PERSPECTIVES ON CYBER RISK 2019

MinterEllison

Contents

Members of our data protection and privacy team who have contributed to the preparation of this report:

Lisa Jarrett, Partner; **Paul Kallenbach**, Partner; **Leah Mooney**, Special Counsel; **Veronica Scott**, Special Counsel; **Belinda Alcock**, Senior Associate; **Ashleigh Fahrenbach**, Senior Associate; **Margaret Gigliotti**, Senior Associate; **Katherine Giles**, Senior Associate; **Susan Kantor**, Senior Associate; **Luci Guyot**, Associate.

Methodology

MinterEllison's fourth annual cyber security survey was completed by more than 110 legal counsel, Chief Information Officers, Chief Operating Officers, Board members, IT specialists and risk managers of ASX 200 and private companies, government agencies and not-for-profit organisations. In contrast to previous years we issued the same survey to all participants.

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

The survey was conducted during November 2018. 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%.

Executive summary

Against the evolving landscape of Australia's privacy and data protection regime, we conducted our fourth annual cyber security survey to assess how Australian organisations are responding to cyber risk. More than 110 senior executives across legal, technology, finance and procurement participated in the survey.

2018 was a watershed year in Australia's regulatory journey. New privacy and data protection laws came into force, bringing Australia closer in line with emerging international standards. As a result, Australian and overseas privacy and data protection regulation has become more stringent, and the penalties more severe.

Numerous recent and high profile examples, both in Australia and overseas, demonstrate that those organisations not designating cyber security as a top priority are exposing their business, customers and reputation to a clear, present and escalating danger.

With this in mind, our latest survey results suggest that more should be done to address this danger. Respondents indicated that they are aware of the cyber threat, and year on year we have seen a significant increase in organisations' acknowledgement and understanding of the risk. However, this has not always translated into appropriate and considered action.

With many organisations now exploring the potential of artificial intelligence, big data and the Internet of Things, the security of data as a right and an asset, as well as a liability and a cost, has taken on an increased significance. Regular, day-to-day activities that, in the past, would not have involved digital interaction may now leave both individuals and organisations exposed.

Organisations cannot afford to be complacent about cyber risk. And with the law consistently outmatched by the pace of technological change, it is incumbent on organisations to develop their own cyber risk framework and set of baseline privacy and data protection rules.

The time to act is now.

We invite you to read our report and consider the implications for taking greater action.

