

Boards and Cyber Resilience

Datapack

Australian
Institute of
Company
Directors

AISA Australian Information
Security Association



Methodology



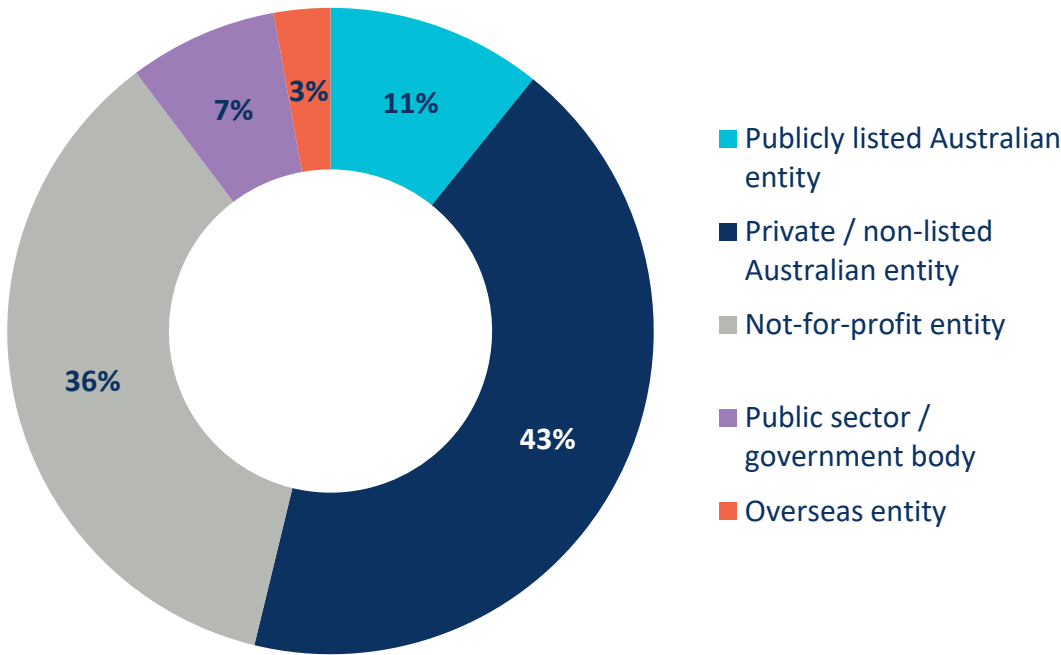
Methodology

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	Annual Turnover	% of sample
Small	Under \$10 million	46%
Medium	\$10 – 250 million	39%
Large	Above \$250 million	15%

