Australian National University

WEAKEST LINKS:
CYBER GOVERNANCE AND THE THREAT TO MID-SIZED ENTERPRISES

Dr Tim Legrand

November 2016

A report by the National Security College in partnership with Macquarie Telecom Group

National Security College

Crawford School of Public Policy

ANU College of Asia & the Pacific

macquarie TELECOM GROUP

CONTENTS

The National Security College is a joint initiative of the Commonwealth Government and The Australian National University

BACKGROUND

The governance of cyber security has become a pressing challenge to both the public and private sector. Currently, cyber crime is the second most-reported economic crime, affecting 32 per cent of organisations,[1] at a cost to the Australian economy that is estimated to be as high as $17 billion annually.[2] Digital vulnerabilities can also threaten considerable reputational damage, as demonstrated by recent cyber attacks affecting the Australian Bureau of Meteorology,[3] Yahoo,[4] Sony[5] and the Australian Bureau of Statistics.[6]

With the release of *Australia's Cyber Security Strategy (2016)*, the Commonwealth has committed to invest $230 million over four years to counter the growing threat of cyber attacks to Australia's economic security. The Strategy underlines how "cultural change will be most effective in mitigating this form of cyber attack" and suggests "cyber security is a strategic issue for leaders – ministers, senior executives and boards – not just for IT and security staff."[7]

However, wider research on the governance of cyber security suggests that, at present, board executives have little awareness of the full implications of digital threats to their organisations. One survey found that more than 90 per cent of corporate executives said they cannot read a cyber security report and are not prepared to handle a major attack.[8] Further, 60 per cent of all attacks targeted small and medium-sized businesses,[9] yet the Strategy's cyber security 'health checks' initiatives are initially confined to executives and boards in the ASX100, and separate initiatives to provide grants to businesses to have their defences tested are confined to small businesses of fewer than 20 employees. Medium-sized enterprises, whose needs are as complex and are as extensively interconnected as many Top 100 businesses, pose a potential 'weak link' in the national cyber security posture.

1 PwC (2016). *Global Economic Crime Survey 2016*, available at: http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html

2 Commonwealth of Australia (2016). *Australia's Cyber Security Strategy*, available at: https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

3 http://www.abc.net.au/news/2016-04-21/australia-admits-it-can-launch-cyber-attacks-turnbull/7343620

4 http://www.abc.net.au/news/2016-09-23/yahoo-hack-hit-500-million-users-likely-state-sponsored/7870534

5 http://www.wsj.com/articles/data-breach-sets-off-upheaval-at-sony-pictures-1417657799

6 http://www.abc.net.au/news/2016-08-10/census-night-how-the-shambles-unfolded/7712964

7 Commonwealth of Australia (2016). *Australia's Cyber Security Strategy*, page 22.

8 Tanium & NASDAQ (2016). *Accountability Gap: Cybersecurity and Building a Culture of Responsibility*, available at http://media.scmagazine.com/documents/223/the_accountability_gap_report__55615.pdf

9 Ibid.

PROJECT DESCRIPTION

With increasing direct and indirect costs incurred by cyber attacks and cyber security, it is imperative to gain evidence-based insights into the governance of cyber security in medium-sized private enterprises and government agencies.

In partnership with the Macquarie Telecom Group, the National Security College designed a research project to acquire qualitative and quantitative insights into the governance of cyber security risks in Australian medium-sized businesses and government agencies. Using an anonymised web-based survey, we invited individuals with cyber security roles or responsibilities to answer a range of questions pertaining to:

- the cyber threats faced by their business/agency
- how these risks were rationalised and reported to the executive team/board
- whether and how cyber threats were communicated to government cyber security initiatives.

The survey acquired 22 separate responses from government agencies and 36 from medium-sized businesses.[10]

10 All participant responses have been anonymised. All invited to complete the survey were provided with a full disclosure of the research aims, research funding and a privacy statement. No inducements of any kind were offered to participants. This research was approved by the ANU Human Research Ethics Committee (Protocol no.: 2016/339).

FINDINGS

Summary

The research discerned widespread frailties in the governance of cyber security among the executive layers of public agencies and private enterprise.

In particular, the findings indicate considerable variation in cyber risk governance arrangements and an absence of cyber risk knowledge at the executive/board level.

Medium-sized businesses report:

> **Considerable variation in their reporting and board-level governance of cyber security risks:** While most businesses (85 per cent) have someone chiefly responsible for cyber security, only 58 per cent of these are on the executive committee, and 69 per cent have other unrelated duties.

> **Insufficient executive knowledge of cyber risks:** 58 per cent of respondents stated their board had a sufficient understanding of cyber risks. Thirty per cent said their board or executive team never receive reports of cyber threats to the company, and 46 per cent said their board discusses cyber security rarely or never.

> **Reluctance to engage with (or unawareness of) government cyber security initiatives:** 29 per cent of respondents would seek to report an attack if they lost client data. Notably, just 21 per cent cited their legal obligation as a reason to report an attack. Awareness of government services was also limited: just 46 per cent were aware of the Australian Cybercrime Online Reporting Network (ACORN), and 47 per cent tended not to report attacks stemming from malware or distributed denial of service (DDoS).

Government agencies report:

> **Cyber risk management is still not prioritised across all agencies:** 84 per cent have an individual chiefly responsible for cyber security, yet only 64 per cent of these sit on the executive team or board, indicating that cyber risk management is not embedded at the highest decision-making levels.

> **Knowledge of cyber risks is still inadequate:** Among these respondents, 41 per cent regard their executive team/board as having poor or limited knowledge of cyber risks, and only 50 per cent of executive teams are provided cyber threat reports monthly or more frequently.

> **Infrequent consideration of cyber risks:** No agency reports reviewing cyber risk management monthly or weekly. This contrasts with private business, where 31 per cent review cyber risk management at least monthly. This reinforces the possibility that the culture of cyber security is not yet mature.

RISKS AND IMPLICATIONS

The patchwork of governance arrangements – shown in the variation of titles, responsibilities and executive team membership – reflects latent problems with executive knowledge over the risks of cyber threats, their responsibilities, and how to improve cyber threat management.

1. **It is likely that medium-sized companies and agencies remain unable to acquire the requisite experience and expertise in cyber security management.** There is significant variance in cyber security roles, processes and internal/external reporting. The relative absence of systematic cyber risk discussion at board level indicates a cyber compliance culture rather than an active cyber risk management culture.
2. **The data indicates that executive/board knowledge of cyber risks is inadequate.** The indication that executive knowledge of cyber risks is poor underlines the reduced capacity to adequately understand, and take seriously, the full range of threats to companies or agencies.
3. **It is likely that the full range of risks are not being adequately reported.** The relatively high levels of tolerance for persistent – and perceived 'low-level' – threats, such as malware and DDoS, suggests that the relevant Australian cyber security initiatives do not receive information on the range of cyber threats faced by Australia. This means authorities may lack the accurate and comprehensive information needed to appropriately prioritise national cyber defence initiatives.
4. **Government cyber security initiatives are not achieving purchase with medium-sized businesses.** With just 38 per cent of companies familiar with CERT Australia (the Computer Emergency Response Team), and 46 per cent with ACORN, medium-sized enterprises are not taking full advantage of the services available to them.

RECOMMENDATIONS

Cyber risk management should be 'normalised' as core board business, asserted as a priority on a par with financial risk management as part of all government and business decision-making.

Benefit: The increasing array of digital risks are integrated into core organisational decision-making, risk assessments, investments and strategy planning. Consequently, executive teams develop better situational awareness of their organisation's key threats and opportunities.

Standardised cyber risk reporting for medium-sized businesses should be developed and promoted to achieve common risk management standards and protocols.

Benefit: A common reporting approach permits greater opportunity for the development of interoperable training, risk assessment and best practices at the executive level. It creates greater opportunities for government to provide broad cyber governance advice.

Companies and government agencies should discern and address, where necessary, low levels of cyber literacy amongst its executive teams.

Benefit: The move towards collective knowledge of cyber risks spreads the burden of risk assessment across the executive team, creating resilience in the organisation's decision-making apparatus. It further avoids the concentration and 'bracketing' of expertise on a single board member (e.g. the Chief Information Security Officer).

Collaboration with government cyber security agencies should become the default policy setting for businesses and agencies; i.e. non-reporting of cyber threats should become the exception, not the rule.

Benefit: The collective security of all Australian companies is enhanced with the timely sharing of threats to public and private organisations. Sharing by default enhances the government's awareness of the threat landscape and improves its capacity to act in the national and sectoral interest.

The Commonwealth should offer incentives to companies and organisations to provide early and full disclosures of cyber breaches. In addition, executive teams should mandate the disclosure of all information security breaches to the relevant government agencies.

Benefit: The early disclosure of information-security breaches enables the government to work with organisations to minimise losses, pursue the perpetrators, and identify wider risks to the sector or public.

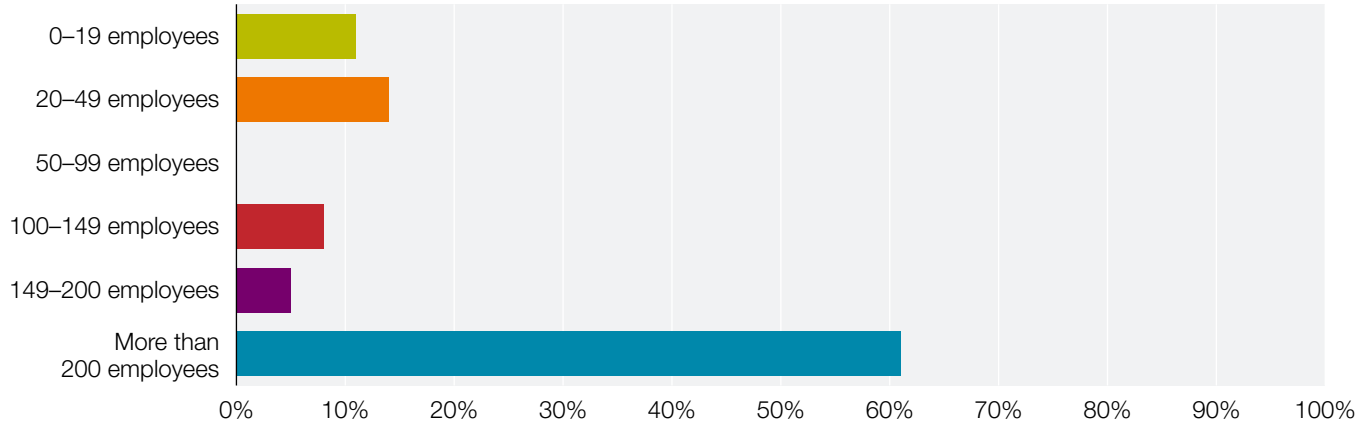
NATIONAL SECURITY COLLEGE & MACQUARIE TELECOM CYBER SECURITY SURVEY

Methodology

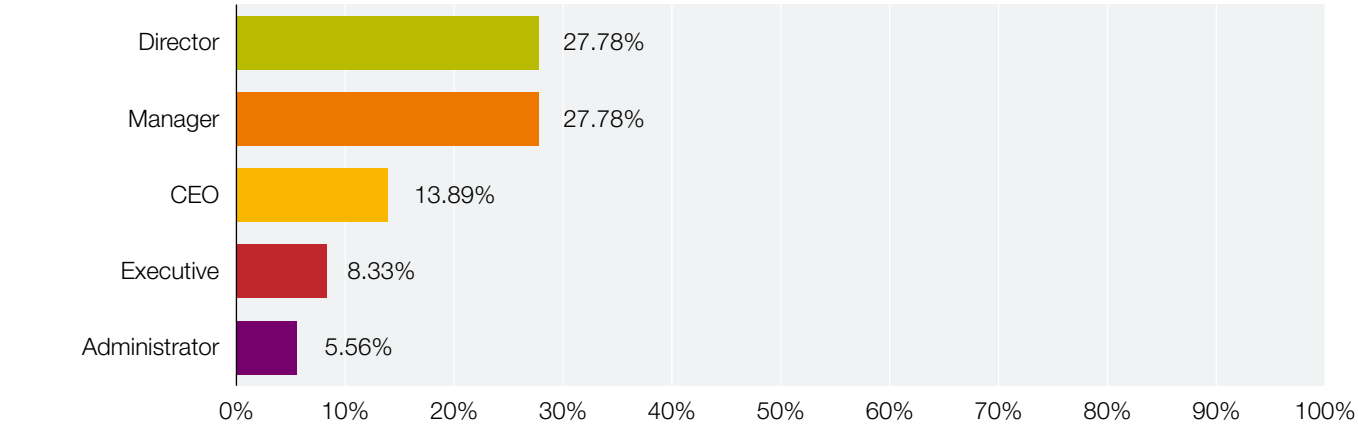
- An Australia-wide cyber security survey targeting the governance of cyber security in federal government and mid-tier industry
- Administered via online survey using 36 closed and open-ended questions
- Targeted cohorts of: (i) medium-sized industry representatives; (ii) government departments/agencies not protected by ASD
- Two separate surveys administered to reflect different challenges and organisational structures of government and industry
- Survey invitations sent to approximately 60 government departments and agencies (targeting individuals with a specific IT mandate in their role); 22 completed the surveys.

Industry findings

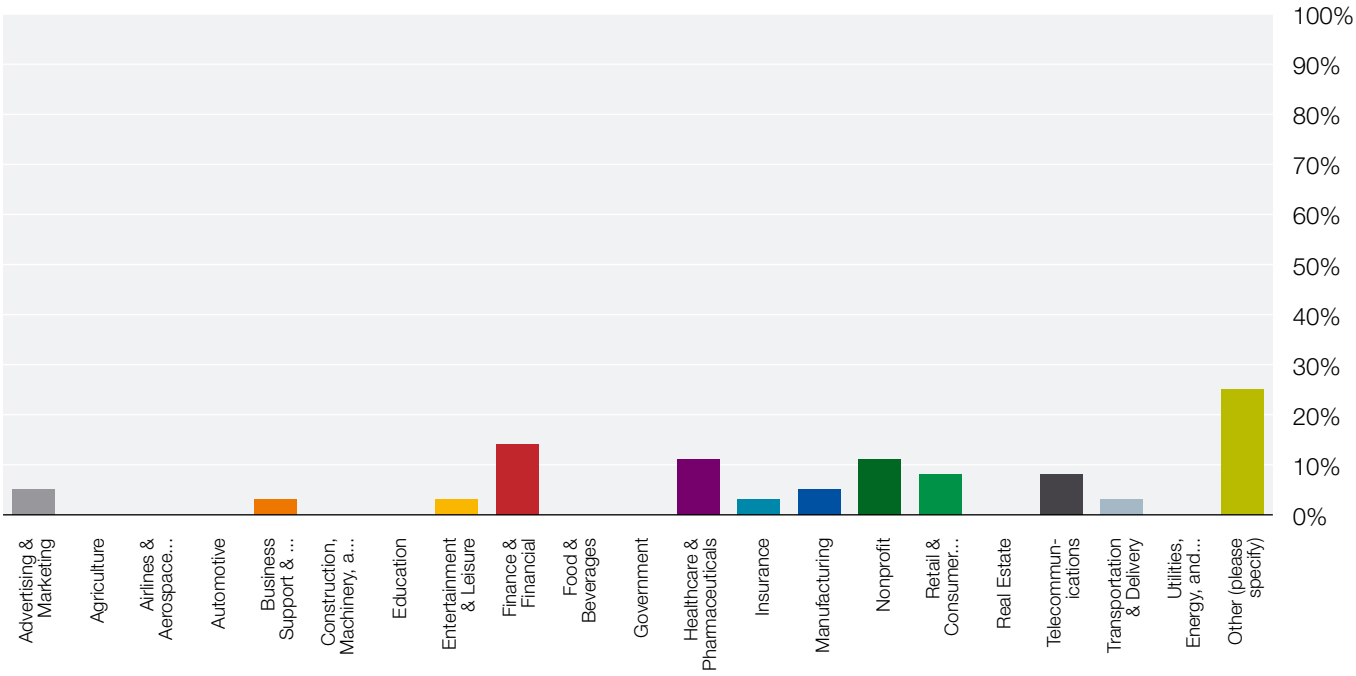
Q1a. What is the size of your company?



