FIRST ADVISERS

CYBERSECURITY: SURVEY OF CORPORATE READINESS FOR MANDATORY REPORTING

In 2018 Mandatory Reporting of Cybersecurity breaches will come into force, bringing with it a sharp focus on how prepared companies are for managing the communication of such high stakes events. As part of FIRST Adviser's sponsorship of the Australian Investor Relations Association (AIRA) 2017 conference, we conducted a brief survey of the ASX300 on both:

- the level of awareness of Mandatory Reporting and the extent to which companies have developed reporting protocols; and
- crisis management plans focused on cybersecurity breaches.

The results of this survey were released at the Australasian Investor Relations Association (AIRA) 2017 Annual Conference as part of a panel discussion entitled "Crisis Management: Managing Cybersecurity Breaches" moderated by FIRST Advisers Executive Director, Victoria Geddes.

PART ONE: DEMOGRAPHIC BREAKDOWN

Questions 1–3

Given the nature of the responsibilities incumbent upon companies with respect to mandatory reporting, we focused on Investor Relations professionals at the target companies. IRO's represented 60% of survey respondents, followed by Company Secretaries at 13%.

The breakdown of responses by sector showed Australian Real Estate Investment Trusts (A-REITs) recorded the highest level of participation (20%), followed by Financials excluding AREITs (19%), Consumer Discretionary (17%) and Metals and Mining (13%). Notably, no companies in the Information Technology sector participated in the survey.

Responses by market capitalisation were distributed relatively evenly. Companies with a capitalisation of between $1.5bn and $3bn contributed the most responses (29%) while companies valued between $750m and $1.5bn were slightly underrepresented with 11% of responses. Remaining categories attracted participation rates of approximately 20% each.

PART ONE: DEMOGRAPHIC BREAKDOWN

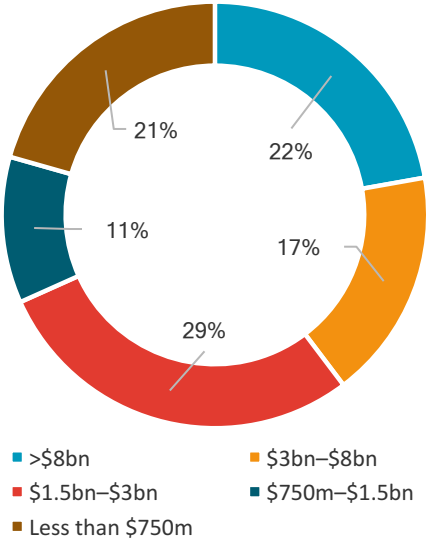
1. Which of the following best describes your position at the Company?

Answers	Participation Rate
IRO	60%
CoSec	13%
CFO	7%
CIO	7%
Corporate Affairs	4%
COO	4%
Other	4%
CEO	2%

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

Sector	Participation Rate
Australian Real Estate Investment Trusts (A-REITs)	20%
Financials	19%
Consumer Discretionary	17%
Metals and Mining	13%
Industrials	7%
Energy	6%
Health Care	6%
Telecommunication Services	4%
Utilities	4%
Consumer Staples	4%
Materials	2%

3. What is the approximate market cap of the Company?



PART TWO: UNDERSTANDING THE THREAT

Questions 4–6

This section of the survey aimed to gauge the level of understanding among senior executives of the negative reputational consequences of a cyberattack, as well as their confidence in existing reporting protocols that have been established to report cyber breaches to the market and/or regulator.

Responses indicated an acute level of awareness and concern for cyber threats; with 95% of senior executives having a clear understanding of cyber vulnerabilities, and 91% of respondents regarding the reputational impact of a cyberattack as either critical (49%) or moderately important (42%).

Concerns related to reputational consequences associated with a cyberattack were greatest among large cap companies (valued at more than $3bn) with 75% rating it as critical to their reputation.

Perhaps reflecting their heightened concern, 88% of large caps reported they were confident or very confident that they are prepared for an attack.

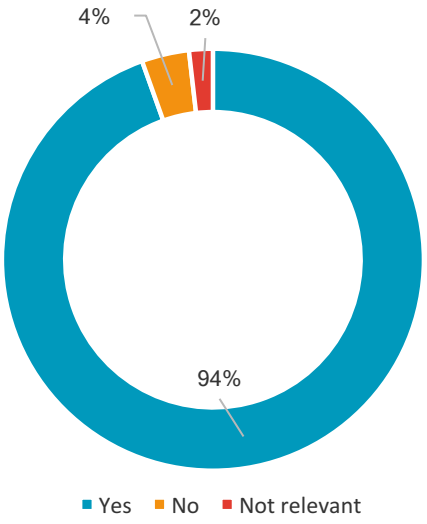
By sector, Financials indicated the highest level of concern (90%); however, they also appeared the most confident in their preparedness (80%).

There was an alarming disparity between companies' confidence in their preparedness for a cyberattack and the reputational impact were one to occur.