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

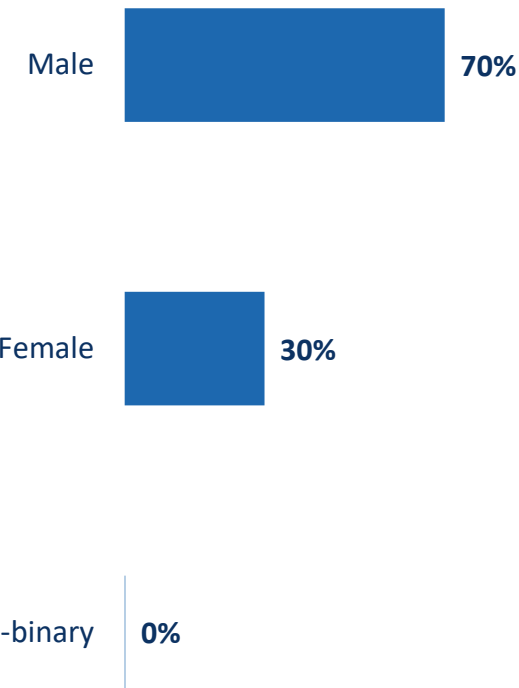


Main Findings

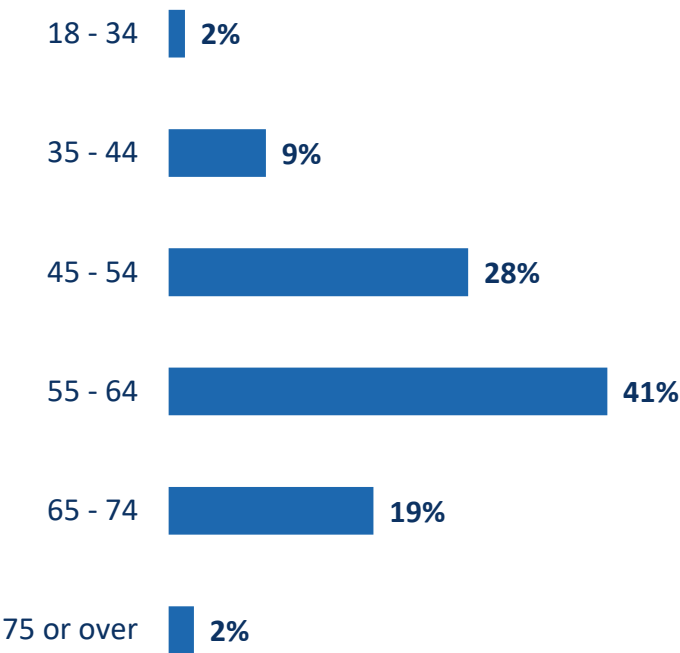


Demographics

Q. Are you...?

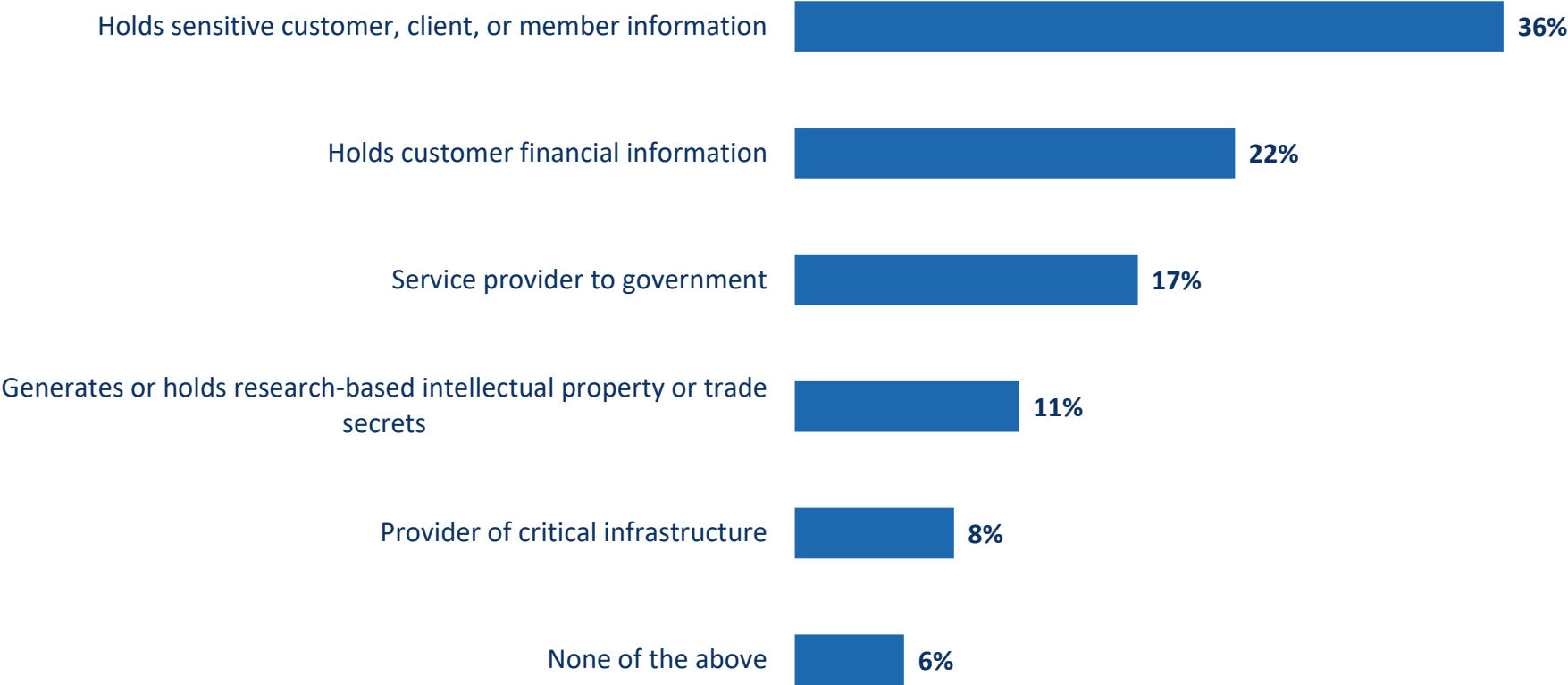


Q. What is your age?



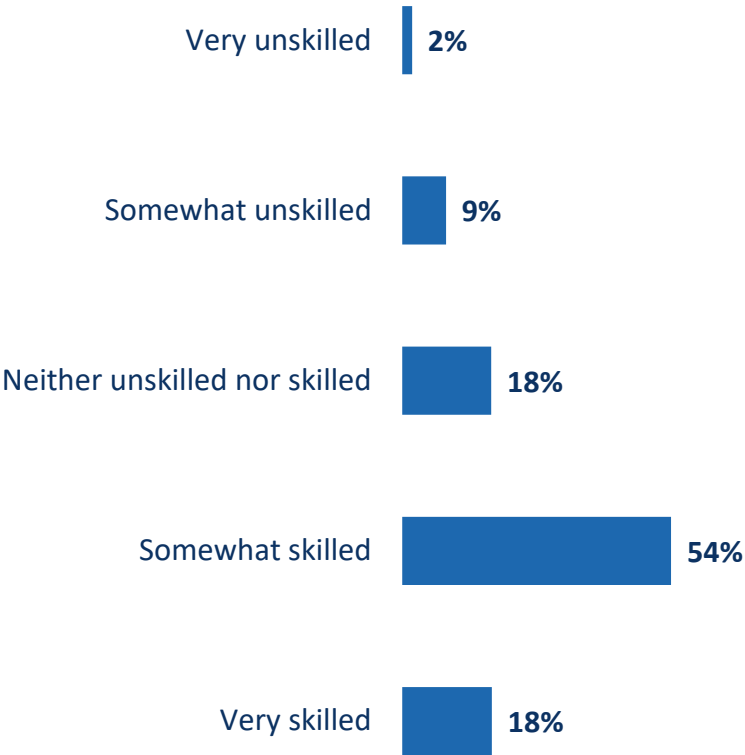
Organisational Characteristics

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