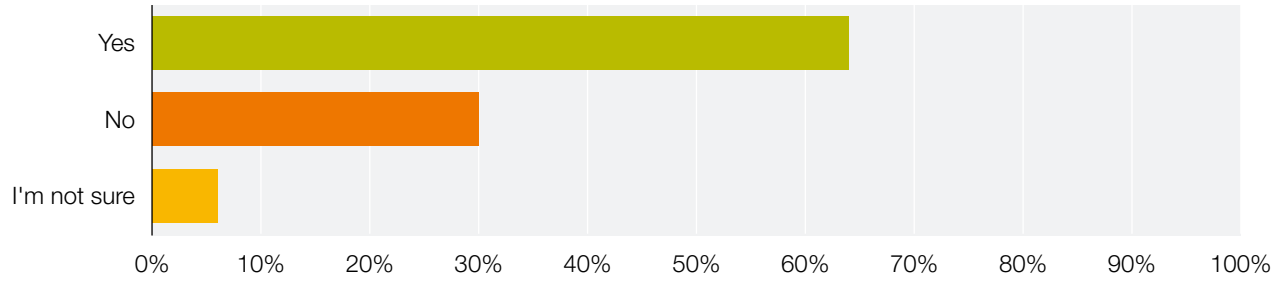
Q1b. What is your role in the company?



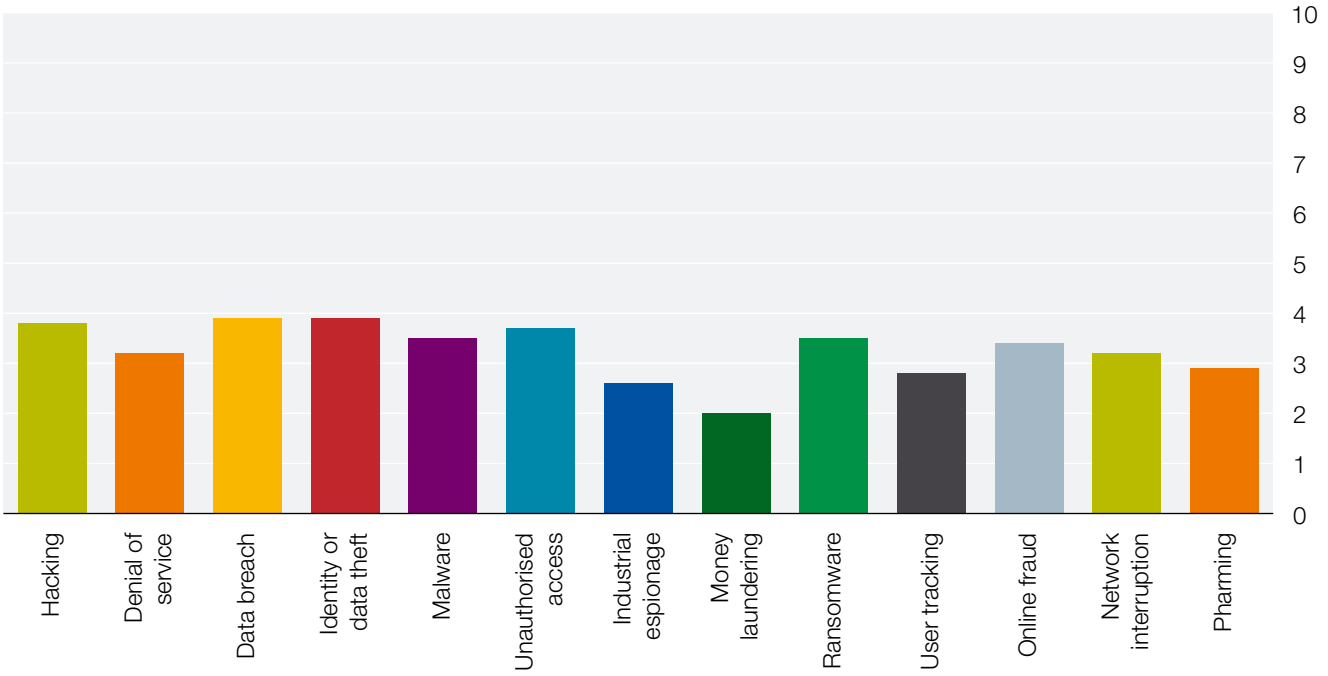
Q2. Which of the following best describes the principal industry of your company?



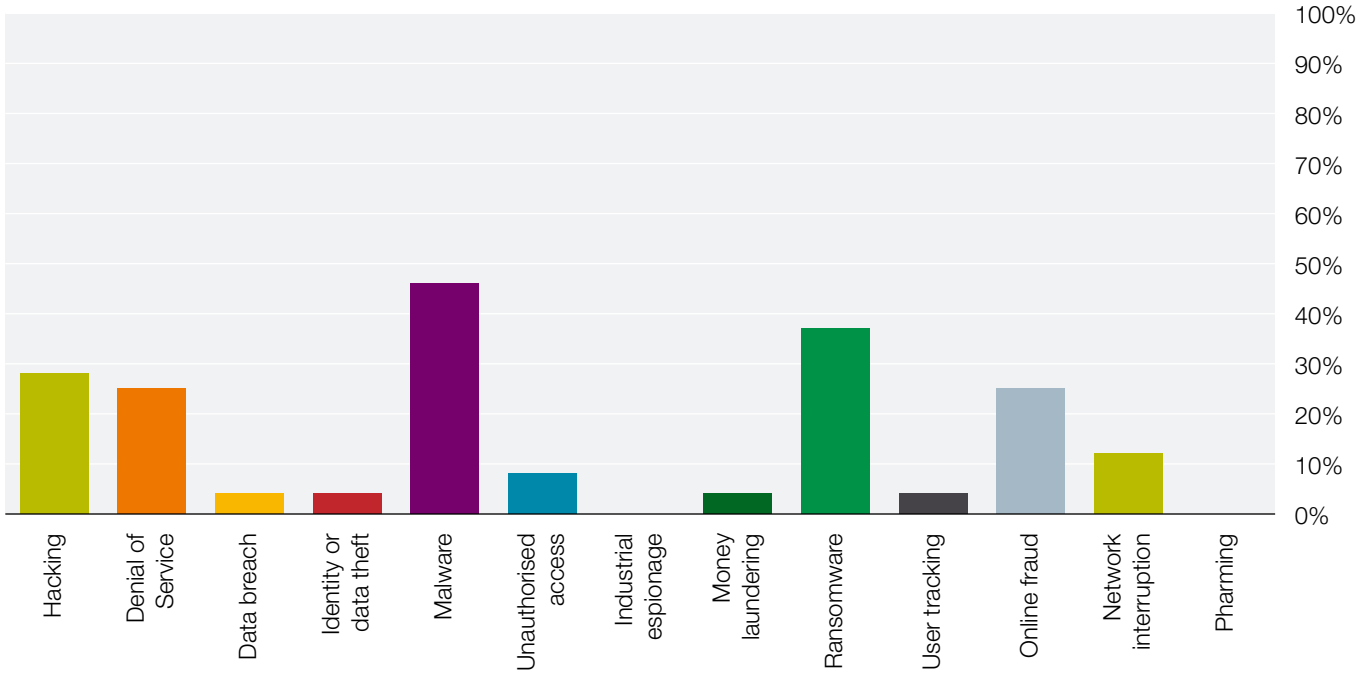
Q4. Does your role entail specific cyber risk assessment duties?



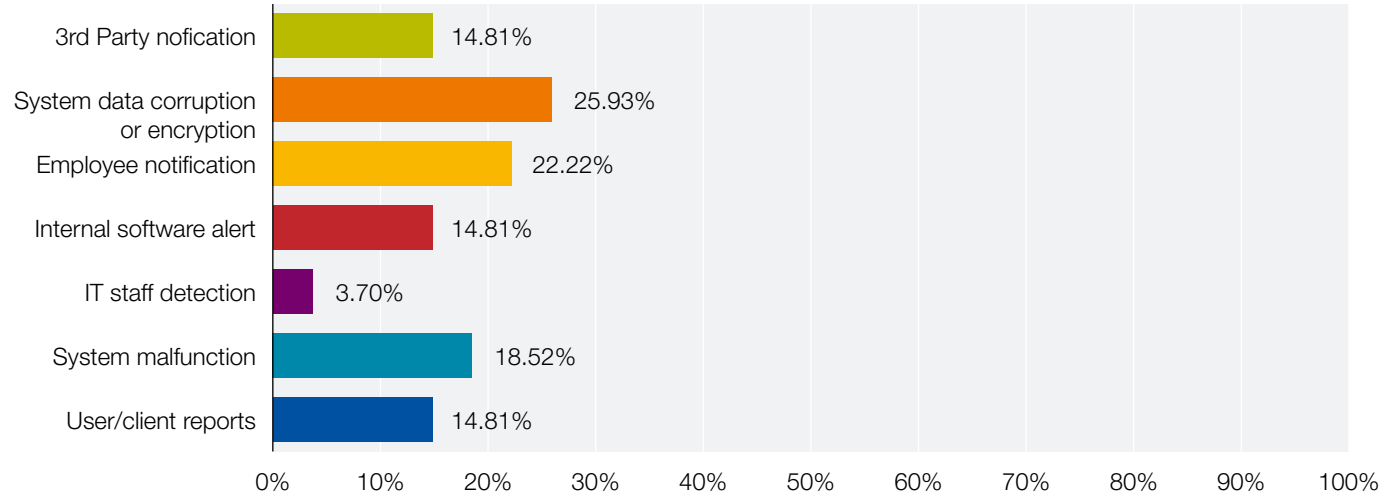
Q5. The following are examples of existing cyber threats. How would you rate the seriousness of these threats to your business?



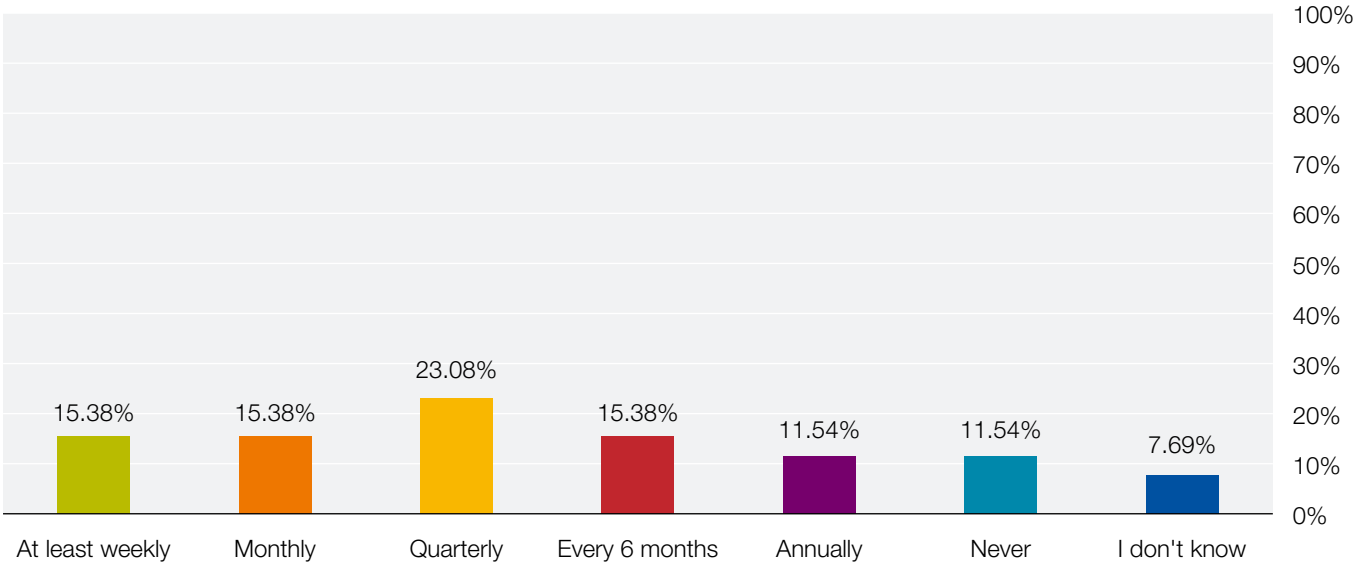
Q6. In the past 12 months, which of the following attacks has your business experienced?



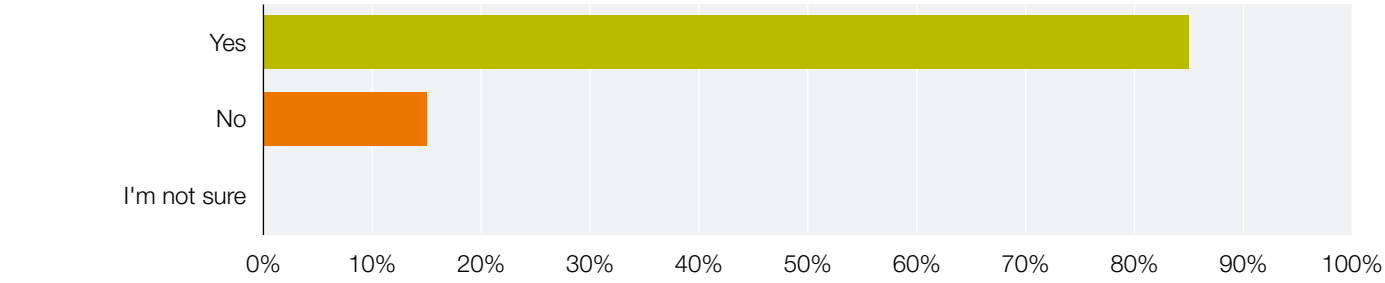
Q7. Thinking about the cyber attacks you have experienced, what is usually the first indication that your business has suffered such an attack?



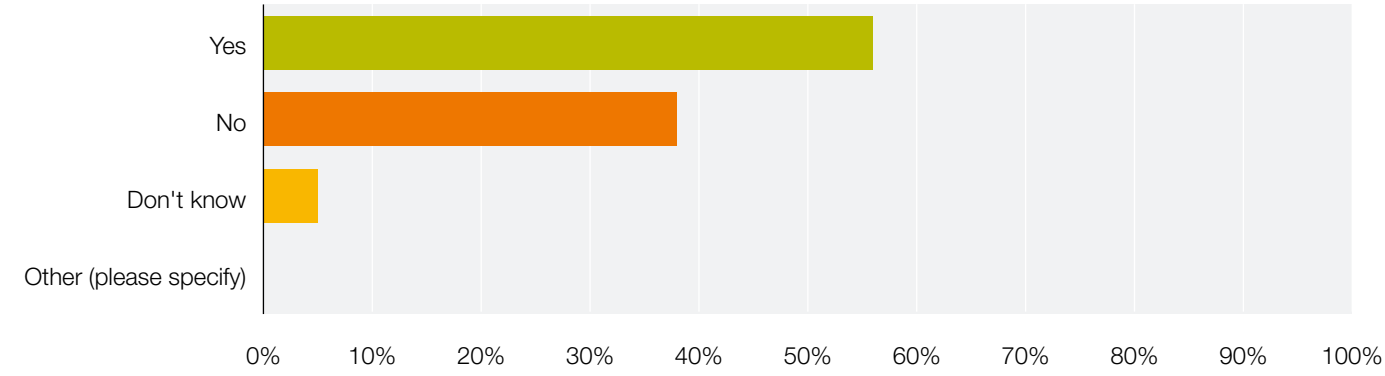
Q11. How often does your business review its cyber risk management?



