



ASX 100

Cyber Health Check Report

**CAPTURING THE OPPORTUNITIES
WHILE MANAGING THE THREATS**

APRIL 2017




Deloitte.



KPMG

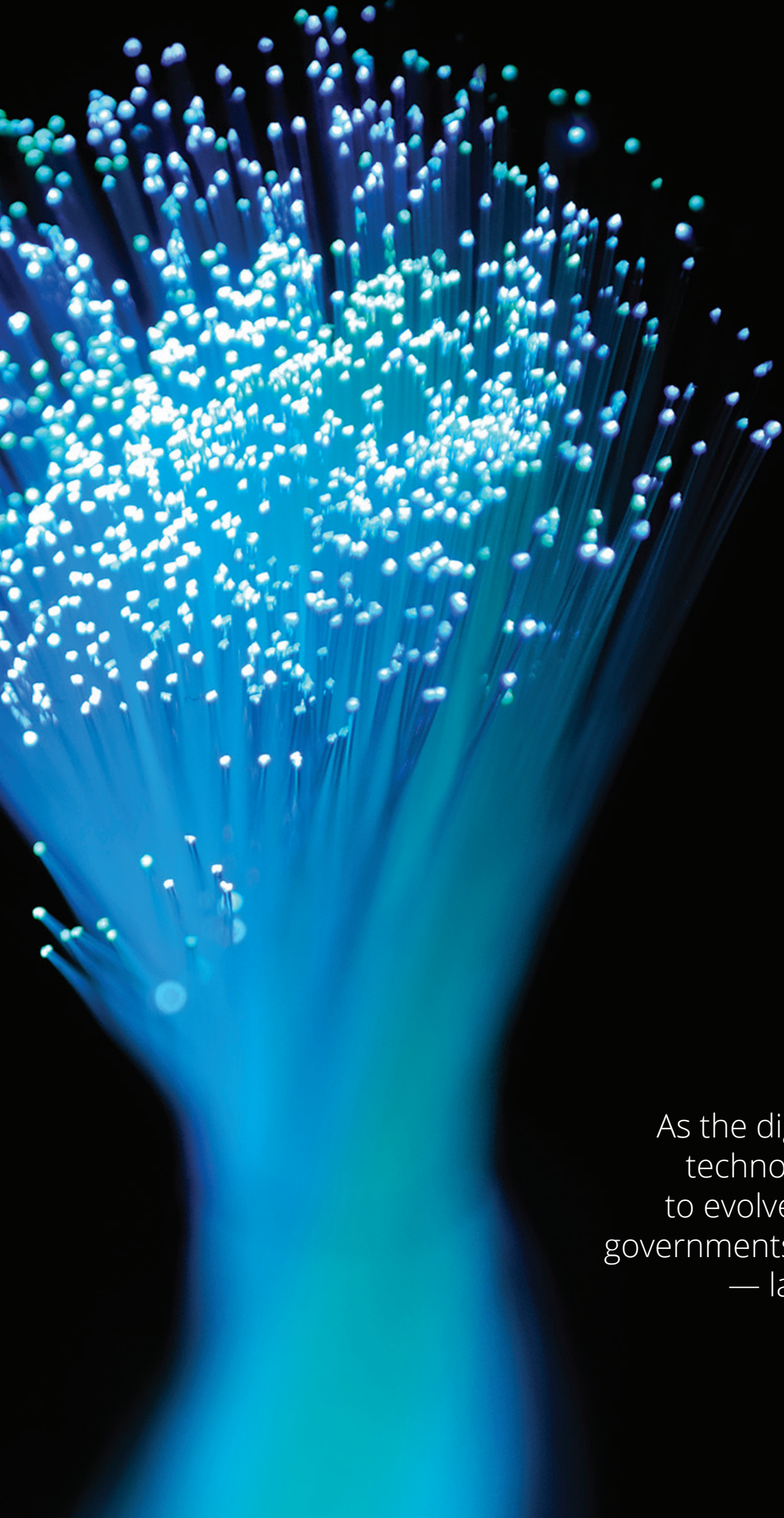




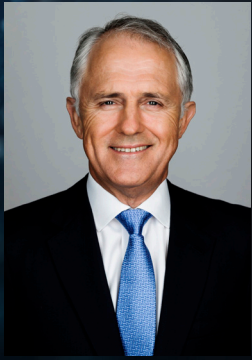
The online economy is growing at twice the speed of the rest of the global economy. To harness its benefits, Australian businesses need to effectively manage their exposure to its risks.

CONTENTS

Prime Minister's Foreword	3
Executive Summary	5
Appendix A Charts	11
Respondent Profile	12
Understanding the Threat	14
Leadership	16
Risk Management	18
Awareness of Help	20
Cyber Incidents	22
Investment and Customer Data	24
Appendix B Survey Questions	25



As the digital world and
technology continues
to evolve so must both
governments and business
— large and small.



The Hon Malcolm Turnbull MP
Prime Minister of Australia

PRIME MINISTER'S FOREWORD

The Internet is the most transformative piece of infrastructure in human history. The pace and growth of the global economy is supercharged by technology. It is in our homes, in our pockets and at the heart of every modern business.

For Australia's top 100 listed companies, innovative technology offers advantage on the world stage. But there are also vulnerabilities that come with being connected. The scale and the rate of compromise is increasing and the methods used by malicious actors are rapidly evolving. For Australia to be truly competitive we need to be world leaders. In business. And in cyber security.

The release of the **ASX 100 Cyber Health Check Report** is therefore significant for Australia's cyber security maturity. Critically, industry led this initiative. This health check was one of the recommendations of Australia's cyber security strategy launched in April 2016. I commend the Australian Securities Exchange, the Australian Securities and Investments Commission and the other participating companies for the leadership they have shown.

Australia's biggest businesses know that they are susceptible to malicious cyber activity – over 80% expect cyber risk to increase in the short-term. But for every big company there are many more small companies without the resources or the know-how to embrace the Internet securely. For every board that talks about cyber security as a real and pressing business risk, there are many more yet to take that step.

The **ASX 100 Cyber Health Check** means we now have a baseline where companies can see how they rate against their peers and can take practical steps to improve their cyber security.

The results of this survey show we have come a long way since I launched the Cyber Security Strategy 12 months ago. It found that many companies have

made significant progress in securing themselves online. And there is a high level of risk awareness and a commitment to put aside competitive differences and take further action. But we can always do more. As the digital world and technology continues to evolve so must both governments and business - large and small.

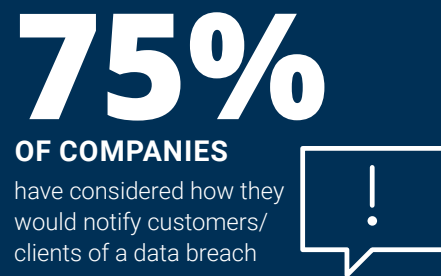
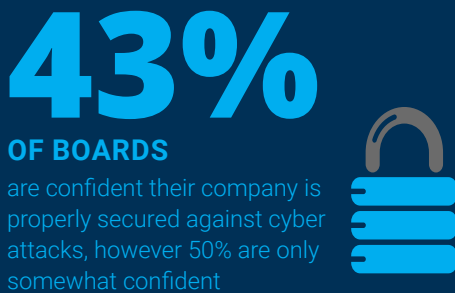
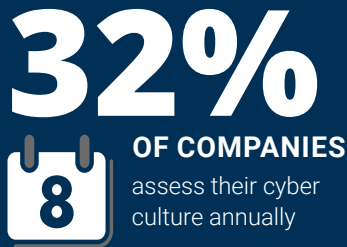
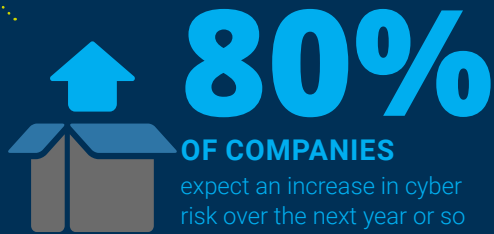
We need lasting cultural change across government and business that positions cyber security to drive trust in our economy. Our businesses are the economic future of Australia and good cyber security is an ongoing journey. Communication and collaboration between governments, business and individuals will be key.