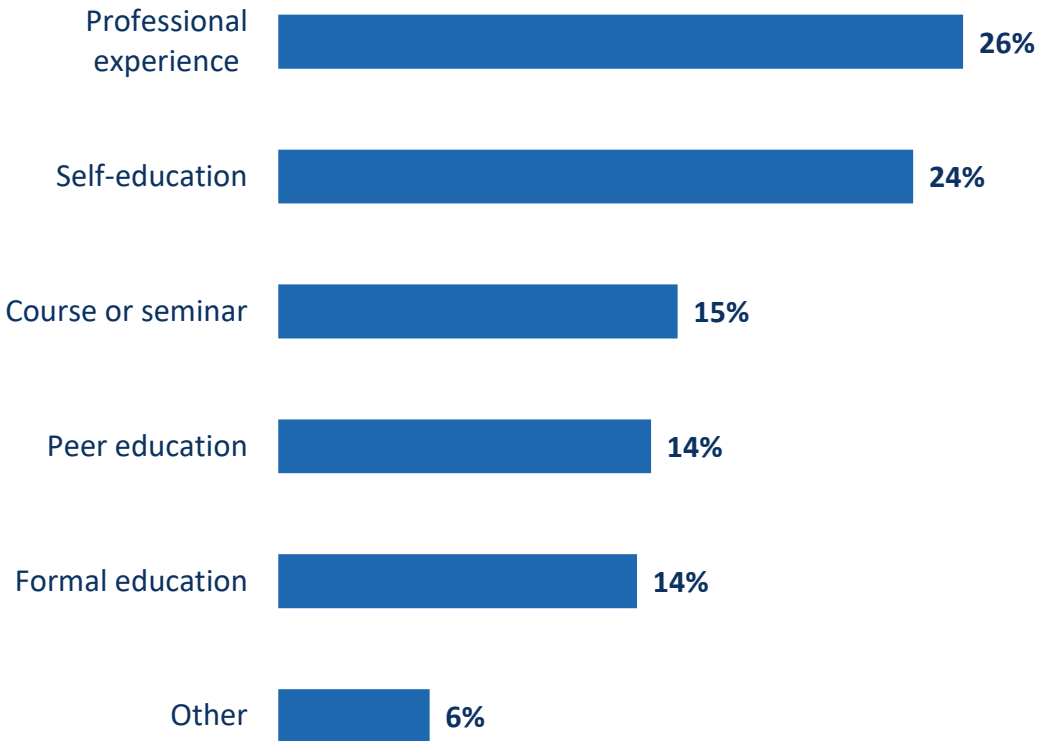


Director Skill Level

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

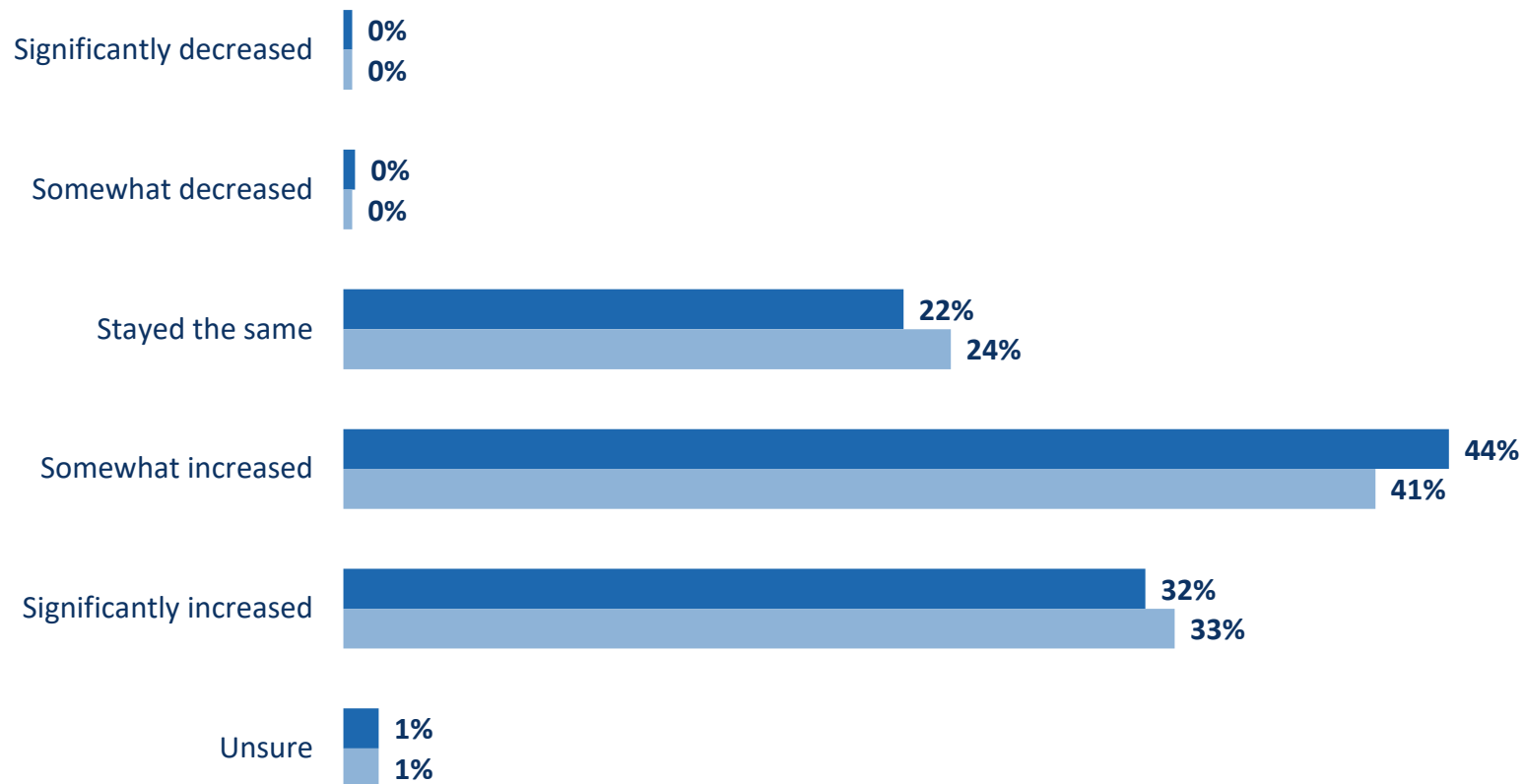


Q. You said that you were [very/somewhat] skilled in understanding how cyber security affects your organisation. Please select any relevant qualification or experience that form the basis of your skill level.