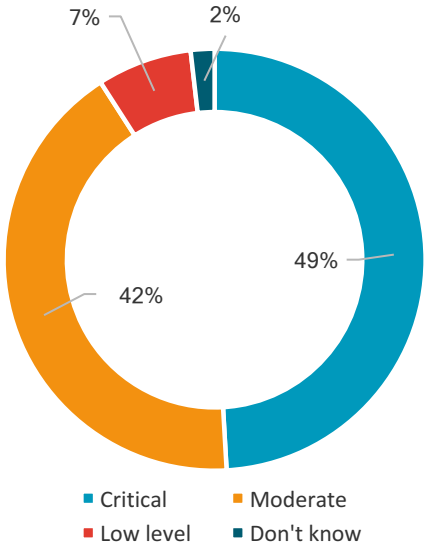
While 91% of companies believe that a cyberattack would have a critical/ moderate impact on their reputation, only 69% were confident or very confident that they were properly prepared for an attack.

PART TWO: UNDERSTANDING THE THREAT

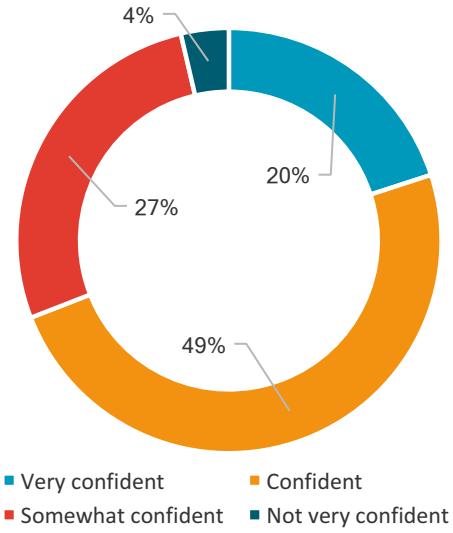
4. Does the senior exec have a clear understanding of which parts of the business, if any, are vulnerable to a cyber attack which could release personal information held by the company?



5. In your view how damaging would a cyber attack be to the reputation of the business?



6. How confident are you that your company is properly prepared for cyber attacks?



49% of companies rated as critical, the likely impact of a cyber attack to the reputation of their business with another 42% viewing it as moderate, so no-one is under any illusion about the potential for serious damage from a cyber breach.

Given that, one would have expected more than 20% of companies to be "very confident" they are properly prepared and not 31% to say they are only "somewhat confident" or "not very confident" at all.

PART TWO: UNDERSTANDING THE THREAT

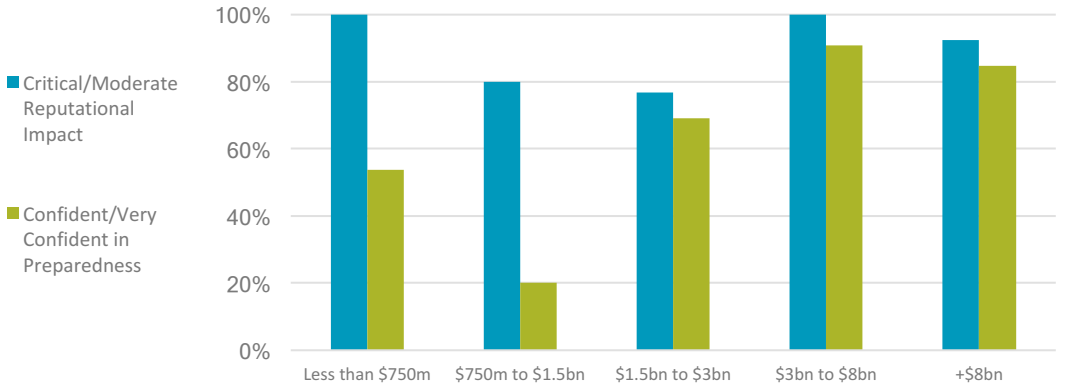
Reputational Impact vs. Confidence in Preparedness

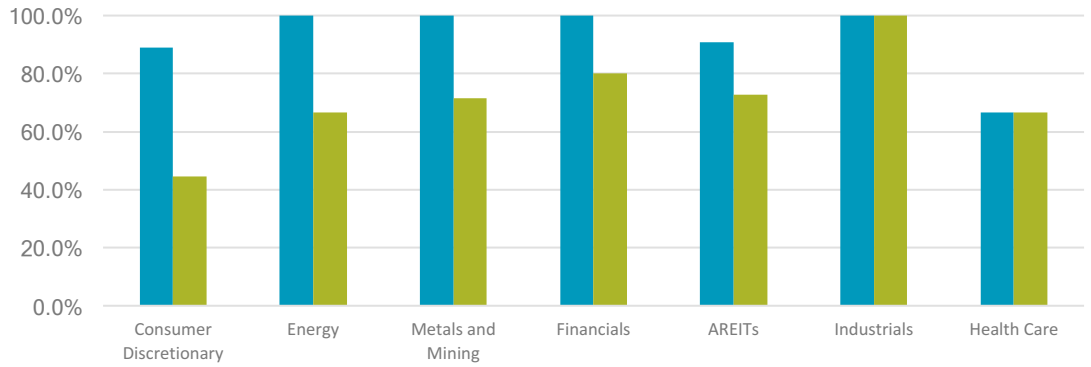
Responses notably differed depending on market capitalisation. Companies above $1.5bn in value exhibited a more appropriate relative alignment of reputational impact and preparedness, compared to smaller participants with fewer internal resources.

