PERSPECTIVES ON CYBER RISK 2018

MinterEllison

In a connected world where business transcends geographic boundaries, every aspect of cyber risk needs to be a key boardroom concern.

Aon, Cyber Insurance Market Update.

Contents

Methodology

MinterEllison's third annual cyber security survey was completed by more than 70 legal counsel, Chief Information Officers (CIOs), Chief Operating Officers (COOs), Board members, IT specialists and risk managers of ASX 200 and private companies, government agencies and not-for-profit organisations. Depending on their role within the organisation, they responded to either the CIO survey or Board survey.

Participants responded to questions about cyber security roles, responsibilities and attitudes within their organisations.

The survey was conducted during November 2017. This report reflects the quantitative results of the survey questions, as well as the respondents' qualitative comments.

All information provided by participants is confidential and reported primarily in aggregate form.

Where appropriate, MinterEllison has used interviewee quotes to support the report's findings and opinions. The views expressed in this report do not necessarily reflect the views of the individual respondents, unless otherwise stated.

We make no representation or warranty about the accuracy of the information, or about how closely the information gathered will reflect actual organisational performance or effectiveness.

This report contains general advice only, and does not take into account your organisation's particular circumstances or objectives.

Due to rounding, responses to the questions covered in this report may not add up to 100%.

Introduction

In the 12 months since we published our last Perspectives on Cyber Risk report, we have seen an increase in the volume and impact of cyber incidents. It is clearer than ever before that no organisation or industry is immune from cyber incidents, and that cyber attacks do not respect political, geographical or organisational boundaries. In 2017, we saw government, state-owned enterprises, public and private companies and not-for-profits affected by cyber attacks across every industry segment. These included finance, retail, hospitality and healthcare, mining and resources, utilities, professional services and education.

High profile cyber incidents that occurred during 2017 include:

- In February 2017, it was discovered that New York's Stewart International Airport had left its server backups exposed to the open internet for more than a year. Materials that were publicly viewable included sensitive documents from the Transportation Security Administration's investigations into the airport's security screening practices.
- Between May and July 2017, hackers gained access to the personal information of more than 143 million customers of credit rating bureau Equifax, including dates of birth and social security numbers. Equifax was criticised for its handling of the incident, particularly its inclusion of a provision in its terms and conditions requiring customers to forfeit their right to sue in order to obtain free credit monitoring. In the wake of the incident, Equifax's CEO resigned.
- In May 2017, the WannaCry ransomware crypto virus swept the globe, affecting hospitals, telecommunications providers, logistics companies and thousands of other businesses. The virus targeted computers running Microsoft Windows, encrypting data on infected systems and rendering data inaccessible. Users were advised they could regain access to their data by paying a ransom amount (in Bitcoin). The spread of this virus was facilitated by its self-propagating mechanism, which scanned for further vulnerable systems and installed and executed itself on those systems.
- In June 2017, a new variant of the Petya ransomware virus (first identified in 2016) spread throughout the Ukraine. It quickly became apparent that this variant – dubbed 'NotPetya' by cyber security experts was even more malicious than Petya, in that it irrevocably encrypted and deleted files on affected systems.
- In 2017, it was revealed that Uber had suffered a data breach in 2016. Hackers had stolen the personal information of more than 57 million Uber users, including names, email addresses and mobile phone numbers. Uber suffered further embarrassment when The New York Times reported the hackers had been paid a sum of USD$100,000 in the guise of a 'bug bounty' to conceal the incident.
- The USA intelligence community was subject to a cyber incident in March 2017, when 8,176 secret CIA documents pertaining to hacking and cybersecurity were published by WikiLeaks under the name 'Vault 7'.

Introduction continued

These documents revealed the location of a CIA Centre for Secret Intelligence covert base within a US consulate and that the CIA had been focusing efforts on monitoring smart phones. They also identified a substantial number of unpatched exploits used by the CIA for surveillance, including Samsung smart televisions that observed individuals, even when the televisions appeared to be off. As a result of the leak, knowledge of these unpatched exploits was spread worldwide.

- In November 2017, the 'Paradise Papers' were made available to media outlets by the International Consortium of Investigative Journalists. Like the 'Panama Papers' before them, these documents were obtained as a result of a cyber attack (which occurred in 2016). The papers revealed tax minimisation strategies implemented by various large organisations, including Facebook, Apple, Uber, Nike, Disney and McDonald's.

These (and many other) incidents demonstrate the numerous means by which cyber incidents may occur, including through deliberate attacks by insiders, malicious activity by external individuals or groups, self-replicating ransomware, 'drive-by' adware, or inadvertent errors made by employees or third party service providers.

However they may occur, cyber incidents have one thing in common – serious consequences for affected organisations, beyond inconvenience, bad PR or disruption to operations. In this regard, we have seen examples of permanent loss of mission-critical data, irreparable damage to reputation for businesses and individuals, and long standing executives resigning or being dismissed in the wake of cyber incidents.

Last year we said that "cyber security can no longer legitimately be considered the domain of IT alone". Not only did the events of 2017 confirm this, they have made clear that Board members, particularly of listed companies, must be fully apprised of cyber risk, as they are ultimately accountable for its management.

It is also more clear than ever before the speed by which, and manner in which that, an affected organisation responds to a cyber incident, is critical to mitigating commercial, legal and regulatory risk and protecting the organisation's reputation.

In light of an ever evolving landscape, in late 2017 we conducted our third annual cyber security survey, to assess changes in Australian organisations' cyber resilience during the course of 2017.

The survey targets legal counsel, risk managers, Board members and senior executives from public and private sector organisations, across a range of industries.

We found that further progress has been made in the past 12 months in relation to organisations' awareness of the importance of cyber risk management. Organisations' concerns about cyber risk have also intensified, unsurprising given WannaCry, NotPetya and the many other high profile cyber incidents that occurred during 2017.