The **ASX 100 Cyber Health Check Report** shows that governance and management of cyber risk are being taken seriously in the boardrooms of Australia's largest listed companies. I encourage these businesses to bring their partners and customers along with them. Prevention and mitigation of cyber threats can only be effective through increased awareness and understanding. By understanding cyber threats, managing the risks and providing strong leadership, Australia will enhance its already strong reputation as a trusted place to do business in the global economy.

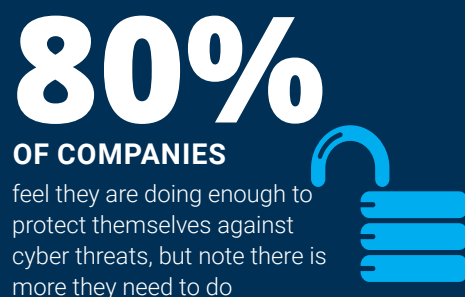
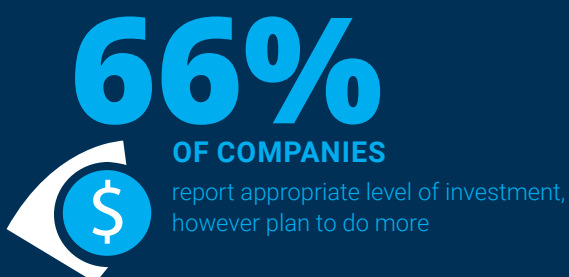
A handwritten signature in blue ink, appearing to read 'Malcolm Turnbull'.

The Hon Malcolm Turnbull MP
Prime Minister of Australia

18 April 2017



But, there is more to be done



EXECUTIVE SUMMARY

A cyber view from the boardroom: capturing the opportunities while managing the threats

The online economy is growing at twice the speed of the rest of the global economy. To harness its benefits, Australian businesses need to effectively manage their exposure to its risks.

Cyber security forms an essential part of public trust and accountability in organisations, which are responsible for protecting personal, corporate and national information.

It is increasingly common for boards to rank cyber risk as a key strategic issue that requires their focus, leadership and governance.

Cyber risk is now an everyday reality. Every organisation faces a daily barrage of malicious cyber activity. The vast majority are unsophisticated and unsuccessful. But the potential for a cyber incident to cause major reputational and financial damage means that boards and management teams are spending more time and resources on developing their understanding and addressing cyber risks.

The **ASX 100 Cyber Health Check** is the first attempt to gauge how the boards of Australia's largest publicly listed companies view and manage their exposure to the rapidly evolving cyber world.

While the extent of cyber risk management varies broadly across companies, this report demonstrates a high level of risk awareness at the top levels of corporate Australia and a commitment to take further action. Significant progress has already been made, but there are gaps when it comes to building organisational preparedness and resilience.

The **ASX 100 Cyber Health Check** is an industry-led initiative that forms part of the Australian Government's Cyber Security Strategy, which encourages government, regulators and businesses to work together to tackle cyber risk. The survey,

which will enable boards and executives to better understand the maturity of their cyber risk management and benchmark it against other companies, identified five key trends:

1. Cyber security is a major and growing risk
2. Tackling cyber risk needs a culture of collaboration
3. Boards take cyber risk seriously and are improving their skills
4. Companies are managing cyber risk better but realise there's still more to do
5. Companies that manage cyber risk effectively define and analyse their exposure.

The **ASX 100 Cyber Health Check** involved the boards of the ASX 100 companies in taking action to strengthen Australia's resilience to cyber attack. The partnership of industry, government and regulators working together demonstrates the critical importance of strong national cyber security to Australian business and the millions of investors who hold shares in Australian companies. The sharing of best practice, and increased awareness and engagement by directors and executives of listed companies are important steps in building the cyber resilience of Australian business.

Amanda Harkness
*ASX Group General Counsel
& Company Secretary*

Cyber security is a major and growing risk

Boards and management increasingly recognise that cyber security is a significant issue.

More than two-thirds of directors (68%) consider that cyber risks are extremely important and 80% expect the likelihood of cyber risk to increase within the short-term. Almost 40% of directors rate cyber risk in the highest category relative to other business risks.

Its inclusion in corporate risk registers, which enable risks and opportunities to be defined and discussed within the broader organisation, is substantial (92%).

While internal awareness is high, there is certainly the potential to boost external engagement on cyber risk. Currently, only 11% of companies proactively reassure customers and investors about their approach.

A year can be a long time when it comes to the pace of technological change. The digital economy is accelerating, and so is cyber risk. Compared to the UK's FTSE 350 survey, a similar survey that was completed in 2015, ASX 100 directors are more than twice as likely to expect the increase in cyber risk to be significant (28% against 13%). Awareness has increased too.

This greater awareness of cyber risk is supported by evidence of increasing attacks. Almost two-thirds (62%) of directors say that the level of attempted malicious cyber activity against their company has gone up over the past year.

Traditionally we talk about cyber as an IT issue and report to the CIO on such issues. Now that boards and directors are becoming responsible for cyber, cyber risk is now being elevated to more of a whole-of-business risk.

Gordon Archibald
Partner, Cyber, KPMG

Tackling cyber risk needs a culture of collaboration

Cyber risk is uniting the business community, regulators and government alike.

This is reflected in the high response rate to the **ASX 100 Cyber Health Check** (76% of the ASX 100), demonstrating a strong commitment to put aside competitive differences and work together for a common cause. Similarly, the four largest professional services firms have collaborated to contribute to this project.

Pooling knowledge and openly sharing experiences can deliver valuable insights that benefit Australian industry and the economy. A clear majority of directors (78%) encourage staff to engage in formal information-sharing to help benchmark, learn from others, and identify emerging cyber threats.

Not only does cyber risk need a united effort externally, it also requires an enterprise-wide approach with leadership by the top levels of management.

At almost every ASX 100 company (99%), the ultimate owner of cyber risk is either the CEO (29%) or another member of the C-suite.

Cyber risk demands attention across all levels and functions. It affects everybody, from the boardroom to senior management, and from the branch office to the engine room of the business.

Three-quarters of companies (75%) have implemented ongoing staff training programs in cyber awareness, with the majority of the remainder planning to do so in the next year. This high level of penetration shows that companies are serious about addressing cyber risk as a whole-of-business concern that is no longer the sole purview of the IT department.

A chain is only as strong as its weakest link. There remain opportunities to reduce potential vulnerability where external access to company systems is granted. Almost a third of companies (30%) haven't yet evaluated the cyber resilience of suppliers, customers and other key external parties that connect to them. A similar level (32%) have only a limited understanding at board level of the extent of information shared with third parties. Indeed, only 37% have a clear understanding of their own key information assets. Boosting this understanding is likely to precipitate greater action.