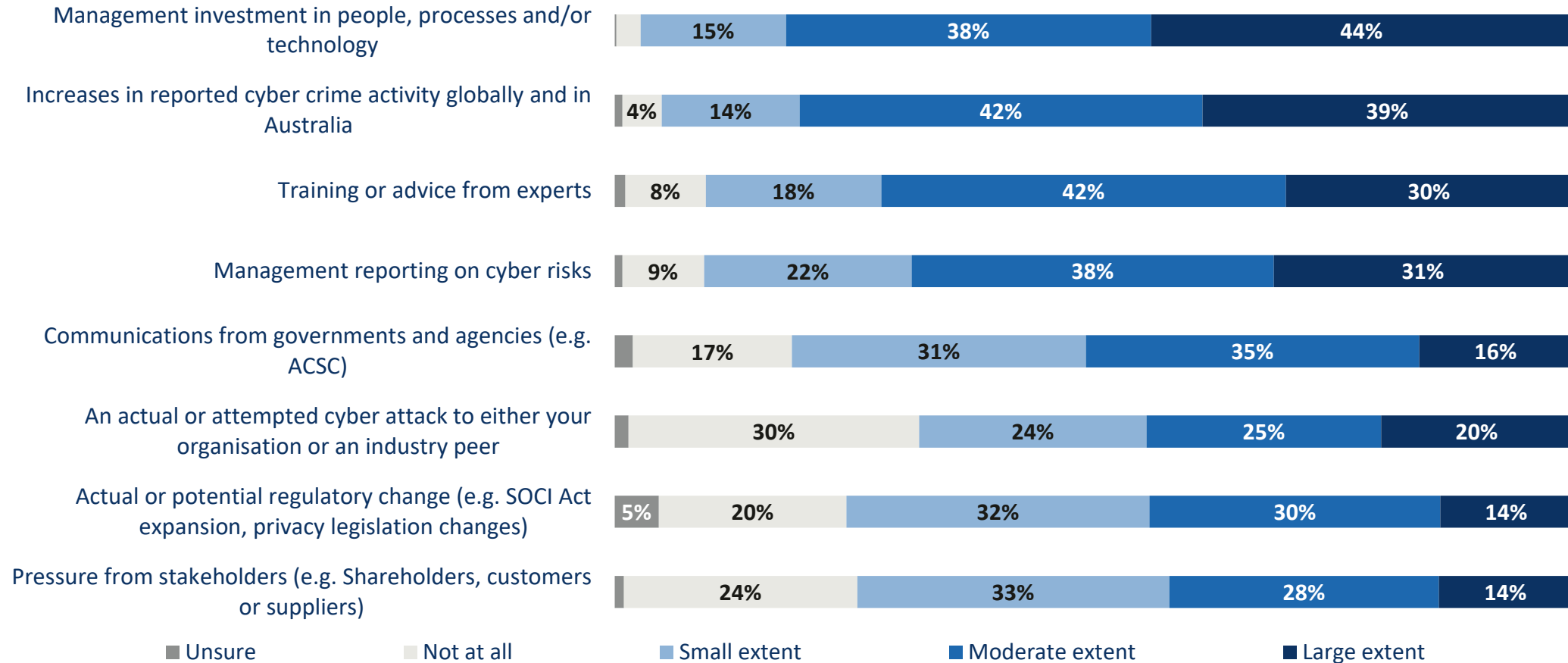
Level of Investment

Q. In the past 12 months, how has the level of investment in the below activities changed in your organisation?



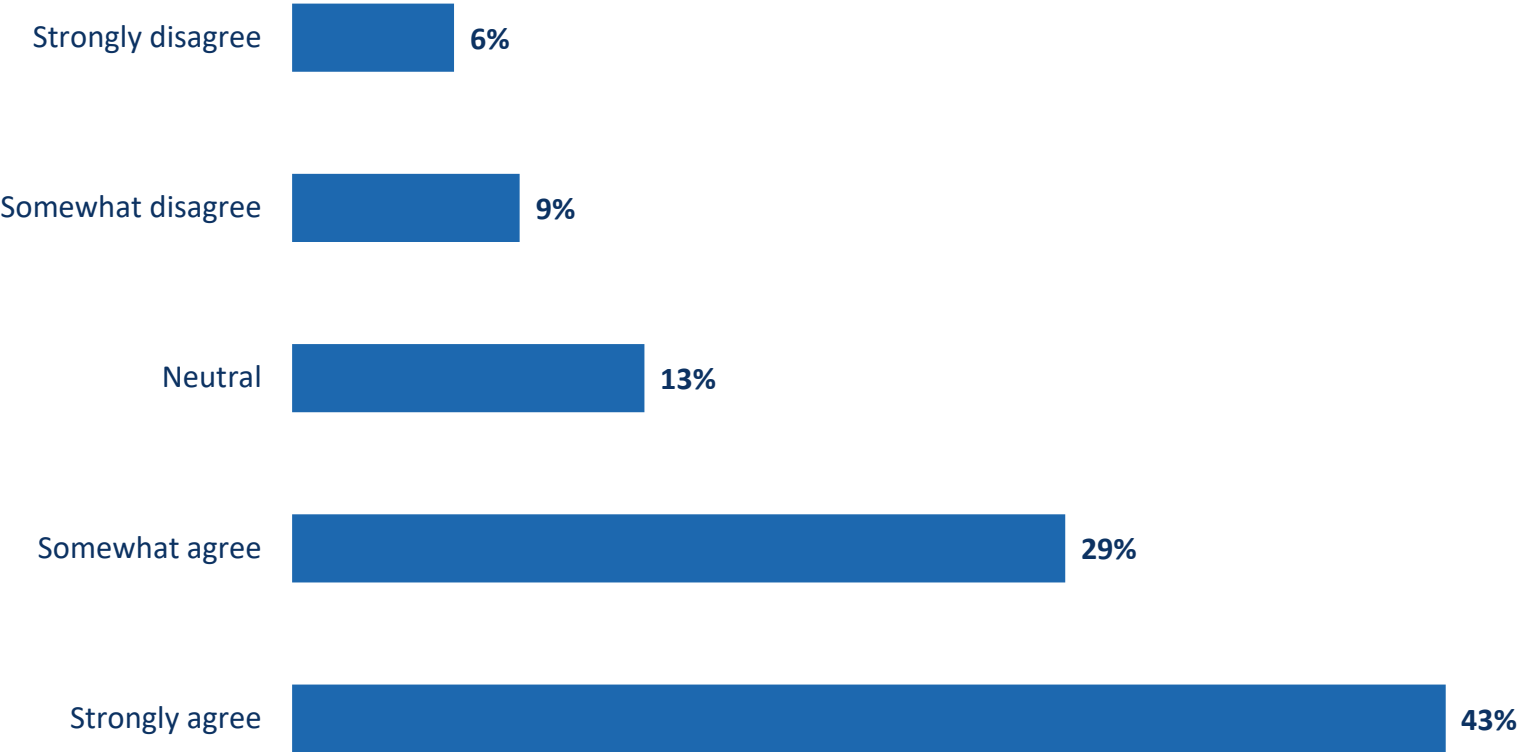
Reasons for Increased Cyber Investment

Q. Over the past 12 months, to what extent have the following factors driven the enhancement of cyber resilience in your organisation:



Cyber as a Board Priority

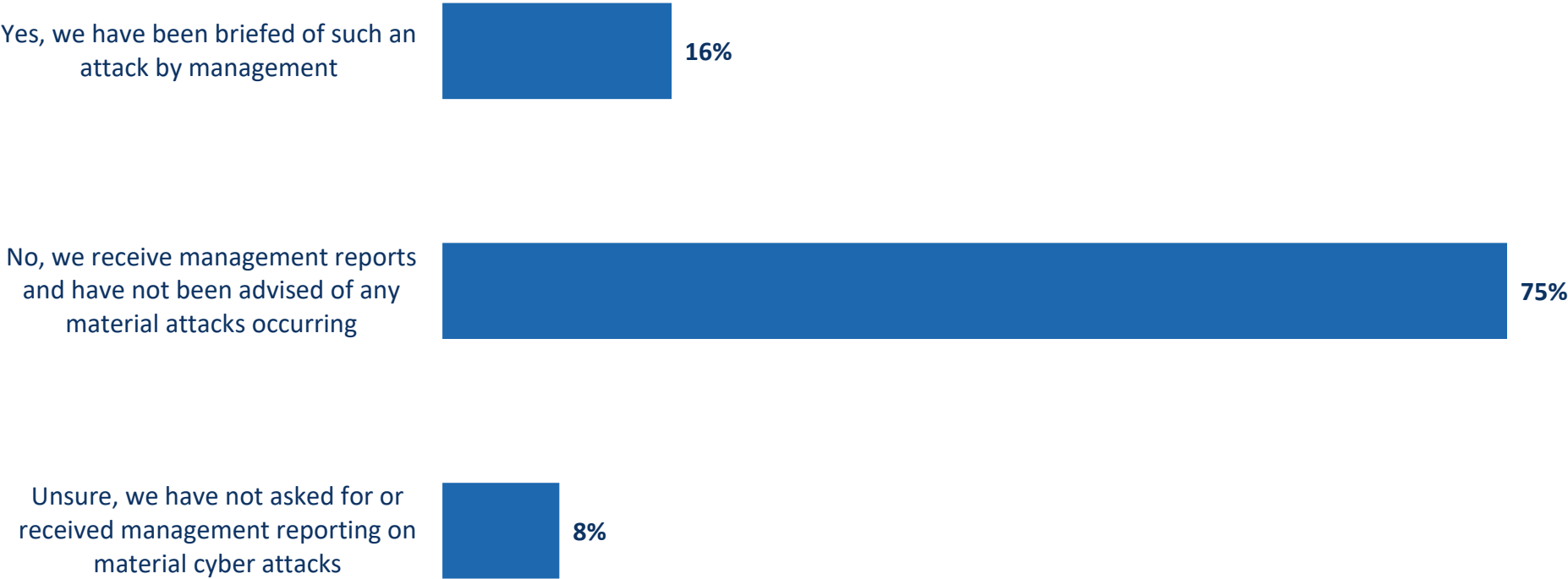
Q. To what extent do you agree with the following statement ‘Cyber security is a high priority issue for my board’?



Subject of Cyber Incident

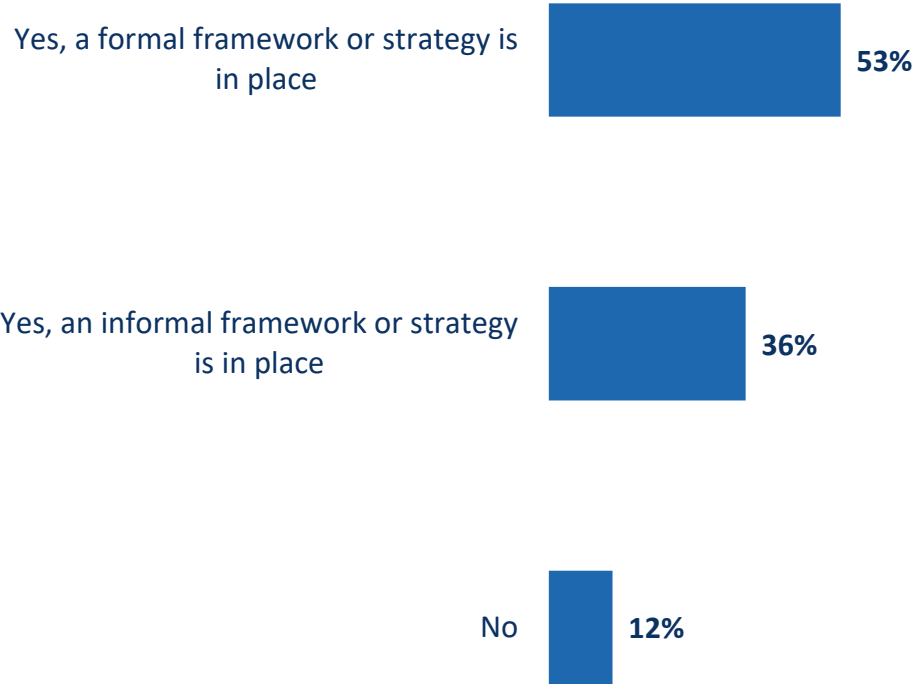
Q. Are you aware if your organisation has been the subject of a material cyber incident* in the past 12 months?

*‘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.

