FIRST ADVISERS

WHITE PAPER

Mandatory Reporting of Cybersecurity Data Breaches – Are You Ready?

Background to Legislation

In February this year the Federal Government passed the Privacy Amendment (Notifiable Data Breaches) Bill 2016, legislating that all organisations that have suffered a cybersecurity breach, or have lost data, have to report the incident to the Office of the Australian Information Commissioner (OAIC) and notify affected customers as soon as they become aware of a breach.

The threshold for notification under the new Act will be more onerous than most other global jurisdictions, with the test based on whether the breach "is likely to result" in serious harm to an affected individual.

Presently, there is no mandatory requirement for an organisation that is the victim of a cyber-attack to inform the OAIC or affected individuals following a data breach involving personal information. The Privacy Act, however, already requires businesses that hold personal information to protect it from misuse, interference and loss, as well as unauthorised access, modification or disclosure, which includes where a business engages third parties to store personal information.

Present predictions by the OAIC suggest that the new mandatory requirements for notification will double the number of reported incidents each year.

The Scheme formally comes into effect on 22 February 2018 with specific carve outs for state governments, local councils and organisations with turnover less than $3 million a year. So every private and public company with annual turnover of $3 million or more, listed or not, will be captured by this change. This has reporting implications for listed companies that go beyond their continuous disclosure obligations which are, as we know, triggered by the materiality test.

Mandatory reporting relieves companies from having to make judgement calls about materiality, any breach that 'is likely to result in serious harm' to an individual will be reportable. This could occur, for example, when there is unauthorised access to, disclosure or loss of customer information held by an entity. Such information includes personal details, credit reporting information, credit eligibility information, and tax file number information. Companies must report the breach within 72 hours.

A failure to report or notify individuals may require companies to make a formal public apology and pay compensation to any affected individuals. Large civil penalties of $360,000 for individuals and $1.8 million for organisations could also apply for serious or repeated non-compliance with mandatory notification requirements.

How Real is this Problem?

In Australia the infrequent reporting of cyber breaches leads to a general sense that 'everything must be OK'. The iceberg analogy springs to mind, with what you see being only a fraction of what is hidden out of sight, as anyone working in the IT industry or specialising in cybersecurity will tell you. Often the breach is discovered by a third party and makes it into the media before any formal acknowledgement by the company. This was the case with nib limited when personal details of customers were displayed on its website for over an hour and with Telstra when the information of more than 15,000 customers was made available online for over a year.

Results from the Australian Cyber Security Centre's (ACSC) 2016 Cyber Security Survey revealed that nine out of every 10 Australian organisations dealt with an attempted or successful cybersecurity breach during fiscal 2015-16 –

and that 58 percent had been successfully compromised. Half of those surveyed also said that external parties informed them of a possible breach before they had detected it themselves.

The Gemalto Breach Level Index, which monitors cyber breaches globally every six months, reported 918 incidents in the first half of 2017, the majority of which (87%) are in the US. In the Asia/Pacific region, which accounted for 5% of all reported breaches during the period, Australia and India lead the pack.

ASIA/PACIFIC 5%

15	Australia	1	Hong Kong
15	India	1	Japan
5	New Zealand	1	Malaysia
3	Singapore	1	Phillippines
2	China	1	Taiwan
2	South Korea	47	INCIDENTS

Identity Theft
49%
global increase

Accounting for
74% **of all reported breaches**

In the first six months of this year there was a **49% increase in the incidence of identity theft globally**, something that has the potential to ruin the victim's life, and this **accounted for 74% of all reported cyber breaches**. Breaches by malicious outsiders increased by 23% compared to the second half of calendar 2016, indicating that organizations are still not adequately addressing this threat. **By 2020 it is estimated that roughly a quarter of the world's population will be affected by data breaches.**

The Gemalto Report notes that most of the regions monitored will see a "significant increase in the number of disclosed breaches and data records as governmental regulation, like Europe's General Data Protection Regulation (GDPR) and (our own) amendments to Australia's Privacy Act, is enforced starting in 2018."

So there is no question that over the next twelve months there is going to be a heightened level of public awareness about the vulnerability of institutions, both government and private, large and small, to cyber attack.

Cybersecurity breaches will impact the share prices of listed companies. A study by IT consultant CGI and Oxford Economics, found two-thirds of firms breached had their share price negatively impacted. Out of the 65 companies evaluated since 2013, breaches cost shareholders over £45 billion.

2/3
firms breached had their share price negatively impacted

The cost of cyber attack to shareholders since 2013
£45bn+

Communication Priorities – a Checklist

There are a couple of issues that the Mandatory Reporting legislation will raise for listed companies.