Boards take cyber risk seriously and are improving their skills

Boards are uniquely positioned to help management tackle cyber risk. They set the tone from the top, can provide a broader viewpoint, and support wider engagement beyond the organisation.

Directors are embracing this responsibility: 93% say that their board colleagues take cyber risk very seriously.

The board (or one of its committees) is directly responsible for holding management to account on cyber risk in the vast majority of ASX 100 companies, with only 3% delegating this role to an executive committee.

Cyber risk is often the domain of either the board's audit or risk committees (64% of respondents), allowing a subset of directors with the relevant skills to focus on cyber risk issues and discuss them with management and external advisers. However, in a significant minority of cases (28%), the main board considers cyber risk, reflecting its significance as a strategic business risk.

The majority of boards receive management reports on cyber security incidents (88%) with more than one-fifth (21%) establishing this procedure within the past year. Over two-thirds (70%) review their cyber security strategy at least once a year. However, the quality of reporting can be improved, with 54% of directors saying that the description in the corporate risk radar of cyber risk's implications is basic. A significant number also say they don't yet have a set of standard cyber security metrics or don't know if they do (63% in total). Giving directors the information they need to monitor key risks and make wise decisions is critical.

There is also potential for greater board engagement on the strategic and control-focused aspects of cyber risk management.

Just 7% of directors say they clearly understand the cyber security of the broader ecosystem in which the company operates and almost two-thirds (63%) say their understanding of the biggest IT security exposures is limited or non-existent.

Establishing cyber resilience should be a critical priority to ASIC's regulated population, to support investor and financial consumer trust and confidence and ensure that our markets are fair, orderly and transparent. Cyber risk must be addressed by all levels of an organisation, and form an integral component of a business' enterprise governance and risk management framework.

Cathie Armour
ASIC Commissioner

While only 8% of directors say they have a clear understanding of the key controls in the company's cyber resilience framework, a further 64% have a reasonable understanding. These are opportunities for further improvement.

Directors clearly demonstrate their personal commitment to furthering their knowledge, with two-thirds (67%) saying they have had information security training in the past year. However, only one-third (33%) of boards received company training over the same period with a further 28% planning to provide it.

This training will prove crucial given only half of directors say the board has a clear understanding of the value of data assets and the potential impact of a cyber intrusion, while just over 40% say the board has a reasonable understanding.



Companies are managing cyber risk better but realise there's still more to do

Directors believe companies are making strong progress in their cyber risk defence. However, far from resting on their laurels, they also recognise that the fight is nowhere near over.

The vast majority (80%) say the company is doing enough to protect itself against cyber threats, but that there is still more to do. This acknowledges the evolving nature of cyber risks and that sound governance is an ongoing journey.

That belief is backed by growing investment in cyber security. A total of 87% of directors believe the company is making an appropriate level of investment and 66% of that group say they still plan to invest more. Nobody believes that the company has overinvested in cyber security.

The majority of companies have put in place operational processes to guard against cyber risk including external vulnerability and penetration assessments (93%), regular internal vulnerability scans (82%), and internal audits of cyber resilience (68%).

More than 60% of ASX 100 companies have also tested what staff would do when faced with a cyber security threat. However, only a third of companies specifically assessed their cyber security culture on a regular basis, with 29% saying they've never assessed it.

Almost 80% of directors consider that the company's response to past cyber attack attempts has been handled well although this does not translate to their confidence about future

Cyber security risk is a pervasive and growing feature of our overall risk landscape. We consider it in the context of our overall risk identification and mitigation framework. As with all our risks, governance oversight is in the first instance provided through our Audit and Risk committee of the board, with semi-annual reporting and discussion by the full board.

**Chair of Board Committee
Respondent**

Cyber security has evolved from an IT issue to a material business risk which management and the board are committed to managing on behalf of shareholders, customers, employees, suppliers and the general public. The company's cyber strategy is about meeting the dual challenge of the digital age - leveraging the opportunities but at the same time managing the risks associated with the digital landscape.

**Chair of Board Committee
Respondent**

cyber intrusions. Only 29% are confident that management can detect, respond to, and manage an incident with minimal impact on the business. This may be partly because cyber risk is increasing and becoming more complex, as well as a greater recognition of the potential costs. It may also be due to a traditional focus on protection rather than detection and response capabilities.

A 2016 global study (*2016 Cost of Cyber Crime Study & the Risk of Business Innovation - Ponemon Institute - Cyber Security Analysis*, Hewlett Packard) put the average cost of cyber crime against Australian corporations at over \$5.6 million per incident and rising. There is also now increased potential for further costs in the event of a privacy breach arising.

Since the **ASX 100 Cyber Health Check** was conducted, the Privacy Amendment (Notifiable Data Breaches) Act 2017 has been passed by Parliament. The legislation makes it mandatory to notify affected individuals if there is a privacy breach of their personal information that is likely to result in serious harm. This is firmly on directors' radar, with 75% confirming they have considered how they would notify customers of such a breach. It also raises the expectation for a board to oversee management's focus on continuous improvement in the understanding of threats, developing a cyber aware culture and the investment in cyber preparedness.

Companies that manage cyber risk effectively define and analyse their exposure

Over a third (34%) of ASX 100 companies have clearly defined their cyber risk appetite – a hallmark of companies that take information security seriously. Of the remaining companies, 28% have a partially defined cyber risk appetite, while 38% have not yet defined their cyber risk appetite to date.

Financial services companies, accustomed to dealing with sensitive financial data online, are consistently the most advanced.

To date, the prevalence of cyber insurance among companies is low, with only 38% of companies currently holding a specific policy. It will be interesting to see if the uptake changes over time.

The boards of companies with a clearly defined cyber risk appetite are also more likely to have:

- greater visibility and understanding of the company's exposure to cyber risk
- a clearer understanding of the organisation's critical information assets and data
- a director who is well versed in cyber security
- a higher overall level of board engagement and education on cyber risk
- an allocated budget for cyber risk management and visibility over the investment in cyber defence initiatives
- specific insurance coverage for cyber risk, and
- greater confidence that there are appropriate controls to protect against, detect and recover from a cyber intrusion.

This analysis provides useful motivation for directors of organisations that have not yet clearly defined their cyber risk appetite.

Where to from here?

As companies continue to expand their digital ecosystems, they understand that it carries risks. They also recognise that the online environment is an inescapable component of contemporary business that brings opportunities as well as danger.

The **ASX 100 Cyber Health Check** shows that governance and management of cyber risk are being taken seriously in the boardrooms of Australia's largest listed companies. If boards continue to instill awareness, build capability and expand understanding, companies will be able to defend against and respond to growing cyber threats more effectively.

The report provides a framework for Australian businesses to better evaluate their own effectiveness in addressing cyber risk, benchmark themselves against others, and identify opportunities for improvement.

Appendix A provides detailed results of the **ASX 100 Cyber Health Check** so that others can deepen their understanding of the risks and improve their governance. The ASX 100 companies that participated in the survey will also receive tailored information on where they rank alongside their peers.

We urge all businesses to continue embracing the level of collaboration demonstrated in this survey and actively work together to mount a stronger defence against cyber risk across Australia and abroad.

This report provides valuable cyber security insights for senior business leaders to consider when building and maintaining trust in a complex and ever changing digital world. It's an important step to increase awareness of the evolving risks facing organisations as we look to build cyber resilience across the business community, and position Australia as a trusted place to do business.

Peter Malan
Partner, PwC Australia

About the survey

All of the top 100 listed companies in Australia were invited to participate in the **ASX 100 Cyber Health Check** on a voluntary basis.