Companies with Market Capitalisation of between $750m and $1.5bn displayed the largest discrepancy, as 80% cited a critical/moderate reputational impact; however, only 20% were confident/very confident in their preparedness.

This disparity was greatest among consumer discretionary companies, of which 89% cited critical/moderate reputational impact, compared to 44% being confident/very confident in their preparedness for one.

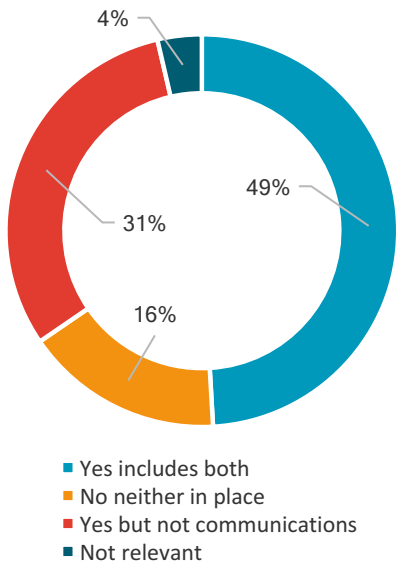
Metals and Mining companies and those in the Energy sector also lagged, with companies in these sectors indicating a critical/moderate impact on reputation, but only around 70% confident/very confident in their preparedness.





PART TWO: UNDERSTANDING THE THREAT

8. Do you have a cyber incident response plan in place which includes a process to communicate the breach to the regulator, the market and customers?

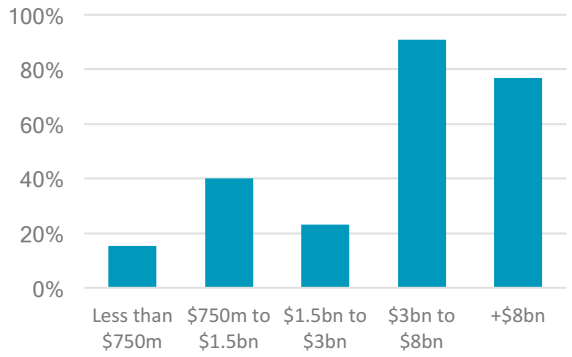


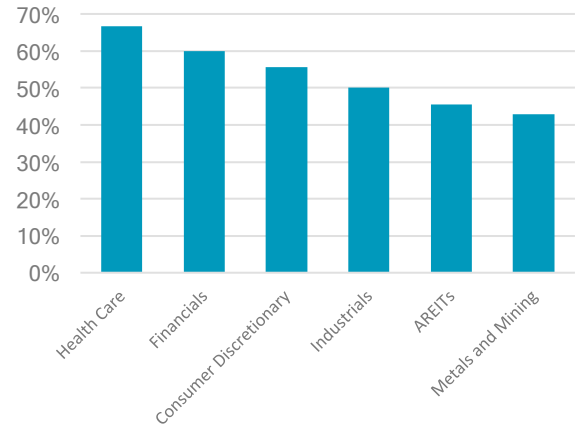
While 80% of companies have an incident response plan in place, more than a third of these don't have any plan for communicating with the regulator, the individuals affected by the breach or the market. Another 20% of companies had not put anything in place at all to manage this risk.

Large cap companies (more than $3bn) were reported as being significantly more likely to be report a breach, with 83% already communicating cyber breaches to the market, compared to only 23% of companies less than $3bn.

By sector, Metals and Mining (43%) and AREITs (46%) lagged with their communications programmes, while Health Care and Financials had higher levels of communication at 67% and 60%, respectively.

Incidence of Companies Whose Plan Includes Communication to the Market





PART THREE: DISCLOSURE OF CYBER RISK

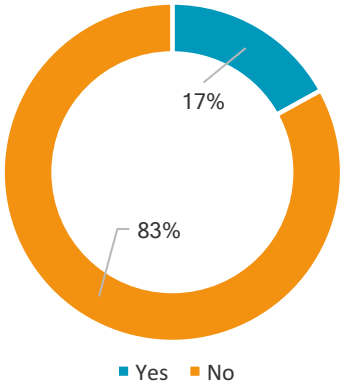
This section of the survey looked at current perceptions of cyber risk by analysts and fund managers, existing reporting protocols that have been established by companies and their preparedness for the obligations imposed upon them by the upcoming mandatory reporting laws.

When asked if they were questioned about cyber risk by analysts and whether they believed investors were factoring it into their risk assessment of the business, **83% of companies reported not having any conversations about cybersecurity risks**.

