Boards and Cyber Resilience

SURVEY FINDINGS

June 2022

Australian Institute of Company Directors

AISA Australian Information Security Association

Contents

Executive summary

Survey results reveal varying levels of maturity in the cyber posture of organisations and the steps boards are taking to build greater resilience. Key findings include:

1. Director awareness of threats, rather than actual attacks or increased Government regulation, is driving increased cyber investment.
2. There is more directors can do to improve their cyber skills and build stronger cyber governance practices, with limited up-skilling currently taking place.
3. Although cyber is accepted as a material risk for many organisations, often there is a lack of formal governance frameworks to support board oversight.
4. Directors of Small and Medium Sized Enterprises (SMEs), Not-For-Profits (NFPs), and public organisations need greater support to overcome resource constraints and to demystify the topic.
5. Almost all Australian organisations have characteristics that make them especially susceptible to a cyber attack.

1. Director awareness of threats, rather than actual attacks or increased Government regulation, is driving increased cyber investment.

In the last year alone, **three in four directors reported increased investment in cyber**, with 33% saying that this investment has increased 'significantly'. Cyber investment is increasing in tandem with investment in digital transformation, a positive sign that organisations are recognising the importance of a defense strategy for valuable digital assets.

Increased cyber investment is due to directors' awareness of the **escalating scale and impact of malicious cyber activity** (81%) and less because of actual or attempted attacks to their companies or peers (44%).

Regulatory changes, such as 2021's amendments to the Security of Critical Infrastructure Act and proposed ransomware reporting requirements, **have been a motivation for increased cyber investment for less than half (44%) of all organisations.**

2. There is more directors can do to improve their cyber skills and build strong cyber governance practices, with limited up-skilling currently taking place.

3. Although cyber is accepted as a material risk for many organisations, often there is a lack of formal governance frameworks to support board oversight.

72% of directors say cyber security is a 'high priority' issue for their board. This finding is consistent with other AICD research[1] which finds that cyber security has, since the beginning of 2021, moved up to the top-ranking issue keeping directors 'awake at night'.

At an organisational level, there appears to be gaps in implementing cyber governance frameworks. Of note, the following findings indicate **there is still room for improvement:**

- Just over half (53%) of directors say their organisation has a formal cyber security framework or strategy in place;
- 39% have made cyber a specific focus of a board committee;
- 36% receive regular reporting on internal training and testing; and
- 21% receive regular reporting on the cyber performance of key third-party suppliers.

1 See AICD's **Director Sentiment Index 2022** which revealed that directors identified cyber-crime and data security as the number one issue keeping them awake at night.

4. Directors of Small and Medium sized Enterprises (SMEs), Not-For-Profits (NFPs), and Government organisations need greater support to overcome resource constraints and to demystify the topic.

The challenges faced by smaller organisations in building cyber resilience have been well documented. Key survey observations confirm this including:

- **Only 36% of directors from small organisations have a formal cyber framework in place, with 45% instead opting for an informal strategy.**
- Around 42% of NFP directors report a formal cyber framework in place, the lowest proportion among the different entity types, with **20% reporting the absence of any cyber framework or strategy (whether formal or informal).**
- Small (63%) and medium (52%) sized organisations are more likely than larger organisations (45%) to have limited resources to dedicate to cyber resilience.

5. Almost all Australian organisations have characteristics that make them especially susceptible to a cyber attack.

89% of directors say their businesses have one or more characteristics that make them especially susceptible to a cyber attack, such as holding sensitive customer, client, or member data, or providing a service to government.

There is, however, a small group that are unaware of their vulnerabilities – 14% of directors from organisations particularly vulnerable to cyber attacks still do not consider cyber security as a high priority board issue.

Methodology

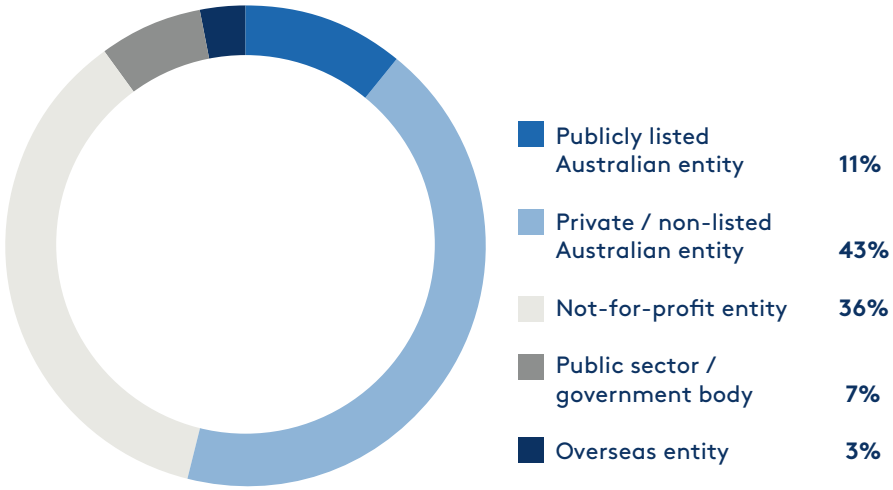
Methodology

Members of the Australian Institute of Company Directors (AICD) and the Australian Information Security Association (AISA) were invited to take part in an online survey between 9 – 27 May 2022. A total of 856 practicing directors participated in the survey and a complete list of questions and results can be found **here**. Participation was on a voluntary basis with no incentive given. Sectoral response rates were largely in line with the composition of the AICD membership.

This survey also uses Annual Turnover to define the size of organisation:

Size	Definition	% of sample
Small	Under $10 million	48%
Medium	$10-250 million	39%
Large	Above $250 million	15%

Q: With regard to your primary Directorship, is it with a...



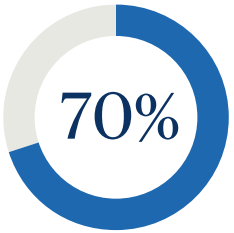
MAIN FINDINGS

Directors' cyber capabilities

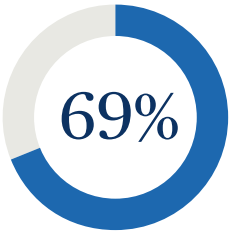
Understanding of cyber governance

- Directors are relatively confident their boards understand key aspects of cyber governance. Seven in ten report an 'adequate' board understanding of the potential impact of a cyber failure and identifying the organisation's critical data and information assets.
- However, there is less understanding of how to respond to a cyber incident, or the legislative and regulatory obligations related to cyber, with 22% of all directors saying they have 'inadequate' understanding of these issues.
- Directors in the NFP and Government sectors have generally lower confidence of cyber governance aspects than their counterparts from the Listed and Unlisted sectors. For example, while 82% and 74% of directors respectively from the Listed and Unlisted sectors say they have adequate understanding of the potential impact of a cyber security incident, only 67% and 60% of directors from the Government and NFP sectors say the same.