Despite this, our findings indicate that for many organisations, much work remains to be done in increasing their cyber resilience and ability to effectively manage cyber risk.

Key findings

one

Organisations are becoming more educated and informed about cyber security

two

While cyber risk awareness continues to increase, many organisations are still not prepared

three

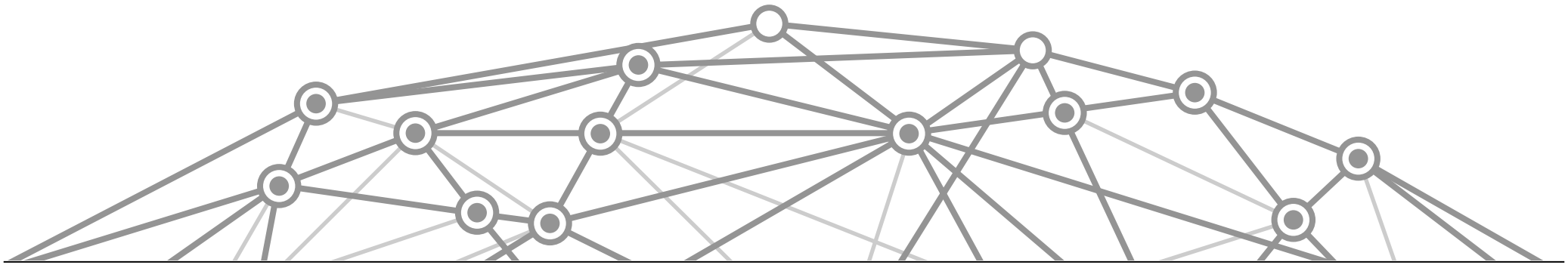
An increasing number of surveyed organisations are taking advantage of cloud services

four

Uptake of cyber insurance continues to rise but it is just one cyber risk management measure

five

While around 40% of surveyed organisations are prepared for the incoming NDB laws, many still have work to do



Finding

one

Organisations are becoming more educated and informed about cyber security

70% of Board respondents have a 'fair' or 'good' understanding of cyber exposure

Growth of the digital economy, teamed with increased use of internet, mobile technologies and the Internet of Things (**IoT**), poses ever-growing challenges for information protection.

Many of the cyber attacks described in our introduction to the report (in particular, the WannaCry ransomware campaign) affected Australian organisations and individuals. This has heightened awareness of the risks that accompany these technological advances.

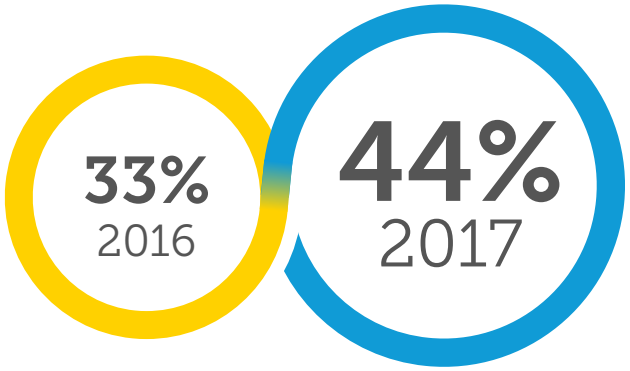
Our most recent survey results reflect this fraught landscape.

More than a third of surveyed organisations indicated they were subject to at least one cyber incident in the last 12 months that compromised their systems or data.

CIO survey respondents who categorised themselves as having a 'good understanding' of cyber exposure increased from 33% in 2016 to 44% in 2017, while those who categorised themselves as having a 'very good understanding' increased from 10% in 2016 to 18% in 2017.

At the Board level, there was an increase from a 'fair' understanding of cyber risk (45%, up from 35% in 2016) and 'very good' understanding (24%, up from 15% in 2016) of cyber risk. Further, the Board survey revealed 82% (up from 65% in 2016) of Boards perceived cyber risk as more of a risk than 12 months ago.

These results suggest organisations are becoming more educated and informed about cyber security, particularly in the lead up to the commencement of Australia's mandatory data breach notification scheme on 22 February 2018 (discussed in detail in Finding 5 on page 17).



CIO survey respondents who categorised themselves as having a 'good understanding' of cyber exposure

> "Cyber security **briefing at board level** would be beneficial"
>
> *Board survey participant*

Finding

two

While cyber risk awareness continues to increase, many organisations are still not prepared

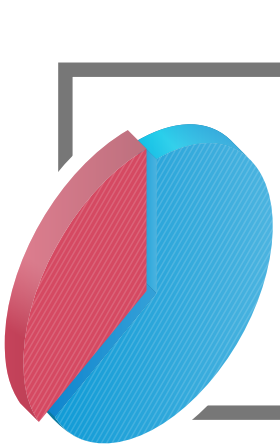
54% of respondent organisations have a cyber incident response plan

Our survey also indicated that 54% of respondent organisations had a cyber incident response plan in place (up from 42% in 2016).

While this represents an increase in readiness, (explained perhaps in part by the commencement of the mandatory data breach notification scheme), it is still concerning that nearly half of surveyed organisations do not have appropriate cyber incident response protocols in place. Further, our survey results indicated approximately only one third of surveyed organisations are testing their cyber incident responses regularly (at least once per year).

Also concerning was a decrease in the percentage of organisations that say they audit their suppliers' IT security practices at least annually (from 34% in 2016 to 21% in 2017).

These results indicate that while awareness continues to increase, many surveyed organisations still have not translated this awareness into effective, tested cyber risk management strategies, protocols, plans and procedures.



Only
one third
of surveyed organisations are
annually testing
their cyber incident responses

Finding

three

An increasing number of surveyed organisations are taking advantage of cloud services

70% of CIO survey respondents are considering cloud service delivery in the next 12 months

Responses to the CIO survey indicated that a wide variety of services are being delivered to organisations via the cloud.

These include email, data storage, access management, IT security, HR performance management, accounting and payroll, productivity applications, mobile device management, and customer relationship management services. The proportion of organisations receiving cloud services has increased from last year's survey in almost every category.