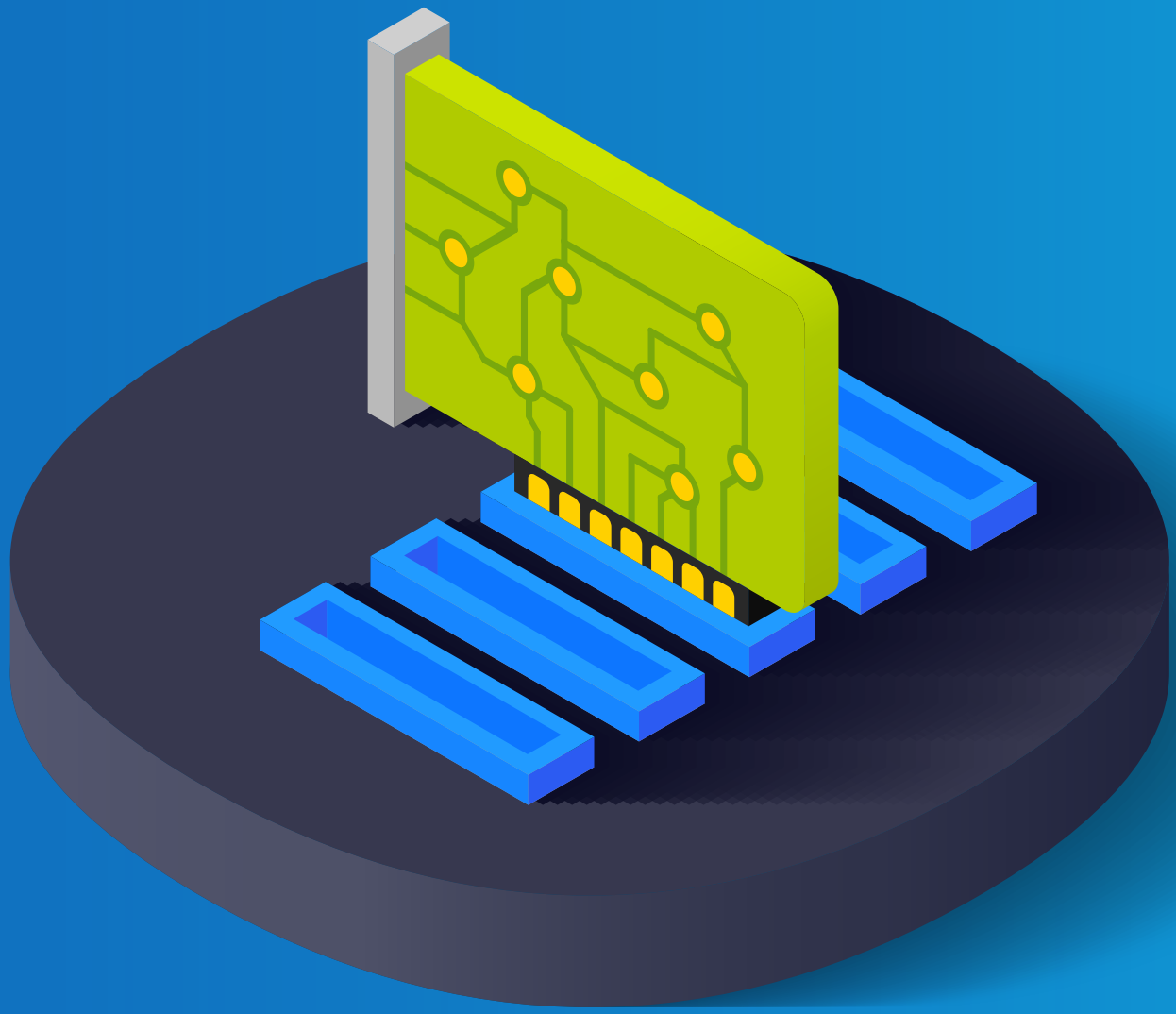
Part one

Our findings in the evolving privacy landscape

In late 2018, we conducted our fourth annual cyber security survey, to assess how Australian organisations are responding to cyber risk in an environment of increasing regulation.

Our survey results indicate a marked increase in awareness and understanding of cyber risk, with more organisations than ever appreciating the importance of adequately addressing an ever growing cyber threat.

However, an increase in understanding is not always translating into the practical steps that organisations must take to effectively mitigate against this threat.



Finding one:
Awareness and understanding of cyber risk continues to increase – for many, it is the 'new normal'

Our survey results suggest greater acceptance of cyber risk as an enterprise-wide issue, rather than just an IT issue. This is a marked change from our first survey in 2015. More than half of respondents told us that cyber risk ranks in the top five risks on their enterprise risk register – a significant increase from our first survey in 2015, when only 29% of respondents gave cyber risk this ranking.

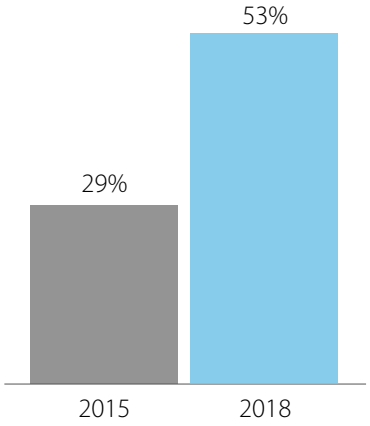
Organisations continue to improve their understanding of cyber risk. In 2017, only 18% of respondents identified themselves as having a 'very good' understanding of their cyber risk exposure, compared with 34% in 2018 – with a corresponding decrease over the last 12 months in respondents who consider they only have a 'fair' or 'poor' understanding of the issue.

This increased understanding has no doubt been assisted in the last 12 months by an increase in public discourse and discussion on cyber risk; an increasing focus on cyber resilience by the Australian Securities and Investments Commission (ASIC), the Office of the Australian Information Commission (OAIC) and other Australian and overseas regulators; as well as organisations' own experience of cyber incidents.

Indeed, more than a third of survey respondents told us that they have suffered at least one cyber attack in the last 12 months which compromised their systems or data.

Many other Australian organisations were indirectly affected by cyber incidents as a result of attacks on their third party service providers and, in particular, their cloud service providers. The PageUp data breach, discussed on page 18, is a recent example of this.

Awareness, however, only goes so far – action must follow to protect organisations against cyber attacks.



Almost twice as many respondents in 2018 view cyber risk as one of the top 5 organisational risks, compared to 2015.

