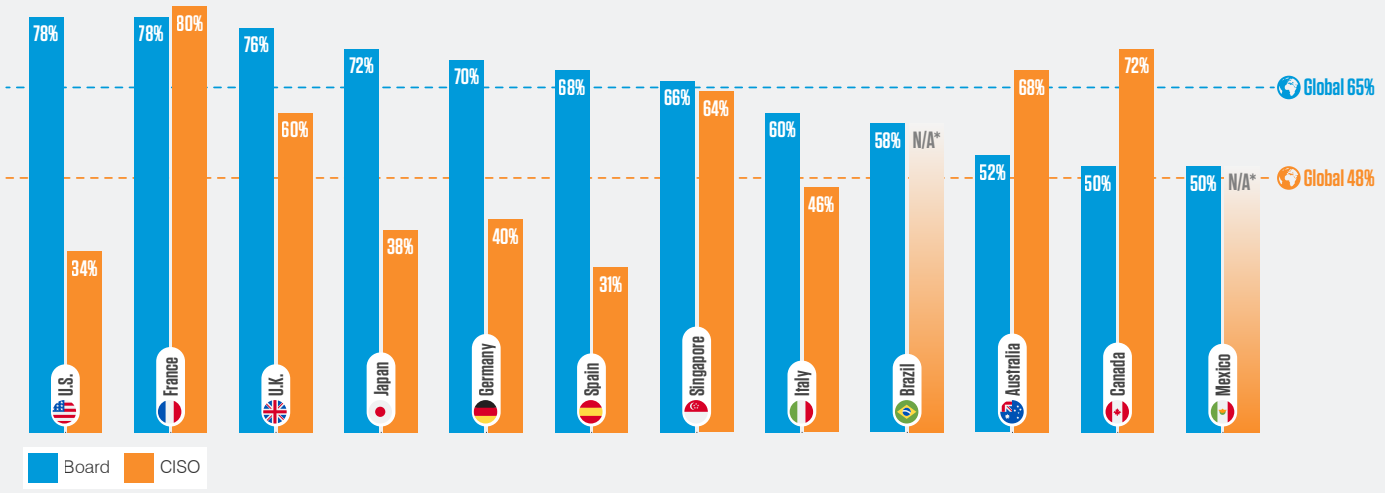
1 https://cams.mit.edu/

Section 1: A boards-eye view of the threat landscape

Like any effective cybersecurity strategy, investigating the board perspective must start by assessing the threat landscape. Just under two-thirds of board members believe that their organisation is at risk of a material cyber attack. This figure drops to **23%** for those who believe the risk is very likely. These figures suggest a boardroom that is at least somewhat aware of the risk posed by today's sophisticated cyber criminals.

But we see a worrying disconnect when we compare these results with our 2022 Voice of the CISO Report (VOTC). Asked the same question earlier this year, just under half of CISOs felt they were likely to experience a material cyber attack within the next year, and **14%** rated the risk as very likely. This disconnect held true around the world, with boards in many countries out of step with their corresponding CISOs.

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



*Brazil and Mexico were not surveyed in the 2022 Voice of the CISO report.

Significant discrepancies emerged within industry sub-sectors, too. Board members in the financial services (**73%**), IT (**73%**) and manufacturing (**70%**) sectors believe they are at a higher level of risk than do their CISOs, who agreed **45%**, **56%** and **54%**, respectively.

That board members and CISOs are not on the same page when it comes to risk may not be surprising, but it is certainly very telling. Most CISOs know too well the difficulties of obtaining buy-in for cybersecurity projects. This difference in perceived threat levels is a significant barrier to the united front that is essential for a successful cybersecurity defence.

"Board members have fiduciary and oversight responsibility for their organisations; therefore, they must understand the cybersecurity threats their organisations face and the strategy their organisations take to be cyber resilient. By virtue of their role in the organisation, board members can have tremendous impact on cybersecurity posture, and our report illustrates that they take this responsibility seriously."