Further, our CIO survey respondents indicated that 70% of organisations are considering adopting further cloud delivery services in the next 12 months.

Against this backdrop, only 29% of CIO respondents said they permit personal information of personnel, customers or suppliers to be transferred and stored outside of Australia.

Our results suggest an increasing number of organisations are taking (or planning to take) advantage of the flexibility offered by cloud based services, while being aware of the risks (be they technical, commercial or regulatory) of transferring and storing personal information overseas.

On the other hand, as noted above, most surveyed organisations are not engaging in regular testing of their own cyber resilience, with an even lower percentage conducting regular audits of the cyber resilience of their key suppliers.

Accordingly, while they may be aware of the risks of outsourcing critical IT and business functions to the cloud, many organisations may not be taking appropriate steps to mitigate against these risks.

Email, data storage, access management, IT security, HR, accounting and payroll are being delivered via the cloud.

Finding

four

Uptake of cyber insurance continues to rise but it is just one cyber risk management measure

Respondents who have **purchased** some form of **cyber insurance**

39% in 2016 VS **62%** in 2017

In our last report we found that cyber insurance uptake had increased among surveyed organisations. Our latest survey responses indicate a significant increase in cyber insurance uptake, with 62% of respondents indicating their organisation has a cyber insurance policy in place (compared with 39% in 2016).

This is consistent with the Insurance Council of Australia's comments that cyber insurance is the fastest growing commercial segment of the Australian insurance market. With the introduction of the NDB scheme, the Australian cyber insurance market is tipped to grow as global insurance houses continue to move into this space. For the moment, however, Australia's uptake of cyber insurance still lags significantly behind that of the established markets in the United States and Europe.

Organisations considering purchasing or renewing cyber insurance products should seek specialist advice to avoid potential gaps in cover. One increasingly common example is a cyber crime enabled by manipulating an individual to transfer a payment to a fraudster's account (known commonly as social engineering), which might fall into a gap between an organisation's cyber risk and crime policies given the "voluntary" nature of the payment. Organisations should therefore ensure that they have adequate insurance cover to protect against social engineering losses.

While cyber insurance is a key risk management measure for many organisations, it is important to remember that insurance should form part of a wider toolkit of risk management measures for organisations, and should not be seen as a panacea for addressing cyber risk. This is especially critical as more organisations move to the cloud (see our Finding 3 on page 12) and are subject to the security arrangements of their third party service providers.

62%

OF RESPONDENTS INDICATED THEIR ORGANISATIONS HAS A CYBER INSURANCE POLICY IN PLACE (COMPARED WITH 39% IN 2016).

Finding

five

While around 40% of surveyed organisations are prepared for the incoming NDB laws, many still have work to do

Australia is joining other countries around the world in **implementing** a **mandatory data breach notification scheme**

The introduction of Australia's NDB scheme, due to commence on 22 February, is widely considered to be long overdue.

The amendments that the NDB scheme will make to the Privacy Act 1988 (Cth) (**Privacy Act**) mean that data breach response planning is no longer a 'nice to have'. Being prepared to act quickly to mitigate, contain and respond to a data breach is a critical legal risk and reputation management strategy.

Many (though by no means all) of our surveyed organisations appear to recognise this need, with around 40% of organisations stating they were preparing for the incoming laws by reviewing policies, data breach response plans and security controls.

Australia is imminently joining a number of its global counterparts in implementing mandatory data breach notification. This will also include the European Union when the General Data Protection Regulation (**GDPR**) begins in May 2018. The GDPR will directly impact many Australian businesses.

Our survey results indicate that many organisations still have work to do in preparing for these laws, as well as implementing the protocols, policies and procedures necessary to mitigate their exposure to cyber risk.

Organisations are preparing for the NDB scheme by reviewing policies, response plans and security controls.

ANATOMY OF A **CYBER ATTACK**

The time to formulate your incident response plans and processes for cyber security is not when your organisation has been subjected to a cyber attack. Rather, your organisation should already have a detailed, battle-tested data breach response plan in place as part of your cyber risk management strategy. One important aspect of creating and updating this plan is to understand how real world attacks have played out, and take the opportunity to learn from them. The Equifax breach, which occurred during 2017, provides an instructive example, given its profile, complexity and impact. The learnings are set out below in four key phases.

PRE-ATTACK

8 MARCH 2017

US Department of Homeland Security's Computer Emergency Readiness Team sends Equifax (and other businesses) a notice advising of the need to urgently patch an exploit within the Apache Struts 2 framework, which Equifax used within its online dispute resolution portal.

9 MARCH 2017

The notice is distributed within Equifax. By the end of March, Equifax's information security department has not identified any systems vulnerable to the exploit.

ATTACK

17 MAY 2017

Attackers first use the exploit to access consumer personal information (**PI**)

29 JULY 2017

Equifax's security department observes suspicious network traffic from the consumer dispute portal, investigates further, and blocks specific traffic

30 JULY 2017

Equifax's security department notices further suspicious network traffic and takes the dispute resolution portal offline. It appears the attackers had continued to access consumer PI between 17 May and 30 July 2017.

INVESTIGATION

31 JULY 2017

Equifax's CEO is notified of the suspicious activity.

2 AUGUST 2017

Equifax appoints lawyers to provide legal and regulatory advice, as well as external security experts to investigate the hack. Equifax also notifies the FBI of the breach.

11 AUGUST 2017

External security experts identify that the attackers may have accessed a database containing a large volume of consumer PI, including names, addresses, birthdates and social security numbers. The large volume of data means affected individuals cannot be immediately identified.

22-24 AUGUST 2017

The Chairman of Equifax's Board and senior management are notified of the breach and start developing a remediation program.

4 SEPTEMBER 2017

External security experts identify approximately 143 million consumers who may have been affected.