Finding two:
Increased awareness and understanding of cyber risk is not always translating into action

Although the situation has improved, there still remains a disconnect between organisations' understanding of cyber risk and the practical steps being taken to mitigate against it.

A lack of action exposes organisations to significant risk, particularly with the commencement of a more stringent regulatory landscape in both Australia and overseas. Recent high profile incidents demonstrate the damage that a serious cyber breach can cause (discussed further on page 9).

There is some improvement over previous years. In particular, 78% of respondent organisations said that they have a data breach response plan in place, an increase from 54% in 2017. Both ASIC and the OAIC have publicly cited the importance of putting in place a comprehensive and tailored data breach response plan that is regularly reviewed and tested against hypothetical data breach scenarios.

In October last year, ASIC released a series of good practice principles, intended to provide practical guidance on how organisations can address cyber risk. These principles include Board engagement, governance, third party management and asset management, as well as routine and detailed scenario planning and testing.

However, only 45% of survey respondents told us they regularly (at least annually) tested their data breach response plans. Failure to regularly test the plan means that organisations may not know whether their plan is as effective as it ought to be and individuals in the plan may not fully understand what their roles and responsibilities are when it comes time to activate it.

Surveyed organisations appear to be aware of the disconnect between awareness and action. We asked respondents to identify what they could do to further enhance their cyber resilience.

Common themes included frequent staff training, conducting more cyber attack simulations, and regularly reviewing their data breach response plans and processes - all strategies endorsed by ASIC and OAIC.

While adopting and implementing cyber resilience is costly in time and effort, disregarding or discounting the very real threat posed by cyber risk can be much more expensive.

To demonstrate their commitment to privacy and data protection, organisations need to include cyber security as an ongoing cost of doing business, factor it into their operations and resource it appropriately, having regard to the assessed risks.

Finding three:
Despite the hype, many organisations are yet to jump on board with AI and big data

Artificial intelligence (AI) and big data solutions are of growing importance for organisations as they seek competitive advantage in the increasing volume of data collected about their customers and from across the supply chain.

However, our survey indicates that many organisations are yet to jump on board, with only 25% of respondents reporting that they currently use, or intend to implement in the next 12 months, AI or big data solutions.

A thorough understanding of the privacy and security impact of these new technologies will be an increasingly important aspect of understanding an organisation's cyber risk profile.

Of those survey respondents who are using, or who plan to implement, AI or big data solutions, only 32% told us that they have undertaken a privacy impact assessment or security risk assessment of those solutions.

Any such assessment should include evaluation of the cyber resilience of third party providers across the supply chain, given the reliance of these solutions on the use of cloud-based processing, analytics and storage platforms. AI and big data solutions are discussed further in Part 3 Looking ahead.

A thorough understanding of the privacy and security impact of these new technologies will be an increasingly important aspect of understanding an organisation's cyber risk profile.

The high cost of cyber breaches

The last 12 months have seen a number of serious cyber incidents occurring across all industries – from financial services, logistics, government and retail to professional services, hospitality, healthcare and transport. The cyber incidents have affected large and small organisations alike.

The most frequent causes of these global incidents were malicious cyber attacks and human error. The OAIC's quarterly reports on the first 12 months of the Notifiable Data Breach **(NDB)** scheme reflect similar findings.

The data affected by cyber attacks remains varied, ranging from customers' personal information to confidential business data. In many cases, organisations were unaware that a cyber incident had occurred until weeks or months later.

In this section we review a number of high profile cyber incidents during 2018 and reflect on their impact on the affected organisations' business, finances, customers, operations and reputation.

- In March 2018, it was discovered that a personality quiz app had been used to collect the personal information of around 87 million Facebook users. By installing the app, 300,000 users shared both their own Facebook data, as well as the data of their Facebook friends. The app's creator, Aleksandr Kogan, made this data available to UK political consulting firm, Cambridge Analytica, which is alleged to have used the information to focus political advertising and campaign efforts (including in relation to the 2016 US election).

  Although Facebook had sought certifications from Kogan and Cambridge Analytica in 2015 that they had deleted all improperly acquired data, it is alleged that Cambridge Analytica may not have done so. Facebook founder Mark Zuckerberg was subsequently called to appear before US Congress to answer questions about the incident, but subsequently refused a similar invitation to testify before British MPs.