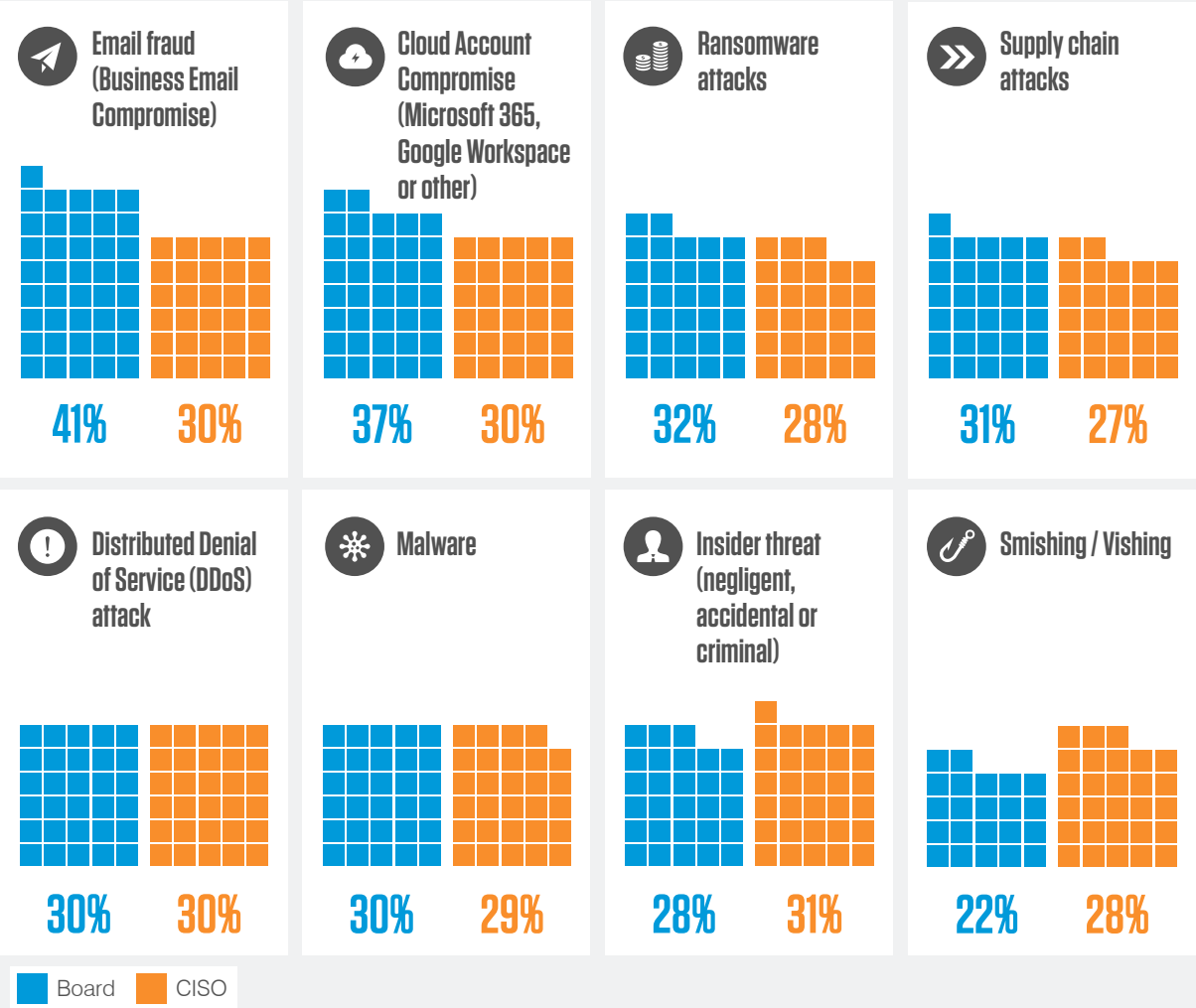
Dr. Keri Pearlson, Executive Director, Cybersecurity at MIT Sloan (CAMS)

Understanding threat actors

There are positives to take from board awareness of cyber attacks more generally. But it matters little if the C-suite does not also understand from where these attacks are likely to originate. That said, there is cause for optimism; board members and CISOs agree on the top concerns.

Surveyed board members rate email fraud and business email compromise (BEC) as their top concern (**41%**), followed by cloud account compromise (**37%**) and ransomware (**32%**). This tracks closely with the concerns of CISOs, who also rank email fraud/BEC and cloud account compromise as top concerns (along with insider threats and DDoS attacks). Notably, board members and CISOs do diverge in one important area: insider threats were not a top concern for boards, but the No. 1 concern for CISOs.

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)



Most of these threats involve email—board members and CISOs alike are rightfully worried about them. Not only is email the No. 1 threat vector for all forms of cyber attack, but it is also the area with most scope for human error. No email protection is 100% failsafe. Some threats will reach the inbox; when they do, your people form the last line of defence. Just one errant click, rushed reply, or malicious download can have severe consequences for your organisation.

Analysing the data by country and industry highlights the differences in board members' perception of the biggest cybersecurity threats.

9 out of 12 surveyed countries consider email fraud/BEC one of the biggest three risks, with Spain (**54%**), Mexico (**54%**) and the U.K. (**52%**) leading the way.

8 out of 12 surveyed countries consider Cloud Account Compromise one of the top 3 risks, with Germany (**50%**) and Japan (**38%**) rating it the highest.

Supply chain attacks are the top concern for board members in France and Singapore.

Ransomware attacks are the top concern for board members in Canada.

Email fraud is the top concern for board members at organisations across retail, IT/tech/telecom, education, healthcare, media/leisure and public sector. For those in financial services, manufacturing and energy/oil/gas, cloud account compromise tops the list. The transport sector is by far most concerned about supply chain attacks.

Assessing preparedness

Most board members are aware of the risk of cyber attacks in the near future. But how has this translated into preparedness? CISOs and board members are aligned here—but the news is not exactly cause for celebration. 47% of all board members believe that their organisation is unprepared for a cyber attack, and about the same amount of CISOs agree.

The alignment between board members and CISOs is relatively positive news, but their level of preparedness is of greater concern. Are only half of the world's organisations really prepared for a material cyber attack? If so, what are they doing that the other half is not? And are they focusing on resilience or just protection? Are they actively and regularly training all users on what to do both to prevent and respond in the case of an incident?

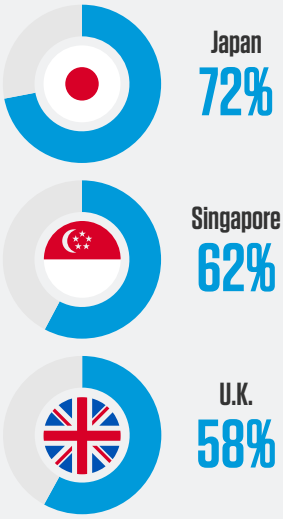
These are all certainly possible. But if anything, it seems more likely that they are underestimating today's sophisticated threats. They are likely focused primarily on protective measures, not ready to respond properly in the event of an attack. They may even have deemed the cyber attacks as "cost of doing business," without fully understanding either the risk or the impact to the bottom line.