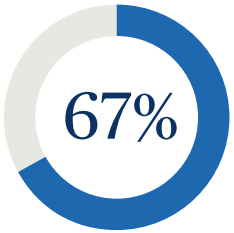
Q: Please rate your board's overall understanding of...



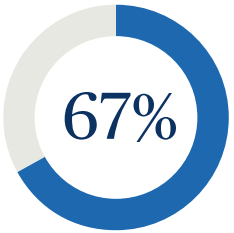
The potential impact of a cyber security incident



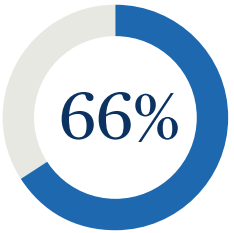
Critical assets in the organisation (eg. key data and information assets)



The board's responsibility in managing cyber risks

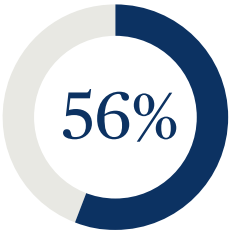


Data governance and security



The current cyber resilience of the organisation

How to respond to cyber incidents



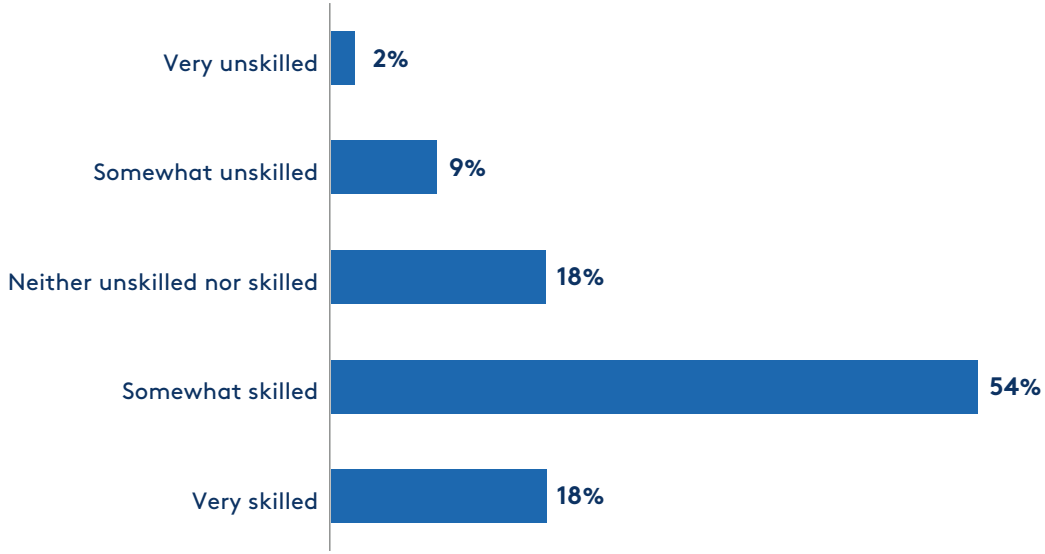
The legislative and regulatory obligations related to cyber

Directors' cyber skill level

- Directors report a high level of confidence in their own cyber capabilities with 71% reporting that they were skilled in understanding how cyber security affects their organisations.
- Only 11% of directors consider themselves unskilled in cyber security and 18% consider themselves neither skilled nor unskilled.

Skilled **71%** vs Unskilled **11%**

Q: Thinking about your position as a director, how skilled are you in understanding how cyber security affects your organisation?



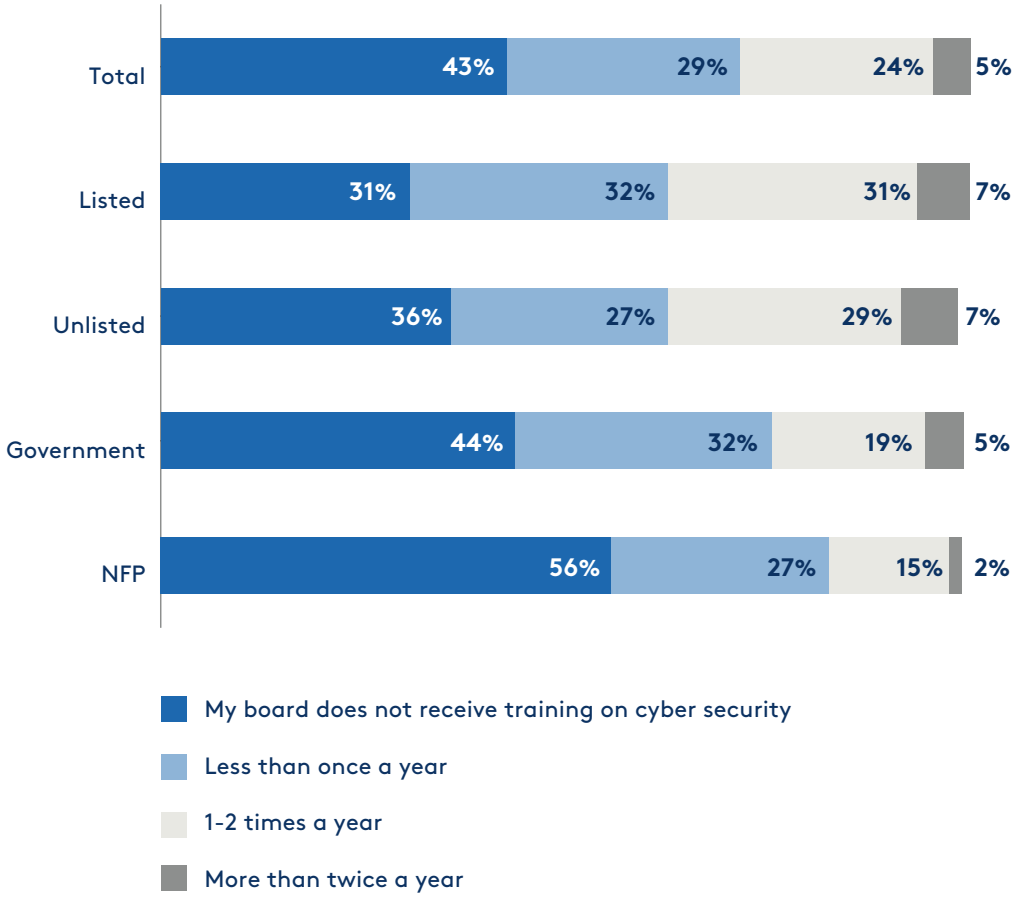
Board cyber training

- In a somewhat surprising result, 43% of respondents report that their boards do not receive any cyber security training. By contrast, 29% report receiving training at least yearly.
- More than half of all directors in the NFP sector (56%) report receiving no cyber training.
- The results suggest the need for a more active approach to ongoing education given the increasing and evolving nature of cyber risk.