  In July 2018, Facebook was fined £500,000 over the incident by the UK Information Commissioner's Office (ICO) – the maximum penalty then available at law. Facebook is also currently facing various lawsuits arising from the incident, including a suit instigated by the District of Columbia, and a class action. The ICO's Reports and Findings provide insights into Commissioner Denham's views of the conduct of all those involved.

- In March 2018, US based athletic clothing manufacturer Under Armour alerted customers to a security breach involving its fitness app, MyFitnessPal. The incident, thought to have occurred a month previously, involved an unauthorised party accessing usernames, email addresses and passwords, affecting around 150 million individuals.

- In May 2018, Australian online human resources company PageUp discovered suspicious activity on its platform, including malware that appeared to facilitate the unauthorised exfiltration of client data. The incident illustrates the challenges arising from organisations' increasing reliance on cloud service providers, and was an early test of Australia's notifiable data breach laws. A more detailed case study of this incident and its impact on Australian organisations is discussed further on page 18.

The high cost of cyber breaches continued

- Phishing, 'SMiShing' (SMS phishing) and payment redirection attacks were widespread in 2018 (and, according to Microsoft, have increased by 250% from the previous year). One example involved e-conveyancing platform PEXA causing property settlement funds to be diverted into a fraudulent bank account. This was achieved by the cyber attacker compromising the conveyancer's account, and substituting the recipient's bank details, in order to redirect funds to the attacker's bank account. PEXA has since implemented a number of security measures to mitigate against such attacks.
- Facebook's data practices were again under scrutiny in September 2018, when it was reported that a vulnerability in Facebook's 'View As' feature may have exposed the accounts of approximately 50 million users. Facebook's Chief Operating Officer, Sheryl Sandberg, was called to appear before US Congress to explain the incident.
- Between August and September 2018, British Airways' website and mobile app were targeted by hackers. Financial and personal information of approximately 380,000 individuals was stolen after card payments made on the airline's website and app were compromised.
- Another airline, Cathay Pacific, suffered a data breach in October 2018. The airline discovered unauthorised access to a system holding information of up to 9.4 million passengers. The airline confirmed that personal information and identifiers, such as passport, identity card numbers, address, contact details and dates of birth, had been accessed, as well as the details of 430 credit cards.

250%

INCREASE IN PHISHING, SMISHING AND PAYMENT REDIRECTION ATTACKS SINCE 2017

- Also in October 2018, Google revealed that a security vulnerability in its Google+ platform, detected in March 2018, had exposed the personal information of up to 500,000 users. It was reported that a 'coding glitch' meant that information that was designated private by users had been accessible to external applications. The vulnerability was thought to have existed since 2015. A second, similar security issue was identified in December 2018.
- In November 2018, the international Marriott Hotel chain reported that it had experienced a data breach that may have exposed the details of up to 500 million guests. Personal information affected included passport details and payment information.

Part

two

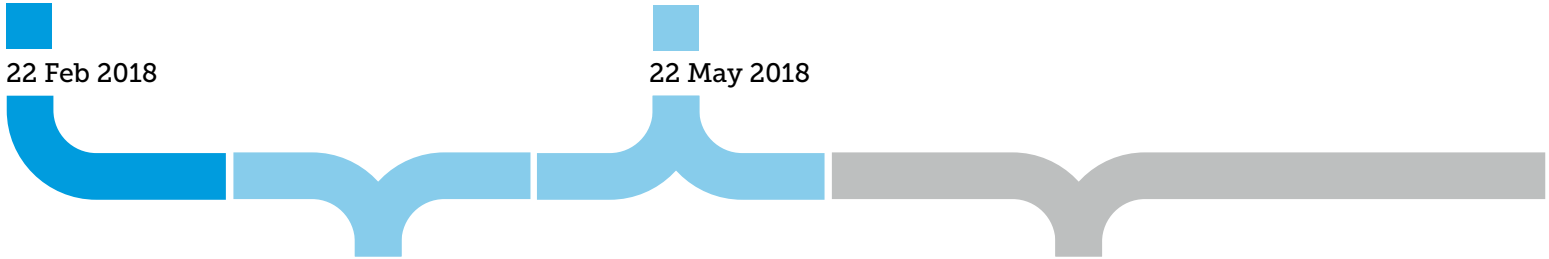
Regulation upped the ante in 2018

Last year saw some of the most significant regulatory developments in Australian and overseas privacy and data protection regimes in many years.