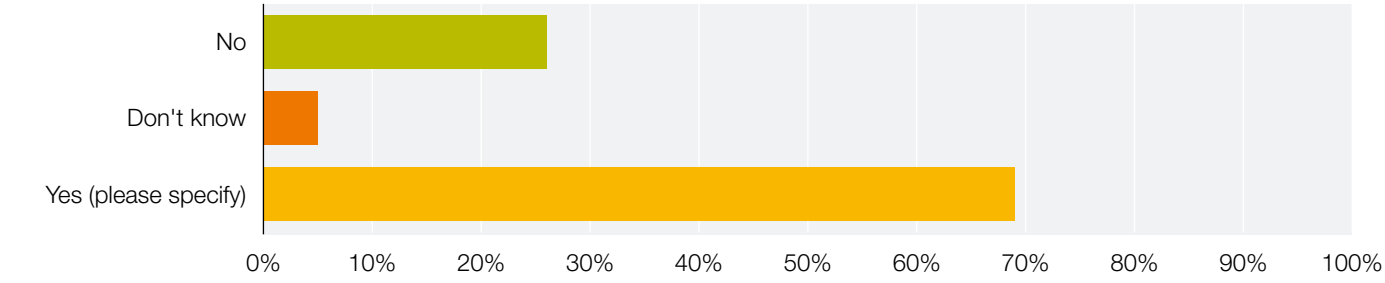
Q12. Do you have someone who is chiefly responsible for information security?



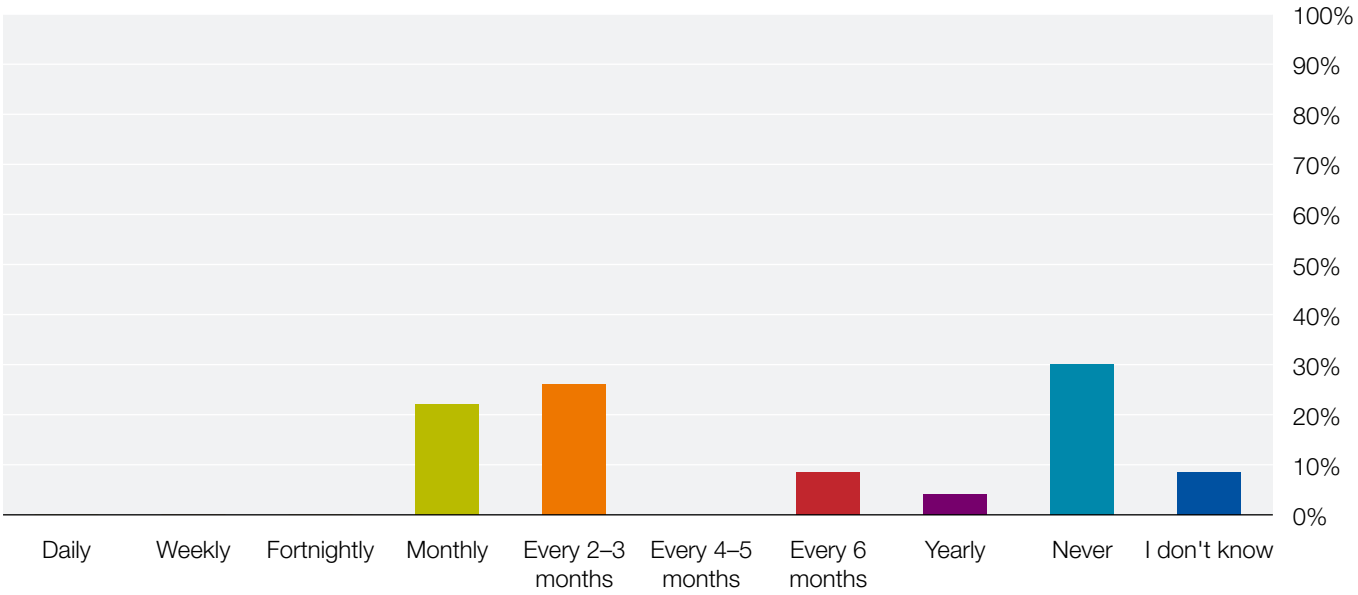
Q14. Does she or he sit within the executive committee?



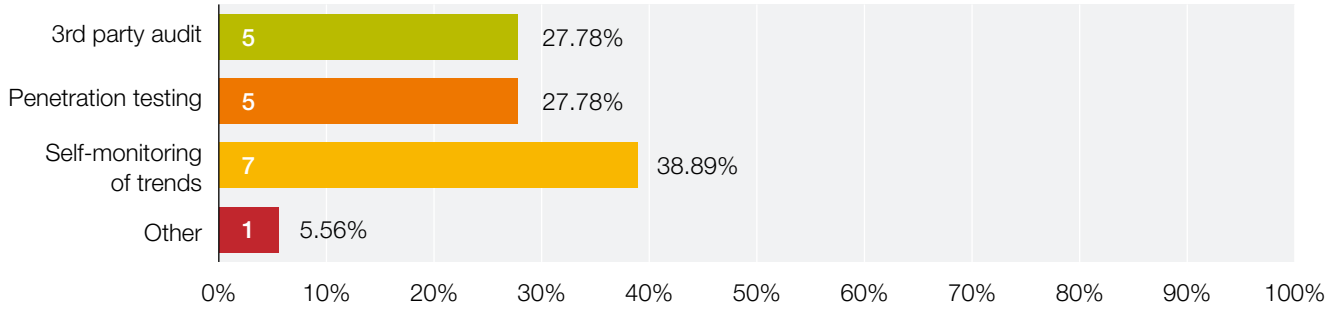
Q15. Does she or he have other responsibilities?



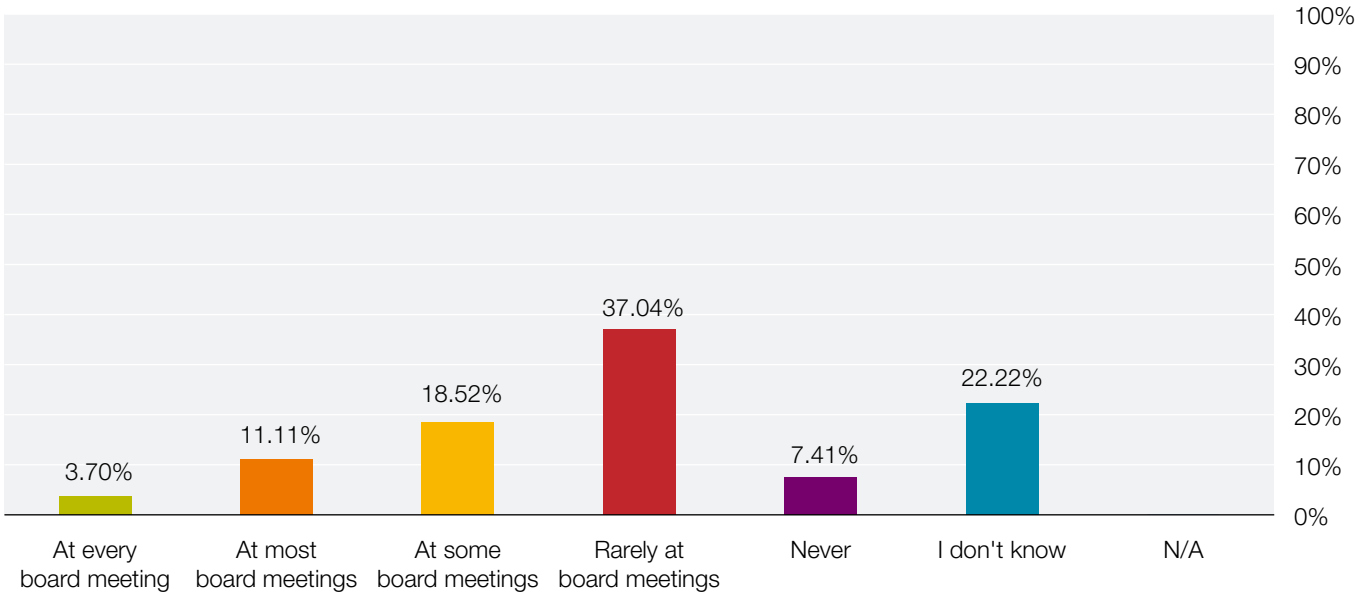
Q17. How often does your board receive reports on cyber threats to the company?



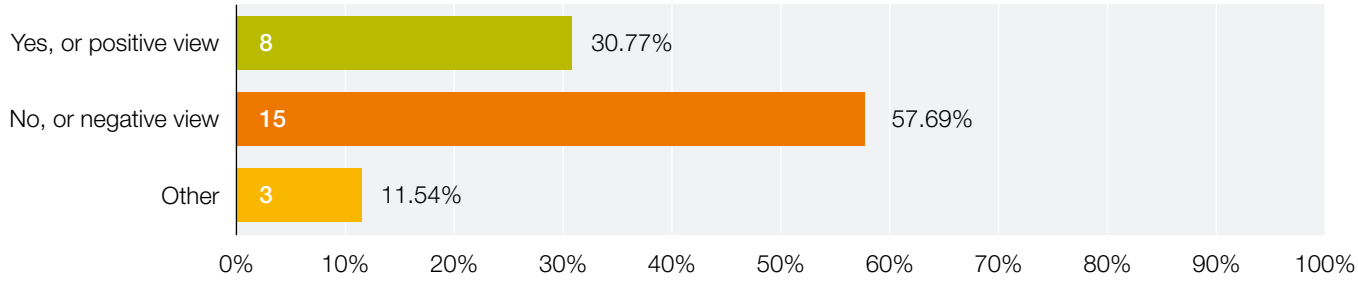
Q18. What measure(s) does your company use to gauge its vulnerability to cyber threats?



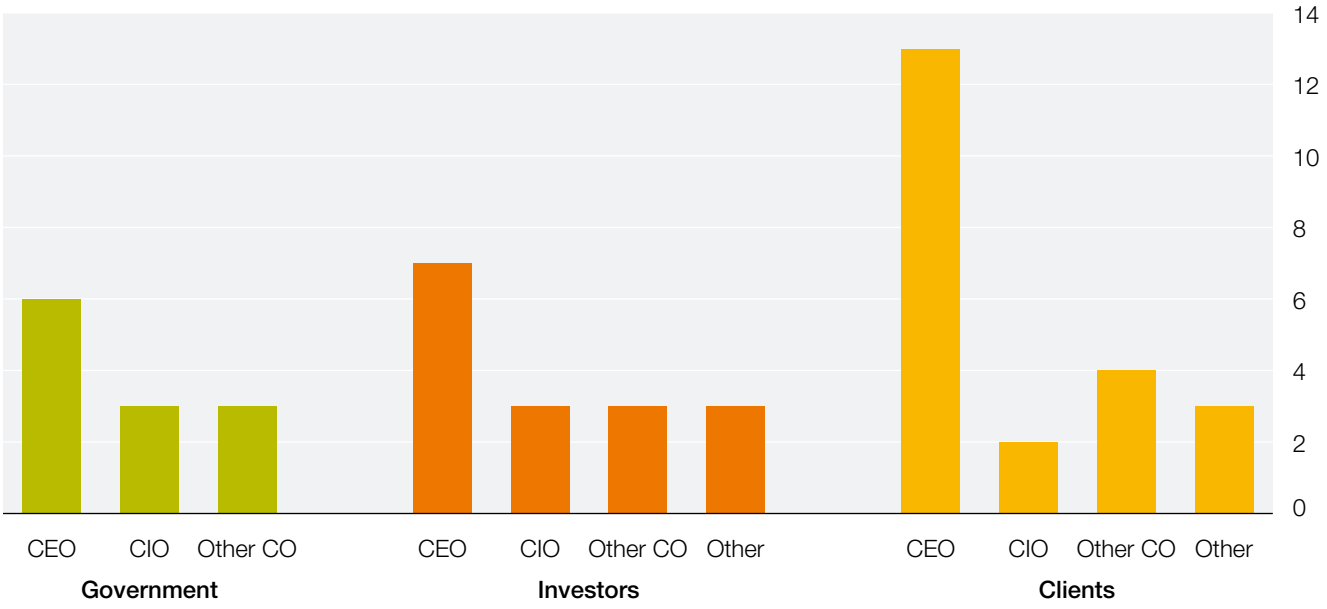
Q19. How often does your board discuss cyber security?



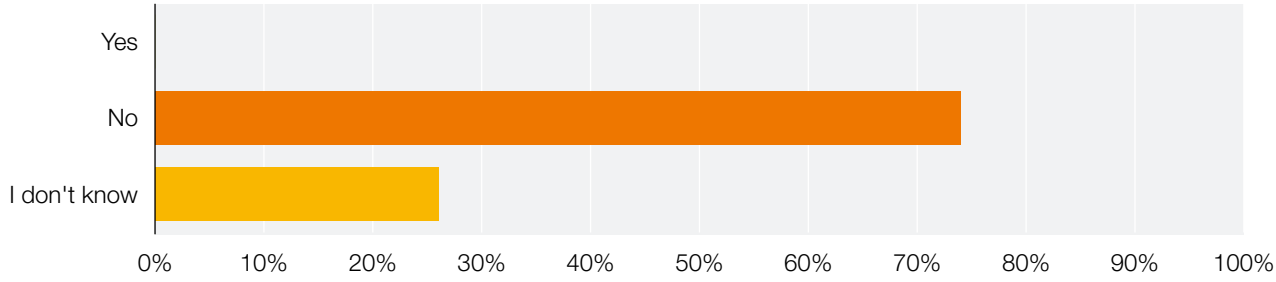
Q20. In your view, does the board have sufficient understanding of cyber risks to your business?