These companies make a significant contribution to Australia's economy and are well placed to lead a national effort to encourage best practice cyber security among all Australian businesses. As at 1 April 2017, the market capitalisation of the ASX 100 was \$1.5 trillion.

The survey was conducted between November 2016 and January 2017.

SCOPE

The survey used a non-technical questionnaire to comprehensively explore the extent of cyber awareness, preparedness and resilience across companies and their boards. It addressed six key areas:

1. Understanding the threat
2. Leadership
3. Risk management
4. Awareness of help
5. Cyber incidents
6. Investment and customer data.

These areas align with the UK Government's similar survey of the FTSE 350, the *Cyber Governance Health Check 2015/16*.

PARTICIPANTS

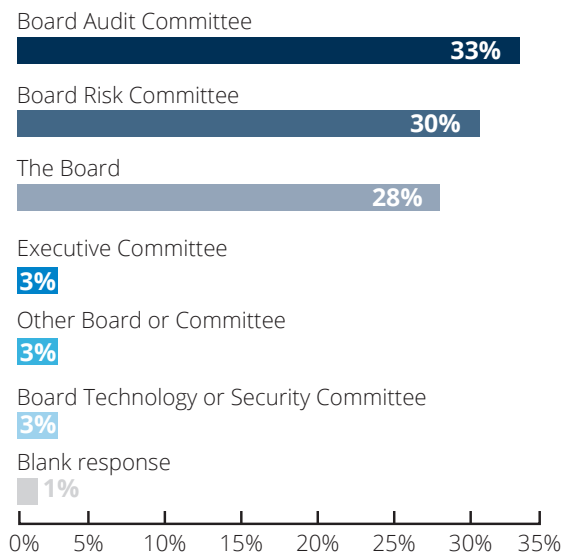
Responses were received from 76 companies in the ASX 100.

The survey was conducted either as an interview with a partner or director from the organisation's audit firm, or as a self-administered online questionnaire.

The overwhelming majority of responses came from non-executive directors (97%). Most (82%) were chairs of a board committee, while 14% were chair of the board. They represented a broad cross-section of industry sectors, as seen on page 12.

The **ASX 100 Cyber Health Check** is the result of collaboration between the Australian Securities Exchange (ASX), the Australian Securities and Investments Commission (ASIC), the Department of the Prime Minister and Cabinet, CERT Australia and professional services firms Deloitte, EY, KPMG and PwC.

Percentage of respondents by cyber risk governance role



Like many others, the company is on a journey with cyber security and building on existing risk capability and culture. Cyber security is a complex challenge which requires a whole of ecosystem response and the company is pleased with the focus and attention the Australian Government, the ASX and ASIC are placing on building the cyber resilience of Australian business and the nation.

Chair of Board Committee
Respondent



APPENDIX A

CHARTS

THIS SECTION OUTLINES THE KEY QUESTIONS
AND RESPONSES FROM THE SURVEY.

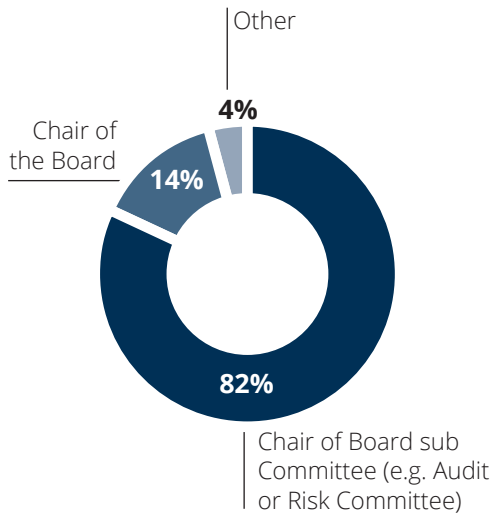
*Please note the following Appendix does not contain a comprehensive set of charts.
Each chart is labelled to match the survey question number in **Appendix B**.*



Respondent Profile

Q1

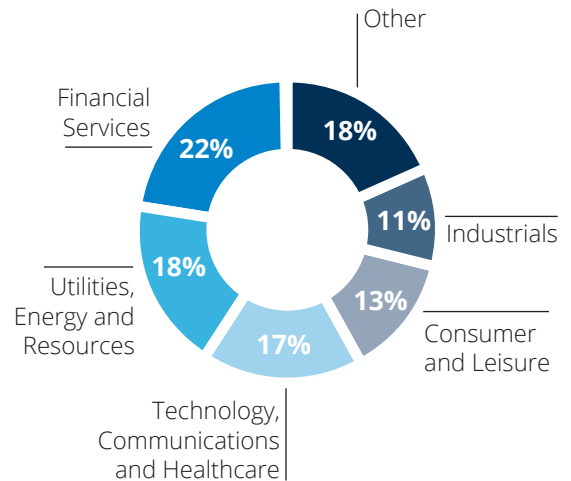
1.2 Which of these titles best describes your role? (Note: preference is for the survey to be completed at the board or committee chair level.)



May not add to 100%
due to rounding

Boards were well represented with the majority of respondents being chairs of boards.

1.3 Which sector classification best applies to the company's main business?



May not add to 100%
due to rounding

Respondents came from a broad range of sectors, with greatest representation from the financial services sector.

1.4 Please indicate which of the following risk factors apply to your company.

Q1

Our shareholder value is significantly dependent on securing and/or keeping secret our critical information assets

27%

We handle high value financial transactions or other assets at high risk from theft or fraud

22%

We run safety-critical automated systems (e.g. failure can put lives at risk)

17%

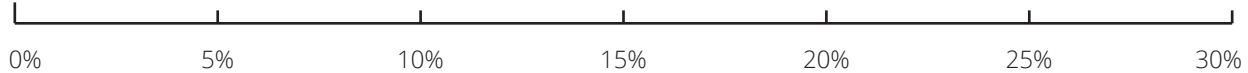
We deliver services vital to the critical national infrastructure

14%

More than 50% of our revenue comes through online interactions

11%

May not add to 100% due to rounding

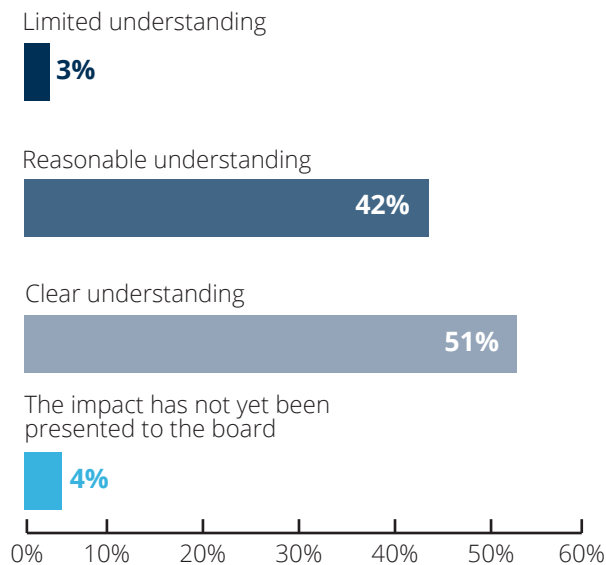


Shareholder value and handling high value financial transactions were the risk factors facing most organisations.