43%

of boards do not receive any training on cyber security

Q: How often does your board receive training on cyber security?



*'Listed' = publicly listed Australian entity; 'Unlisted' = private/non-listed Australian entity; 'Government' = public sector/government body; and 'NFP' = not-for-profit entity.

MAIN FINDINGS

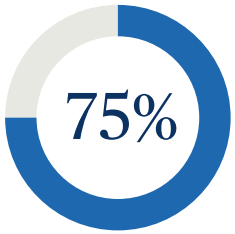
Cyber governance practices

Cyber as a board priority

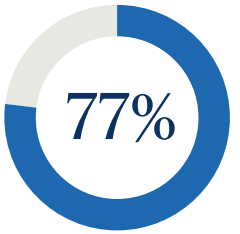
- Seven in ten directors say cyber security is a high priority issue for their board. This proportion is highest in the Unlisted sector (77%) and lowest in the NFP sector (66%).
- The data shows that directors that prioritise cyber have:
  - More targeted governance practices (such as making cyber a specific focus of a board committee or appointing directors with cyber skills);
  - More regular cyber training for board members;
  - More regular reporting to the board on cyber issues (such as on the execution of the organisation's cyber strategy); and
  - Better organisational cyber security practices (such as identifying the organisation's critical assets and procedures).

72% **say cyber security is a high priority issue for their boards**

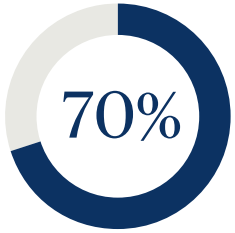
Q. To what extent do you agree with the following statement 'Cyber security is a high priority issue for my board'*



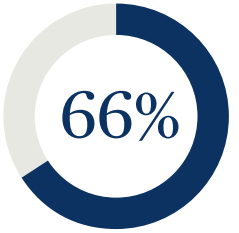
Listed: Publicly listed entity



Unlisted: Private / non-listed entity



Government: Public sector / Government body



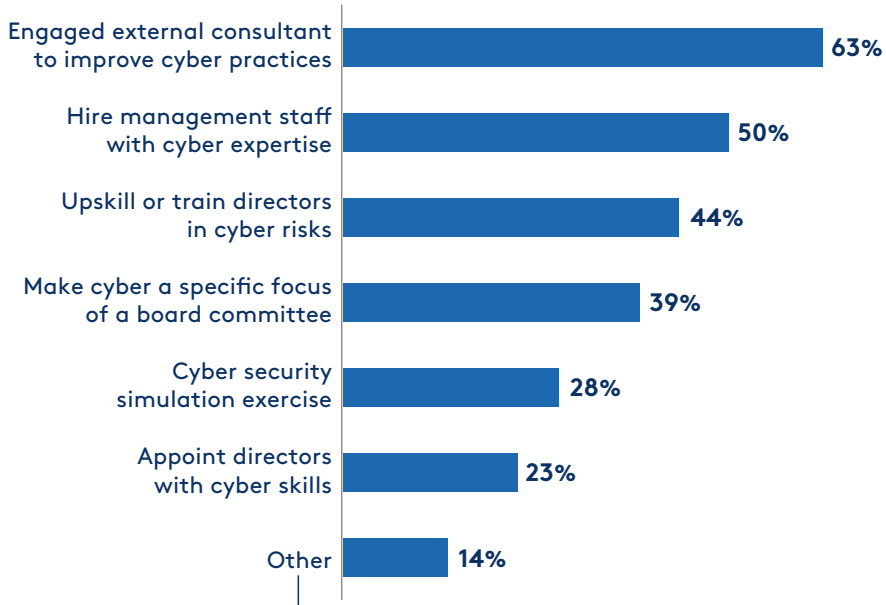
NFP: Not-for-profit entity

*'Somewhat' + 'Strongly Agree' only

Board cyber practices

- The utilisation of external consultants to improve cyber expertise is pronounced, with almost two in three (63%) reporting that they engage external cyber experts. Similarly, there is a clear push for greater cyber expertise within management with half of directors saying that has been a focus for their board.
- Only 44% of directors indicate receiving training in cyber risk, and even fewer (23%) have appointed directors with cyber skills.
- There also appears to be relatively limited use of committee structures to support cyber governance (39%), infrequent utilisation of simulation exercises (28%) and sporadic management reporting on key cyber issues (see next page).

Q. Below are some practices that boards have engaged in to prevent cyber incidents and build cyber resilience. Which of these activities does your board engage in? Please select all that apply.



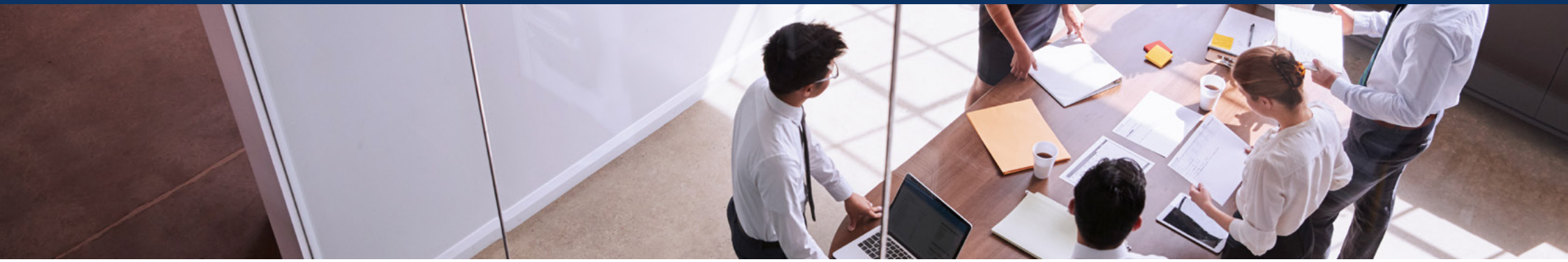
'Improve staff education, training, and awareness'

'Customer education on data security'

'Improve regularity of board reporting on key cyber issues'

'Pressure on suppliers to demonstrate cyber practices'