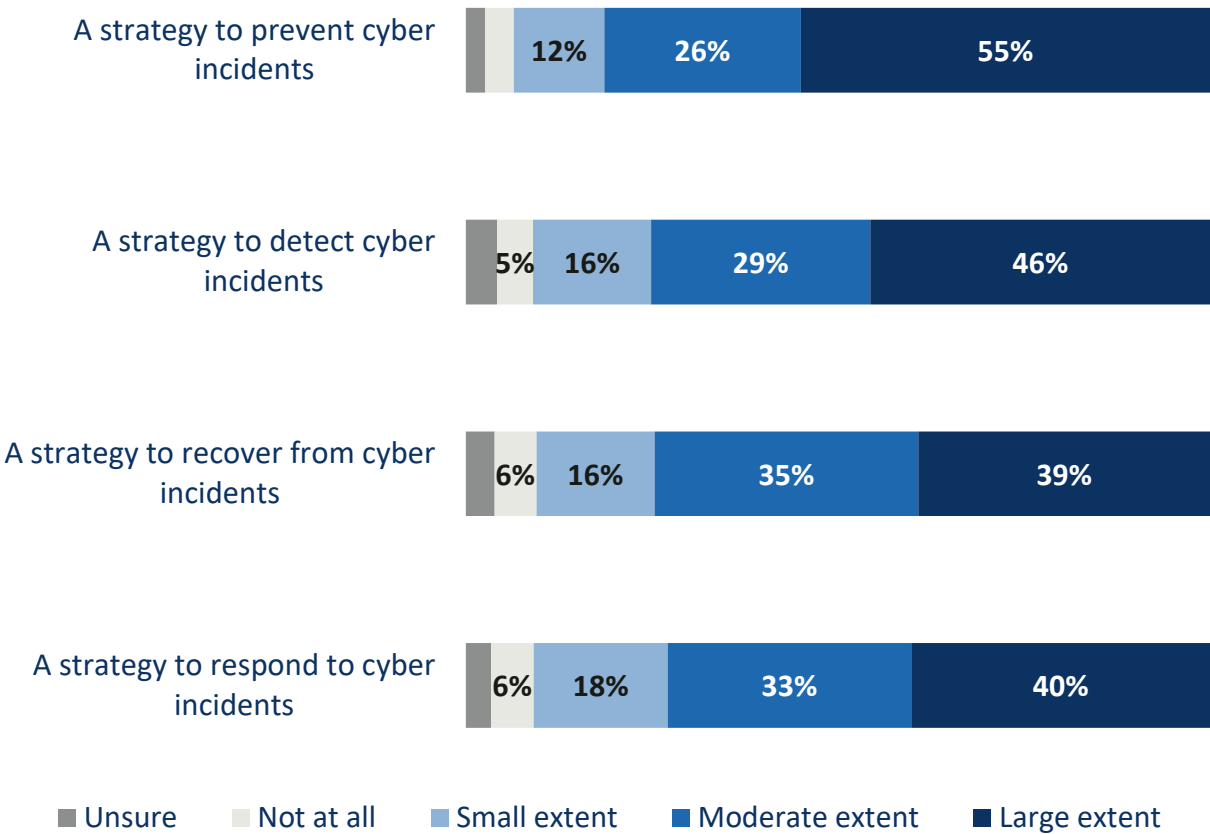


Organisational Cyber Security Framework and Focus

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

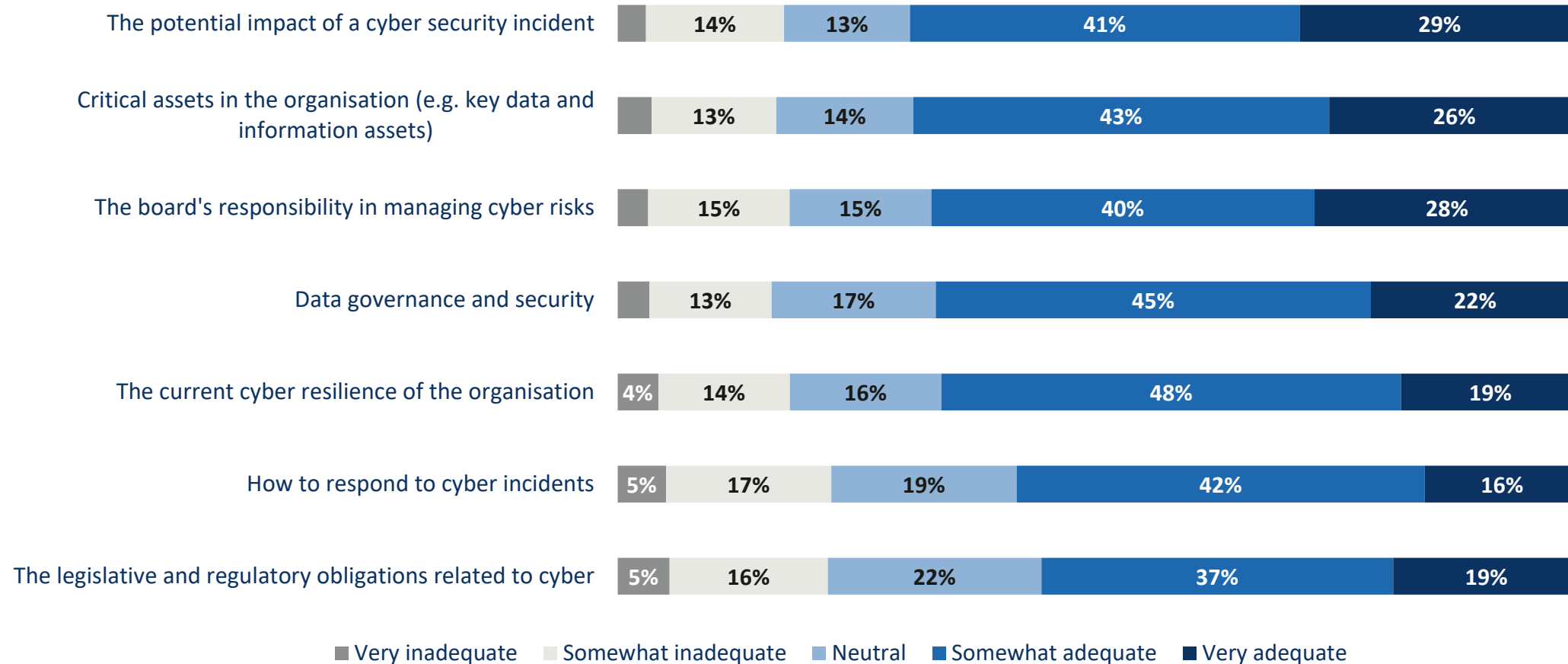


Q. To what extent does your organisation's cyber security activities focus on the below areas?



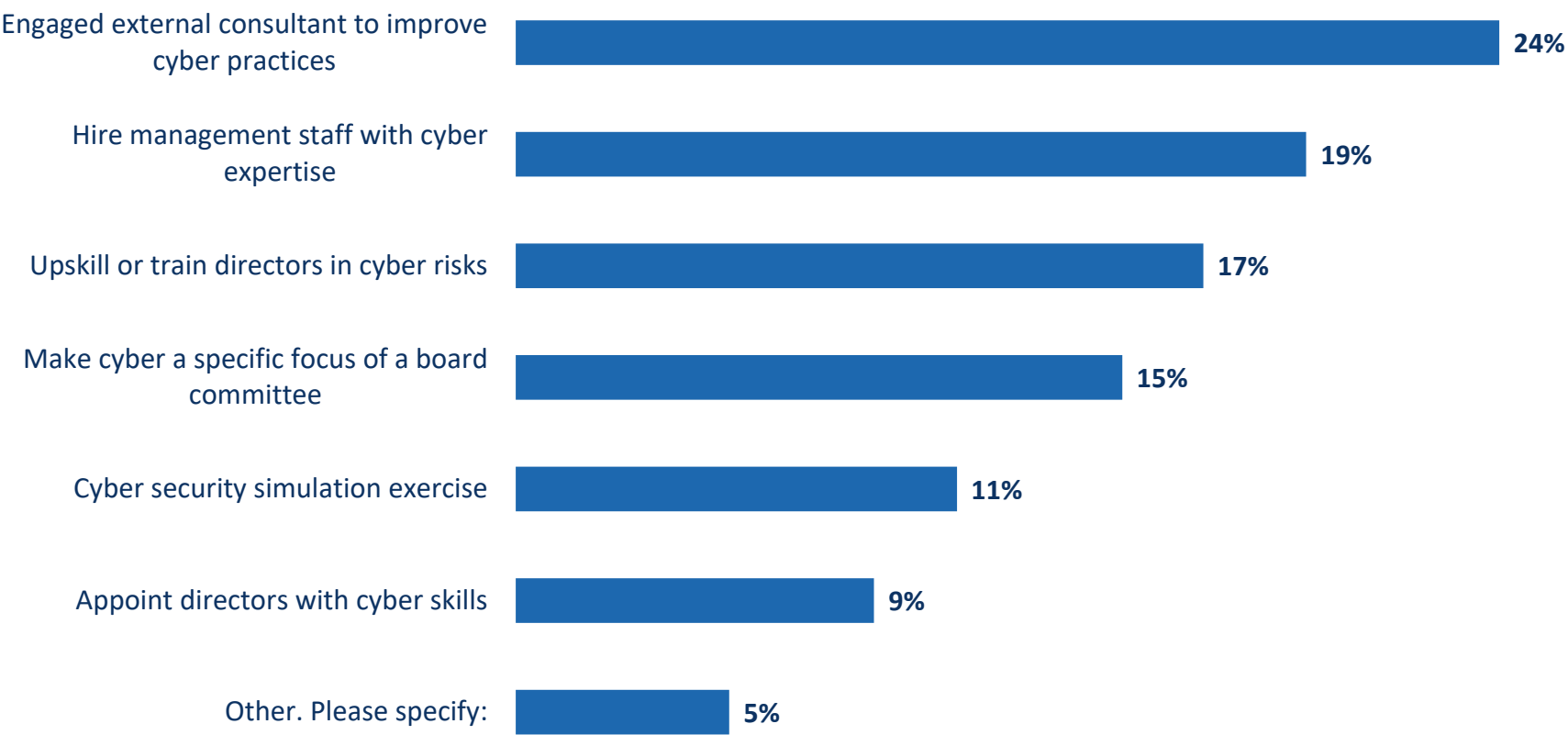
Board's Understanding of Cyber Concepts

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



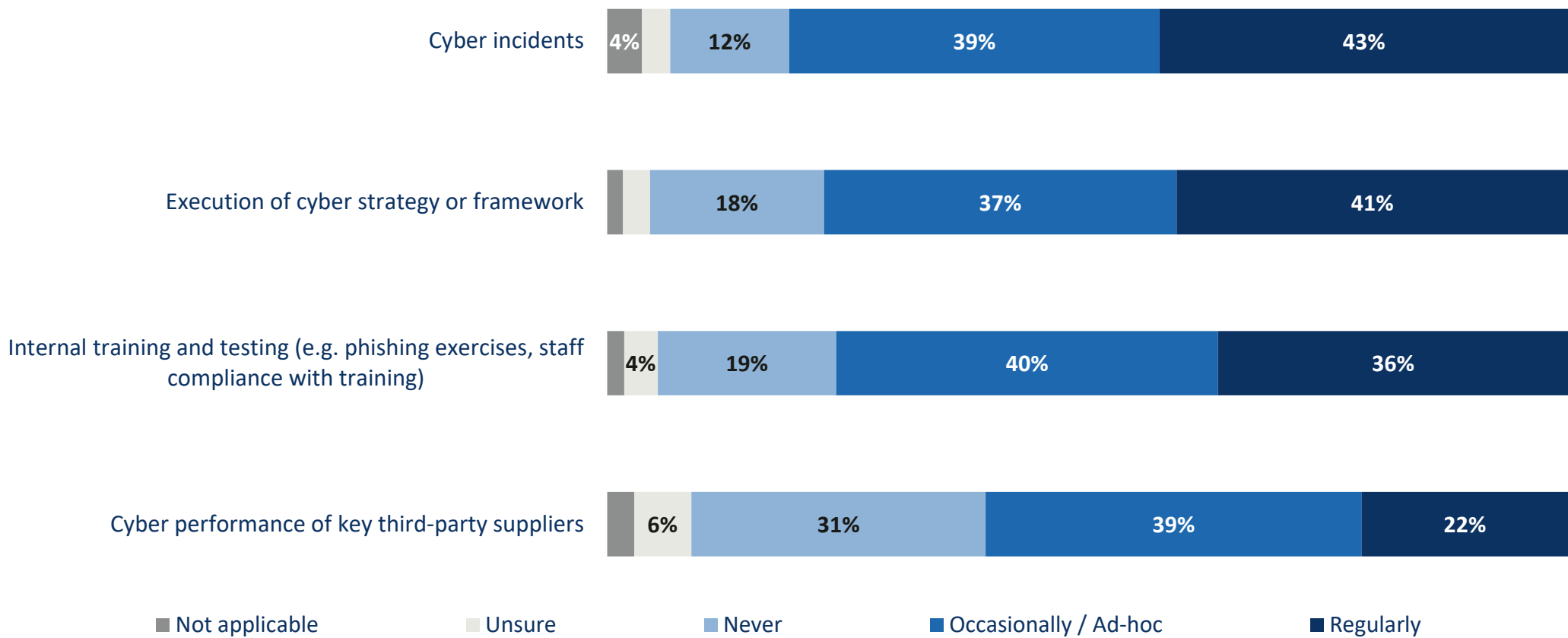
Board Practices to Build Cyber Resilience

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.