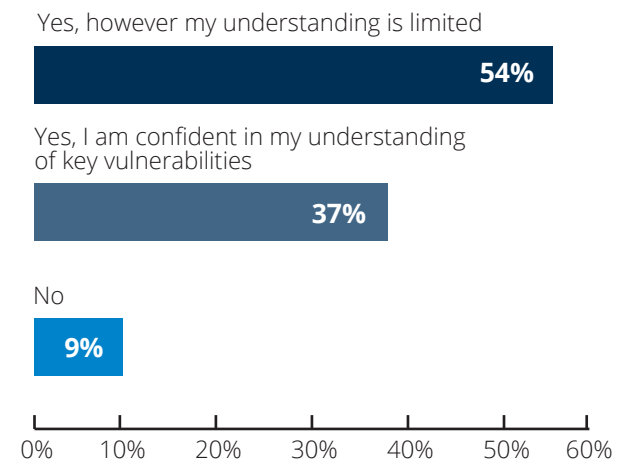
Understanding the Threat

Q2

2.3 What is the board's understanding of the potential impact from the loss of or disruption to key information and data assets?



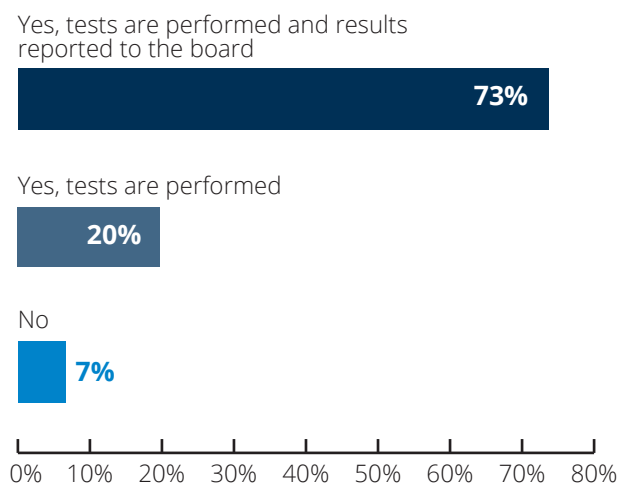
2.7 Do you understand where the biggest vulnerabilities/risk exposures are in your IT security perimeter?



Key information and data assets include IP, financial, corporate, strategic, and customer/personal data. The loss of or disruption to key information and data assets can impact on customers, share price and/or reputation.

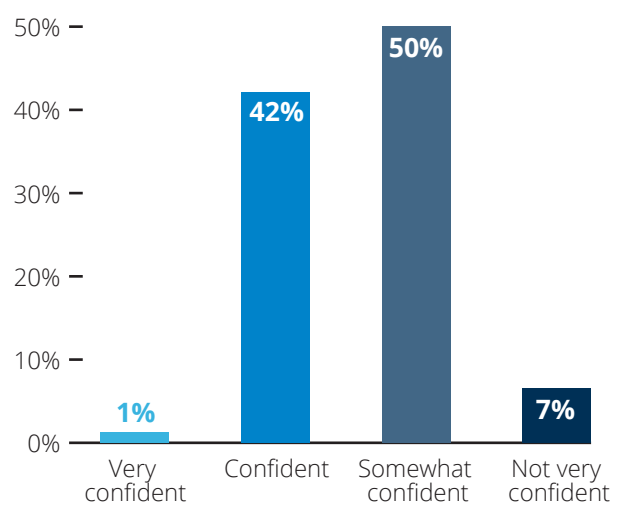
The majority reported a limited or no understanding of biggest vulnerabilities/risk exposures in the IT security perimeter.

2.8 Does your organisation engage external parties to perform regular vulnerability or penetration assessments?



Engaging external parties to perform regular vulnerability or penetration assessments is the norm for most organisations.

2.11 How confident are you that your company is properly secured against cyber attacks?



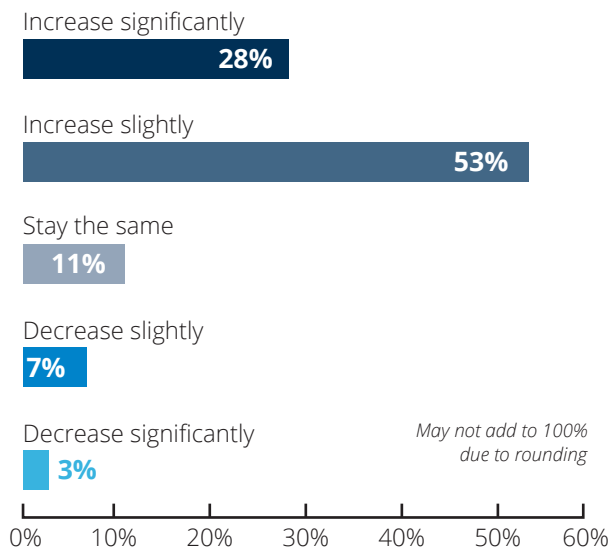
That half are only 'somewhat' confident they are properly secured against cyber attacks indicates there is more work to do to by organisations to understand and protect against cyber threats.

Q2

Leadership

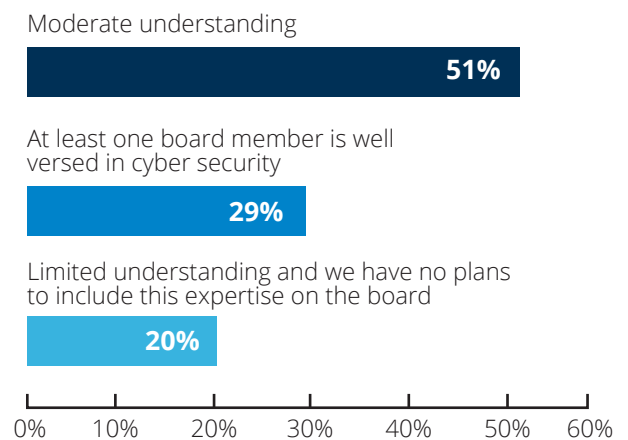
Q3

3.1 Is cyber net (residual) risk expected to increase or decrease, in terms of likelihood of occurrence over the next year or so?



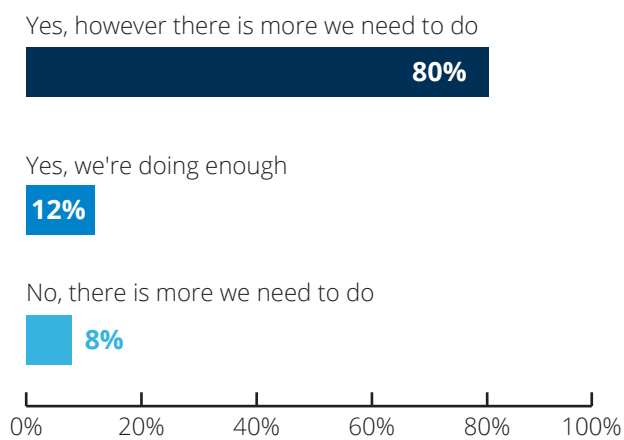
Most respondents expect the likelihood of cyber attacks to increase over the next 12 months or so.

3.6 Does the board include a director with a good understanding of information security and cyber security in particular?

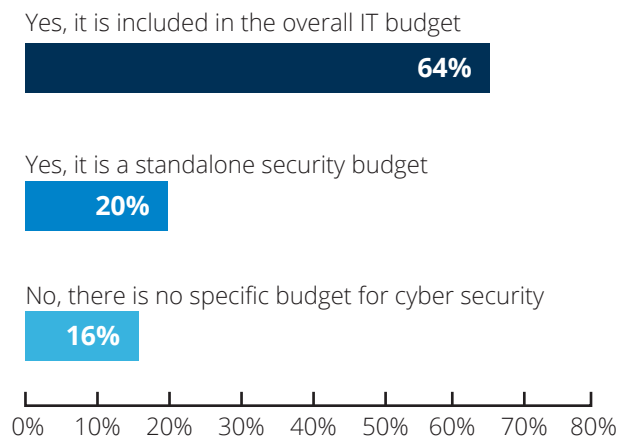


20% of respondents have no plans to include information security or cyber security expertise on their board.