LESSON: 9 MARCH 2017

Use risk management protocols – Implementing risk management protocols when identifying vulnerabilities can lessen the risks of a failure to patch, such as:

- identifying a senior manager responsible for overseeing vulnerability patching
- requiring two separate signatures for sign off on high risk vulnerability patching to ensure cross checking
- encouraging the use of 'white hat' hackers to confirm high risk vulnerabilities are removed

LESSON: 2 AUGUST 2017

Ensure you have a battle-tested data breach response plan – Developing (and regularly testing and updating) your data breach response plan ensures you are best placed to quickly identify and implement relevant actions (see page 24 of this report for more information regarding data breach response planning)

ANATOMY OF A **CYBER ATTACK**

7 SEPTEMBER 2017

Equifax publicly announces the breaches.

7 SEPTEMBER 2017

Equifax launches its remediation program which includes the provision of credit file monitoring by three credit ratings agencies, the ability for consumers to 'lock' their Equifax credit file and obtain copies of their credit reports and its scanning of the 'dark web' for one year to identify potential sales of the affected consumer PI.

8 SEPTEMBER 2017

Equifax attracts media criticism for including a mandatory arbitration clause and class action waiver in the terms and conditions that affected individuals agreed to when signing up to the breach monitoring service. The combined effect of these provisions was to potentially restrict individuals' ability to sue Equifax, join a class action or join a class or joint arbitration. Shortly after this criticism, Equifax removes the clause.

8 SEPTEMBER 2017

Equifax attracts media criticism for extended call centre wait times experienced by those affected by the breaches.

9 SEPTEMBER 2017

A software engineer creates a fake 'phishing' version of the Equifax remediation program website using a similar URL. The official Equifax twitter account accidentally links consumers to the fake website. The software engineer explains he created the website and registered the domain to raise awareness.

15-26 SEPTEMBER 2017

Equifax's Chief Information Officer, Chief Security Officer and Chief Executive Officer resign.

REMEDIATION

LESSON: 7 SEPTEMBER 2017

Time your announcement carefully – Equifax notified the public three days after being advised by experts of the scale of the attack. When timing any announcement, your organisation will need to take into account the circumstances of the cyber attack, as well as applicable Australian and overseas laws. For example, Equifax's former CEO stated that Equifax first notified the FBI so it could determine how to proceed in light of any criminal investigation, and also to allow time to prepare Equifax's network for copycat attack attempts following the announcement. Any decision to delay an announcement will need to be justifiable in order to withstand both regulatory and public scrutiny.

LESSON: 8 SEPTEMBER 2017

Review your policies when developing response plans and consider what legal terms are appropriate for services you may offer to affected individuals – Equifax's former CEO later explained that the clause was included inadvertently, as a result of using standard form terms and conditions. In light of your response plans, your legal advisors can identify (prior to any breach occurring) the extent to which standard terms and conditions associated with remediation services may need to be modified to retain legal protections and enable effective delivery of the service, but still protect the organisation's reputation.

LESSON: 9 SEPTEMBER 2017

Regularly test and update your response plan – Testing your organisation's response plan in advance of an attack and running or 'gaming' breach scenarios and responses will ensure everyone is prepared and understands their roles. Your response plan might be 'red teamed', that is tested as if in response to a real breach, without telling employees. This experience will allow your organisation to evaluate points of weakness, and rectify these to avoid unnecessary criticism when an actual breach occurs.

LESSON: 15-26 SEPTEMBER 2017

Responsibility for cyber risk management ultimately lies with the Board and executive – The Board and members of the C-suite will ultimately be held responsible for the breach (even if the breach was the fault of employees or third party contractors). The Board must ensure its members and management have the necessary resources, expertise and preparation, having regard to the organisation's risk profile, ensuring they are ready to effectively respond to the inevitability of a cyber incident occurring.

Australia's Notifiable Data Breaches scheme

Overview

On 22 February 2018 the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) will commence. It will insert a new Part IIIC into the Privacy Act which will require 'eligible data breaches' to be notified to the Office of the Australian Information Commissioner (OAIC) and affected individuals.

It will create new obligations in addition to the rules in the Privacy Act which are set out in the Australian Privacy Principles (APPs), the obligations in Part IIIA in relation to credit reporting, and the tax file number (TFN) provisions.

One of the core rationales for mandatory data breach notification is that if serious harm to an individual is likely to occur due to a data breach involving their personal information, receiving notification of the breach can allow them to take action to protect themselves from that harm. For example, after receiving notification that their personal information may have been compromised in a data breach, an affected individual might change their online passwords, cancel their credit card or monitor their bank accounts. An anticipated subsidiary benefit of increased transparency from the NDB scheme will be increased trust in organisations and public confidence in digital commerce.

Australia's Notifiable Data Breaches scheme continued

Does the NDB scheme apply to my organisation?

Subject to some narrow exceptions, the NDB scheme applies to all entities already covered by the Privacy Act.

More specifically, it applies to those entities which the Act requires to take steps to secure various categories of personal information (i.e. APP entities, credit reporting bodies, credit providers and TFN recipients). Entities that have Privacy Act obligations in relation to particular types of personal information (such as small businesses required to secure TFN information) must provide notifications of eligible data breaches in relation to those types of personal information only. Data breaches affecting information types that fall outside the scope of their obligations under the Act (such as employee records) do not need to be notified.

However, even if not strictly required by the Privacy Act, entities should still consider whether to voluntarily provide notifications of data breaches, if they conclude it would support compliance with their ongoing data security obligations under the APPs, Part IIIA or the TFN rules.

What is an eligible data breach?

An eligible data breach occurs to an entity when personal information they hold is subject to:

- **unauthorised access or disclosure** (or, where the information is lost, unauthorised access or disclosure is likely to occur); and
- a **reasonable person** (in the entity's position) would conclude that the access or disclosure would be **likely to result in serious harm** to any of the individuals to which the information relates, unless an **exception** applies.