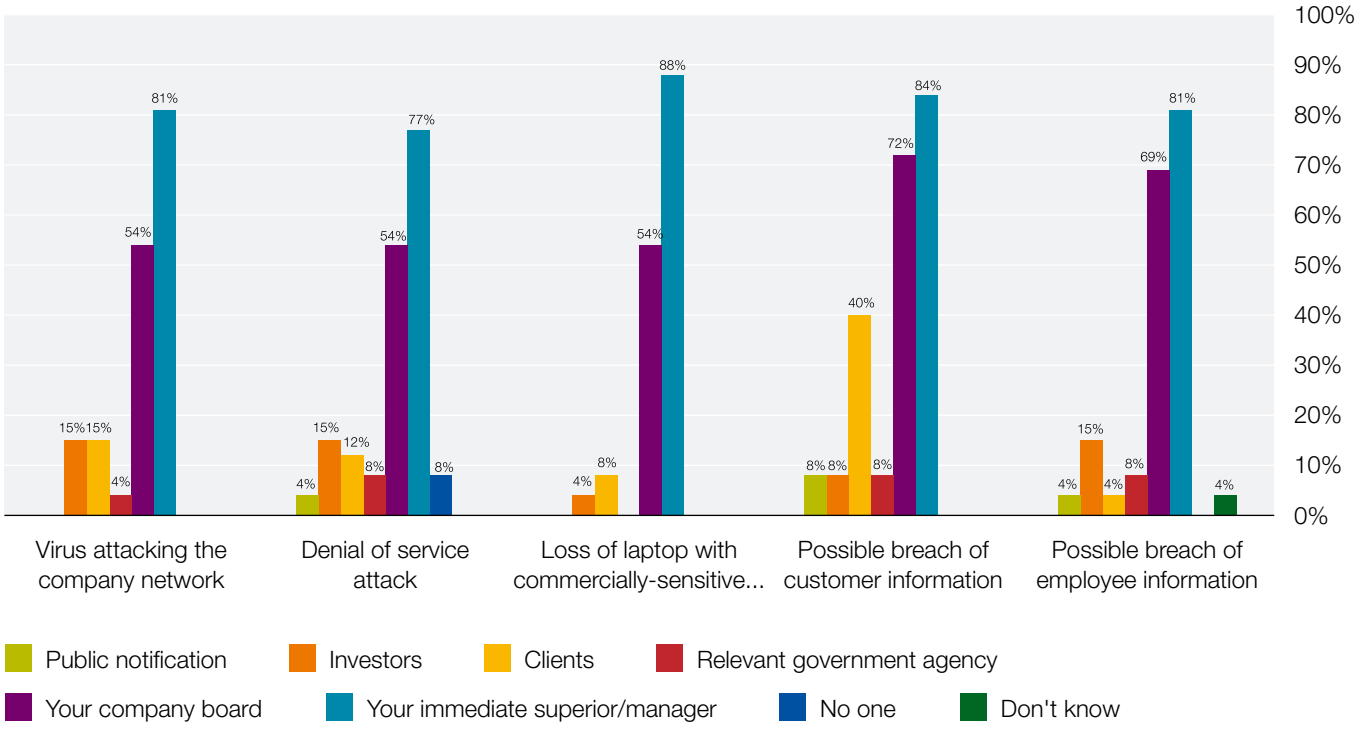
Q21. In the event of a cyber attack resulting in the loss of information or business continuity, who in your business is responsible for notifying (a) government; (b) investors; (c) clients?



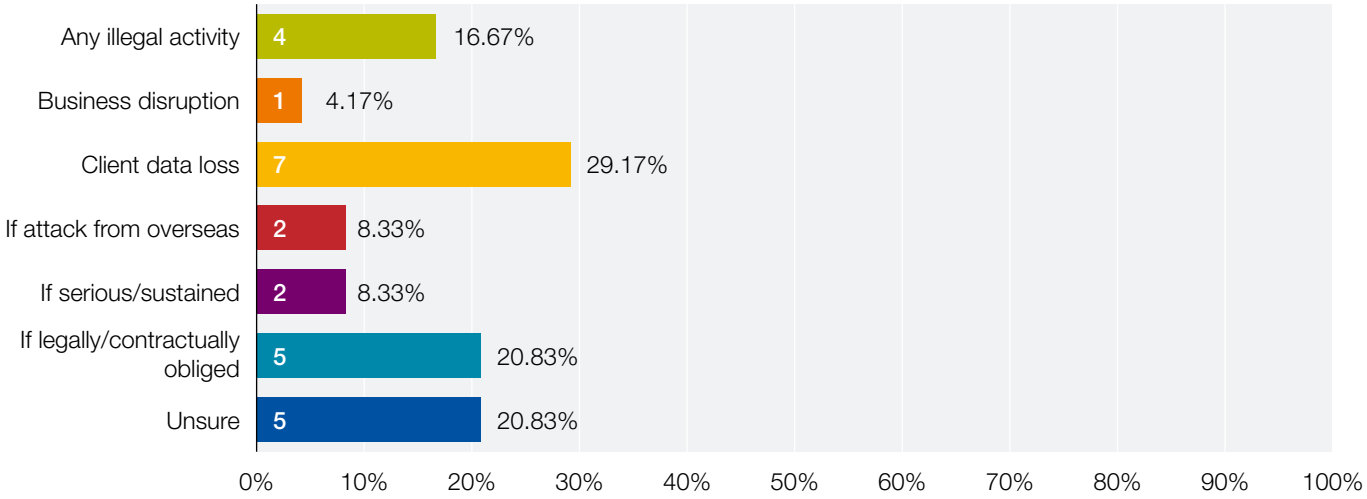
Q24. Do you provide information on your cyber risk management in your annual report?



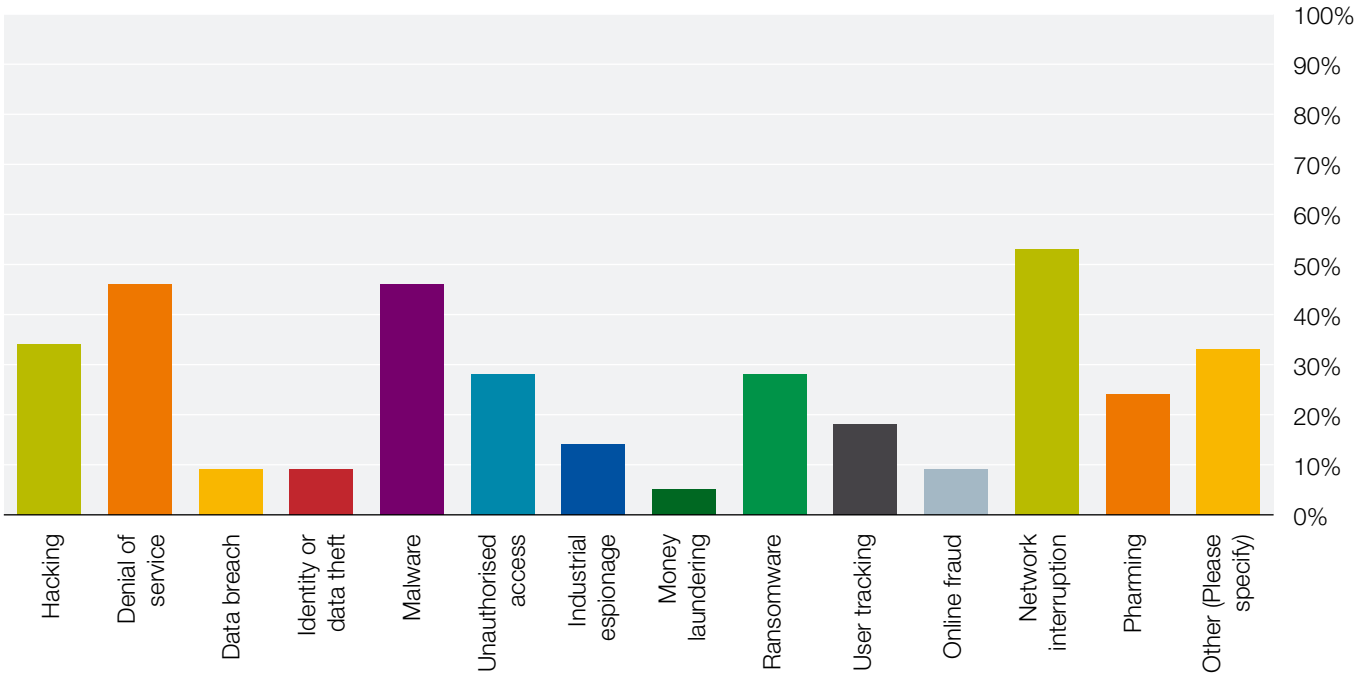
Q25. If the following incidents were to occur, to whom would you report the following incidents? (Select all that apply)



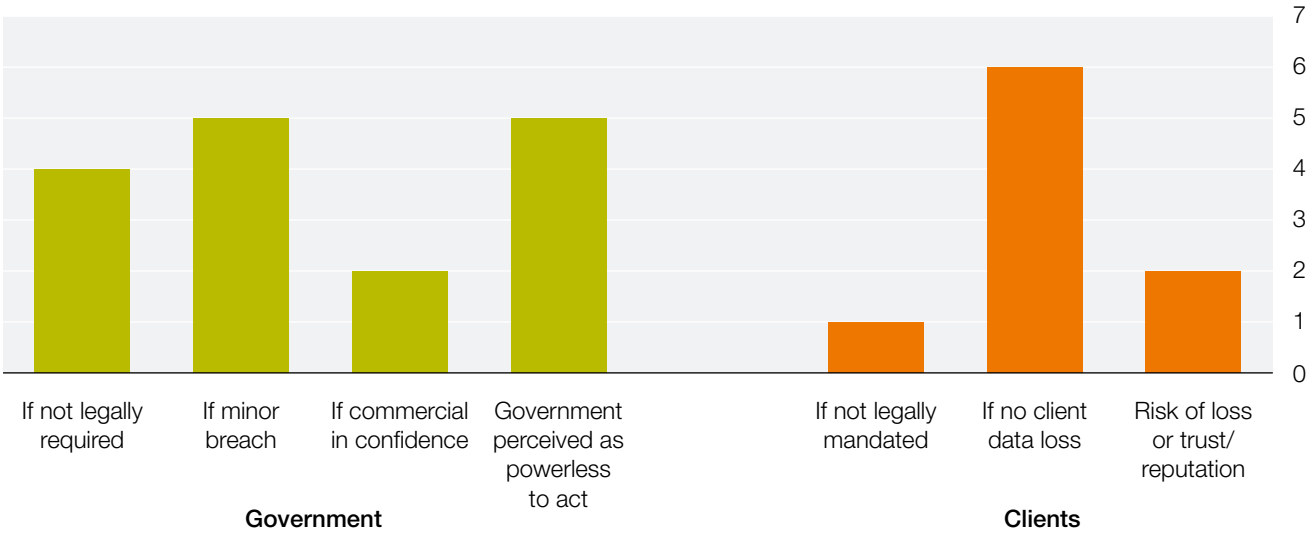
Q26. Under what circumstances would you actively seek to report a cyber attack to a relevant government agency?



Q27. Are there any types of cyber attack you do not tend to report to government agencies?

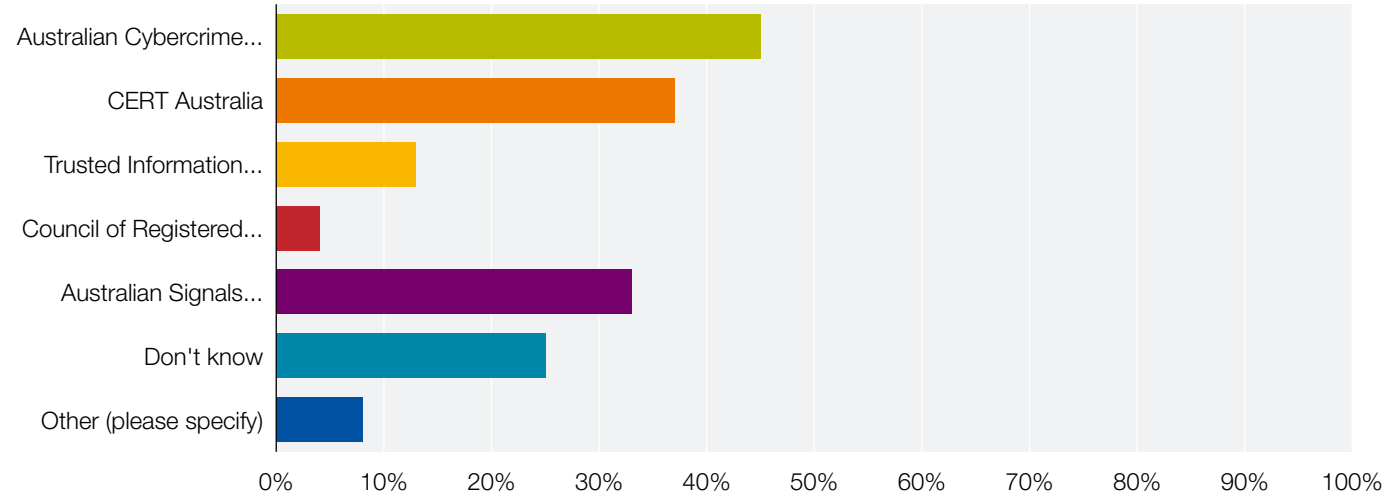


Q28. In your view, under what circumstances do businesses tend to refrain from reporting a cyber attack to government or clients?



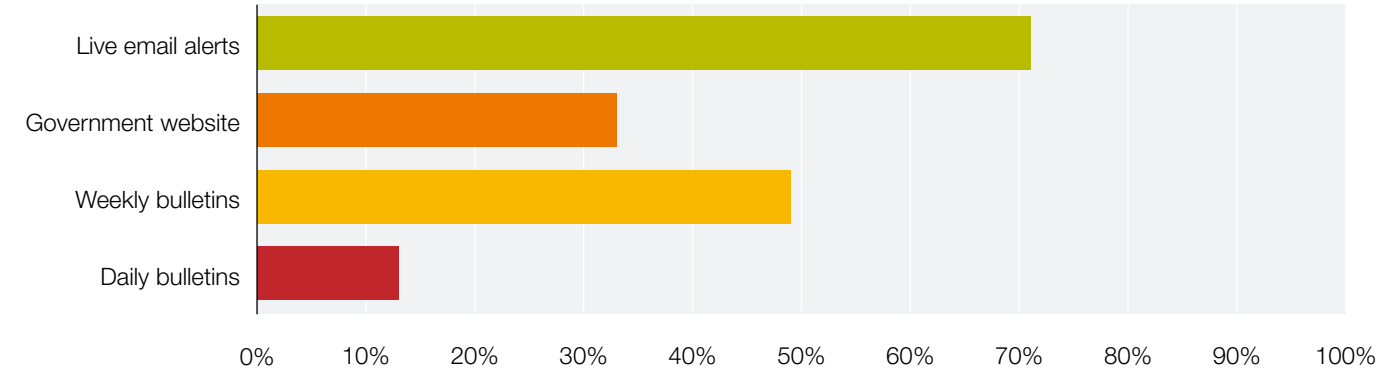
Scale: number of respondents expressing the identified sentiment or similar

Q29. What cyber security initiatives are you familiar with?



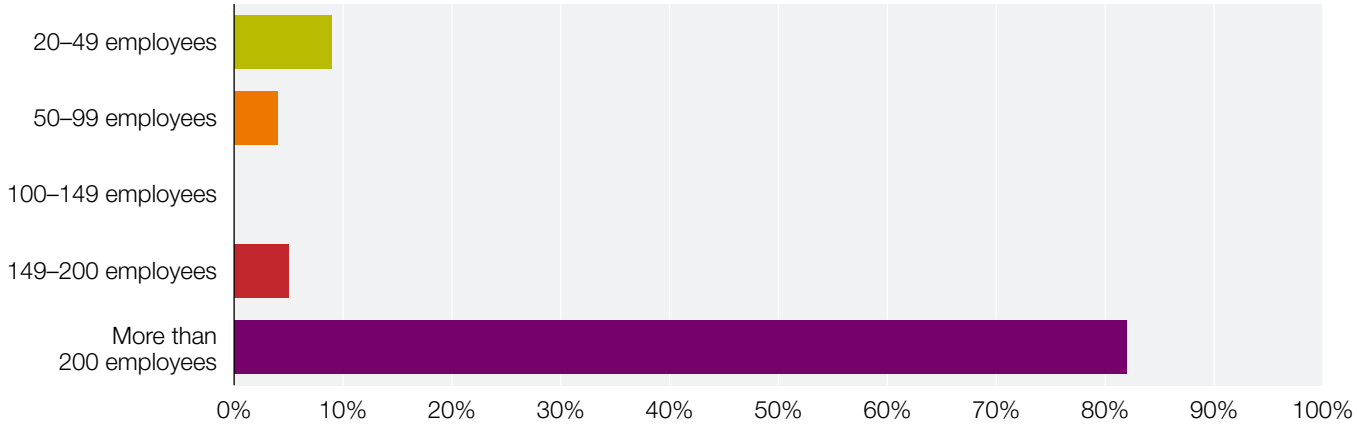
Q30. Have you engaged with any of these initiatives over the past 12 months? How would you rate your interaction?