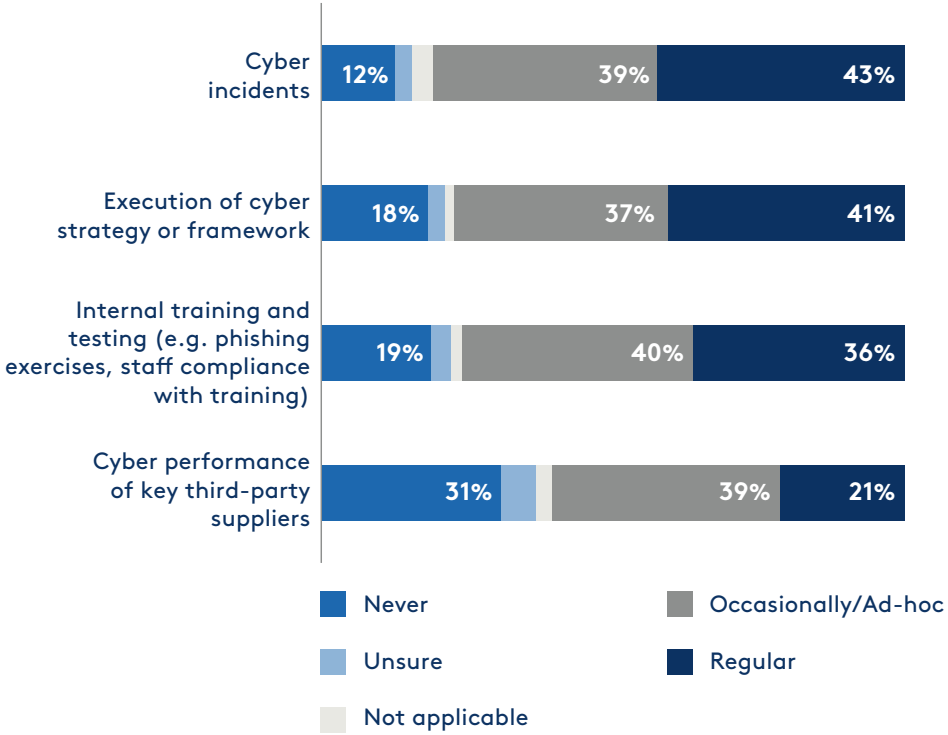
'Assigning management specific cyber responsibility'



Cyber reporting to the board

- Despite cyber security being a high priority for 72% of respondents, board reporting on key cyber issues is less regular.
- Only 36% of board receive regular reporting on internal training and testing, which may not send the appropriate message around the importance of cyber vigilance amongst staff.
- Only one in five directors (21%) receive regular reporting on cyber risk from supply chain relationships. Suppliers can pose increased risk for organisations given the degree of system interconnectivity and data-sharing that is now part of everyday business operations.
- The results suggest boards must set higher expectations around the information they receive from management including the format, frequency and level of detail.

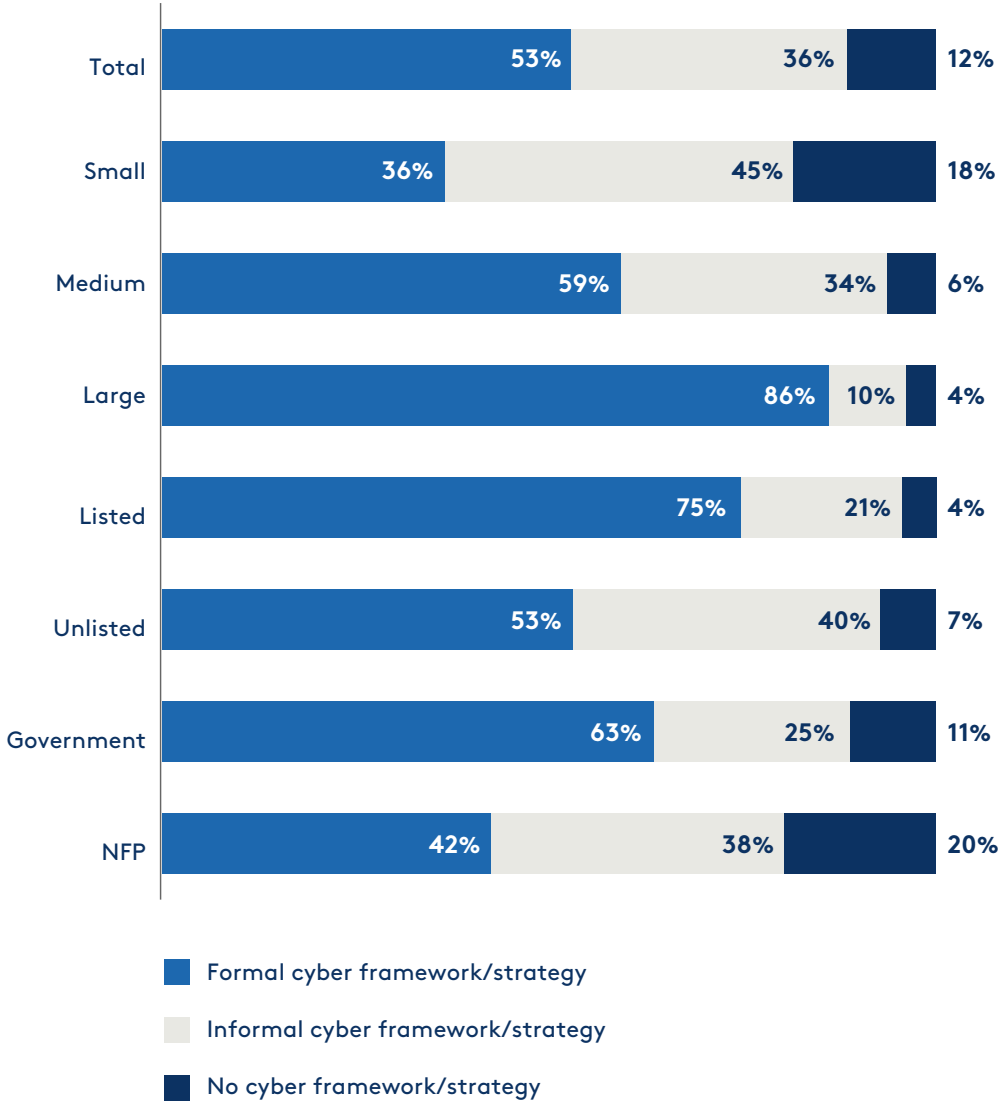
Q: How often does your board receive reporting on...



Establishing a cyber framework or strategy

- With cyber a high priority for most boards, it is unsurprising that more than half (53%) of directors report having a formal cyber security framework or strategy in place. This was considerably higher for Listed entities (75%). Higher revenue organisations reported the most formal structures (86% of directors).
- For small organisations however, only 36% have a formal cyber framework in place, with 45% instead opting for an informal strategy.
- Only 42% of NFP directors have a formal cyber framework in place, the lowest proportion among the different entity types. Of concern, one in five NFPs report the absence of any cyber framework, suggesting a lack of organisational readiness to prevent and respond to potential attacks.

Q: Does your organisation have a cyber security framework or strategy in place?



Key cyber governance measures

- Survey results suggest that many organisations may be unprepared for the impact of a cyber attack. While 73% of organisations have practices that identified the organisation's critical assets and processes, less than half (49%) have quantified the impact of a cyber attack and only 36% have conducted a cyber simulation exercise.
- Worryingly, only half of directors (51%) report that their organisations have tested employee cyber awareness such as through quizzes or simulating attacks like phishing emails.
- Application of cyber security frameworks such as the NIST framework, ISO 27001, or the ACSC's Essential Eight are only applied by half of all organisations (50%) and only 38% of small organisations.