This misplaced sense of confidence continues when it comes to data loss. Overall, three-quarters of surveyed board members believe that their organisation's data is adequately protected. Those in the U.S. (**88%**), Spain (**88%**) and Brazil (**86%**) are the most confident. On the other hand, most also consider data loss a top concern, suggesting somewhat less faith in their data protection and recovery capabilities.

Many also see data protection as an area in need of bolstering, with **75%** of board members citing information protection and data governance as a top priority. Those in Brazil (**92%**), Japan (**86%**) and France (**84%**) agree with this sentiment the most.

How prepared do board members feel they are to cope with a targeted cyberattack in the next 12 months?

Top 3 Countries Least Prepared



CISOs feel least prepared in Australia, U.K. and Germany.

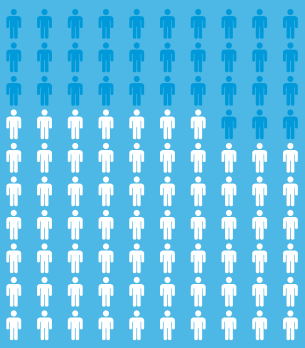
Board members in the education sector feel the least prepared (**62%**). Those in energy/oil/gas and transport (both **23%**) feel most prepared.

Spotlight on: The people problem

Despite some overconfidence in how prepared their organisations are for a potential cyber attack, board members are under no such illusions when assessing their biggest risk factor: human error. Two-thirds (**67%**) believe human error is their biggest cyber vulnerability. That this is most keenly felt in traditionally stricter corporate cultures such as Germany (**80%**), France (**78%**) and Japan (**74%**) shows just how aware the world's boards are about the role of people in cybersecurity.

Controls, perimeter defences and technology alone are not enough. With **82%** of successful cyber attacks involving the human element[2], our people are on the front line—and boards must protect them accordingly.

Statistics show that most cyber attacks happen because of some type of human error. That means making sure people throughout the organisation, including board members, know what to watch for and what to do should they encounter a questionable email, link or website. Board members have both a personal and professional role to play. They, too, can be targets of cyber criminals who want to get into companies. Board members also have an oversight role to play as they evaluate the plans CISOs put forth to manage this problem.



67%

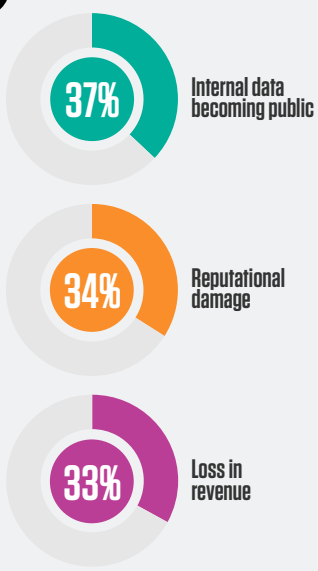
believe human error is the biggest cyber vulnerability.

Counting the consequences

Board members were mixed when asked about the consequences of most concern. When asked about their greatest concerns in the event of a cyber incident, they ranked internal data becoming public (**37%**), reputational damage (**34%**) and loss in revenue (**33%**) at the top. Board members' top concerns clearly reflected their focus on their broader oversight and fiduciary responsibility for the entire organisation.

While these are undoubtedly valid concerns, they are not the same as those cited by CISOs in our earlier report. As outlined in Voice of the CISO, significant downtime is the number one concern of CISOs (**37%**), followed by disruption to operations and impact on business valuation (**36%**). Operational downtime hits revenue streams and customers in direct and immediate ways.

Top concerns of board members in the event of a cyber incident.



Around the world, the U.K., Canada, France and Singapore view the impact of a material cyber attack on their organisation's reputation as the most pressing concern.

In Italy and Spain, loss in revenue is the most pressing concern.

Significant downtime is top of mind for those in Germany and Australia.

Internal data becoming public was the top concern for board members at IT/tech/telecom, healthcare, manufacturing, media/leisure and public sector organisations.

Significant downtime is of most concern to transport and retail, while disruption to operations worries financial services, business and professional and energy/oil/gas.

2 Verizon. "2022 Data Breach Investigations Report." May 2022.

This difference of opinion, of course, comes from the different perspectives each role brings to the organisation. CISOs primarily see their role as keeping attacks from disrupting the business and as enabling the business to continue to function despite cyber attacks. At public organisations, however, board members represent shareholders. They are most concerned with protecting the value of their investments, which can decline when the organisation suffers in reputational damage or lost revenue. Remarkably, the board members' concerns varied by country and industry.

On the regulations front, a resounding majority of board members (**80%**) believe that organisations should be required to report a material cyber incident to the government within a reasonable timeframe. Just **6%** disagree.

This is a stark contrast to conventional wisdom that reporting is more detrimental to reputation, potential fines and litigation than holding off. The finding suggests that boards are now much more willing to work together with regulators. Boards in Brazil (**92%**), the U.K. (**90%**) and the U.S. (**86%**) feel this most keenly. Agreement is at its lowest in Australia (**50%**).

Board members at organisations in the media/leisure (**88%**), IT/tech/telecom (**87%**) and manufacturing (**85%**) sectors were most supportive of a reporting requirement. The least supportive are energy/oil/gas/utilities (**58%**).

Almost **9 in 10** (**88%**) respondents whose organisation is privately owned agree with reporting requirements compared with more than **7 in 10** (**71%**) whose organisation is publicly owned.

"Board Directors have not only realised the importance of cyber risk, but are spending more time with their CISOs recognising the risk posture and more importantly, understanding the incident response plan."