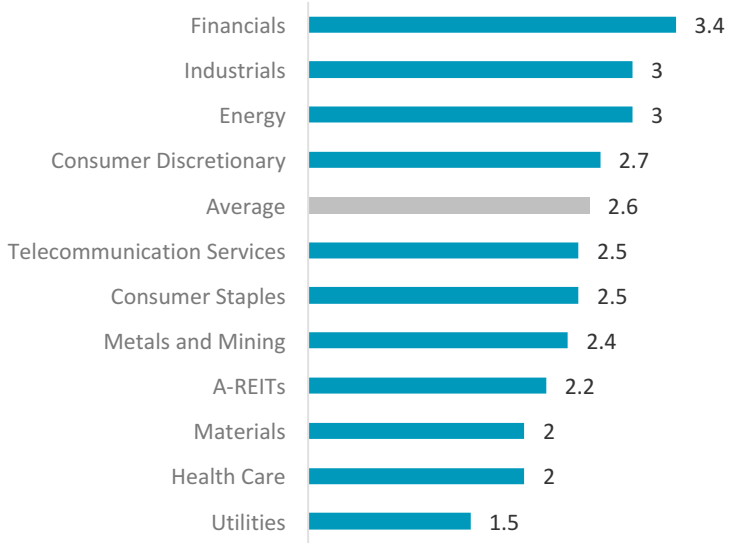
In terms of the market's focus on cybersecurity as a key risk in its valuation of their business, companies rated this as 2.6 on average. Financials (ex-AREITs) recorded the highest rating at 3.4, while Healthcare and Utilities recorded some of the lowest ratings at 2.0 and 1.5, respectively.

There was no discernible relationship between the capitalisation of a company and the market's focus on cyber risk with respect to their business.

9. From your discussions with analysts and investors, do they ask about cyber risk or factor this into their risk assessment of the business?



10. On a scale of 1 to 7, with 1 being oblivious and 7 highly concerned, where would you rate the market's focus on this as a key risk in its valuation of your business?



PART THREE: DISCLOSURE OF CYBER RISK

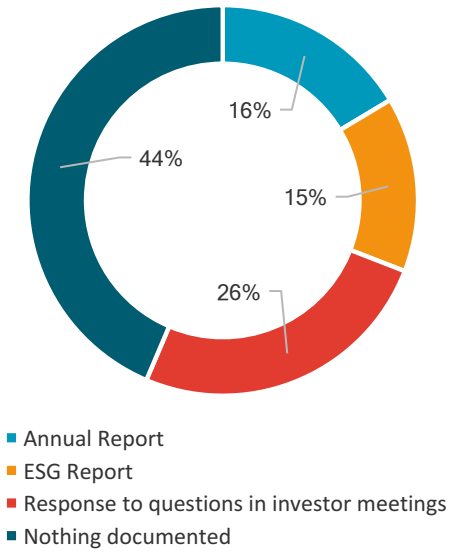
An obvious place to start reporting on cybersecurity is referencing it in the Annual Report or ESG Report. However, only 31% of companies we talked to did this, with 26% addressing it by including Cyber risk as part of their Q&A pack when meeting with investors.

Startlingly, 44% of companies did not have anything documented regarding their approach to cybersecurity.

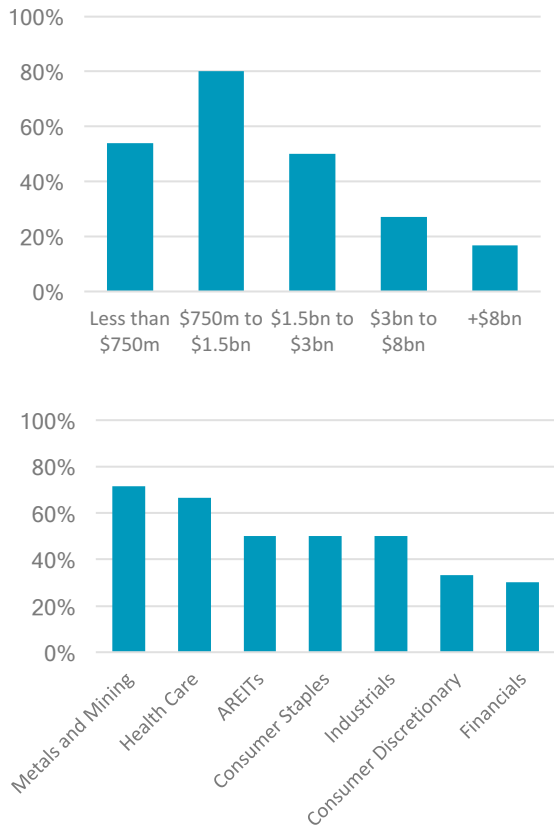
This was particularly so for Metals and Mining Companies (71%) and disturbingly, Healthcare companies (55%) who did not document anything.

By market cap, 57% of companies with market caps below $3bn did not report having anything documented, compared to 22% for companies with market caps above $3bn.