Q34. What would you say is the best way for government to communicate cyber risks to your business?

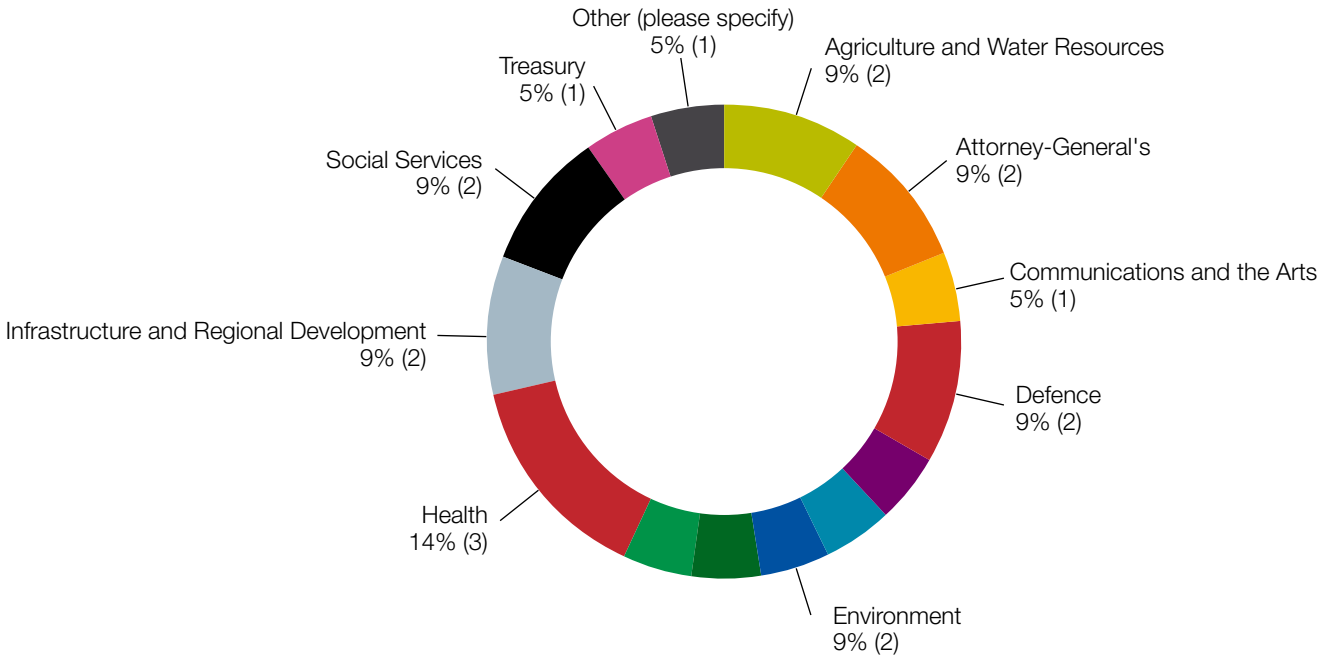


Commonwealth agency findings

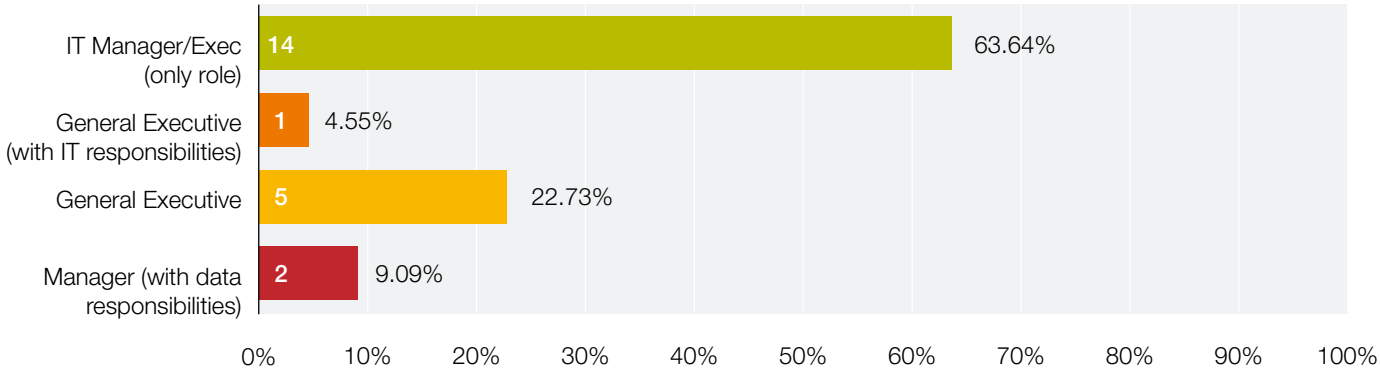
Q1. What is the size of your agency?



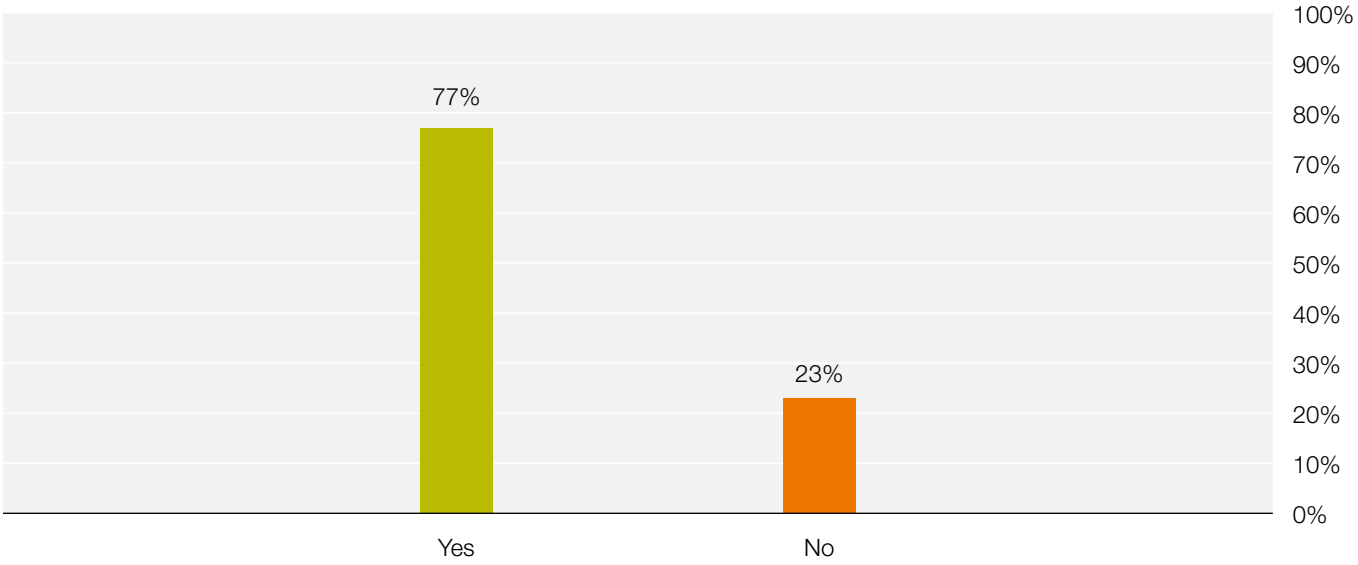
Q2. Which of the following best describes the portfolio to which your agency belongs?



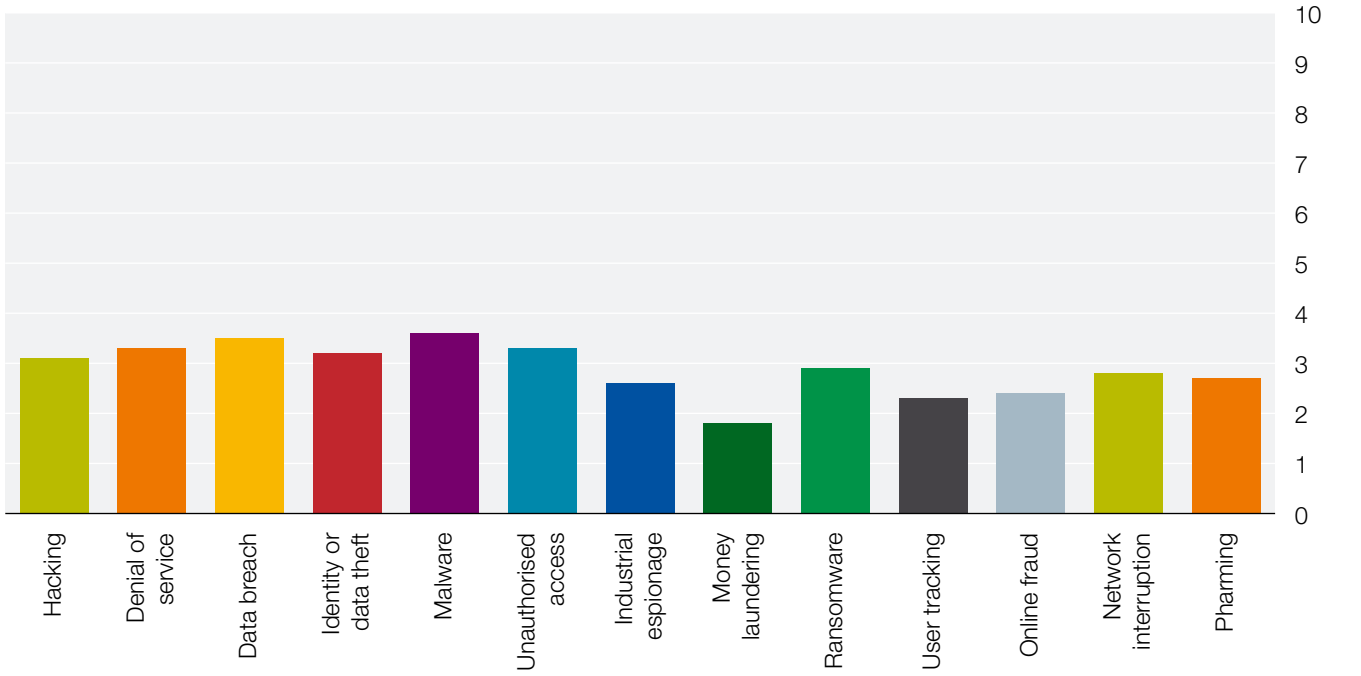
Q3. What is your role in your agency?



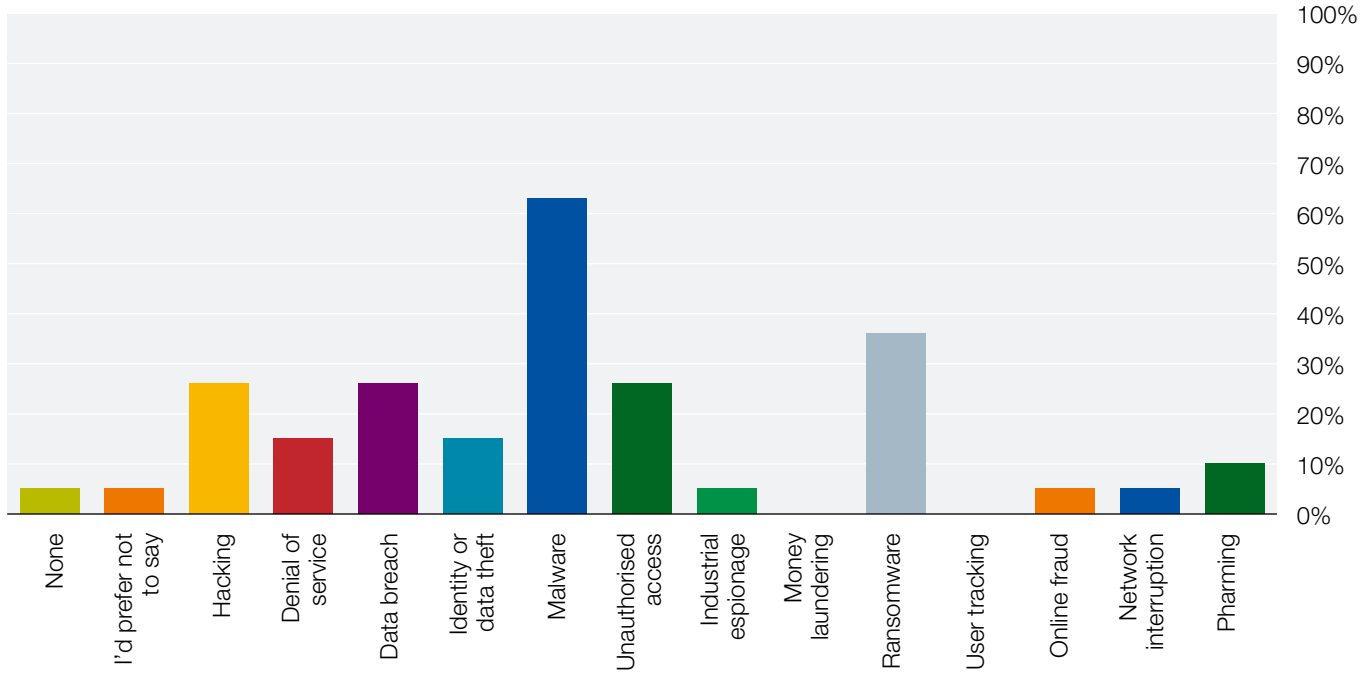
Q4. Does your role entail cyber risk assessment duties?



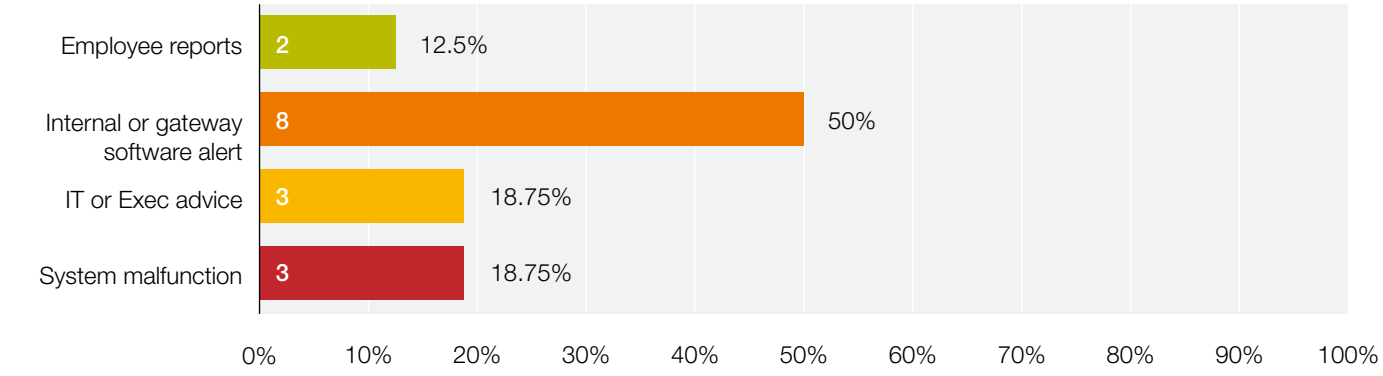
Q5. The following are examples of existing cyber risks. How would you rate the seriousness of these risks to your agency?