Julie Cullivan, Board Director

Section 2: Cybersecurity posture and the boardroom

Despite a level of misplaced confidence, board members are at least aware of the risks posed by cyber threats. Most also understand the pivotal role that their people play in these threats achieving success. Many also appear to recognise the systemic impact of cyber (third party risk, supply chain and people), with **75%** agreeing they have such an understanding.

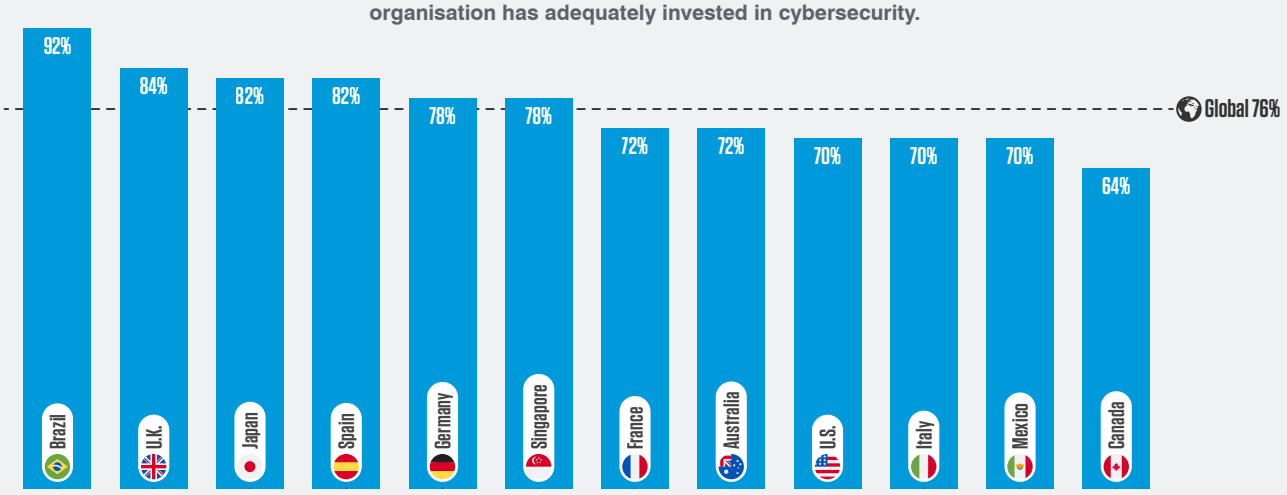
But while it is tempting to take this finding at face value, there is likely more here than meets the eye. Board members may indeed understand systemic risk in that they know what it entails. But their views on the impact of cyber threats on their organisations suggest they don't fully appreciate its consequences. Systemic risk has the potential to cause such widespread damage that private information becoming public and reputational impact would likely be the least of the board's concerns. Should an attack happen, getting the organisation back into operation quickly and effectively would likely take precedence.

Brazil (**88%**), Spain (**88%**) and the U.K. (**84%**) are most confident in their boards' understanding of systemic risk.

Canada (**56%**) and Australia (**54%**) are the least confident.

We found a similar level of confidence in budget levels. A clear majority (**76%**) of board members feel that their organisation has made adequate investments in cybersecurity. The interesting follow up for this question is how the respondents define "adequate investments."

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



Board members likely feel that their organisation's investment is adequate because they have not experienced a cyber incident. Any cyber defence is good enough—until the moment it isn't. The conventional approach is to invest in multiple layers of protection under the misguided assumption that the more layers of protection in place, the better.

"Adequate investment" could imply that protections are in place, but that detection, recovery and response may still be lacking. Or it could mean that organisations have invested in technologies but fall short in organisational protections such as training and awareness. Regardless, a continued feeling of adequate investment will require increasing investment over time to ensure new vulnerabilities and threats are properly managed, and resilience continues to be a high priority.

Board members feel strongly that their companies have adequately prepared employees in ways that increase cybersecurity. Just over three-quarters (**76%**) of board members reported that they believe employees understand their role in protecting their organisation against cyber threats. This is surprisingly high, given much evidence to the contrary. Our research has repeatedly found that most users do not know what is expected of them in a breach. And only **57%** of organisations run company-wide security awareness training programmes[3].

Board members in Brazil (**92%**), the U.K. (**82%**) and Germany (**80%**) are most in agreement that employees understand their role in protecting the organisation against cyber threats.

Keeping cybersecurity on the agenda

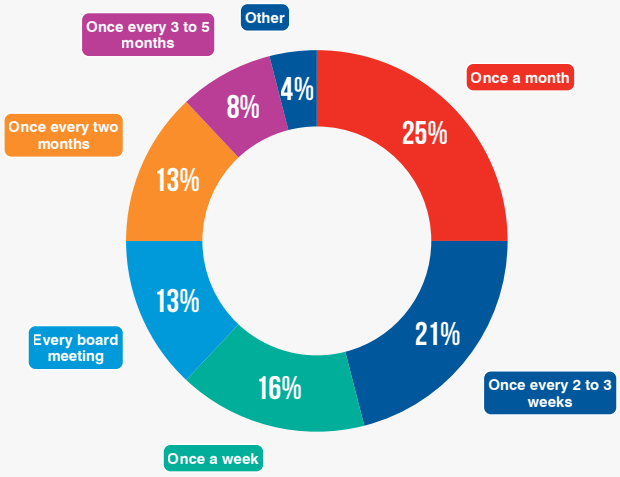
When pitted against rapidly evolving and increasingly sophisticated threats, cybersecurity is never simple. Protections must be adapted to the threats of the day, and the organisation must continually educate, motivate and reward their people for their role in keeping things secure.