11. How does a company report to investors on its approach to cybersecurity?

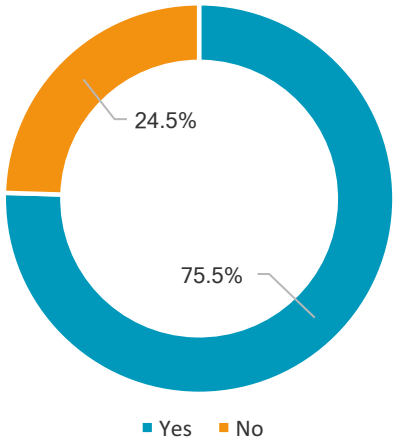


Incidence of Companies with No Documented Approach to Cybersecurity

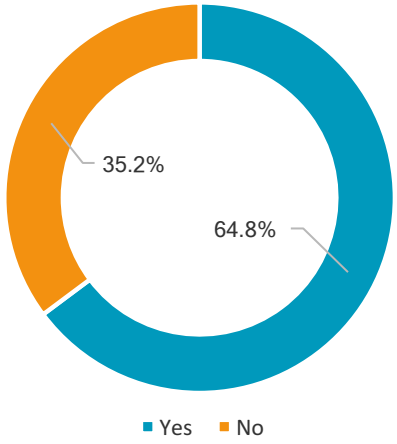


PART THREE: DISCLOSURE OF CYBER RISK

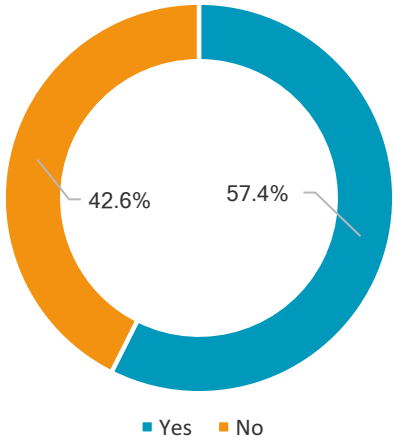
12. Are you aware of the new Mandatory Reporting requirements that will be enforced in early 2018?



13. Are you prepared for Mandatory Reporting early next year and if not what needs to change?



14. Do you know the name of the agency you will be required to report breaches to under the new legislation?

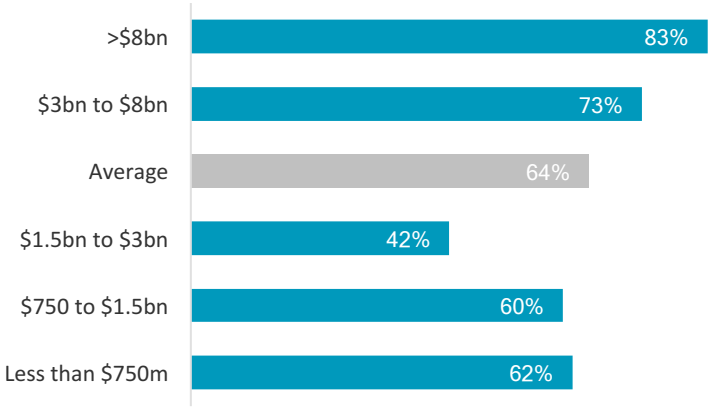


To highlight the work still to be done around the disclosure element of Mandatory Reporting, while 76% are aware it is coming, 35% acknowledged they are not prepared for it and 43% couldn't name the agency to which they would be reporting in the event of a breach. Those who are not prepared are alert to the issue, but are in the process of determining the impacts of the changes on the company, consulting with their service providers on coordinated response plans, and finalising the format of those communications.

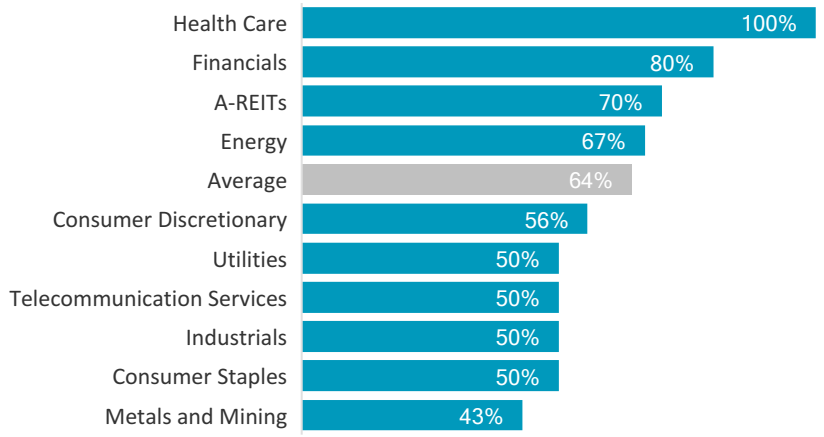
PART THREE: DISCLOSURE OF CYBER RISK

Companies that Consider themselves Prepared for Mandatory Reporting

Responses by Market Cap



Responses by Sector



Large cap companies (above $3bn) view themselves as prepared which would be expected given the internal resources typically available . While 60% of small caps (under $1.5bn) are getting there, the surprise was the level of unpreparedness (58%) amongst the mid cap companies.