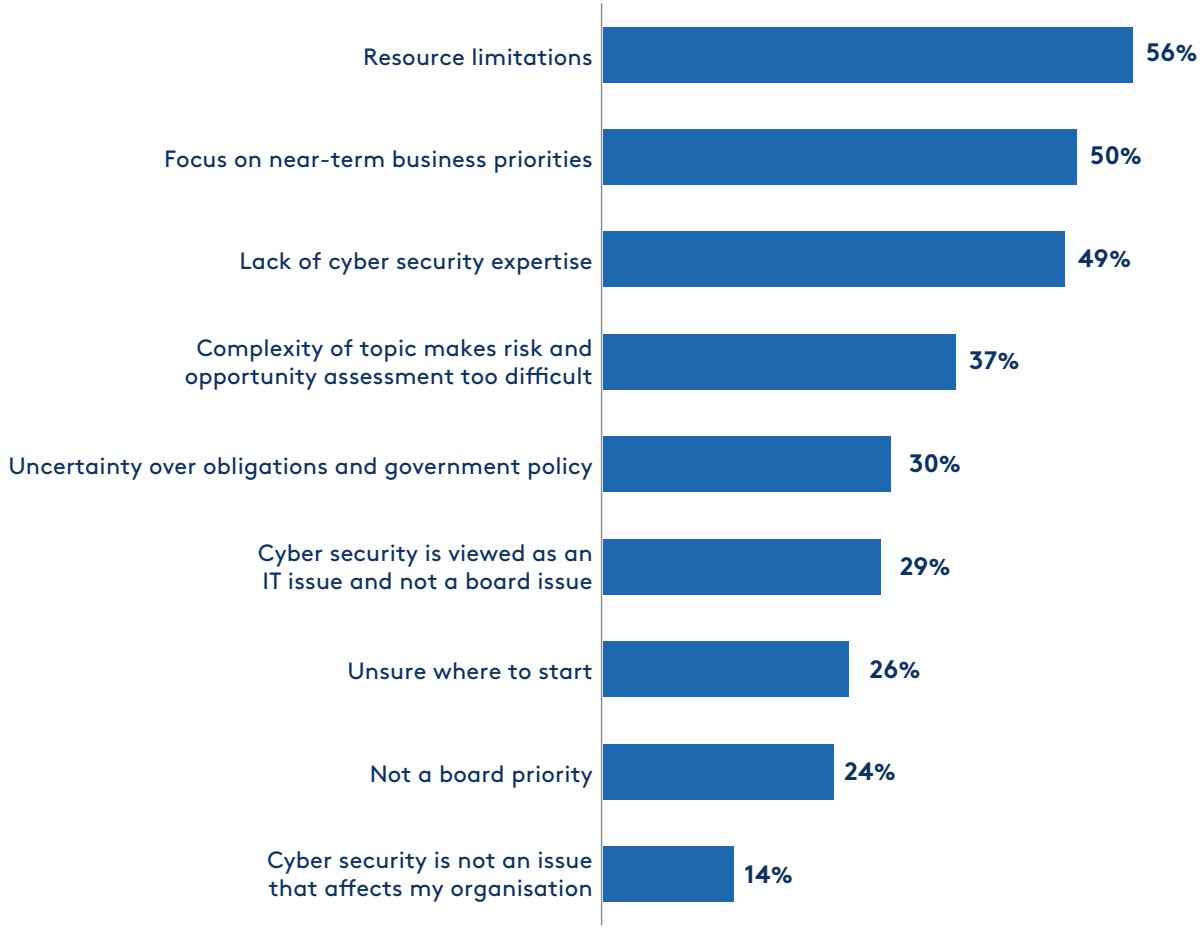
Q. Below is a list of organisational practices to prevent cyber incidents and build cyber resilience. To what extent does your organisation engage in the following practices?*

*Moderate + Large extent only

Challenges to improving cyber practices

- More than half of directors (56%) state that a lack of resources is impeding the improvement of organisational cyber practices. This number increases to 64% for NFPs.
- While 49% are experiencing difficulty in accessing appropriate cyber security expertise, this proportion increases to 59% for Government organisations.
- Evidence suggests more can be done to demystify the topic of cyber, with 37% of directors seeing the issue as too complex and one in four directors (26%) unsure where to start.

Q. Below is a list of challenges that directors have told us they face when attempting to improve cyber practices in their organisations. To what extent do the following challenges apply to your board?*



*Moderate + Large extent only

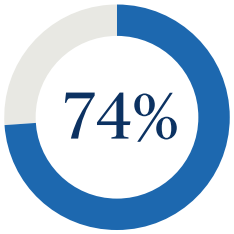
MAIN FINDINGS

Incidents, investment and insurance

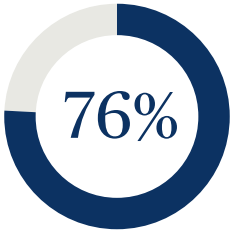
Reasons behind increased cyber investment

- Investment in cyber security is increasing at the same rate as investment in digital transformation. Around three in four directors (74%) report increased organisational investment in cyber.
- The decision to increase cyber investment is driven more by directors' awareness of reported cyber activity (81%) than because of actual or attempted attacks to their companies or peers (44%).
- Regulatory changes such as 2021's amendments to the Security of Critical Infrastructure Act and proposed amendments to the Privacy Act are motivating factors for less than half (44%) of all organisations.

Q. Over the past 12 months, to what extent have the following factors driven the enhancement of cyber resilience in your organisation? Please select all that apply.*



Organisations that have increased investment in cyber security



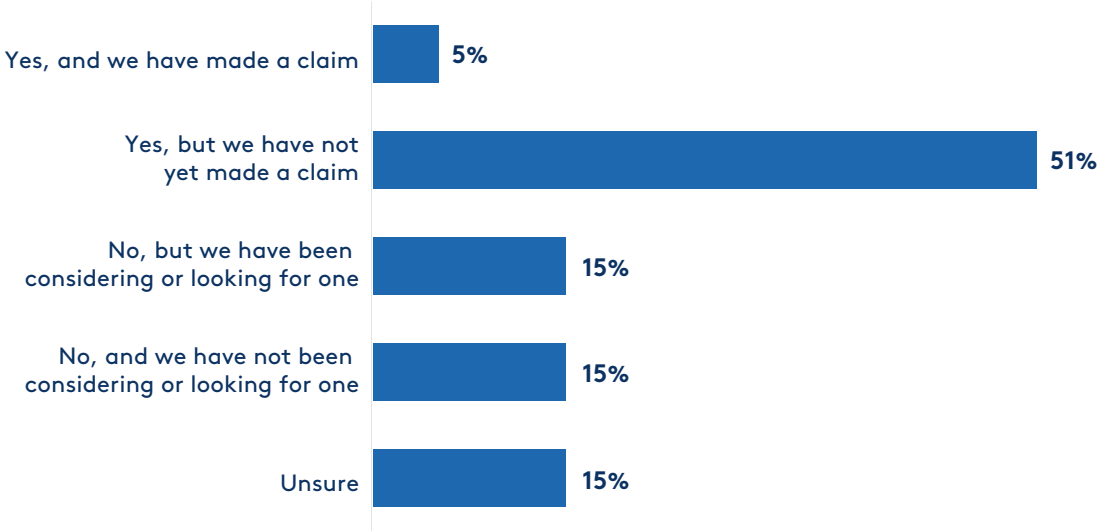
Organisations that have increased investment in digital transformation