Q3

3.7 Do you feel the company is doing enough to protect itself against cyber threats?

Most organisations feel there is more they need to do to protect themselves against cyber threat.

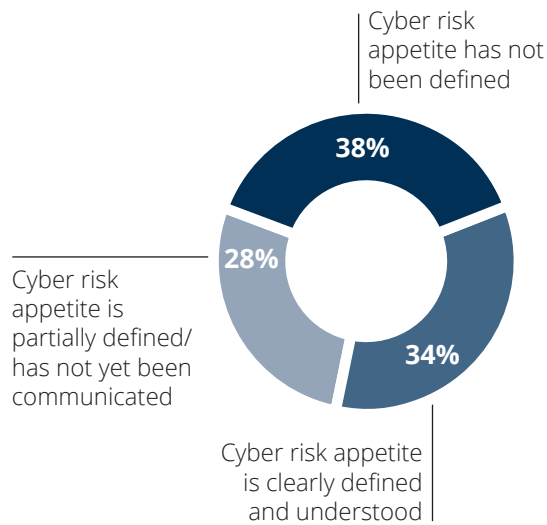
3.14 Does your organisation have a specific cyber security budget?

Many organisations have allocated a cyber security budget, but for most it is still included in the overall IT budget rather than being standalone.

Risk Management

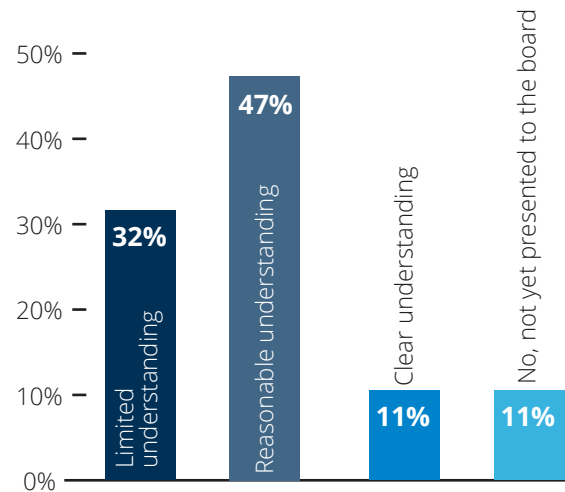
Q4

4.3 To what extent has your board explicitly set its appetite for cyber risk, both for the existing business and for new digital innovations?



Most respondents have either not defined or only partially defined their cyber risk appetite.

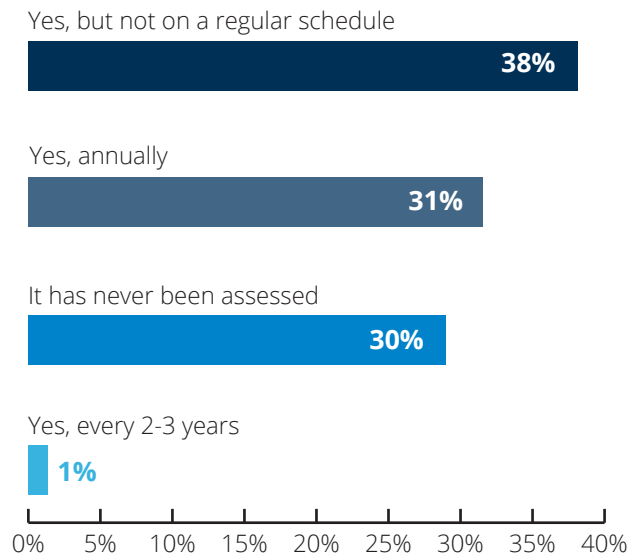
4.5 Does the board have an understanding of where the company's key information or data assets are shared with third parties?



May not add to 100% due to rounding

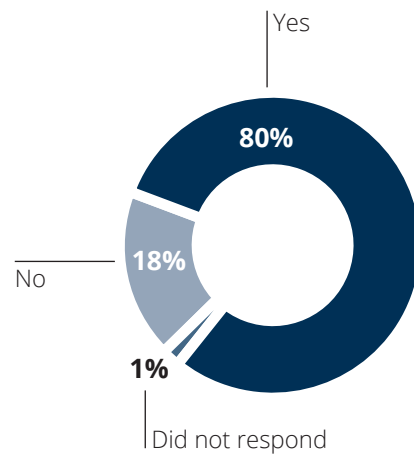
Third parties includes suppliers, customers, advisors and outsourcing partners.

4.12 Does the organisation assess its cyber security culture?



Assessment of cyber security culture is not yet done on a regular basis for the majority of organisations.

4.13 Do you have a clear understanding of your company's disclosure requirements regarding a cyber breach?



May not add to 100% due to rounding

A large majority of organisations have a clear understanding of their disclosure requirements, which is particularly important given the new data breach notification regulations that have recently been enacted.

Awareness of Help

Q5

5.4 Have you considered using cyber insurance?

Yes, we have considered it and decided not to implement a policy

36%

Yes, we are implementing a policy in the next 12 months

16%

Yes, we have a cyber insurance policy

38%

No

11%

May not add to 100% due to rounding

0% 5% 10% 15% 20% 25% 30% 35% 40%

5.6 Has your organisation implemented an ongoing cyber awareness training program for staff?

Yes, in the last 12 months

54%

Yes, it has been in place for over 12 months

21%

No, however we plan to implement a program in the next 12 months

18%

No

7%

May not add to 100% due to rounding

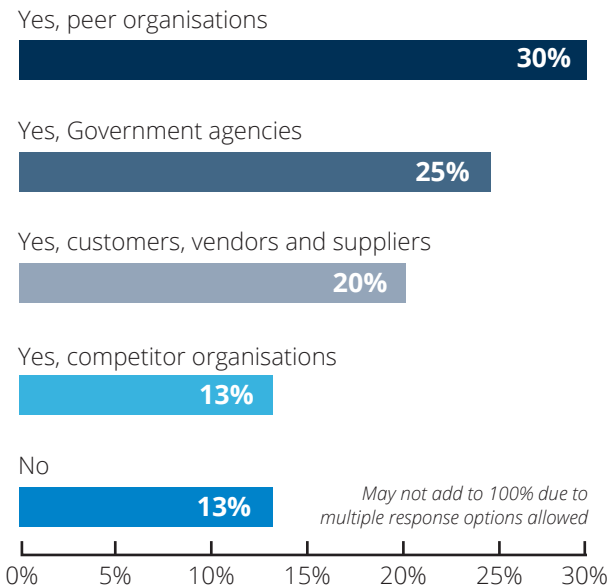
0% 10% 20% 30% 40% 50% 60%

Almost as many respondents have considered and decided against a cyber insurance policy as those who actually do have a policy.

For most organisations cyber awareness training programs are a fairly recent practice.