Sectors exhibiting below average preparedness included Metals and Mining (43% - the lowest overall level) and Consumer related companies (50-55%).

The sectors which self reported the highest rates of preparedness for the new Mandatory Reporting Requirements were Healthcare (100%), Financials (80%) and A-REITS (70%).

PART FOUR: CYBER INCIDENTS

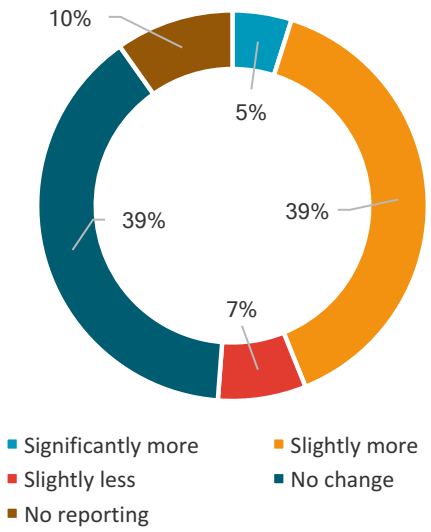
This section focussed on the incidence of cyberattacks for the surveyed companies, including their responses to those attacks, and how their existing cybersecurity framework coped with those compromises.

We also looked at the specific crisis management plans implemented by companies and the extent to which they are routinely reviewed and tested.

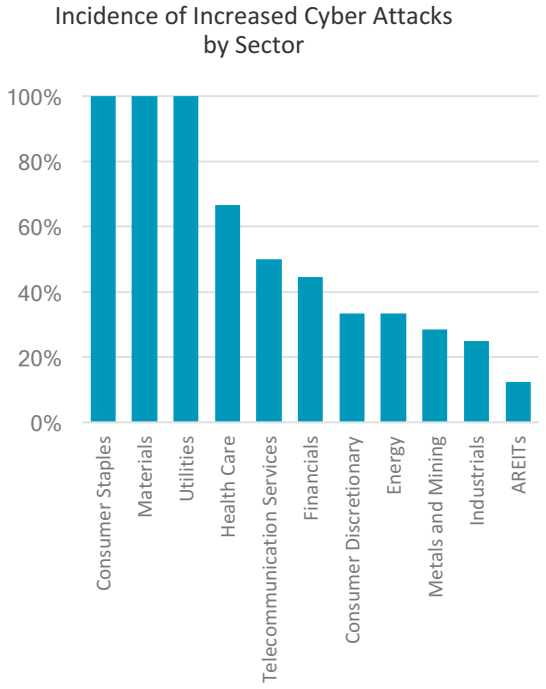
All the evidence gathered in Australia and globally points to rise in cyber activity. This was supported in the survey with 44% of companies reporting a slight or significant increase in the number of attempted cyberattacks this year, compared to last year.

Half of the surveyed companies experienced the same number of cyberattacks as the previous year, while only 7% experienced a reduction.

15. Has the company experienced more or fewer cyber attempts over the past year?



By sector, two-thirds of Healthcare and 44% of Financials, both high risk sectors, experienced an increase in the number of cyberattacks in the last 12 months. This may partially explain their heightened communication of and preparedness for breaches.



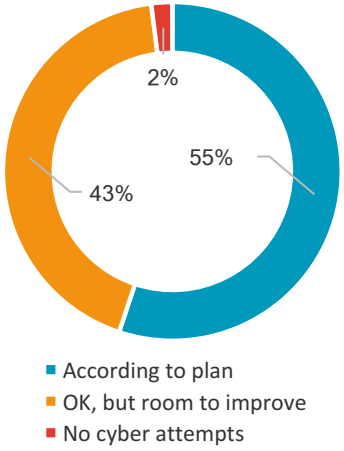
PART FOUR: CYBER INCIDENTS

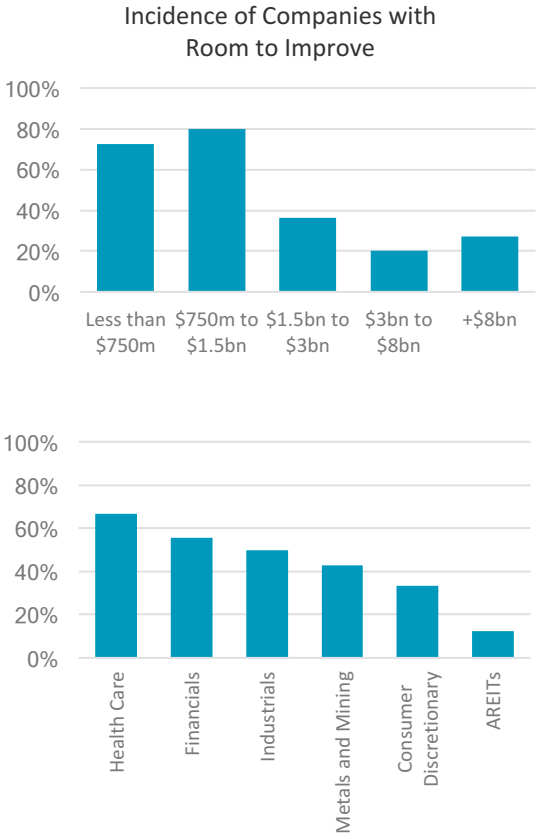
When asked how well they believed the company fared with its response to prior compromises and concerns, roughly half of all respondents admitted they believed that they had room to improve.