*Moderate + Large extent only

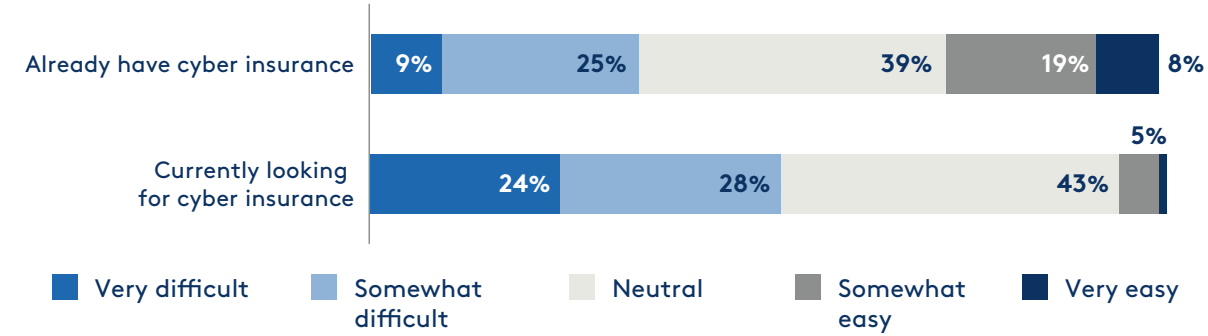
Utilisation of cyber insurance

- More than half (56%) of directors report having a cyber insurance policy in place with another 15% currently in the market for cover.
- Importantly, 15% of directors are unsure if their organisation has a cyber insurance policy. This proportion increases to 37% for organisations in the Government sector, suggesting a lack of awareness of the product's capabilities.
- Consistent with other reports, the survey reveals a hardening insurance market. Among organisations which already have a cyber policy, only a third of directors (34%) found the process of finding the right policy difficult, while this number jumped to more than half (52%) for those that did not currently have cover but would like to purchase some.

Q. Does your organisation currently have a specific cyber insurance policy?



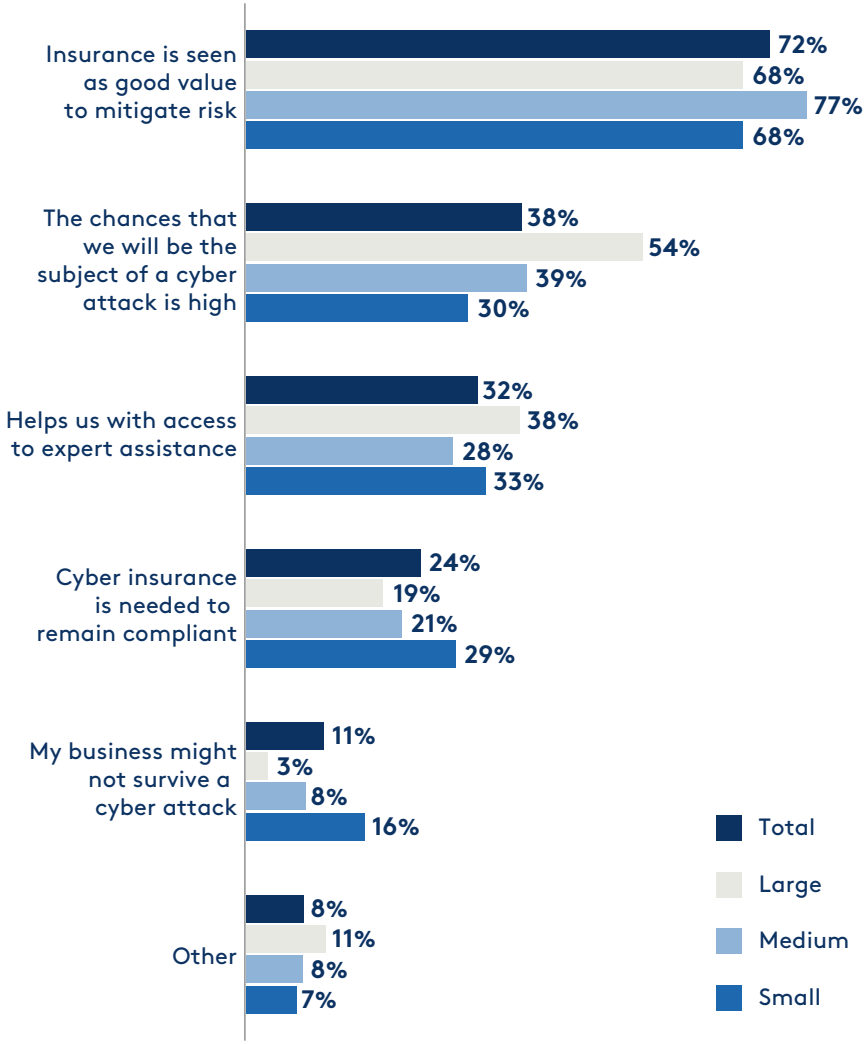
Q. How difficult has it been to find a policy that was suitable for your organisation?



Reasons for obtaining cyber insurance

- Of those who have obtained cyber insurance, 72% do so to mitigate against the risk of a cyber attack. However, directors must be careful that their organisations does not allow cyber coverage to compensate for a lack of internal cyber preparedness.
- Larger organisations are more likely to buy cyber insurance because they believe the likelihood of being attacked is high, while small businesses are more likely than other entity types to be fearful of going out of business should an attack occur.
- Directors from larger organisations see a key benefit of cyber insurance as access to expert assistance (38%). Going through the process of seeking insurance can be an informative exercise to identify organisational gaps and areas requiring focus or capability uplift for both large and small organisations.