The good news is most board members reported keeping the issue of cyber defence regularly on the agenda. Of those surveyed, **76%** said they discuss security matters at least once a month. This is encouraging. But given the daily barrage of threats facing most organisations, it may not be enough.

Privately owned companies are more likely (82%) than publicly owned companies (70%) to discuss cybersecurity matters at least once a month.

The greater concern is the **24%** of businesses failing to discuss this important topic on a regular basis. When a board takes notice and makes cybersecurity a priority, there is a trickle-down effect throughout your organisation. Every level of the organisation begins to make security a priority, and that builds and strengthens a culture of cybersecurity. A stronger culture builds a hardier defence against cyber threats.

How often does your board discuss cybersecurity matters?



76% discuss security matters at least once a month (including 1% more often than once a week)

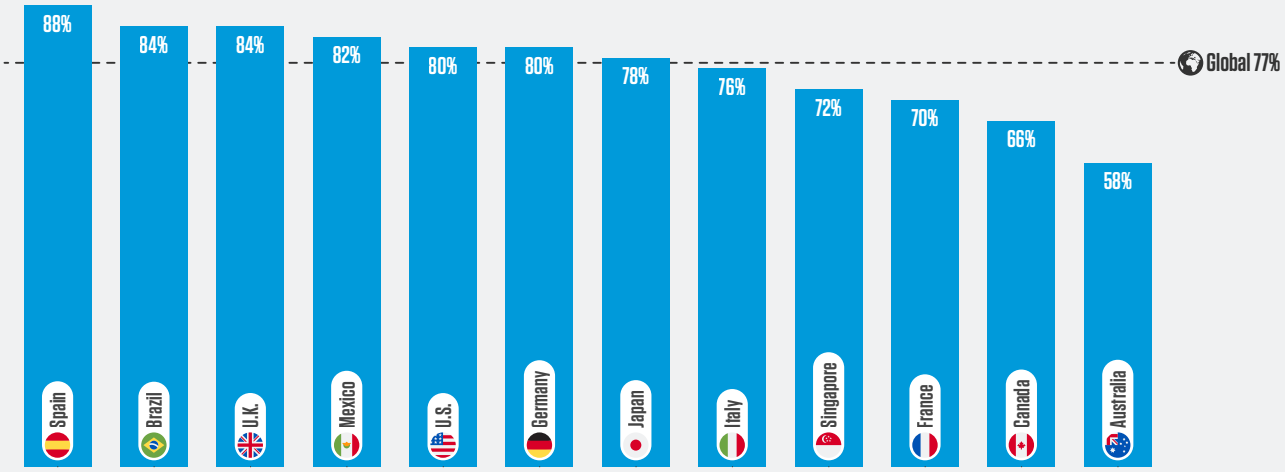
Privately owned companies are more likely (**82%**) than publicly owned companies (**70%**) to discuss cybersecurity matters at least once a month.

Similarly, most (**77%**) board members believe cybersecurity is a top priority for their board. While the voice of cybersecurity has been growing louder in the boardroom for some time now, this figure is auspiciously high. The frequent cybersecurity events of the past few years, especially the large number that have made headlines, have put pressure on executives and dramatically highlighted cybersecurity's critical role in protecting organisations and keeping them operating. It is encouraging to see this urgency being reflected at the board level.

Board members in Spain (**88%**), Brazil (**84%**) and the U.K. (**84%**) reported the highest level of agreement that cybersecurity is a top priority. At the other end of the scale, just **58%** of Australia's board members agreed with this statement. The overall percentage tracks with the finding that nearly three-quarters of survey respondents sit on boards where at least one member has cybersecurity expertise. Organisations that prioritise cybersecurity are also likely to support that commitment with cybersecurity expertise in the boardroom.

3 Proofpoint. "2022 State of the Phish Report." February 2022.

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



Boards in Brazil (**90%**), the U.K. (**84%**) and Germany (**82%**) are the most likely to have at least one member with cybersecurity experience.

The U.S. and Canada are least likely to have at least one board member with cybersecurity experience. Both were reported at **62%**.

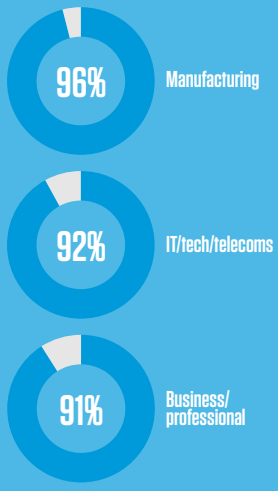
Globally, **73%** of boards have at least one member with cybersecurity experience.

In further good news, almost three-quarters of boards have received some form of training on how to respond to a cyber incident. Still, it bears repeating that this is of little use if that training is not carried out on a regular basis. Security best practice is like muscle memory. It must be forged over time through repetition so that it can be reliably called upon when required. The more it is exercised, the stronger the muscle.

Spotlight on: Budget

A considerable majority (**87%**) of board members expect their cybersecurity budget to increase over the next 12 months, while just **5%** expect a decrease. The U.S. (**98%**), Germany (**96%**), Spain (**94%**) and Brazil (**94%**) have the highest levels of expectation, while it is at its lowest in Australia (**66%**), where **22%** also expect budgets to go down.

Because most respondents feel their organisations have adequately invested in cybersecurity, this finding suggests that board members know that they cannot sit still. The threat landscape is constantly evolving and cyber defences must follow suit.



Board members in the manufacturing (96%), IT/ tech/telecoms (92%) and business/professional (91%) sectors are most likely to expect an increase in their cybersecurity budgets.