The incidence of companies that believed they had room to improve tended to be negatively correlated with the company's market capitalisation. The number of smaller companies (less than $1.5bn) that indicated they had room to improve (75%) was significantly higher than larger companies above $1.5bn (28%).

By sector, healthcare (67%) and financials companies (56%) tended to believe they had room to improve, whereas AREITs (13%) and consumer discretionary (33%) companies recorded the lowest levels of room to improve.

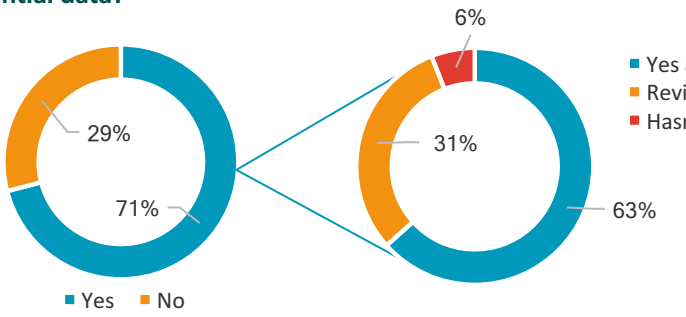
16 From your own recollection, how well did the company respond to those compromises and occurrences?





PART FOUR: CYBER INCIDENTS

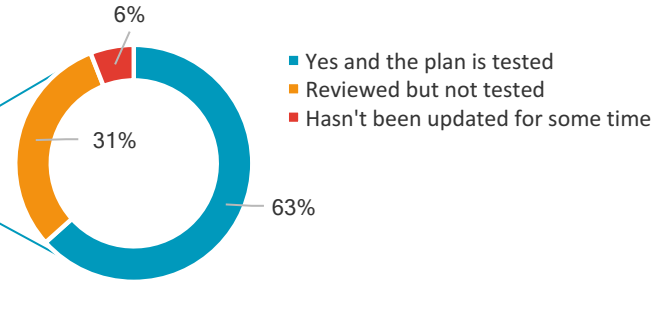
17. Do you have a specific crisis management plan in place for how you would notify your customers, clients, ASX and, early next year, the regulator of a breach of confidential data?



Responses to these questions revealed that 71% of respondents have a crisis management plan for addressing cybersecurity breaches; however, less than two-thirds of these companies have actually tested it.

Companies with a market cap of less than $1.5bn were the least prepared, with only half indicating they had a crisis management plan for cyber in place. A similar percentage of Metals and Mining, Consumer Discretionary and Healthcare companies had cyber plans.

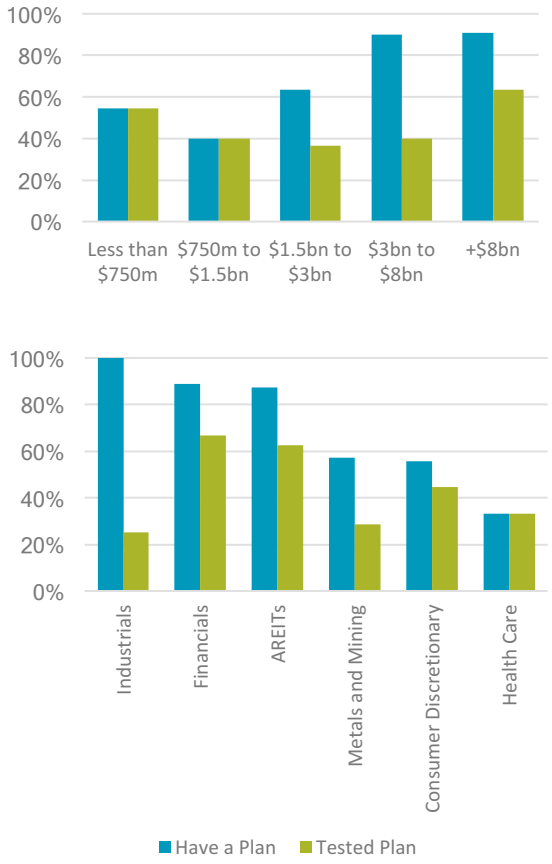
18. Is that plan reviewed annually and tested to ensure all parties understand what needs to happen in the event that a breach needs disclosing?



Of those companies with a cyber crisis management plan, A-REIT's recorded the highest rate of testing (83%) followed by Financials (75%), while Metals and Mining (50%) and Industrials (25%) were among the lowest.

Although companies with a higher market cap tended to be more likely to have a specific cyber crisis plan, the rate of testing tended to decrease with size. All companies with a market cap below $1.5bn tested their plans, whereas testing amongst companies in the $1.5bn-$3bn and $3bn-$8bn capitalisation brackets decreased to 57% and 44%, respectively.