If an entity suspects it may have experienced an eligible data breach, the NDB scheme imposes a positive obligation on that entity to conduct a reasonable and expeditious investigation to determine whether there are actual grounds to believe a data breach has occurred. The organisation must take all reasonable steps to complete this investigation within 30 days of first identifying the suspected breach.

Once an entity determines there are reasonable grounds to **believe** there has been an eligible data breach (whether as a result of the investigation or otherwise), it must promptly notify the Information Commissioner at the OAIC, as well as any individuals at risk of serious harm from the breach. 'Serious harm' is not defined, and may include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.

These obligations are summarised on the following page.

STEP ONE
ASSESSMENT

OBLIGATION

Positive duty to conduct a reasonable and expeditious assessment if an eligible data breach is **suspected**

Determine (based on this assessment) if there are reasonable grounds to **believe** that there has been an eligible data breach

TIMING

Take all reasonable steps to conduct and complete the assessment (where an eligible data breach is suspected) within 30 days

STEP TWO
NOTIFY OAIC

OBLIGATION

Prepare statement about breach and provide to Information Commissioner

TIMING

As soon as practicable after becoming aware that there are reasonable grounds to **believe** that there is an eligible data breach

STEP THREE
NOTIFY INDIVIDUALS

OBLIGATION

If practical, take reasonable steps to notify the contents of the statement to individuals:

- to whom the relevant information relates; or
- who are at risk from the eligible data breach.

Where notifying particular individuals is not practical, publish the statement and take reasonable steps to publicise the contents of the statement

TIMING

As soon as practicable after the statement to the Information Commissioner (in step 2) is prepared

Where possible, an entity should take remedial action to reduce potential harm to individuals. If the remedial action is successful and means that serious harm is no longer likely to occur, then notification may not be required. Other exceptions to notification include where law enforcement bodies form the view that their activities are likely to be prejudiced, or the Information Commissioner makes a declaration to that effect (either on its own motion or on the application of the entity). Notification can also be postponed by the Information Commissioner in certain circumstances.

Further, where a data breach affects personal information held by more than one entity, and one of the entities has complied with the relevant requirements of the NDB scheme, this will be an exception that the other entities can rely on not to conduct an assessment and/or not to notify. For example, where the access, disclosure or loss that constituted the eligible data breach of one entity is an eligible data breach of one or more other entities:

- if one entity has made an assessment as to whether there has been an eligible data breach, the other entities are not required to undertake the same assessment;
- if one entity has notified the Information Commissioner and affected individuals (as required by the NDB scheme), the other entities are not required to provide the same notifications.

This exception will be relevant where, for example, a cloud storage provider suffers a data breach, affecting the data of its clients. Both the cloud storage provider and the affected clients will have notification obligations under the NDB scheme. Ideally, the contract between them should clarify who will have principal carriage and control of the data breach notification process.

However, it is important to bear in mind that if no assessment or notification has been made, all entities affected by the eligible data breach will be in breach of the NDB scheme.

Organisations can prepare for the NDB scheme by knowing what data they hold and developing a data breach response plan

What are the consequences of failing to notify?

The OAIC bears primary responsibility for enforcing the NDB scheme. In the event of an organisation's failure to notify an eligible data breach in accordance with the scheme, the Information Commissioner has wide ranging powers to:

- conduct an investigation
- make a determination on a privacy complaint, including in relation to the payment of compensation
- seek an enforceable undertaking
- in the case of a serious or repeated interference with the privacy of an individual, seek a civil penalty order from the Federal Court of up to $420,000 for an individual and $2.1 million for a company.

To date, in its approach to enforcement, the OAIC has shown a preference for seeking enforceable undertakings and making determinations (including awarding compensation at the lower end of the scale). Regulatory guidance issued by the OAIC in relation to the NDB scheme suggests the OAIC will continue this approach for at least the first 12 months following the commencement of the NDB scheme, as the OAIC has stated that its focus during this period will be on education and the facilitation of compliance.

How should your organisation prepare for NDB?

Step 1: Understand and document the information your organisation holds and its information flows, including:

- the kinds of information held (including by overseas recipients)
- the types of individuals whose information is held
- how and where the information is stored
- how the information is secured (at rest and in transit)
- who can access the information
- how the information is destroyed.

Step 2: Develop a data breach response plan and related policies, procedures and practices. This means your organisation should:

- identify your data breach response team and their respective roles and responsibilities
- develop (or update) your data breach response plan, which should set out:
  - how data breaches will be reported internally, escalated, contained and remediated. This includes other services or providers that may be required to support the data breach response and notification process, such as insurers, external PR, forensic IT and legal.
  - the organisation's obligations to notify relevant regulators (including the OAIC and overseas regulators, where applicable), affected individuals, and third parties (such as law enforcement bodies or pursuant to any contractual obligations the organisation may have)
  - a process for capturing 'lessons learnt'
- develop notification and other communication templates
- consider establishing specific alternate contact method ready to go (such as a subdomain for your website or a 1800 number).

As at the date of this report, the OAIC had advised it is updating its *Data breach notification — A guide to handling personal information security breaches* and *Guide to developing a data breach response plan* resources to develop a comprehensive guide to data breach management responsibilities and best practice. Organisations should consult this guide once it becomes available. In the interim, they may wish to adopt a checklist (similar to the one set out on the next page) in conjunction with the NDB flowchart released by the OAIC.

What should you be doing to protect personal information?

Take reasonable steps to protect personal information from:

- misuse, interference and loss; and
- unauthorised access, modification or disclosure.

When does a data breach occur?

A data breach occurs if any personal information is subjected to unauthorised access or disclosure or loss likely to result in unauthorised access or disclosure.

An example checklist

PHASE 1
Report
What should an employee or contractor do?

- Report an actual or suspected data breach to the Privacy Officer as soon as possible
- Keep any actual or suspected data breach confidential
- Preserve and/or record evidence of the suspected or actual data breach

PHASE 2
Investigate, Contain, Escalate
What should the Privacy Officer do?