Q. What are the motivations behind your organisation obtaining cyber insurance? Please select all that apply.



MAIN FINDINGS

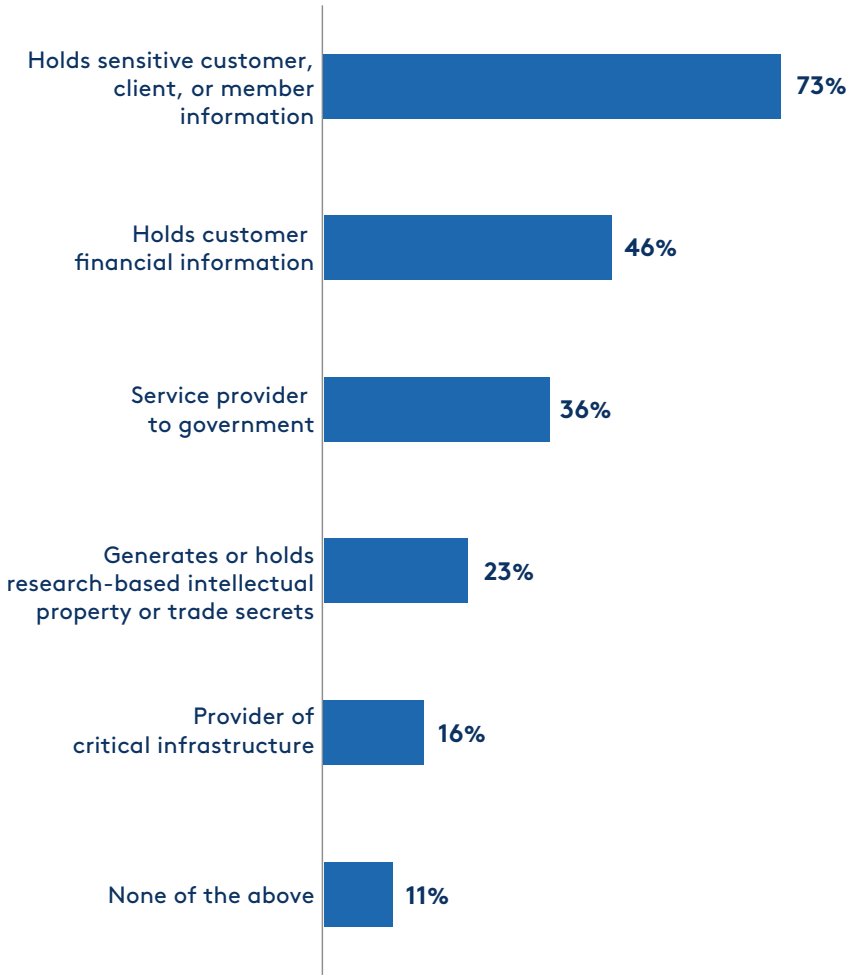
Sectoral insights

Organisational characteristics & cyber vulnerability

- Nine in ten directors say their organisations have characteristics that make them especially susceptible to a cyber attack.
- Almost three in four directors report their organisations hold sensitive client information (73%) and just under half hold customer financial information (46%).
- Unfortunately, not all vulnerable organisations are aware of their increased vulnerability; 14% of respondents who have characteristics that make them vulnerable to cyber attacks still do not see cyber as a high priority for their boards.
- Compared to their Listed (88%) and Unlisted (86%) counterparts, Government and NFP sector organisations are more likely to have characteristics that make them vulnerable due to the sensitive nature of the data they hold (94% and 92% respectively).

89% of companies are particularly vulnerable to cyber attacks

Q: Please select any of the below characteristics that might apply to your organisation.



The NFP and Government sectors

- Despite the higher risks faced by NFPs and Government organisations, these sectors have the least proportion of directors that are skilled in cyber.
- Government and NFP boards are also less likely to prioritise cyber security, have a lower understanding of cyber governance, and have less frequent cyber reporting to the board.
- NFP organisations are least likely to have a sophisticated cyber security system in place, with less than half (42%) of such organisations having a formal cyber security framework or strategy in place. This increases the likelihood that they will be targets of cyber crime.

		LISTED	UNLISTED	GOVERNMENT	NFP
DIRECTORS	SKILLED DIRECTORS	76	76	71	66
BOARDS	CYBER SECURITY AS A HIGH PRIORITY BOARD ISSUE*	75	77	70	66
	ADEQUATE UNDERSTANDING OF CYBER GOVERNANCE#				
	Board's responsibility in managing cyber risks	85	72	54	59
	Current organisation's cyber resilience	84	71	62	55
	Critical assets in the organisation (e.g. key data and information assets)	80	74	60	62
	The legislative and regulatory obligations related to cyber	70	58	49	50
	REGULAR REPORTING ON CYBER ISSUES				
	Cyber incidents	71	43	46	32
	Execution of cyber strategy or framework	62	43	46	30
	Internal training and testing (e.g. phishing exercises, staff compliance with training)	58	40	38	25
	Cyber performance of key third-party suppliers	30	26	19	14