Incidence of Testing for Cyber Plans



FIRST Advisers is an investor relations and corporate communication specialist with an in-house call centre for shareholder engagement campaigns.

Our investor relations advisers undertake Perception Research for corporates with financial markets participants including brokers and fund managers.

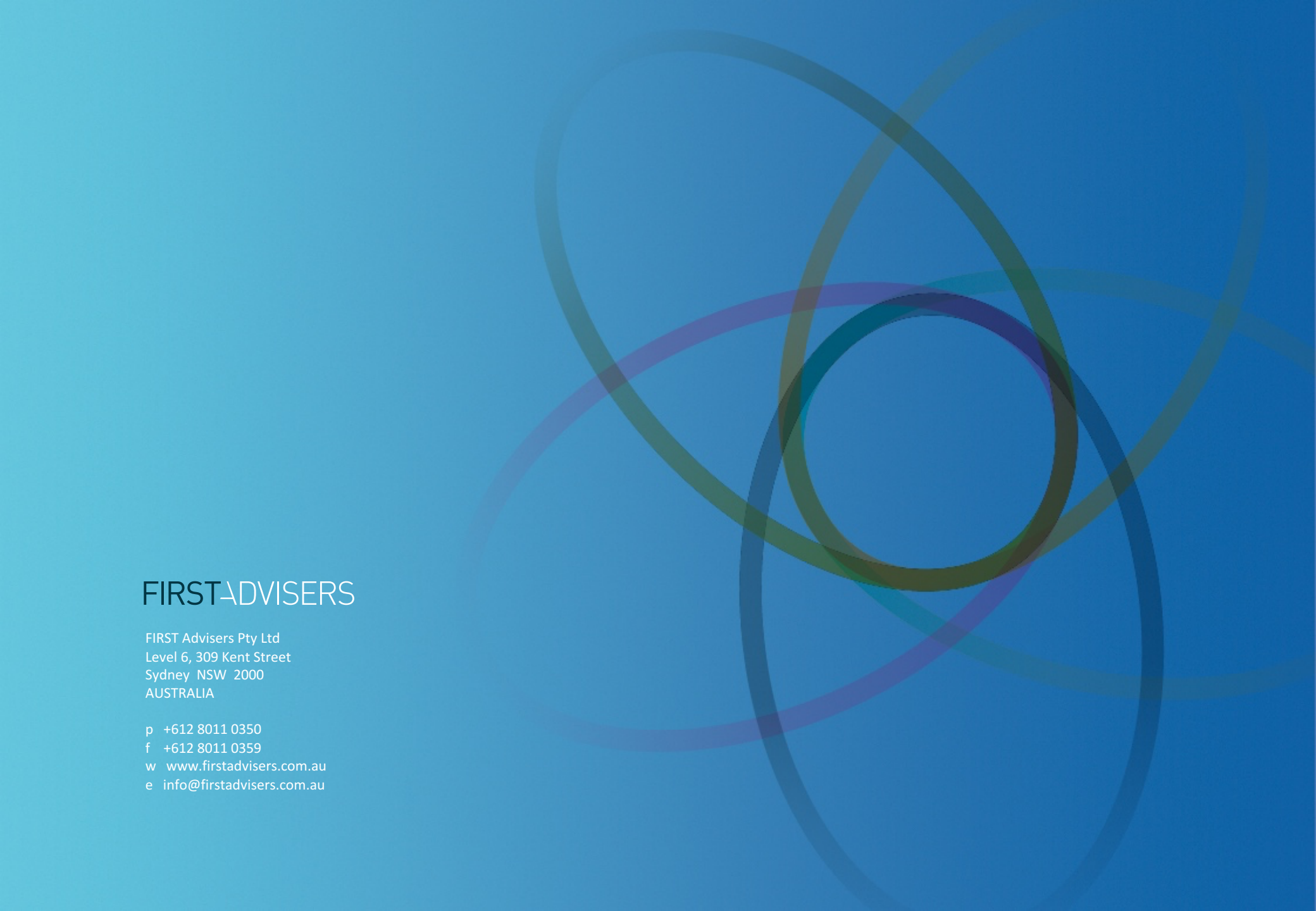
Our Corporate Communication experts engage with the financial media to help raise a company's profile and project an accurate corporate narrative.

Our shareholder engagement team undertakes solicitation for votes (AGMs, EGMs, Scheme Meetings), acceptances (takeovers) and support for capital raisings.

Our combined expertise and ability to reach a wide audience to tap into their views on issues specific to financial markets is unique.

If you are interested in Perception Research, Proxy Solicitation or a Customised Survey targeting companies, fund managers, asset managers, brokers or retail shareholders, give us a call.

Contact Ryan Wong
Business Development
p +612 8355 1001
e rwong@firstadvisers.com.au



FIRST ADVISERS

FIRST Advisers Pty Ltd
Level 6, 309 Kent Street
Sydney NSW 2000
AUSTRALIA

p +612 8011 0350
f +612 8011 0359
w www.firstadvisers.com.au
e info@firstadvisers.com.au