Public sector and energy/ oil/gas/utilities (73%) are the least expectant.

Section 3: Examining the CISO's relationship with the boardroom

With cybersecurity now front-page news, the role of the CISO has taken on greater prominence in most organisations. 90% of board members responded that they have a CISO in their organisation. Where once boards perceived their CISO to have limited remit—defend against cyberattacks—the role is now rightfully regarded by many as more of an enabler to uninterrupted mission-critical operations. That recognition, in turn, has elevated this role from security infrastructure overseer to business partner.

More surprising, however, is that **10%** of businesses of size do not have a dedicated CISO overseeing cyber strategy. The respondents in this study were all from organisations with more than 5,000 employees—every one of them should have a cybersecurity leader.

100% of respondents in Mexico said their company has a CISO, followed by 98% in Brazil, the U.S., Singapore and Spain. The lowest level of CISO representation on the board is in Australia (70%).

Board-CISO relations

Interaction between CISOs and their board appears to be an area for attention and improvement. Just half of board members regularly interact with their CISO; around a third say they see the CISO only when the latter is presenting to the board. While **73%** say these presentations occur regularly, this may not be enough. Bringing the CISO into the boardroom on a regular basis, and not just for presentations, shows that cybersecurity is a priority of the board. As addressed earlier in this report, board priorities have a trickledown effect on the entire organisation.

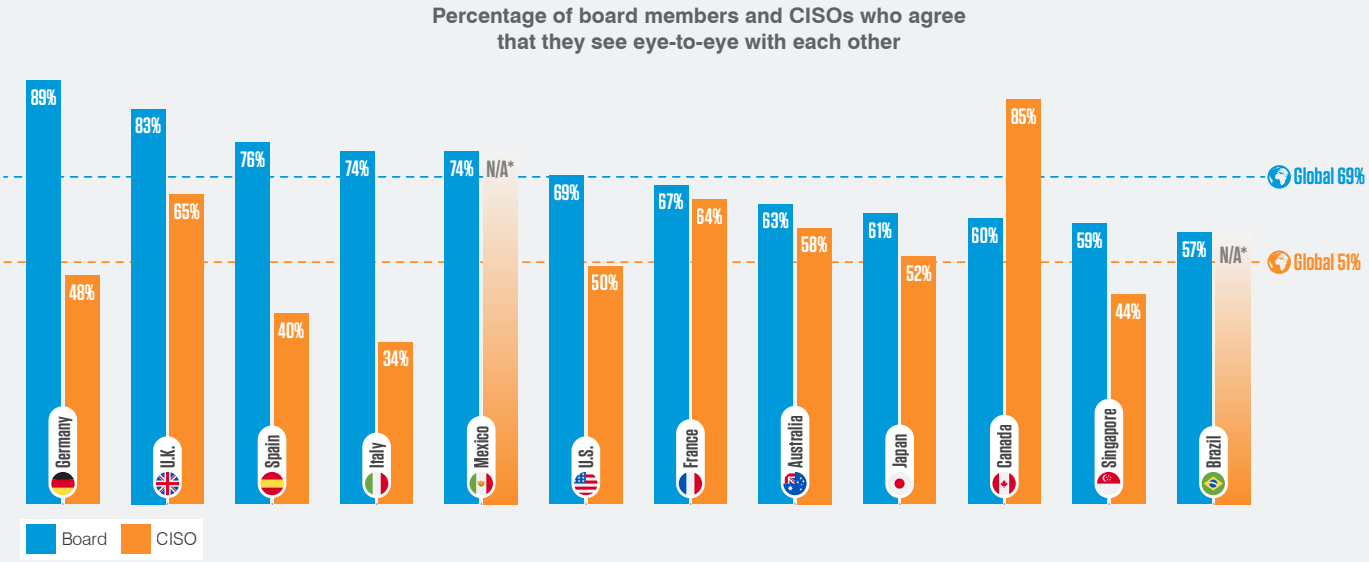
Regular CISO interaction with the board is highest in Italy (**67%**), Germany (**59%**) and the U.K. (**55%**). It is lowest in Mexico (**26%**).

Board members can show their commitment to keeping the organisation secure with greater interaction with their CISOs. Board meeting reports and presentations are just the beginning. Ask questions of your CISO. Follow up on headlines or news reports of breaches in other organisations with questions about how that type of breach might happen in your organisation. Find other ways to personally support the CISO and the mission. These efforts will increase the likelihood that the rest of the organisation makes cybersecurity a day-to-day priority.

Board members and CISOs do not always see things the same way. While over **two-thirds** (**69%**) of board members say that they see eye-to-eye with their CISOs, just **51%** of CISOs feel the same way. Underpinning this disconnect could be the finding that only **67%** of board members believe they understand cybersecurity matters well enough to have an informed discussion with their CISO. Or it could be related to the unique focus of each role (as mentioned earlier in this report). Often, CISOs report on statistics about security protection that are too technical or not focused on the business metrics that matter most to board members.

"A clear message stands out for CISOs. While their cyber technical expertise is highly valued, the board also greatly values the CISO's ability to translate their technical aptitude into a risk management context and conversation."

Bob Zukis, Founder & CEO, Digital Directors Network



*Brazil and Mexico were not surveyed in the 2022 Voice of the CISO report.

Both board members and CISOs can help close this gap. Boards must take steps to keep cybersecurity on the agenda. The CISO, meanwhile, must deliver concerns and recommendations in a business-first-manner. For example, board members are less interested in threat detection metrics than in how threat detection can affect revenues and reduce business risk. CISOs should avoid jargon and overly technical language and instead speak the language of the board and the business. Then they will be seen as business partners who understand the broader impact of their work and respected colleagues of their executive peers.