*Somewhat + Strongly Agree only

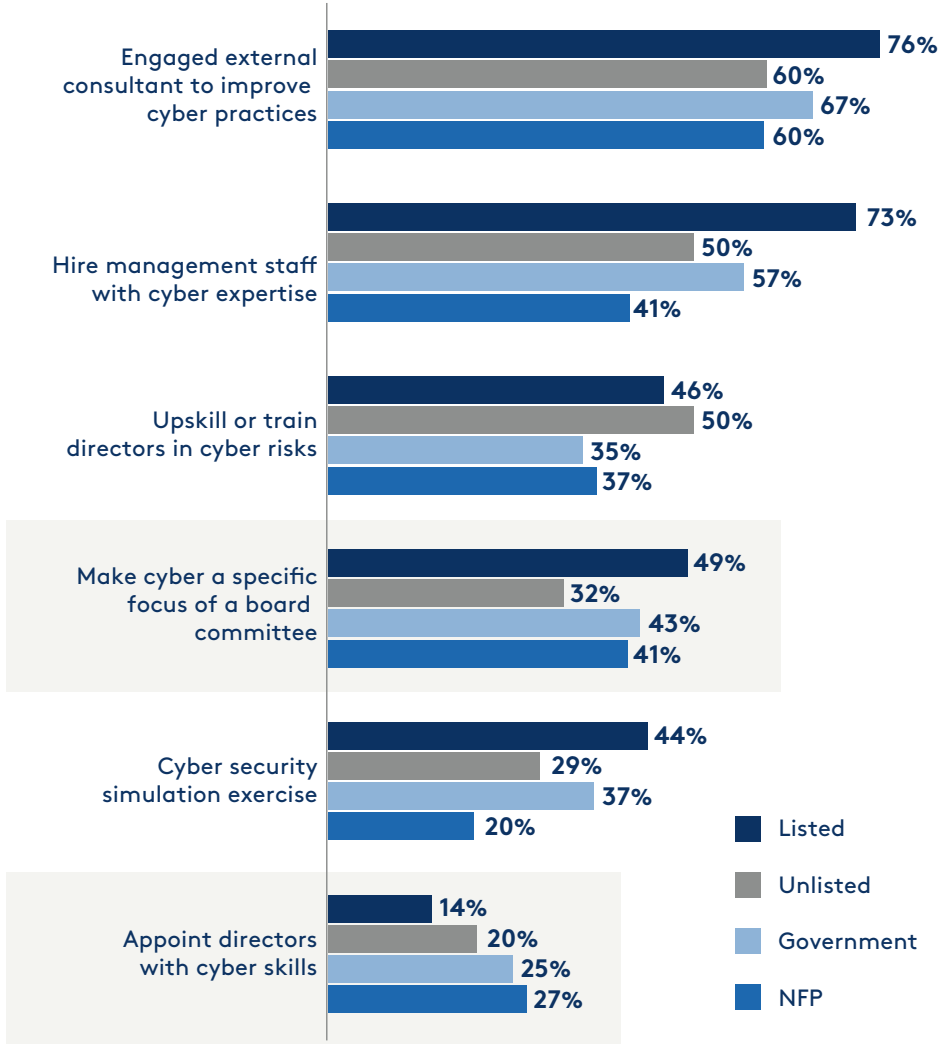
#Somewhat + Very Adequate only

Listed organisations

- Listed companies generally have more advanced cyber practices, perhaps because they are more likely to have been the subject of a 'material cyber incident'# (22%, compared to only 15% of NFPs). Consequently, three in four have a formal cyber security framework in place.
- In terms of board practices, less than half of all Listed companies have made cyber a specific focus of a board committee (49%), and only a small proportion (14%) have appointed directors with cyber skills - the lowest proportion among all entity types. This suggests a greater reliance on management to have the necessary expertise. Almost a third (31%) of all boards of Listed companies do not receive regular training on cyber security.
- In terms of reporting, only 30% of Listed company directors report receiving regular reporting on the cyber performance of third-party suppliers.

#'Material cyber incident' defined as a critical cyber security incident that has a significant impact on the provision of essential goods and services; and the event has materially disrupted the availability of those essential goods or services. See datapack for more details, available **here**.

Q: Below are some practices that boards have engaged in to prevent cyber incidents and build cyber resilience. Which of these activities does your board engage in? Please select all that apply.*

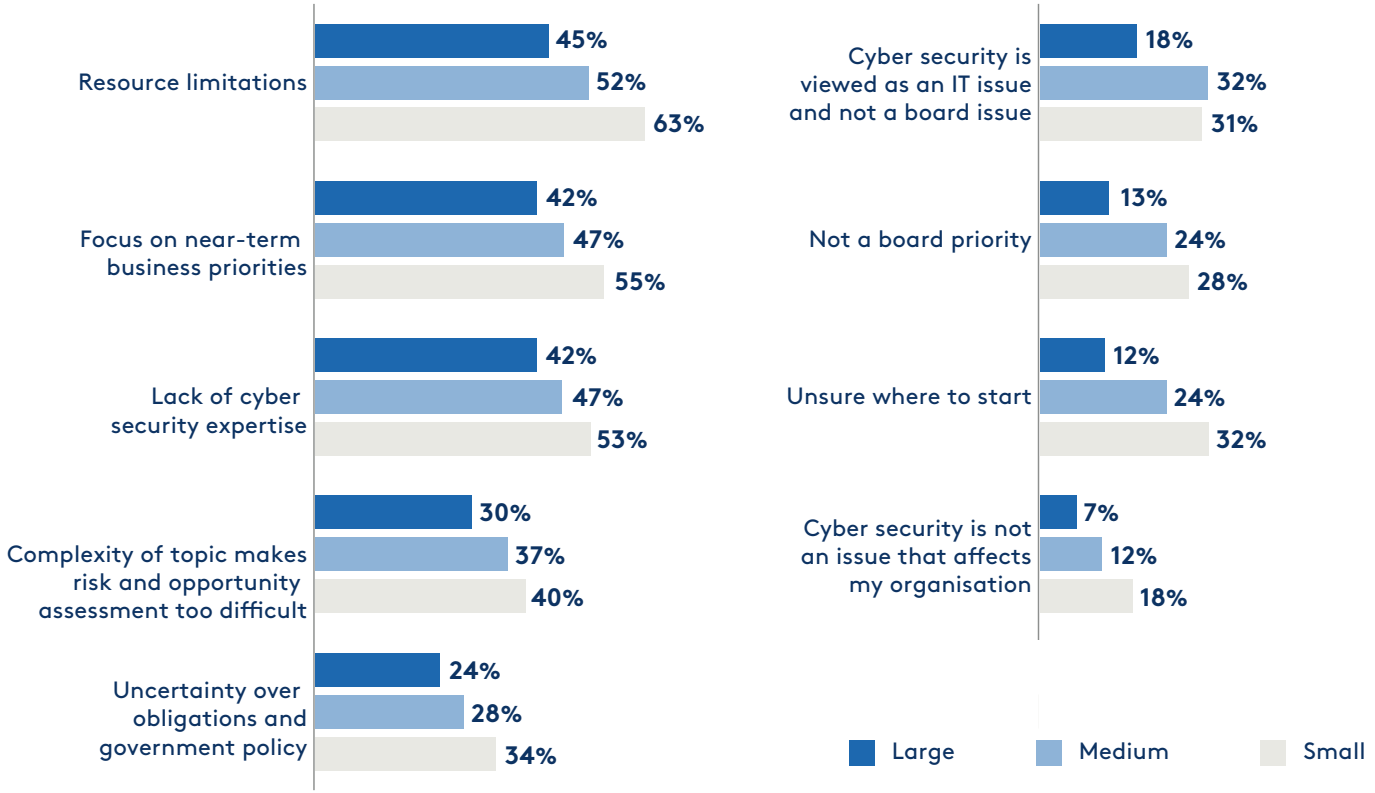


*Moderate + Large extent only

Small and Medium Sized Enterprises (SMEs)

- SMEs consistently face more significant barriers when attempting to implement good cyber security practices. For example, small (63%) and medium (52%) sized organisations have limited resources which cyber security has to compete for (compared to 45% of large organisations).
- Worryingly, almost a third of all directors from SMEs see cyber security as an IT issue and not a board issue. Around four in ten directors from small organisations see the topic as too complex.
- Directors from SMEs are also significantly more unsure of where to start on their cyber journey, with the complexity of cyber security as a topic being cited as a key inhibitor.

Q: Below is a list of challenges that directors have told us they face when attempting to improve cyber practices in their organisations. To what extent do the following challenges apply to your board?*



The Australian Cyber Security Centre (ACSC) has developed the **Small Business Cyber Security Guide** which is a good starting point for those looking to protect themselves from common attacks.

*Moderate + Large extent only

For more information about the results:

E: policy@aicd.com.au

JOIN OUR SOCIAL COMMUNITY

aicd.com.au

08299-3-5_22