- Review the data breach report and undertake a preliminary investigation
- Assess options for containing and/or remediating the data breach and undertake any urgent actions
- Assess whether the incident is a data breach
- Convene a meeting of the Data Breach Response Team (if there is a data breach)

PHASE 3
Assess
What should the Data Breach Response Team do?

- Assess the nature and extent of the breach and risk of serious harm to affected individuals
- Ensure all appropriate containment and remediation actions are taken
- Record the investigations and evidence obtained to date
- Engage with internal stakeholders and external suppliers as necessary

PHASE 4
Notification
Where there is a real risk of serious harm

- Notification to the OAIC and affected individuals is mandatory
- Notification should be made as soon as practicable after becoming aware of reasonable grounds to suspect an eligible data breach
- The Data Breach Response Team must assess how affected individuals should be notified
- Where possible, affected individuals should be contacted directly
- Consider whether you are contractually or legally required to notify any other persons (i.e. insurer, contractors)
- Consider whether other entities could provide assistance (i.e. law enforcement, cybercrime, external legal or insurer)

PHASE 5
Review
What should you do to prevent future data breaches?

- Complete any further investigations into the cause of the breach
- Consider whether your privacy procedures, practices and/or systems can be improved
- Consider whether your response to data breaches can be improved
- Report to the Privacy Officer

Step 3: Other actions that should be taken include:

- Board adoption of cyber security policies, procedures and controls (taking into account the organisation's regulatory obligations including compliance with privacy and data protection legislation and, if it is a listed company, continuous disclosure obligations);
- appointment of a Board member with cyber security expertise (or alternatively, appointment of an independent expert who can present to the Board on cyber security issues);
- reviewing annual budgets for IT security and data protection expenditure;
- conducting due diligence on the cyber resilience of key suppliers and customers;
- reviewing and updating contracts with key suppliers that handle or hold data or information on your organisation's behalf, ensuring that appropriate contractual obligations are imposed on those suppliers, including in relation to:
  - data protection, storage, backup and recovery requirements and standards
  - compliance with applicable privacy and data protection laws (including laws to which the organisation is subject but that may not apply to the supplier)
  - audit rights in relation to security and data protection
  - ensuring the organisation maintains ownership of its data and data is returned or destroyed when the services end
  - ensuring the organisation maintains control of the mandatory data breach notification process
  - placing restrictions on the supplier's ability to transfer data outside of Australia
  - appropriate allocation of risk in the event of a cyber incident
  - restricting the supplier's ability to subcontract key aspects of its services (particularly to overseas providers)
  - the imposition of disaster recovery and business continuity requirements
- reviewing insurance cover and considering if cyber insurance is required (or, if already in place, that it is sufficient);
- training the Board, executive and all staff on privacy and data security obligations and the identification, reporting and escalation process for data breaches. Regular refresher training should also be conducted with the aim of developing a culture of cyber awareness within the organisation;
- implementing and regularly testing and updating the organisation's business continuity, disaster recovery and data breach response plans.

Additional resources

The OAIC has published a number of resources to help organisations comply with their obligations under the NDB scheme. These are available on the OAIC's website.

International developments

Data moves beyond and does not recognise borders. As Australian businesses seek to participate in the global digital economy, the long arm of overseas regulation has become an increasingly important consideration. If Australian organisations conduct business in one or more overseas jurisdictions, outsource functions to overseas service providers (including cloud service providers) or themselves supply services to overseas clients, they need to understand the extent to which overseas privacy and data protection laws may apply to the personal information they process.

This includes data security regulations as well as mandatory data breach notification requirements imposed in their contracts or that have extraterritorial application. The threshold for notifiable data breaches will not necessarily be the same as the 'likelihood of serious harm test' under Australia's NDB scheme.

The incoming EU GDPR will have a global impact and apply to any organisation, whether 'data controller' or 'data processor'

APEC's Cross Border Privacy Rules System

Australia is working towards participating in APEC's Cross Border Privacy Rules System (**CBPRS**) this year. The CBPRS is a regional, multilateral, cross-border data transfer mechanism with an enforceable privacy code of conduct, comprising a baseline set of common principles and standards. Its objective is to enable effective information privacy protection and the free flow of information. The CBPRS includes rules for preventing harm to individuals through obligations such as reasonable security safeguards. This requires organisations to take measures to detect, prevent, and respond to data breaches as well as regularly test these measures.

The European Union's GDPR

The EU General Data Protection Regulation (2016/679) (GDPR) will take effect from 25 May 2018. It will replace the Data Protection Directive (95/46/EC) and will have immediate, direct effect on all EU Member States. Its commencement signifies a landmark year for privacy and data protection because, importantly for Australian businesses, its impact will be global. Its stringent data security and privacy protection standards will have extraterritorial effect.

More specifically, the GDPR will apply to any organisation, whether a 'data controller' or a 'data processor', that:

- has an establishment in the EU; or
- processes the personal data of data subjects, where the processing activities relates to:
  - the offering of goods and services (whether for a charge or not) to individuals who are in the EU (this will also extend to the EEA countries of Norway, Lichtenstein and Iceland once they adopt the GDPR); or
  - monitoring the behaviour of individuals in the EU in relation to behaviour that takes place in the EU.

Understanding the scope of GDPR

There are no small business or employee records exemptions under the GDPR.

'Personal data' is defined in a similarly broad way to 'personal information' in the Australian Privacy Act. The definition of 'processing' is also broad, and means any act or practice done to or in connection with the handling of personal data during the data's lifecycle (whether automated or not). This includes collection, recording, retrieval, use, and disclosure by transmission.

The effect of the GDPR is significant for Australian businesses, because its application will extend to organisations that carry out any act or practice that involves or affects personal data of relevant EU individuals. Australian businesses will therefore need to understand whether they are a 'data controller' or 'data processor' of that personal data (and any corresponding obligations).