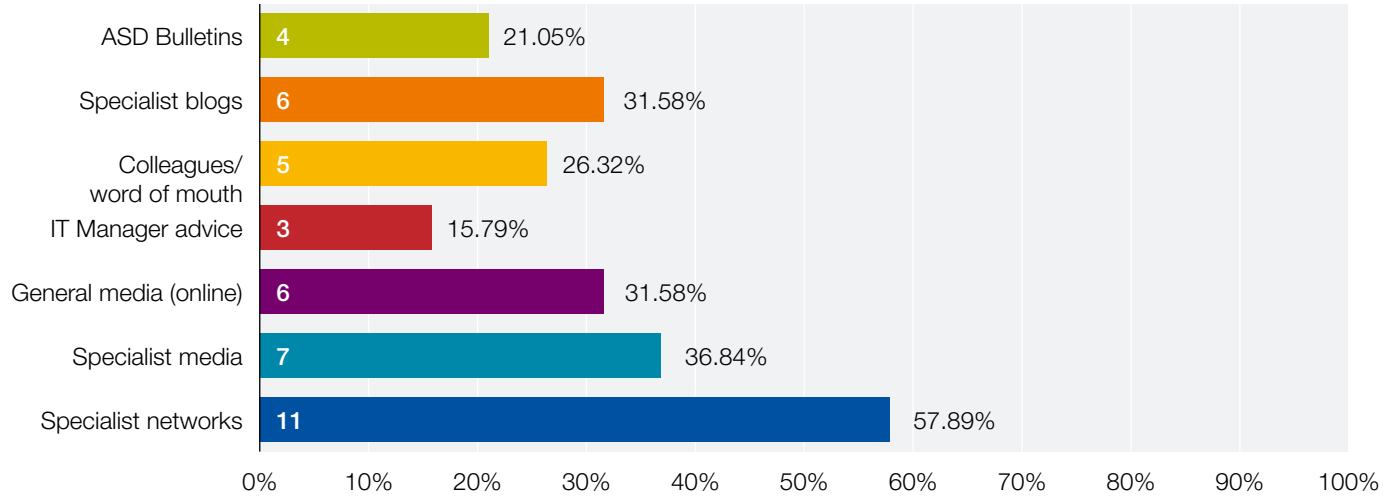
Q6. In the past twelve months, which of the following attacks has your agency experienced?



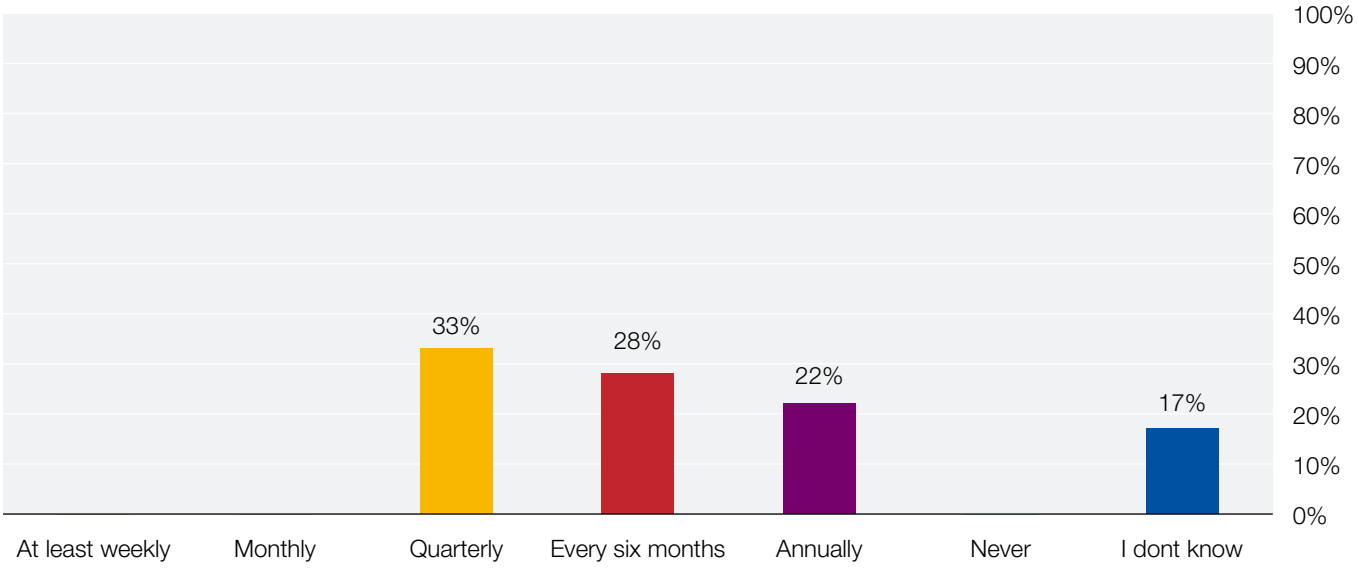
Q7. Thinking about the cyber attacks you have experienced, what is usually the first indication that your agency has suffered such an attack?



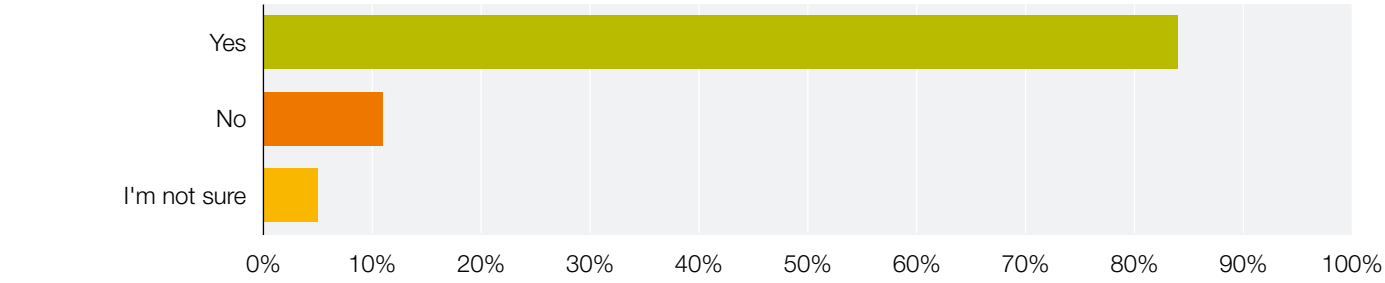
Q9. How do you personally stay informed on cyber security issues and threats affecting your sector?



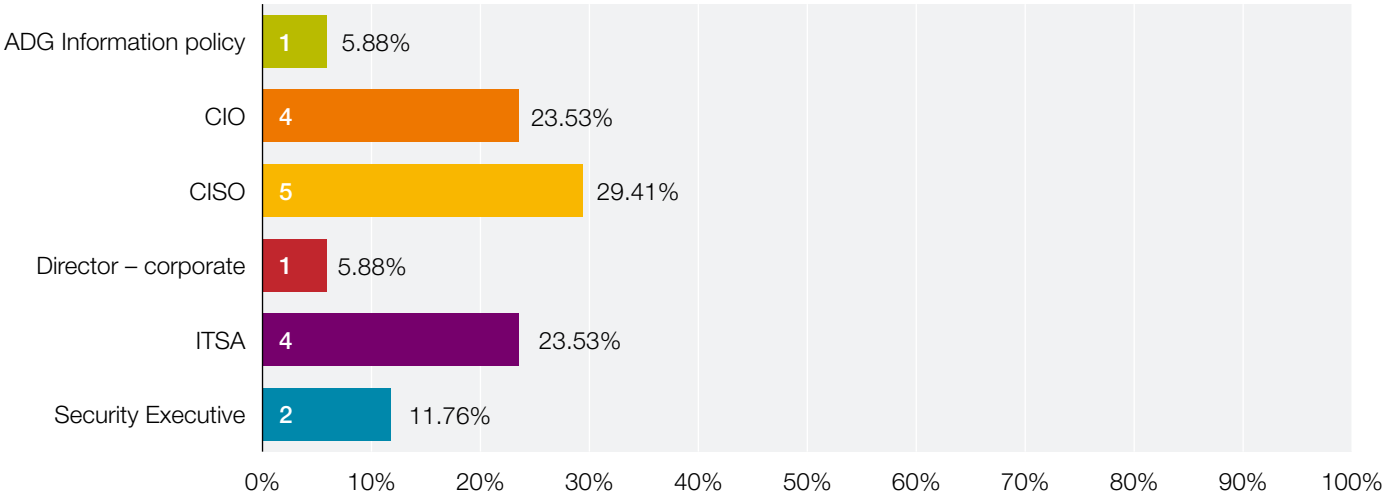
Q11. How often does your agency review its cyber risk management?



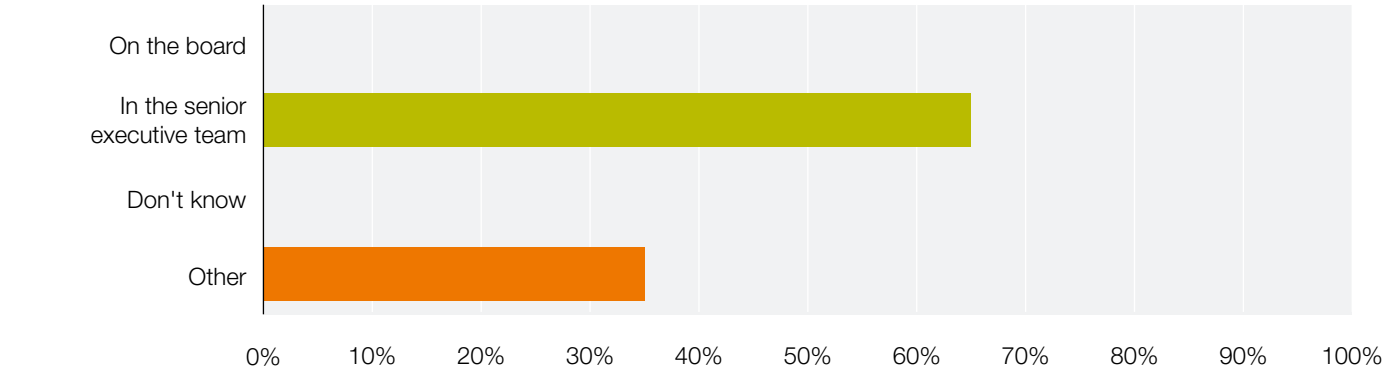
Q12. Do you have someone who is chiefly responsible for information security?



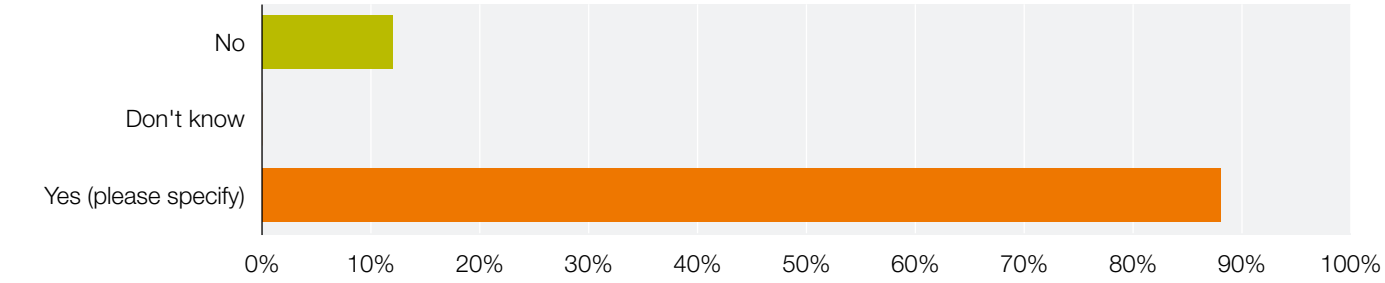
Q13. What is the job title of the individual responsible for information security in your agency?

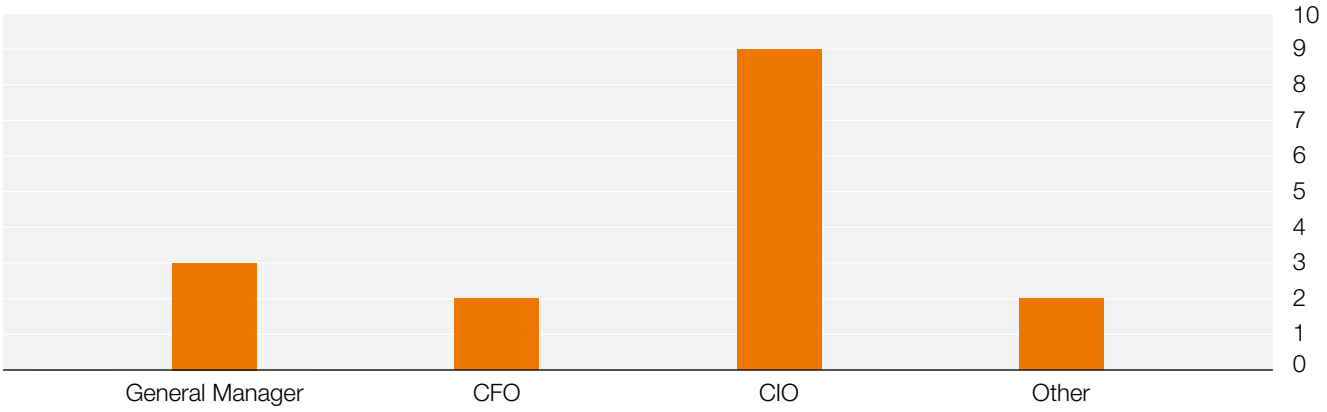


Q14. Where in your agency's governance structure is she or he located?



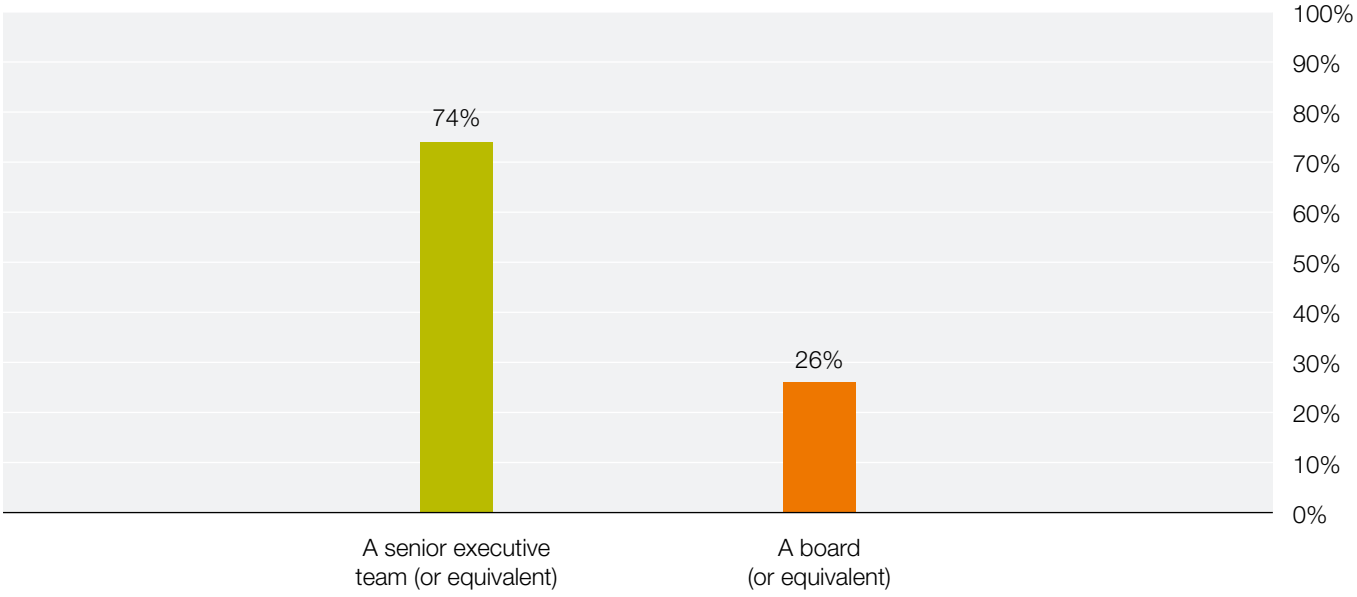
Q15. Does she or he have other responsibilities?