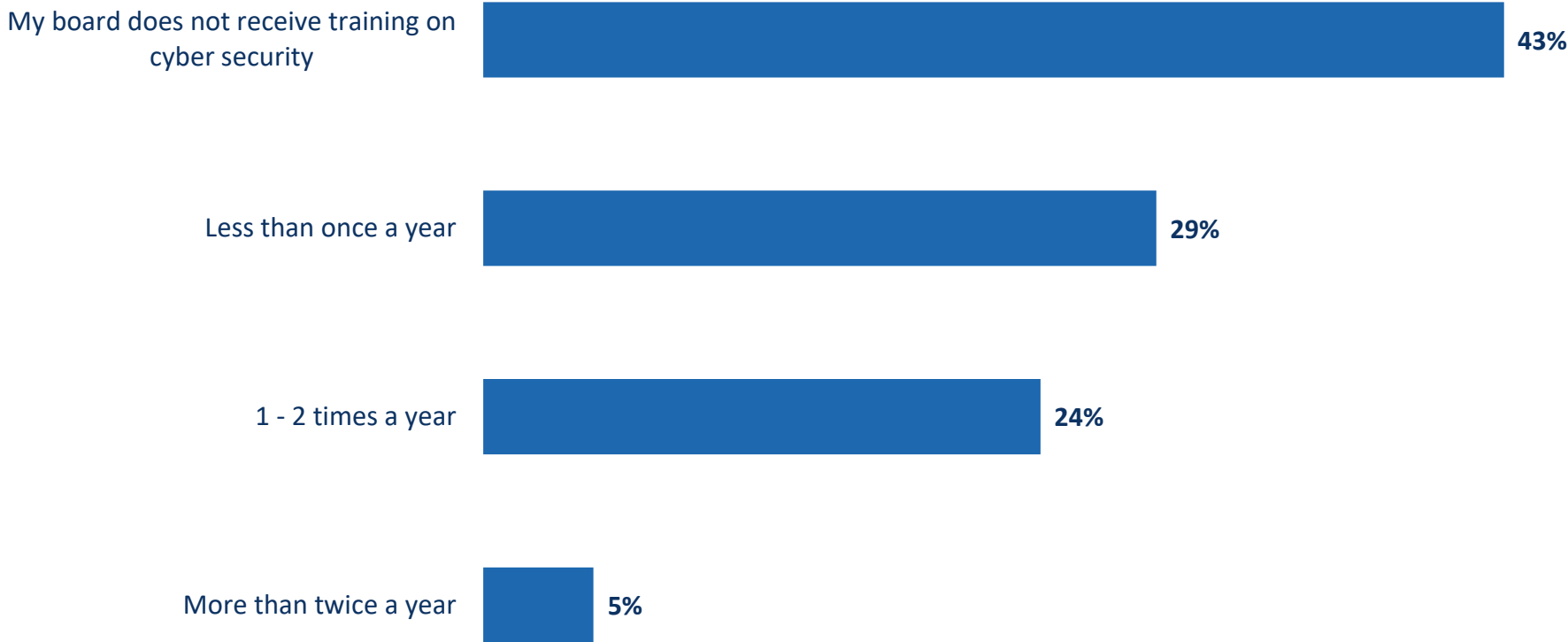
Frequency of Board Reporting

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



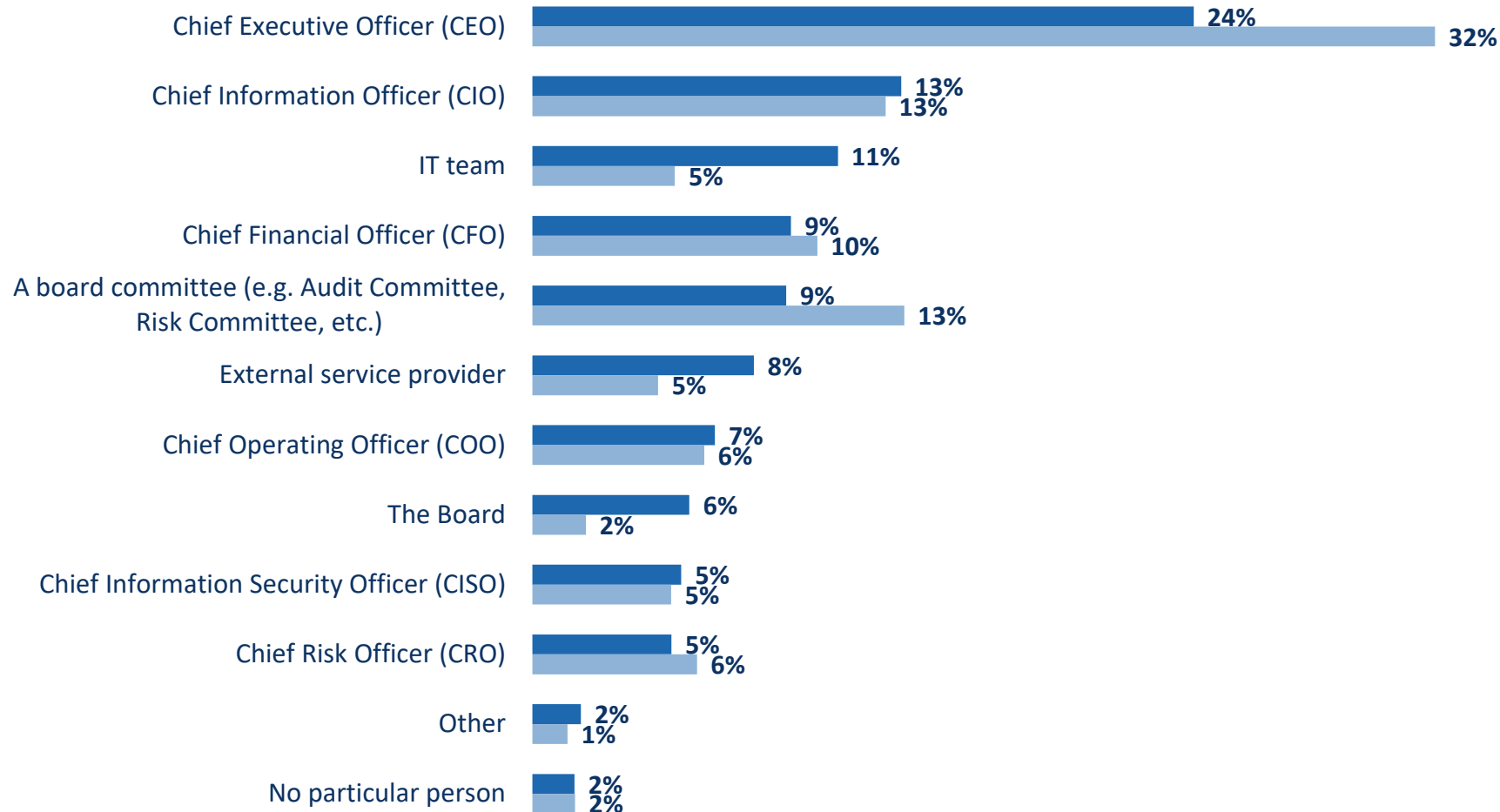
Board Cyber Training

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



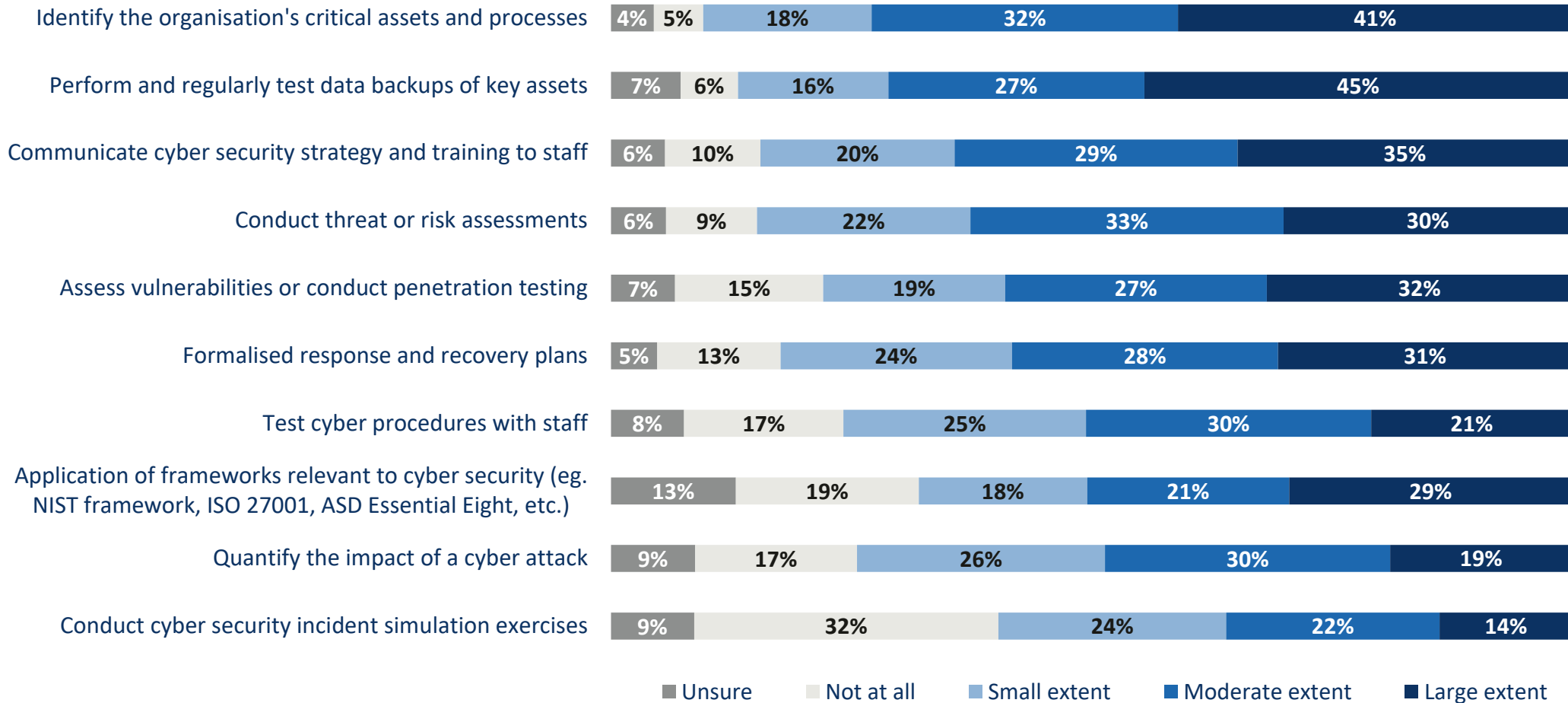
Responsibility for Cyber Security

Q. Who is primarily responsible for: (a) building cyber resilience in your organisation; and (b) reporting to the board on issues related to cybersecurity? Please select maximum 3 options in each row.



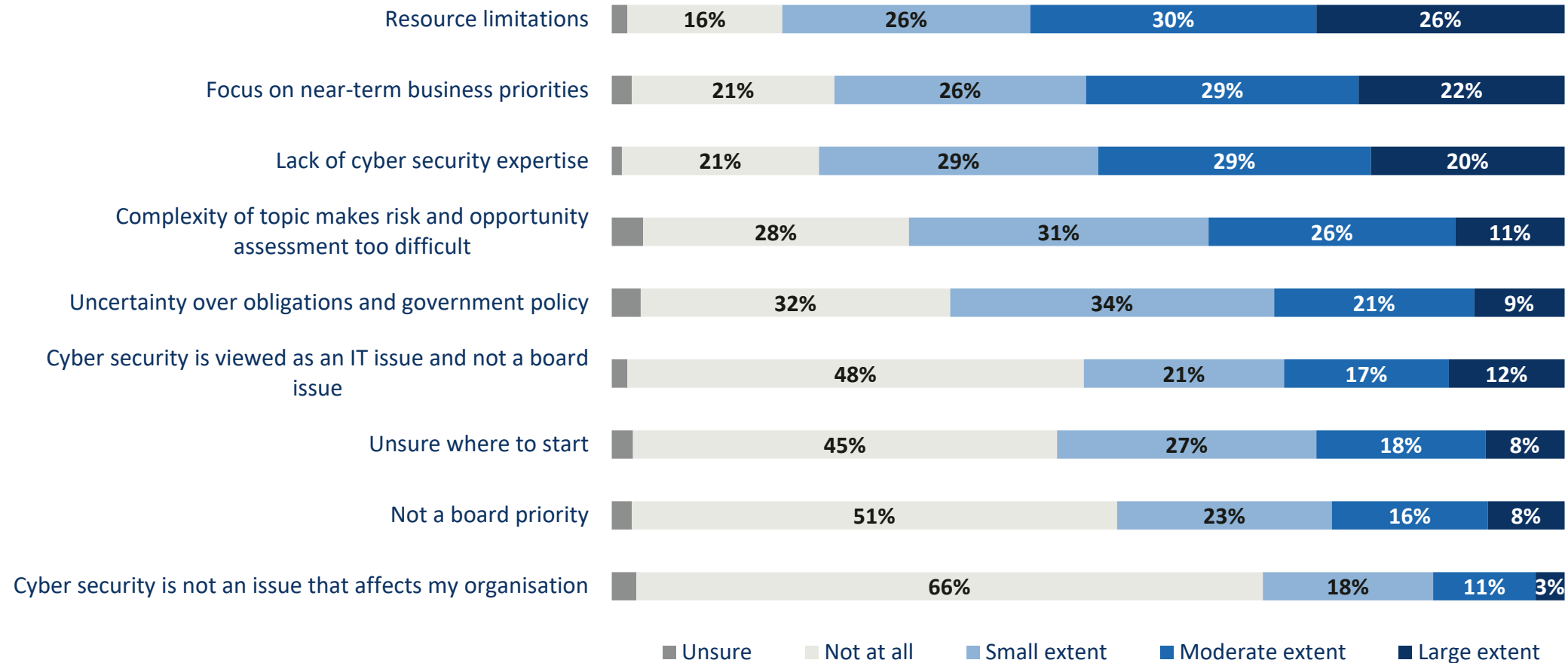
Organisational Cyber Resilience Practices

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?