Q5

5.9 Does the board encourage the cyber security team to engage in data sharing arrangements with other organisations in its environment? *Select all that apply.*

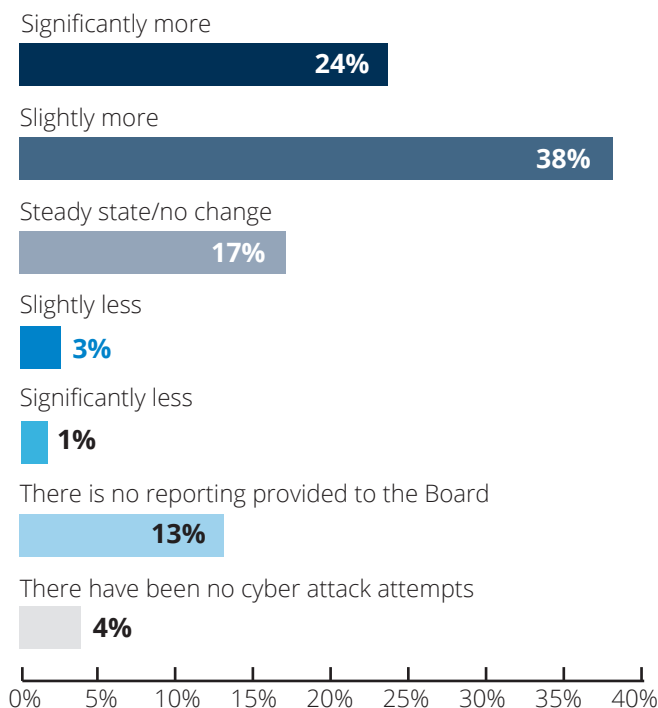


Most respondents report some level of data sharing with other organisations.

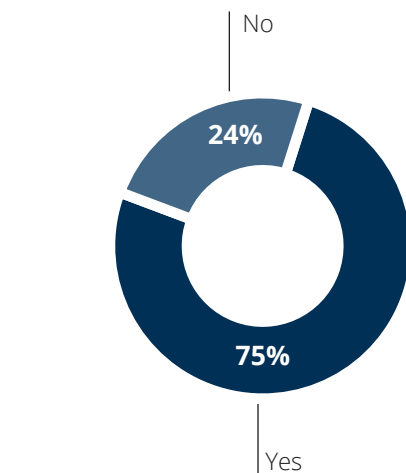
Cyber Incidents

Q6

6.1 From reporting provided to the board, has the company experienced more or fewer cyber attacks over the last year?



6.4 Have you considered how you would notify your customers or clients of a breach of their confidential data?

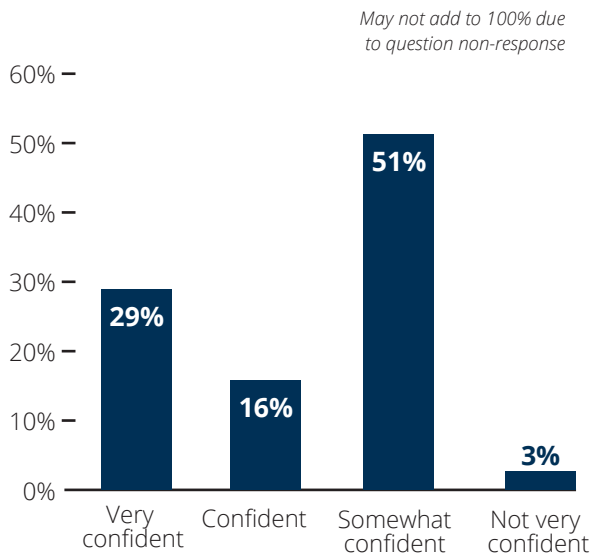


May not add to 100% due to question non-response

Cyber attack attempts were on the rise for most respondents in the last 12 months.

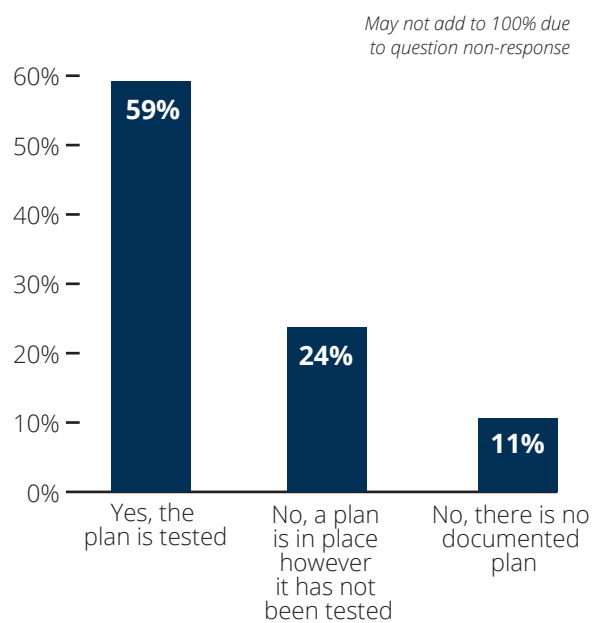
Nearly a quarter of respondents still need to determine how they would communicate a confidential data breach.

6.5 Are you confident in your organisation's ability to detect, respond and manage a cyber intrusion to minimise impact to your business?



It appears that more needs to be done around detecting and responding to cyber intrusions given the majority response of only 'somewhat' confident.

6.6 Does the organisation have a documented and approved response, recovery and resumption plan and is the plan tested?



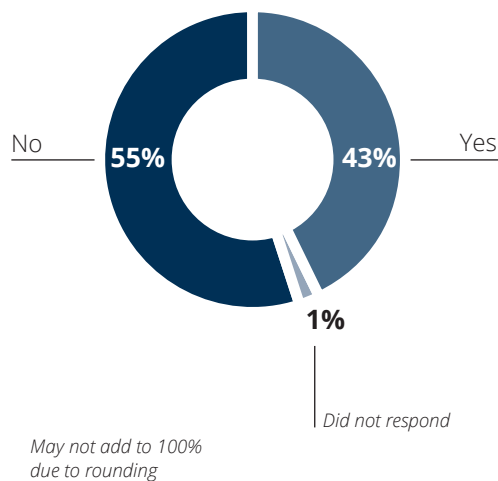
Most respondents appear to be prepared for what to do after a cyber attack occurs.

Q6

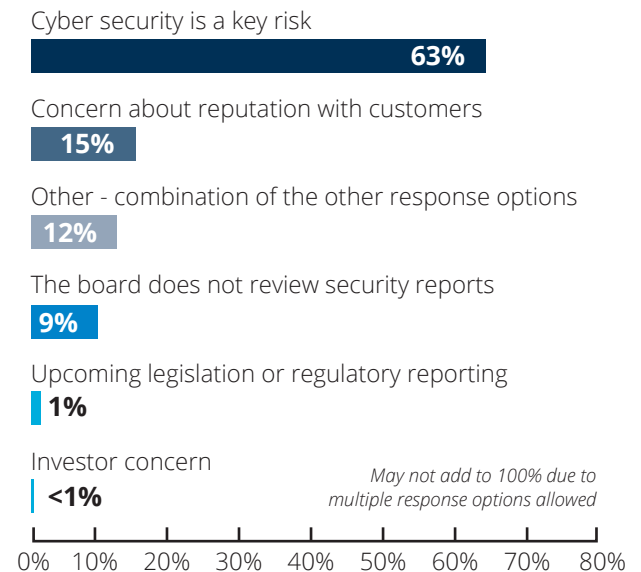
Investment and Customer Data

Q7

7.1 Does the board review and challenge reports on the security of customer data?



7.2 What are the drivers of the board's review of security reports? **Select all that apply.**



It appears that at the moment boards don't have a lot of input into the security of customer data.

Cyber security is a key driver of board reviews of security.