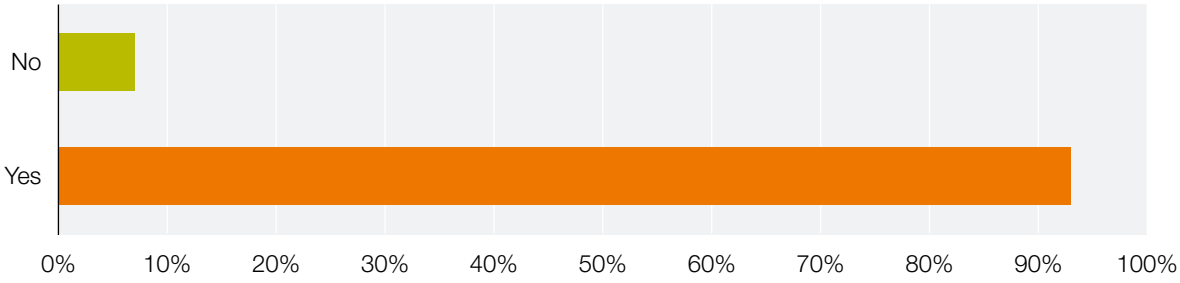


Other responsibilities specified

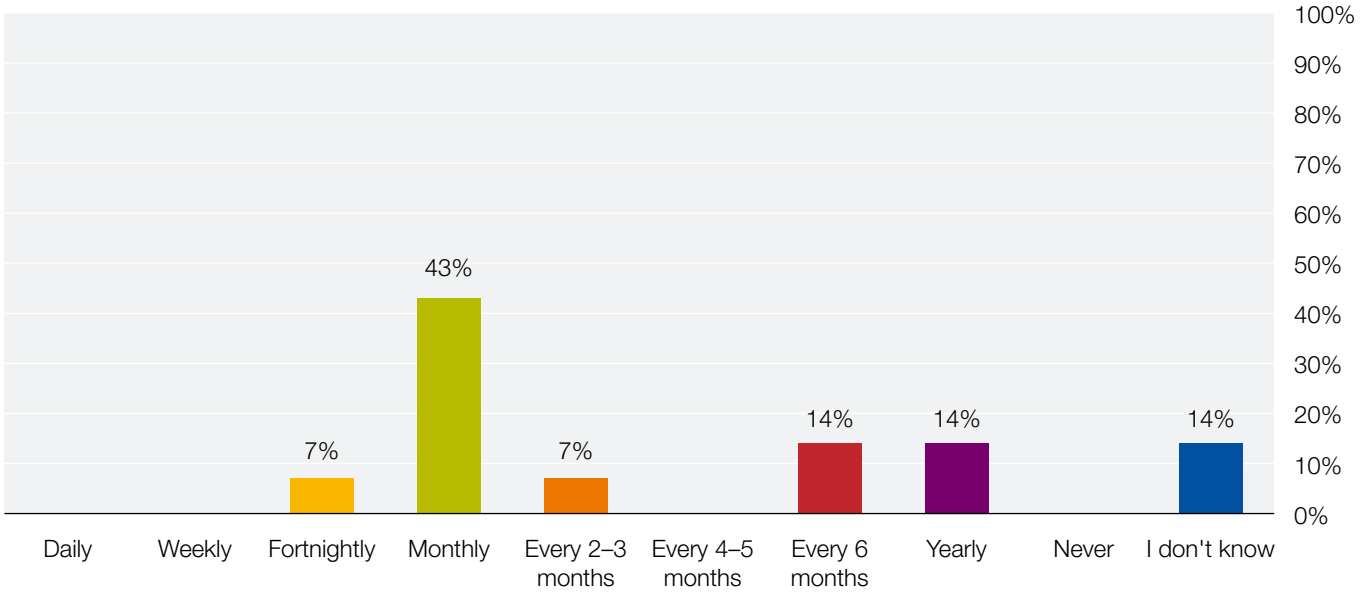
Q16. What is the highest level of leadership for your agency?



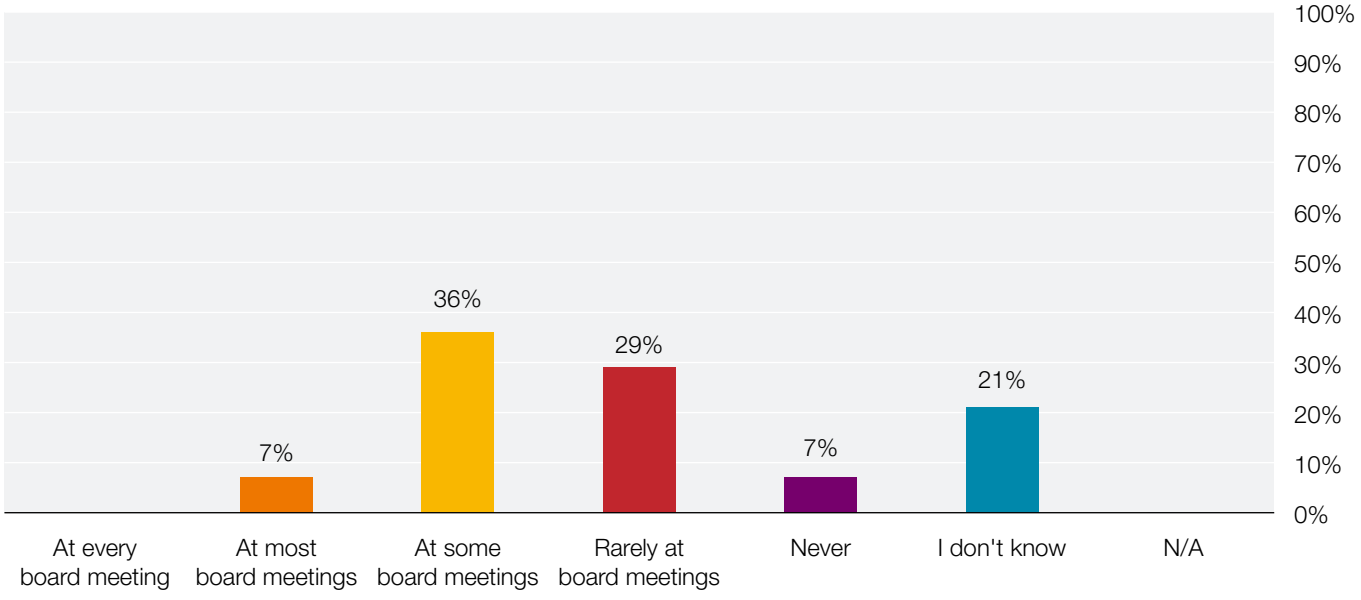
Q17. Do you have an 'escalation trigger' to report a cyber attack to your senior executive team (or equivalent)?



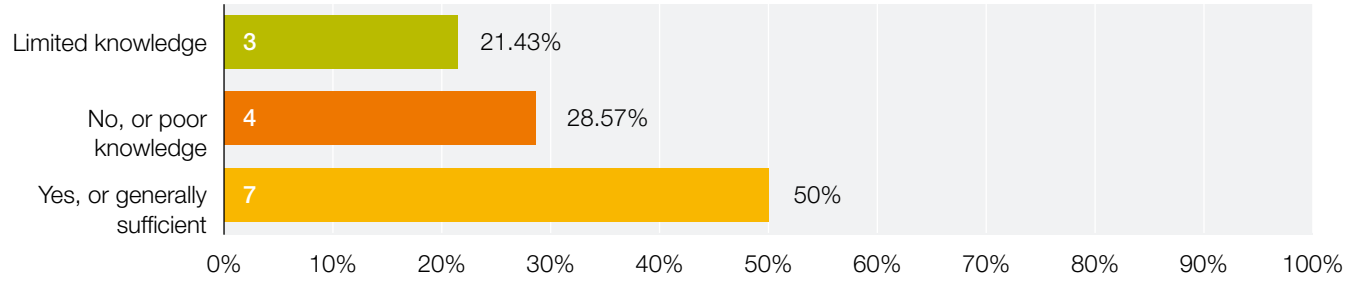
Q18. How often does your senior executive team (or equivalent) receive reports on cyber threats to the agency?



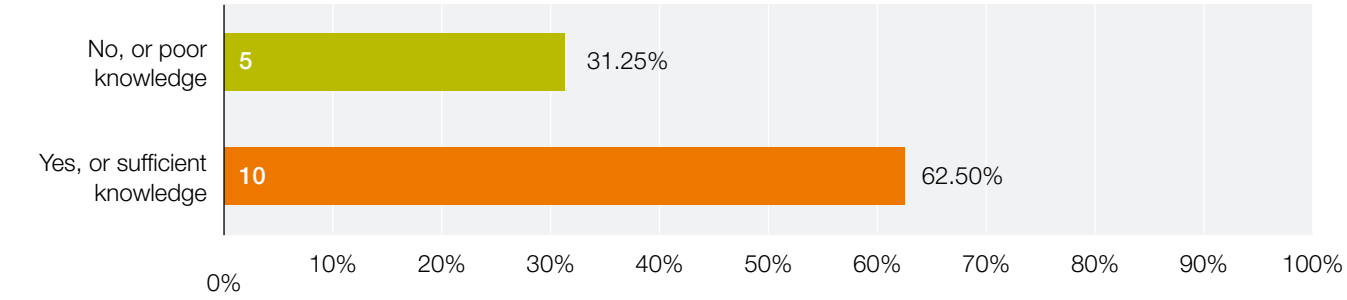
Q20. How often does your senior executive team (or equivalent) discuss cyber security?



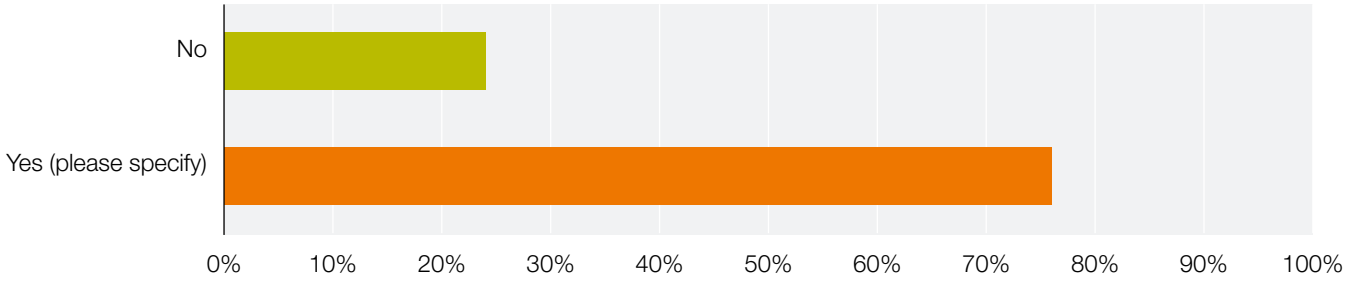
Q21a. In your view, does your agency's senior executive team (or equivalent) have sufficient understanding of cyber risks to your business?



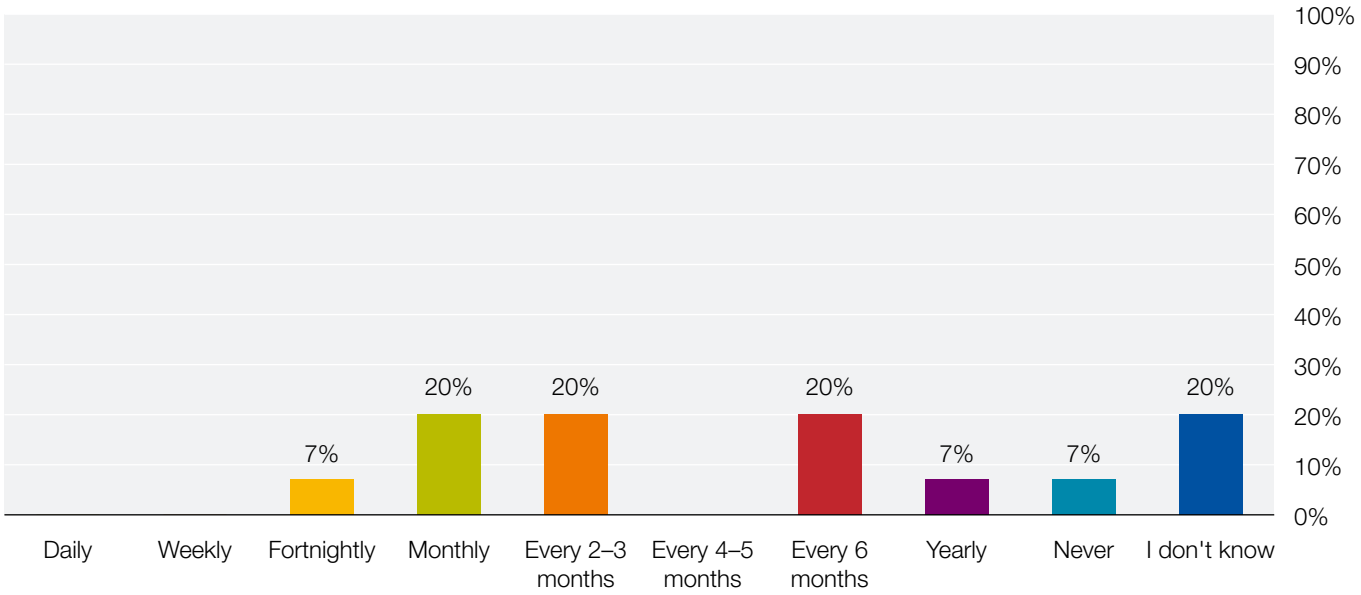
Q21b. In your view, does your agency's board (or equivalent) have sufficient understanding of cyber risks to your business?



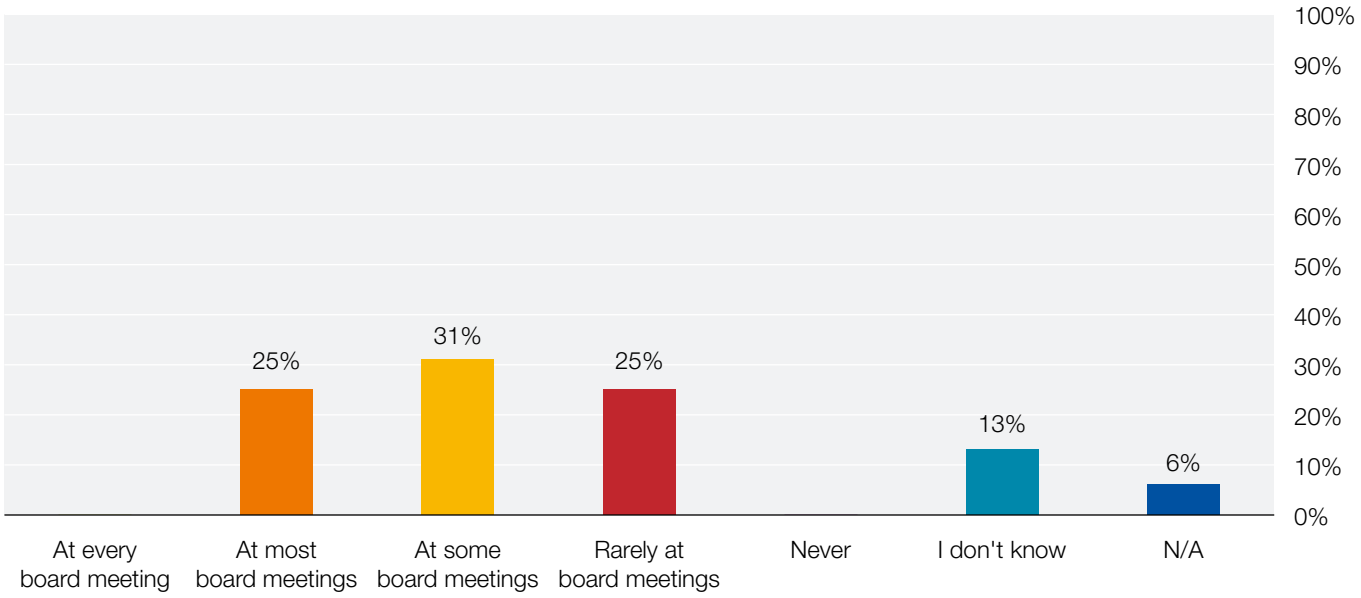
Q22. Do you have an 'escalation trigger' to report a cyber attack to your board (or equivalent)?