First, is demonstrating to shareholders that a company understand the risk and that policies and procedures are in place to protect against such events. Second is having a communication plan that is detailed, up to date and periodically tested in readiness for managing a reportable cyber breach when (not if) it occurs.

Readiness – demonstrating capability and resilience

Both retail and institutional investors can go to the company's annual report as a first point of reference for checking whether cybersecurity is treated as an operational risk and how it is managed. Whether companies choose to include this in their Statement of Risks, appears to be somewhat arbitrary. For example two of the four banks don't single it out for special mention, despite the fact that data security is clearly core to their licence to operate, while major companies such as Origin Energy, Telstra and Myer do.

We expect that companies will feel compelled to address, if they haven't already, the inclusion of a statement on cyber risk in the annual report or ESG report. The increased public awareness of this as an issue will make it difficult to ignore. This shouldn't be a formulaic or a tick the box exercise, but one that provides appropriate acknowledgement that the board is aware it is a factor that could affect future financial or operational performance, describes the impact it could have and what the Company is doing to manage it.

The large industry funds, institutional investors and investment banks that have in-house research capability, including dedicated governance teams that focus on ESG issues, undoubtedly have this risk on their radar. They have greater access to boards and management teams and such issues are typically raised by shareholders directly with the Chairman in closed meetings in the lead up to AGM season. AMP for example has for many years had an active interest in cybersecurity and have even gone so far as to say that how a company answers questions about cybersecurity provides valuable insights into the general quality of the company's governance and risk management.

If a detailed Q&A in relation to cybersecurity hasn't already been part of the standard briefing pack prepared by companies for such meetings, we strongly recommend that it is on the agenda for 2018.

For corporate advisers and the ASX, when setting out guidelines for preparing companies for listing, their exposure to cyber risks should become a standard inclusion in the risk section of any Prospectus.

Being Prepared to Respond

Being unprepared for a cyber event is not an excuse these days and, while IT teams may have been able to manage breaches discretely and invisibly behind the scenes, companies will no longer be able to hide behind the veil of secrecy. Nor is it an option to pass the responsibility for reporting to third party contractors who are paid by companies to manage their IT. If your customers have their data breached, it is your problem.

As IR professionals you need to be informed about your company's cybersecurity risk profile, so there are a number of questions you should starting asking. For example:

- Do you have customers/clients who would be at risk if you have a data incident involving loss of personal information?
- What is the company doing to mitigate data breach risk?
- What are the director's cybersecurity qualifications and role in cybersecurity oversight?
- What steps is the company taking to protect its key cyber assets, including employee education?

Prepare an Incident Response Plan

Having a plan in place ahead of time is recognised as being the No. 1, most effective-communications approach to data security. This includes the following:

1. Assemble a core group of executives to act as the Communications Response Team. Clarify roles and responsibilities, ensure 24 hour contact details are shared and designate the ultimate decision-making authority. Keep this team lean but make sure IR is included.
2. Know all the key internal and external stakeholders and the channels to reach them. This will include the Office of the Australian Information Commissioner and understanding exactly what information you must provide. You will need to take reasonable steps to notify the individuals affected, including publication of a notification online. Keep employees informed and provide guidance to those dealing with customers on how to respond to inquiries.
3. Know and develop relationships with the critical influencers in government, the regulatory bodies, ASIC, APRA, ASX, unions etc.
4. Identify your lobbying, forensic investigators, legal and communications partners because you will need support.
5. Test your plan.

Crisis Management including Market Disclosure

ASX's continuous disclosure obligations already require companies to inform the market when the nature of a breach is likely to have a material effect on the price or value of its securities. As of February 2018 any data breach involving personal records will be notifiable to the OAIC within 72 hours, which means it becomes public.

The whole issue of how much to communicate about a breach is a topic in itself given that facts can often be elusive in the first 24 hours and cyber incidents are by nature very complex. A cybersecurity incident is a crisis, so it is important to make haste slowly. Meet disclosure requirements promptly but communicating information early which later proves inaccurate can damage credibility. A safer approach is to talk about how the company is addressing the incident, what it is doing to support those impacted and to prevent a recurrence. Communicating with shareholders through a carefully crafted ASX Release built around what is known and what processes are in place to identify the scope of the problem, is better than leaving the market to do its work through rampant speculation. Working closely with the company's legal and communications advisors is a given at this time.

Survey Results on Australian Listed Companies Preparedness for Mandatory Reporting

FIRST Advisers surveyed the ASX300 companies during September and October 2017, seeking feedback on their readiness for Mandatory Reporting of Cybersecurity breaches in 2018. This paper summarises its findings.

Perhaps not unsurprisingly, the responses were sharply divided according company size and sector.