While the GDPR does not have retrospective effect, to the extent that any personal data collected prior to the commencement of the GDPR is further processed in relation to an Australian business's offering of goods or services to EU individuals, this processing would be subject to the GDPR.

GDPR data security and breach notification

The GDPR requires data controllers and processors, having regard to the risks to EU individuals, to implement appropriate technical and organisational security measures to secure their personal data. Article 33 of the GDPR also imposes strict mandatory data breach notification obligations.

For the purposes of complying with these obligations, the GDPR defines 'personal data breach' broadly, as any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any personal data.

This largely reflects the data security

obligations that apply under Australian Privacy Principle 11.1. Australian businesses that are subject to the GDPR will need to take steps to ensure that their data breach response plan aligns with the additional requirements under the GDPR. This will also depend on whether they are data controllers or processors of personal data.

Data controllers will be required to report data breaches that affect the personal data of the EU individuals to the relevant EU Data Protection Authority (**DPA**) without delay, and if feasible, within 72 hours of becoming aware of the breach. Otherwise, they must be able to explain any delay in notifying. The more serious the breach, the swifter the response that will be expected. To support compliance with this obligation, data processors must, without undue delay, notify data controllers of any data breach of which they become aware. Like the NDB scheme, the GDPR scheme also prescribes the contents of the breach notification.

The threshold for reporting data breaches to DPAs is lower than the threshold for reporting data breaches to the Australian Information Commissioner under the NDB scheme. Only those data breaches that are "unlikely to result in a risk" to a person's rights and freedoms are exempt from the notification requirement. These rights and freedoms have broad compass, and include any limitation of rights. They include the types of harm recognised in the NDB scheme's 'serious harm' test – encompassing physical, material or non-material harm such as significant economic or social disadvantage, discrimination, damage to reputation, loss of control over personal data, identity theft and fraud.

Conversely, the threshold for communicating data breaches to affected EU individuals is higher. Similar to the NDB scheme, only data breaches that are likely to result in a **high risk** to the rights and freedoms of the individual must be notified without undue delay. The stated objective of communicating the breach to the individuals is the same as in the NDB scheme – to allow them to take precautions and mitigate the effect of the data breach. The communication must include prescribed content, and there are similar exceptions to notifying affected individuals as under the NDB scheme.

These include:

- remediation – where measures have been taken by the data controller so high risk to individuals is no longer likely;
- technology protections – the data controller has implemented appropriate technical protections, such as encryption, which were applied to the personal data to render it unintelligible to anyone who is not authorised to access it; or
- disproportionality – communicating with the individuals would involve disproportionate efforts (in which case some other form of effective communication is required).

Data controllers are also required to document each incident "comprising the facts relating to the personal data breach, its effects and the remedial action taken".

The nuances of these provisions are still being worked out, but failure to comply with the GDPR's notification requirements may result in regulatory action, enforcement activity and very large fines (depending on the obligation infringed, of up to EUR 20 million or 4% of global annual turnover).

Canada's mandatory data breach notification scheme

In June 2015, Canada amended its Federal Personal Information Protection and Electronic Documents Act to require organisations to report any "breaches of security safeguards" involving personal information where it is reasonable to believe the breach creates a real risk of significant harm to an individual. While these amendments have passed Parliament, they will not come into force until appropriate regulations are finalised. This is expected to happen later this year.

In the meantime, Alberta, which introduced a mandatory data breach notification regime in May 2010, is the only province in Canada to have such a regime. Similar to Australia's NDB scheme, organisations subject to Alberta's Personal Information Protection Act must notify Alberta's Privacy Commissioner if there is a "real risk of significant harm" to an individual as a result of the loss of, or unauthorised access to or disclosure of, their personal information.

Other existing or proposed overseas mandatory data breach notification schemes

United States

With the exception of Alabama, New Mexico and South Dakota, all US States have mandatory data breach notification regimes, each with differing thresholds for when notification must take place. Failure to report a data breach could also result in an investigation by the US Federal Trade Commission (**FTC**), which has broad authority to take action against organisations who engage in deceptive or unfair practices. The FTC may take enforcement action and issue fines against such organisations. US State attorneys may also initiate their own investigations into data breaches.

South Africa and South Korea

Both South Africa and South Korea have mandatory data breach notification regimes in their laws, although the regime in South Africa has not yet commenced. In comparison to the NDB scheme, the notification thresholds under these regimes are lower:

- in South Africa, a requirement to notify the Information Regulator is triggered when there are "reasonable grounds to believe" that the personal information of a data subject has been accessed or acquired by any unauthorised person (subject to certain exceptions);
- in South Korea there are two notification regimes with different thresholds. The Personal Information Protection Act (PIPA) requires reporting if the data breach meets the threshold determined by the Enforcement Decree of the PIPA. Currently, this is when the number of affected data subjects exceeds 10,000 individuals. However, under the Promotion of Information and Communications Network Utilization and Data Protection Act, if any loss, theft or leakage of personal data occurs, the IT service provider must notify the affected user immediately. They must also notify the Korea Communications Commission within 24 hours of the details and circumstances, and the remedial steps planned. In June 2017, South Korea's largest cryptocurrency exchange, Bithumb, reported that the personal data of more than 30,000 customers had been stolen after an employee's computer was hacked. The data was reportedly used to deceive customers into allowing the hackers to withdraw funds from their accounts. The data breach was reported the day after it was discovered.

New Zealand

New Zealand has indicated its intention to introduce a mandatory data breach notification regime, but at this stage, data breach notification remains voluntary. The former New Zealand Government announced reforms to overhaul the nation's Privacy Act, following a Law Commission report that recommended, among other items, introducing mandatory reporting in the event of serious data breaches. However, despite ongoing pressure from the New Zealand Privacy Commissioner, these reforms have yet to be addressed.

Looking ahead

Over the past 10 years we have seen an increased awareness of the importance of data in business, whether for price discrimination, to identify opportunities for revenue growth or cost reduction, drive innovation, or even repackage and sell.