APPENDIX B

SURVEY QUESTIONS



All Survey Questions

Q1: Respondent Profile

- 1.1** In order to optimise results, we request that this questionnaire is not passed to the Chief Information Officer (CIO) or others to complete on your behalf. However, if you have done so, could you please indicate who has supported you in completing this questionnaire.
- 1.2** Which of these titles best describes your role? (Note: preference is for the survey to be completed at the board or committee chair level.)
- 1.3** Which sector classification best applies to the company's main business?
- 1.4** Indicate which of the following risk factors apply to your company (select all that apply).

Q2: Understanding the Threat

- 2.1** Does the board have a clear understanding of what the company's key information and data assets are (e.g. IP, financial, corporate, strategic, customer/personal data, etc)?
- 2.2** Does the board have a clear understanding of the value of those key information and data assets (e.g. financial, reputational, etc) to the company, a competitor or criminal?
- 2.3** What is the board's understanding of the potential resulting impact (e.g. on customers, share price or reputation) from the loss of or disruption to those key information and data assets?
- 2.4** Does the board periodically review key information and data assets (especially confidential data) to confirm the risk management, legal, ethical and security implications of retaining them?
- 2.5** Does the board receive regular high level intelligence from the CIO/Head of Security on who may be targeting your company, from a cyber perspective, and their methods and motivations?

- 2.6** Does the board encourage its technical staff to enter into formal information-sharing exchanges with other companies in your sector and/or across the economy in order to benchmark, learn from others and help identify emerging threats?
- 2.7** Do you understand where the biggest vulnerabilities/risk exposures are in your IT security perimeter?
- 2.8** Does your organisation engage external parties to perform regular vulnerability or penetration assessments?
- 2.9** What level of understanding do the directors have regarding the cyber security of the ecosystem (e.g. vendors, suppliers, customers) within which the organisation operates and the risks emanating from the ecosystem?
- 2.10** What level of understanding do the directors have of the key controls in operation in the cyber resilience framework?
- 2.11** How confident are you that your company is properly secured against cyber attacks?
- 2.12** Do you use public cloud services and, if so, are the risks clearly documented and understood?

Q3: Leadership

- 3.1** Is cyber net (residual) risk expected to increase or decrease, in terms of likelihood of occurrence, over the next year or so?
- 3.2** In your view, how important are cyber risks to the business?
- 3.3** Which of the following statements best describes how cyber risk is handled in your board governance process?
- 3.4** Who is the company's most senior "risk owner" for cyber?
- 3.5** Where, in governance terms, is the "risk owner" for cyber held to account?
- 3.6** Does the board include a director with a good understanding of information security and cyber security in particular?

- 3.7** Do you feel the company is doing enough to protect itself against cyber threats?
- 3.8** Do you feel board colleagues take cyber risk sufficiently seriously?
- 3.9** Have you personally undertaken any form of cyber security/information security training in the last 12 months?
- 3.10** Has your board undertaken any form of cyber security/information security training in the last 12 months?
- 3.11** Given the risks you face, how appropriate is the investment you are making around cyber defences?
- 3.12** How has the board sought to reassure investors and customers of its robust approach to cyber security?
- 3.13** When did your board start receiving incident reports on cyber security?
- 3.14** Does your organisation have a specific cyber security budget?
- 3.15** Does your organisation have an information security policy that complies with a global standard?
- 3.16** Do you have a good understanding of the legal and regulatory requirements regarding cyber security, including reporting and privacy obligations?
- 4.5** Does the board have an understanding of where the company's key information or data assets are shared with third parties (including suppliers, customers, advisors and outsourcing partners)?
- 4.6** Has the cyber resilience of key third party providers (e.g. vendors, suppliers) and clients/customers that connect to your organisation been assessed?
- 4.7** Do cyber risks form part of the assessment of risk for all new projects and significant transactions (e.g. mergers and acquisitions)?
- 4.8** Does your organisation conduct testing of staff to determine the security risk culture (e.g. sending phishing emails to staff requesting a document to be opened)?
- 4.9** Does your organisation have sufficient skilled resources to deal with cyber risks?
- 4.10** Is the organisation's assessment of cyber risk tolerance informed by the role of the organisation in the sector (e.g. critical infrastructure)?
- 4.11** How often is the cyber resilience framework independently assessed?
- 4.12** Does the organisation assess its cyber security culture?
- 4.13** Do you have a clear understanding of your company's disclosure requirements regarding a cyber breach?

Q4: Risk Management

- 4.1** Does the company's risk register include a "cyber risk" category?
- 4.2** In the risk register, how well described are cyber risks, and the potential consequences for the business?
- 4.3** To what extent has your board explicitly set its appetite for cyber risk, both for the existing business and for new digital innovations?
- 4.4** Where risk is a product of likelihood and magnitude, how significant or important is cyber risk, when compared with all the risks the company faces?
- 4.14** How frequently does the board review the cyber security strategy or roadmap?

Q5: Awareness of Help

- 5.1** The Australian Signals Directorate (ASD) suggests that 85% of threats can be mitigated by implementing the ASD top 4 strategies. Have you implemented the ASD top 4 mitigation strategies (i.e. application whitelisting, patching common applications (e.g. MS Office), patching operating systems and restricting administrator privileges)?

- 5.2 Does your organisation perform benchmarking or self-assessment against a recognised standard?
- 5.3 Are the results of the benchmarking or self-assessment discussed at the board, including the identified gaps?
- 5.4 Have you considered using cyber insurance?
- 5.5 Does your organisation's Internal Audit (or other independent assurance function) team conduct cyber resilience audits?
- 5.6 Has your organisation implemented an ongoing cyber awareness training program for staff?
- 5.7 What is the primary source of information for directors to stay informed and current on cyber security topics?
- 5.8 Does the board ratify the cyber security strategy and framework?
- 5.9 Does the board encourage the cyber security team to engage in data sharing arrangements with other organisations in its environment (select all that apply)?
- 5.10 Does the organisation perform regular internal vulnerability scans (e.g. by the security team)?
- 5.11 Does the organisation perform regular external penetration testing?
- 5.12 Does the organisation use a set of standard metrics to quantify or trend the cyber risk?
- 5.13 Has your organisation established a partnership relationship with the national Computer Emergency Response Team (CERT)?

Q6: Cyber Incidents

- 6.1 From reporting provided to the board, has the company experienced more or fewer cyber attack attempts over the last year?
- 6.2 From your own recollection, how well did the company respond to those compromises and occurrences?
- 6.3 Where, in governance terms, were these compromises and occurrences considered (select all that apply)?
- 6.4 Have you considered how you would notify your customers or clients of a breach of their confidential data?
- 6.5 Are you confident in your organisation's ability to detect, respond and manage a cyber intrusion to minimise impact to your business?
- 6.6 Does the organisation have a documented and approved response, recovery and resumption plan and is the plan tested?

Q7: Investment and Customer Data

- 7.1 Does the board review and challenge reports on the security of your customer's data?
- 7.2 What are the drivers for the priority of the board's review of security reports?



Pooling knowledge
and openly sharing
experiences can deliver
valuable insights that
benefit Australian
industry and
the economy.



Contact details

ASX Customer Service

T: 131 279 (from within Australia)
T: +61 2 9338 0000 (from overseas)
E: info@asx.com.au

ASX Media Relations

T: +61 2 9227 0218
E: media@asx.com.au

www.asx.com.au

To the extent permitted by law, ASX and its employees, officers and contractors shall not be liable for any loss or damage arising in any way, including by way of negligence, from or in connection with any information provided or omitted, or from anyone acting or refraining to act in reliance on this information.

ABN 42 004 523 782

ASX April 2017



Deloitte.