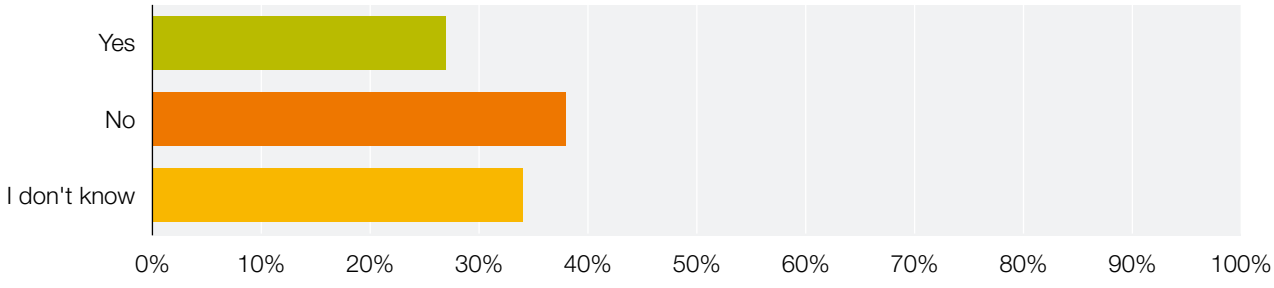
Q23. How often does your board (or equivalent) receive reports on cyber threats to the agency?



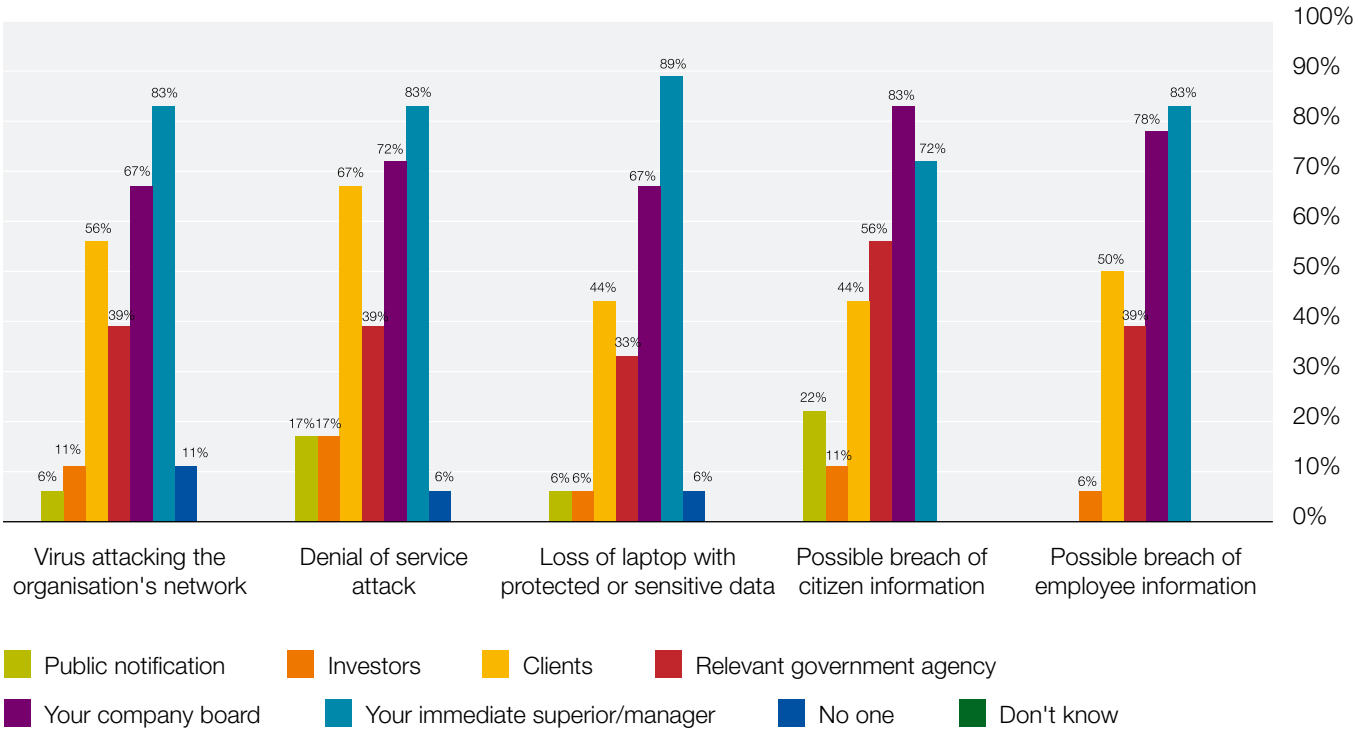
Q25. How often does your board (or equivalent) discuss cyber security?



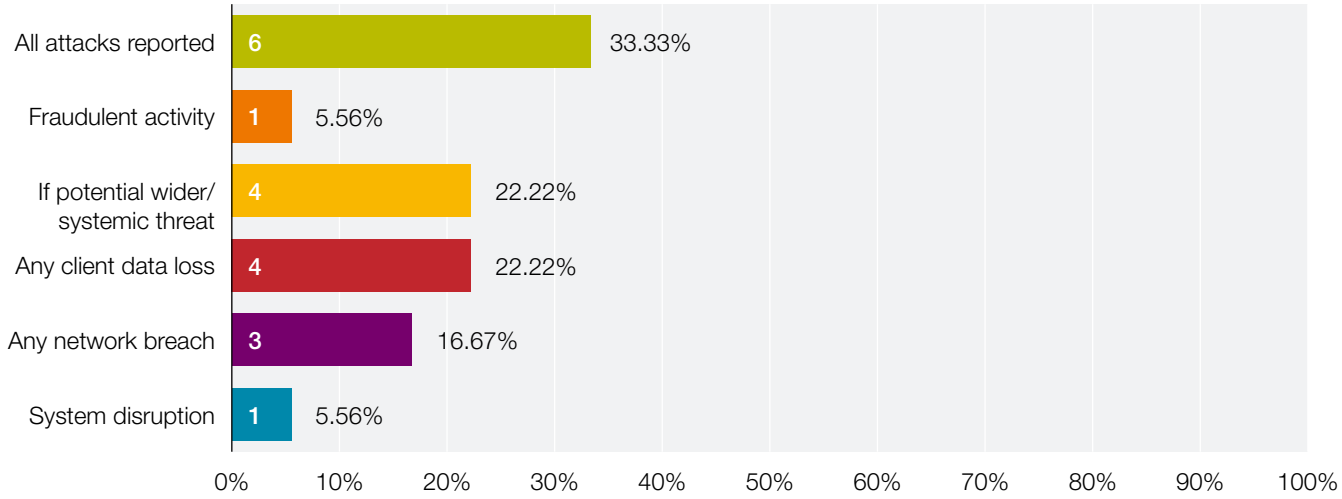
Q30. Do you provide information on your cyber risk management in your annual report?



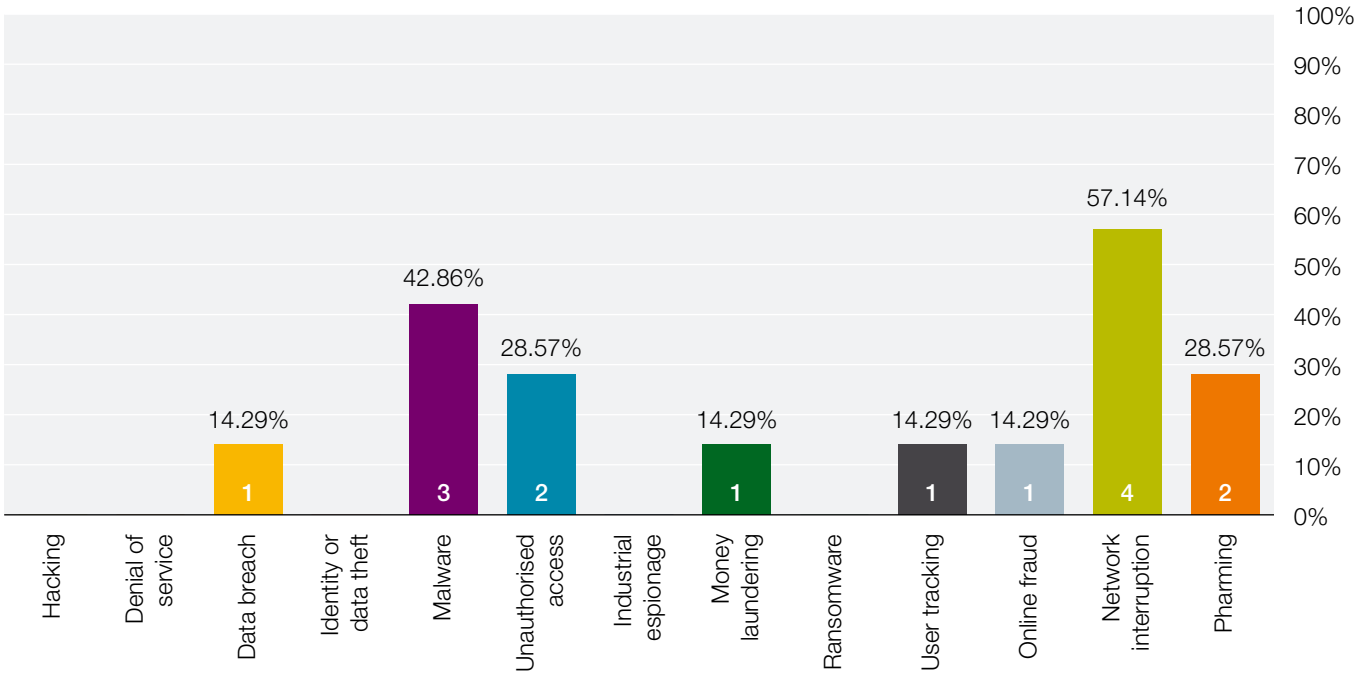
Q31. If the following incidents were to occur, to whom would you report the following incidents? (Select all that apply).



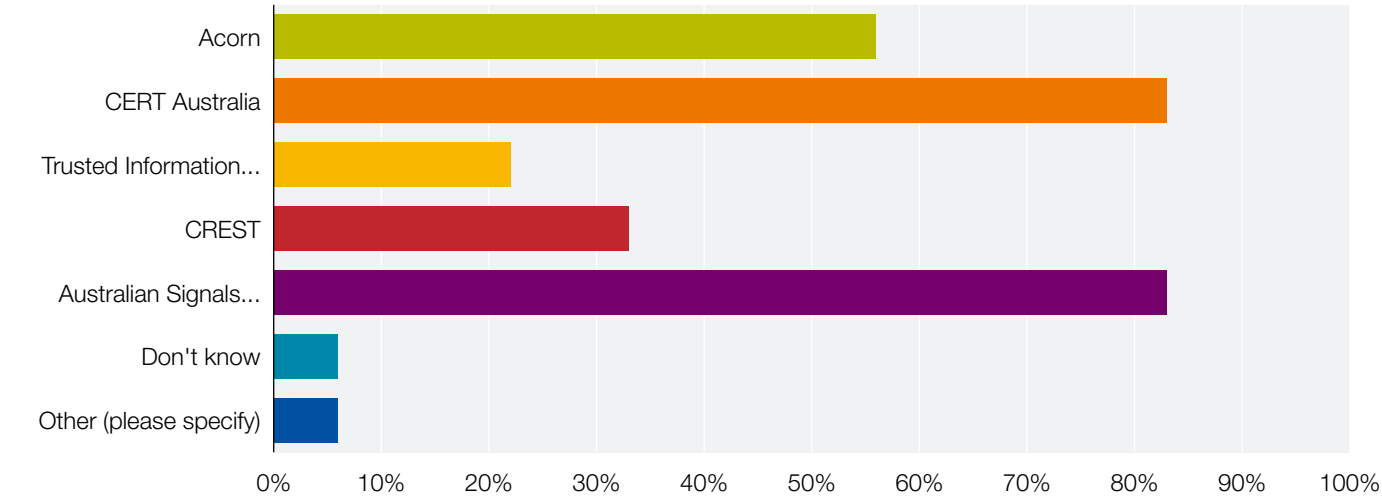
Q32. Under what circumstances would you actively seek to report a cyber attack to a relevant government cyber security agency?



Q33. Are there any types of cyber attack you do not tend to report to government cyber security agencies?

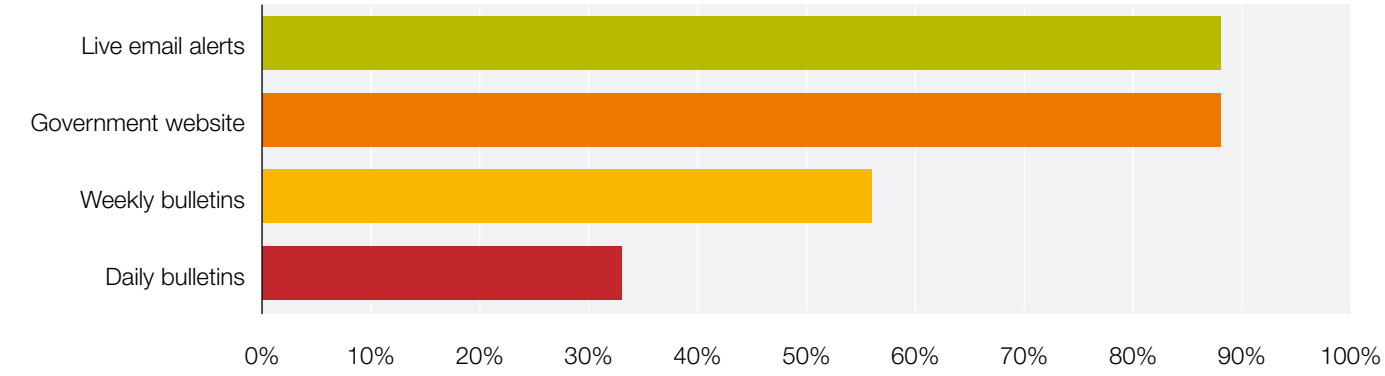


Q35. What cyber security initiatives are you familiar with?



Q36. Have you engaged with any of these initiatives over the past 12 months? How would you rate your interaction?

Q39. What would you say is the best way for government cyber security agencies to communicate cyber risks to your agency?



CONTACT US

National Security College
GJ Yeend Wing (Crawford Building #132a)
1 Lennox Crossing
The Australian National University
Acton ACT 2601
Australia

T +61 2 6125 1219
E national.security.college@anu.edu.au
W nsc.anu.edu.au
@NSC_ANU
linkedin.com/company/national-security-college

CRICOS Provider No. 00120C