Board members in Germany (**89%**), the U.K. (**83%**) and Spain (**76%**) see eye-to-eye with their CISOs the most. Relations are at their lowest in Brazil (**57%**).

"The board and CISO relationship is entering a new phase and has never been more important. The rapidly evolving cyber risk environment and proposed regulations are transforming boardroom cybersecurity expertise. As a result, the role of the CISO is evolving away from technical specialist to business executive who can understand where business value is coming from and articulate to the board how to protect it."

Betsy Wille, Director, The Cybersecurity Studio (former Abbott CISO)

What do boards expect of their CISO?

The traits most desired of the CISO by their boards differ depending on location and industry. But in general, board members reported that they most value cybersecurity experience (**49%**), technical expertise (**44%**) and risk management (**38%**). These findings suggest a heavy focus on protection over resilience.

Technical expertise is, of course, an essential requirement when making technology purchasing decisions. But when it comes to keeping an organisation operational in the face of a cyber attack, CISOs also require a broader understanding of business management. Elevating board member expectations of the CISO will help build more meaningful, business-focused relationships.

5 out of 12 countries consider cybersecurity experience to be the most valuable skill in a CISO, with the U.S. (**64%**) and Brazil (**62%**) leading the way.

5 out of 12 surveyed countries consider technical expertise to be the most valuable skill in a CISO, with Spain (**56%**) and the U.K. (**54%**) rating it the highest.

Communication skills are seen as most valuable for CISOs in Japan and Australia.

Cybersecurity experience is the most desired CISO skill for board members at organisations across IT/tech/telecom, education, financial services, manufacturing, media/leisure, business/professional and transport.

Conclusion: Actionable Insights for Board Members

Only two-thirds of board members believe their organisation is at risk of a material cyber attack, and even less than that believe the risk is very likely. Board members in most countries had markedly different perceptions of cyber risk than their CISOs, indicating a large opportunity for discussion between these two very important players in an organisation's cybersecurity leadership. These conversations must take place regularly and in the language of business, rather than the tech jargon of security.

Board members' top concerns around the source and impact of cyber attacks indicate an understanding of the high risk that human error plays in creating vulnerabilities for their organisation. The CISO and other operational leaders have the ultimate responsibility to put programmes and culture in place to drive the behaviours of their employees. But board members have two roles to play here, too. One is as a member of the organisation—board members must personally adhere to the organisation's protocols around minimising human risk. But the second is as a role model. The more the board makes cybersecurity a priority, the more other leaders will do the same. That trickles down throughout the organisation. See it as an opportunity to supercharge the cybersecurity culture and change the dialogue from something the security team must do to something everyone must do. Every single person plays a part in keeping the organisation secure.

Board members also can improve their organisation's defensive posture by keeping cybersecurity front and centre on their agenda. They can help their CISOs become business partners instead of security infrastructure overseers. Here are just a few key ways the board can help improve their organisation's security strategy for both protection and resilience:

- Elevate cybersecurity to an agenda item every time the board meets. Placing this on the board agenda will keep it a high priority item with needed regular visibility.
- Create a customised board dashboard of relevant metrics to show areas of success and areas in need of improvement. The ability to regularly view important business and cyber metrics will help board members understand the trends their organisation experiences as well as see progress from cyber investments over time.
- Build cybersecurity muscle so everyone knows how to protect from and respond to an incident. Board members want to understand their role in the event of an incident, and conducting regular table top exercises will teach them how to respond.
- Regularly interact with cybersecurity leadership to build stronger relationships between the board and cyber leaders. The more familiar they become, the more likely they will begin to see eye-to-eye and align their priorities around the most important cybersecurity decisions.

After all, keeping the lights on is everyone's priority and board members just want to ensure that cybersecurity risk is properly managed so their organisation is resilient to any attacks that come their way.

"Making security a high priority helps drive the conversation forward—but those conversations will have limited success if the board members and their CISOs don't speak the same language or share the same goals. A better alignment of the two sides around priorities will go a long way in improving their organisations' protection and resilience. Boards must find opportunities to forge strategic partnerships with their CISOs to work collaboratively toward their common goals of minimising their organisations' risks and increasing their organisations' cyber resiliency."

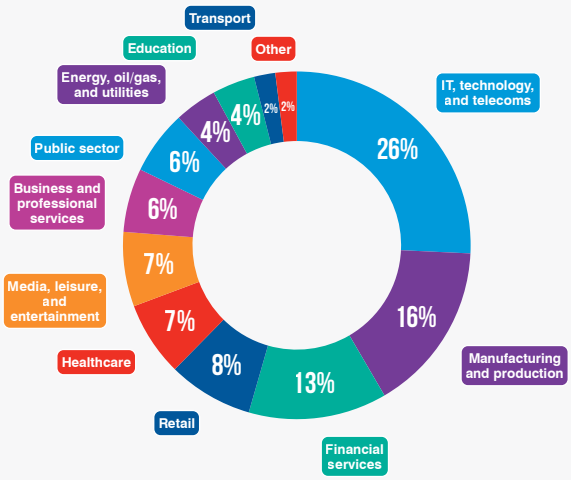
Dr. Keri Pearlson, Executive Director, Cybersecurity at MIT Sloan (CAMS)