58% of Mid cap companies and half of those operating in the consumer sector, telcos, utilities and industrials stocks have yet to establish frameworks for reporting on or addressing this risk. Large cap companies, particularly those in the Financials and Healthcare sectors – two sectors most at risk of this type of breach – indicated they are ready for the new reporting environment.

85-90% of large cap companies are also well prepared for dealing with cyber attacks more generally, with comprehensive response plans in place that cover all key stakeholders. 44% of small cap companies (less than $1.5bn market cap) still have work to do on this front.

Significantly, there is a very low level of awareness within the investment community with companies rating the market's focus on cybersecurity as a risk factor as close to 'negligible' in its valuation of their stock.

Awareness Level

95% of senior executives have a clear understanding of their cyber vulnerabilities and their awareness of the impending Mandatory Reporting regime is high at 75%. There is, however, significant variance across sectors with a high level of awareness (90-100% of companies) in the Energy, Healthcare, Utilities and Financials sectors.

At the other end of the scale only half the companies in the Metals and Mining, Telco, industrials and consumer staples sectors admitted to being aware of mandatory reporting with companies in the Metals and Mining sector most 'in the dark' (14%) when asked the name of the agency they would be reporting to.

However, there is an even lower level of awareness within the investment community regarding cyber risk.

On a range of 1 to 7, companies rated market awareness as 2.6 on average (with 1 being oblivious and 7 highly concerned) when asked where they would rate the market's focus on this as a key risk in its valuation of their business. The rating increased to 3.4 for Financials.

83% of companies said that analysts never asked about cyber risk.

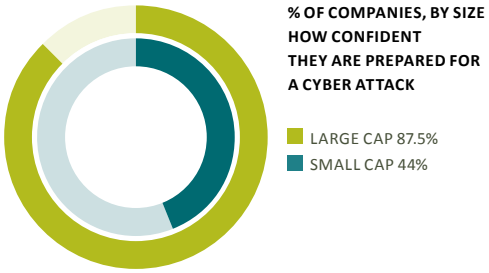
Preparedness

Companies can gain the confidence of investors by documenting or discussing their approach to cybersecurity. It is one way of acknowledging that this is an integral part of a company's approach to risk management. 30% of respondents included reference to this in either the annual report or ESG report, with another 26% ensuring that board/management are well prepared to respond to questions on the topic in investor meetings.

However 40% of companies did not mention cyber risk in any documentation or address it in meetings. Companies in the Metals and Mining (71%) and Healthcare (67%) sectors as well as small to mid-cap companies (56%), those with less than $3bn market cap, stood out.

While 49% of respondents viewed a cybersecurity breach as critical, and another 42% as moderately damaging to the reputation of the business (particularly Financials and companies with a market cap of $3bn+), only 20% were 'very confident' that their company was properly prepared to deal with a cyber breach.

Large cap companies were much more confident (87.5%) than smaller cap companies (44%) to manage an attack.



The sectors that were least confident they were properly prepared for an attack were Metals and Mining (43% of companies) and Consumer discretionary (44%).

Incident Response Plan in Place

80% of companies could confirm they have a cyber incident response plan that is targeted to communicating the incident to the agency, but less than half (49%) combined this with a broader communications plan that included reporting to the market and shareholders.

Large cap companies are generally well organised (83%), ensuring they have response plans in place that are comprehensive and cover all key stakeholders. Less well-resourced small cap companies are struggling to meet this standard (23%).

The high level of preparedness for an attack reflects the experience of 37% of companies reporting an increase in attempted cyber breaches compared to last year, particularly those in the Financials (85%) and Healthcare (67%) sectors.

Nevertheless, just under half of companies (44%) say they have room to improve, based on their handling of prior incidences. The majority (75%) of these were small caps (market capitalisations less than $1.5bn).

Cybersecurity Crisis Management Plan in Place

70% of company respondents have a crisis management plan for managing cybersecurity breaches, a similar finding to that reported by the ACSC's 2016 Cyber Security Survey. 70% of those have tested or reviewed it with companies in the Industrials, Financials, and AREIT sectors being the most proactive.

Of the 30% of companies with no plan in place, the sectors with the majority of companies in this position (50-66%) were in the Healthcare, Telco and Resources sectors and small cap companies (50%) with <$1.5bn market cap.

If you would like a copy of our survey on Listed Company Readiness for Mandatory Reporting, visit our website www.firstadvisers.com.au

FIRSTADVISERS

Investor Relations
Corporate Communications
Transaction Communication Services
Digital and Document Design
Shareholder Analytics
Proxy Solicitation

Level 6, 309 Kent Street
Sydney NSW 2000 Australia
T +61 2 8011 0350
E info@firstadvisers.com.au

Find us on:
firstadvisers.com.au