The Productivity Commission recognised the importance of data in its 2017 report on *Data Availability and Use*, observing that "data is a strategic asset with great potential and should be treated and managed as such", but that challenges exist in balancing the tension between access to data by government and private sector for the benefit of society, and individual privacy.[1]

One of the key aspects of balancing these tensions is the creation of robust institutional and governance arrangements regarding data use, to build public trust and social licence for Australian government and business.[2] The Productivity Commission called for legislation and a regulatory regime surrounding the use, sharing and release of data. However, the NDB scheme is just one step towards building the necessary public trust and social licence.

Data's central place in commerce and society is readily apparent from the increase in data collection from consumers by means that are passive or invisible. In the near future, we will continue to see these models evolve, with the rapid adoption of Internet of Things (IOT) devices providing further opportunities for organisations to passively collect consumers' data. At the same time, where this information is of potential value to criminals, the increased adoption of IoT may encourage more attempts to breach service providers' systems to obtain data. To this extent, the NDB scheme will be even more important over the coming years.

Against this backdrop, the introduction of data breach regimes in Australia and elsewhere will continue to place increased pressure on businesses which may also face rising costs and expenses.

This not only flows from the cost of notification itself, but also because of the preparation necessary to operate under, and comply with, these new regulatory regimes. This includes staff training, insurances costs, and expenditure on IT, legal and other resources and services. Our survey indicates that while most Australian organisations are well aware of cyber risk and the need to address it, much remains to be done in increasing their cyber resilience and their ability to effectively manage cyber risk.

Looking ahead continued

The full effect of mandatory data breach notification, in a world where social media means news of a data breach quickly spreads, is yet to be seen. Given only 114 breaches were voluntarily reported to OAIC in the 2017 financial year, [3] we would expect the number of breaches reported by Australian organisations to significantly increase, perhaps by an order of magnitude.

An increase in representative complaints and class actions triggered by the harm caused by a notified data breach is also likely, and is a trend we have seen most recently in the US. This will most likely affect organisations who are shown to have been deficient in managing their cyber risk, including failing to implement effective and tested cyber risk management strategies, protocols and procedures.

On the positive side, increased efforts in data breach prevention, containment and remediation, as well as swift notification, should help mitigate and redress harm, maintain trust and strengthen customer relations. In some cases, if handled properly, it may enhance an organisation's reputation. This was the case with the Australian Red Cross, whose proactive and skilled handling of a data breach affecting donor records in 2016 was widely praised. When notified of a data breach, customers can be understanding and supportive of an organisation. That is, if the communication and breach response is handled correctly, is personalised and done from their perspective, and the breach was not the result of the organisation's non-compliance or poor data security practices.

The GDPR is likely to become the new global benchmark in data protection, including data security and breach response. The changing regulatory landscape and approach of regulators in response to data security and breaches and the challenges of addressing cyber risk suggest a common, best practice approach that incorporates accountability and transparency, principles that already exist in Australia's national privacy framework.

Ultimately, the implementation of a best practice approach to cyber risk and cyber security can only be achieved through leadership at the Board and executive levels, including recognition that valuing data, and its protection, is now a critical imperative for every Australian organisation.

Endnotes

1. Productivity Commission, 'Data Availability and Use: Overview & Recommendations', (Report no. 82, 31 March 2017)
2. Above no 1.
3. Office of the Australian Information Commissioner, 'Annual Report 201-17' (Annual Report, 19 September 2017), page 20.

MinterEllison's cyber security team can help you address and mitigate cyber risk

Conduct independent cyber risk reviews and Board-level cyber risk assessments.

Review third-party supplier contracts
to ensure that they appropriately address privacy and data protection issues, and do not inappropriately transfer cyber-related risks to your organisation.

Develop, review and update data breach response plans
as well as related policies and procedures, such as privacy and document retention policies.

Advise on privacy, data protection and cyber-related legal and commercial issues.

Develop and deliver cyber risk and privacy compliance tools
through face-to-face and online training (including via our award winning Safetrac online compliance system).
You can try our customisable sample cyber security course online.

Conduct privacy audits and impact assessments
including in relation to cloud-based products and services.

Plan for, respond to and rebuild from, a data breach or cyber incident
including breach coach services (where MinterEllison leads the data breach response process).

Advise on cyber insurance issues
including assisting with cyber risk advice coverage issues, and strategic management of notifications and claims arising from cyber risk losses.

Contacts

Paul Kallenbach
Partner
T +61 3 8608 2622
M +61 412 277 134

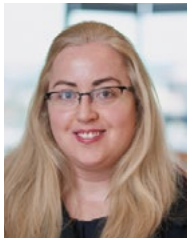
Anthony Lloyd
Partner
T +61 2 9921 8648
M +61 411 275 811

Anthony Borgese
Partner
T +61 2 9921 4250
M +61 400 552 665

Amanda Story
Partner
T + 61 2 6225 3756
M +61 423 439 659

Cameron Oxley
Partner
T +61 3 8608 2605
M +61 417 103 287

Veronica Scott
Special Counsel
T +61 3 8608 2126
M +61 411 206 248



Leah Mooney
Special Counsel
T +61 7 3119 6230
M +61 421 587 950

John Fairbairn
Partner
T +61 2 9921 4590
M +61 410 475 965

Glossary

cyber attack A deliberate act that seriously compromises national security, stability or prosperity by manipulating, denying access to, degrading or destroying information systems or the information resident on them.

cyber incident An occurrence that actually or potentially results in adverse effects on information systems or the information resident on them.

cyber security The safeguards and actions that can be used to protect against cyber incidents.

cyber risk Operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information systems or the information resident on them.

cyber resilience An organisation's ability to prepare for, respond to and recover from a cyber incident (including its ability to operate during, and adapt to and recover from, a cyber incident).

data breach A situation where information (usually including personal information) is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference, often as a result of a cyber incident.