Methodology

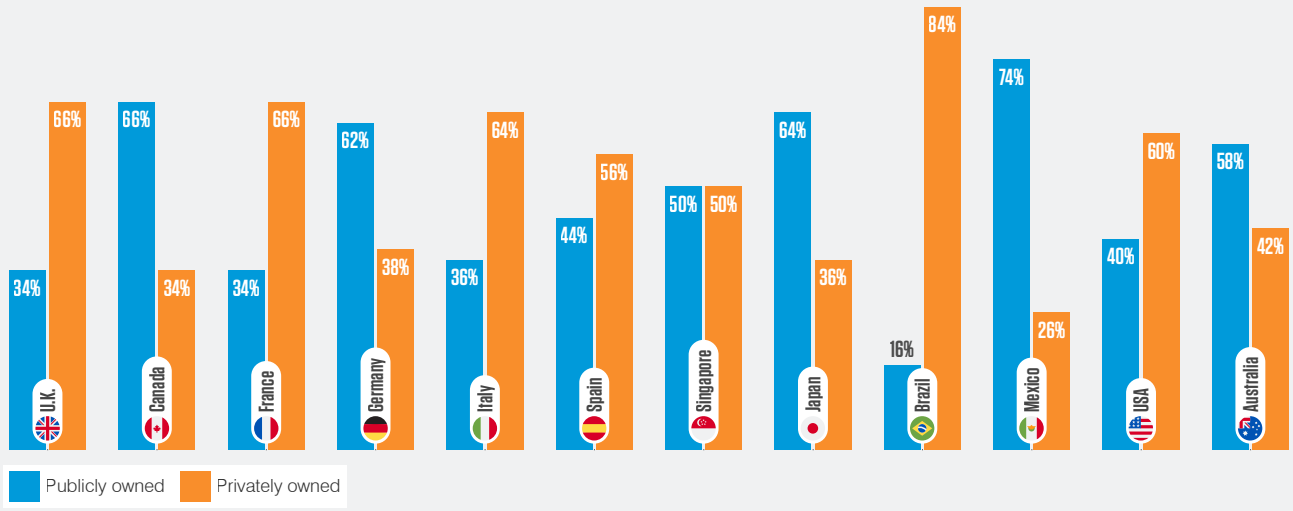
The Proofpoint Cybersecurity: The 2022 Board Perspective survey was conducted by research firm Censuswide between August 11 and August 22, 2022. It surveyed 600 board directors from organisations of 5,000 employees or more across different industries in 12 countries. 50 board directors were interviewed in each market, which included the U.S., Canada, U.K., France, Germany, Italy, Spain, Australia, Singapore, Japan, Brazil and Mexico. 3,941 board directors were invited to participate in the survey, resulting in a response rate of 15%. The data was analysed by the Proofpoint resident CISO team. The data was also reviewed and this report coauthored by researchers from the Cybersecurity at MIT Sloan (CAMS) research consortium. The results, insights and implications are the opinion of the authors based on the data analysis.

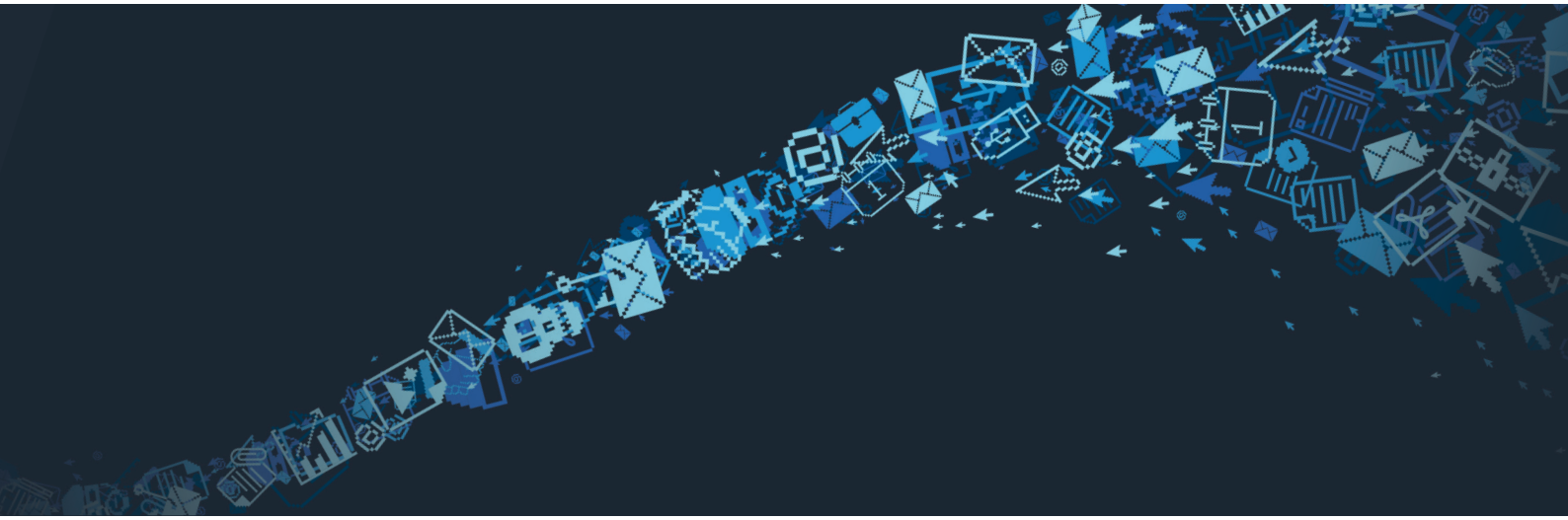
Censuswide complies with the MRS Code of Conduct and ESOMAR principles.

Within which primary sector is your organisation?



Is your organisation 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 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**.

proofpoint.

0401-003-02-01 09/22