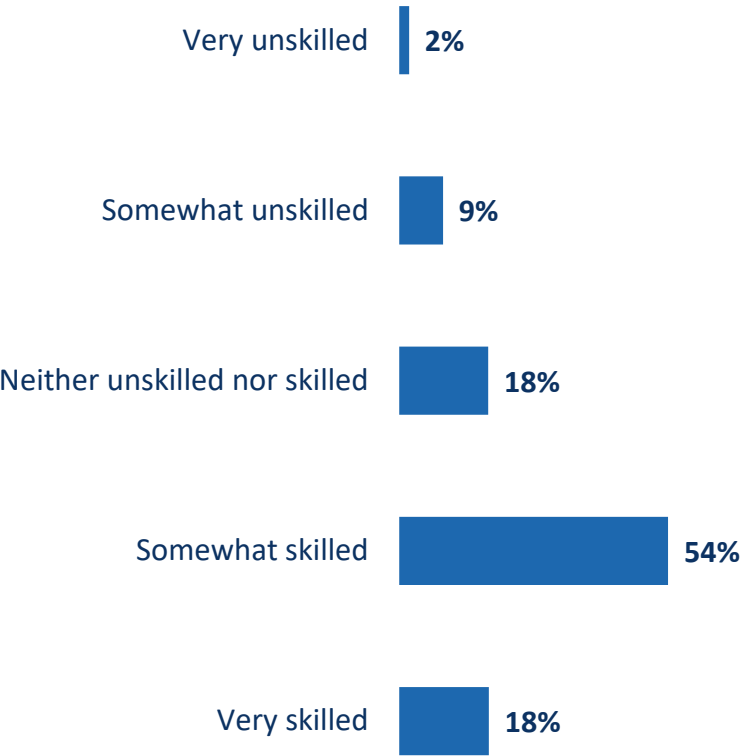
Challenges Faced by Boards

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?

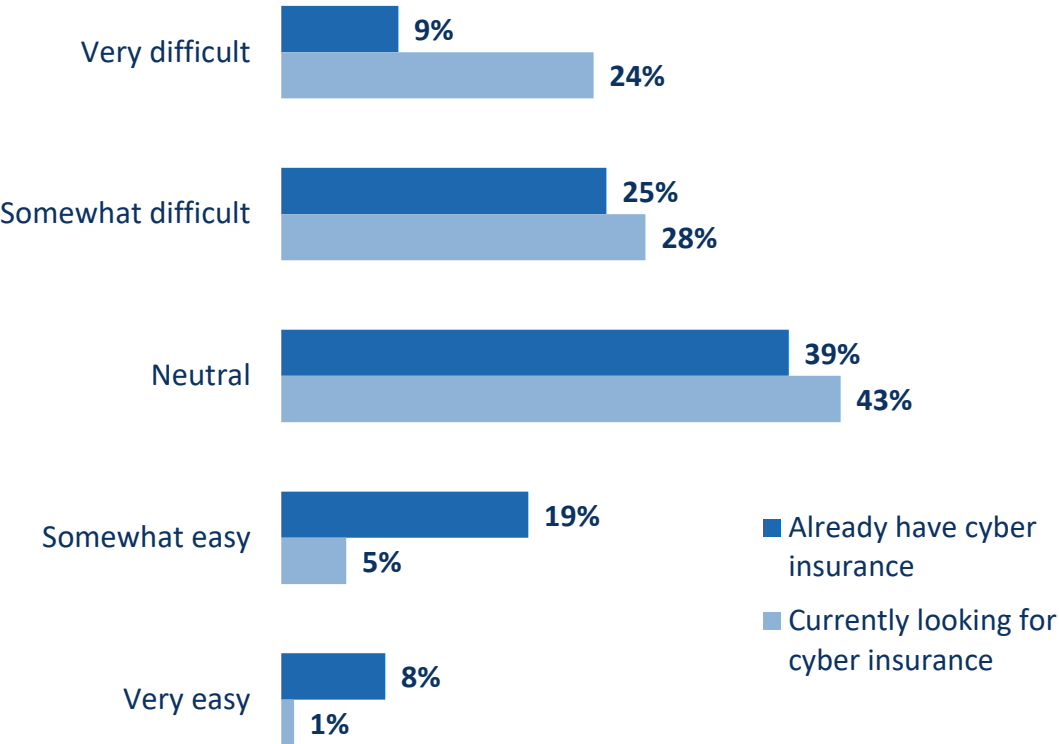


Cyber Insurance Policy

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

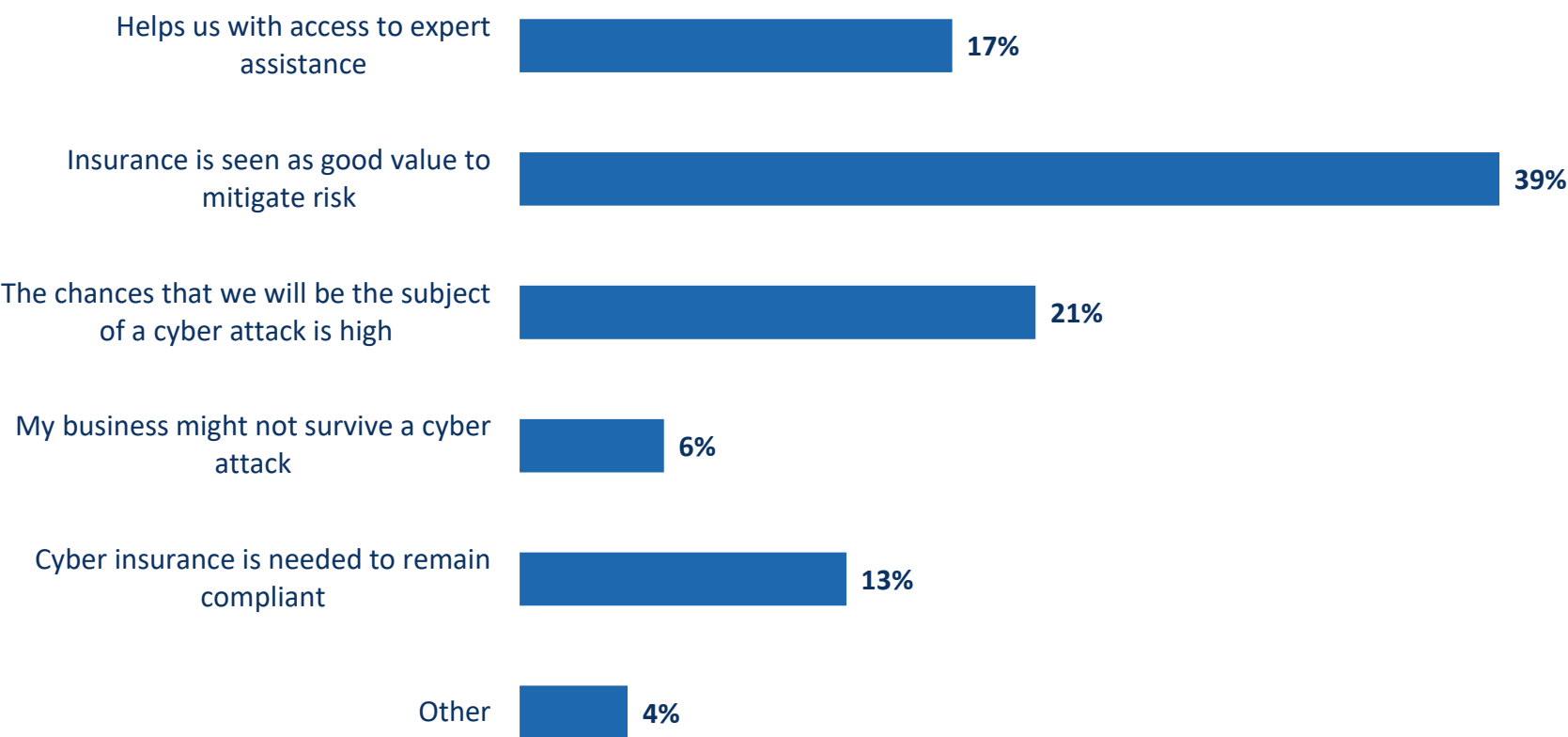


Q. You said that you [already have cyber insurance/are currently looking for cyber insurance], how difficult was it to find a policy that was suitable for your organisation?



Reasons for Obtaining Cyber Insurance

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





THANK YOU

For more information about the results:

E: policy@aicd.com.au