The evolving Australian and international privacy and data protection landscape

Australia's NDB regime commenced requiring organisations subject to the Australian Privacy Act 1988 (Cth) **(Privacy Act)** to notify the OAIC and affected individuals when an 'eligible data breach' happens to them. The NDB scheme is further discussed on page 14.

The European Union's General Data Protection Regulation **(GDPR)** commenced. Its extraterritorial reach means that many Australian organisations may need to comply with requirements under both Australian and EU privacy laws. In addition, many Australian organisations that would not otherwise fall within the GDPR are being contractually required by their customers to comply with the regime. Although the GDPR is, in many respects, similar to the requirements under the Privacy Act, there are important differences. The GDPR is further discussed on page 20.



22 Feb 2018

May 2018

The Australian Federal Government announced the implementation of a 'consumer data right' **(CDR)**. The CDR is intended to provide Australian consumers with greater control of their data, and will commence initially in the banking sector on 1 July 2019. The Australian Competition and Consumer Commission **(ACCC)** is leading the implementation of the CDR, in conjunction with the OAIC and CSIRO's Data61.

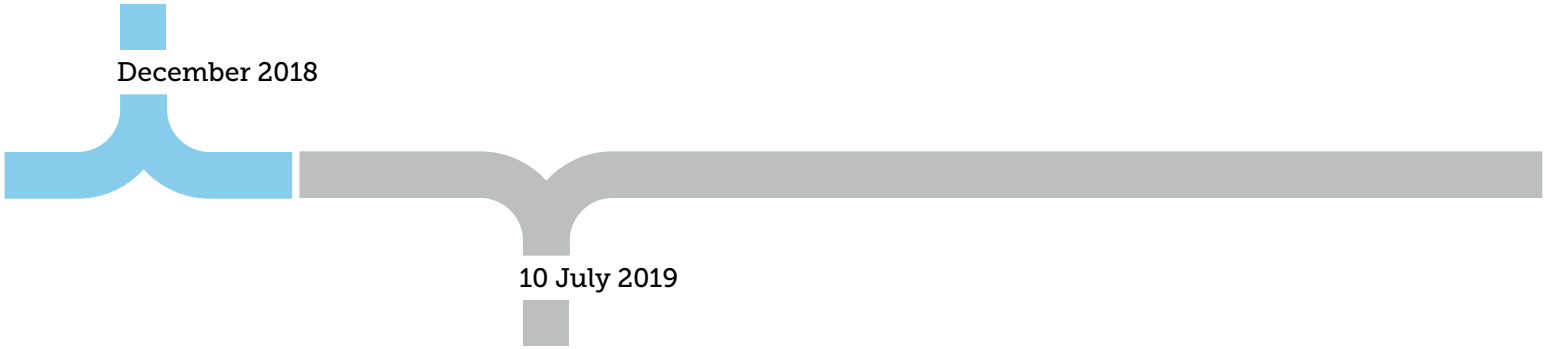
22 May 2018

1 July 2018

The Privacy (Australian Government Agencies - Governance) APP Code 2017 (Government Agencies Code) commenced. It applies to Commonwealth Government agencies subject to the Privacy Act, and specifies which agencies must comply with the privacy by design requirements in Australian Privacy Principle (APP) 1.2.

The evolving Australian and international privacy and data protection landscape continued

The ACCC released its Preliminary Report on the Digital Platforms Inquiry **(Preliminary Report)** which highlights the changing relationship between businesses and the community. Businesses across all sectors now treat data as a valuable proprietary asset. However, according to the ACCC, businesses are not placing enough importance on how they handle consumers' data. In particular, the ACCC highlighted the need for organisations to be more transparent about their data handling practices, and recommended further regulatory reform to mandate this. The ACCC also flagged that it is currently investigating potential breaches of the Australian Consumer Law as a result of representations made to users about the collection and use of their data. This reflects the approach taken by the US Federal Trade Commission for some time now, and the long-anticipated claims for misrepresentations made by organisations in their privacy and public-facing security policies may materialise in Australia in the next 12 months.



A new prudential standard, CPS 234 (Information Security), will take effect requiring banks, insurance companies and other entities regulated by the Australian Prudential Regulation Authority (APRA) to, among other things:

- have robust mechanisms to detect and respond to information security incidents, maintain appropriate plans to respond to information security incidents, and test the effectiveness of those security controls; and
- notify APRA of any material information security incidents as soon as possible (and no later than 72 hours). These requirements are in addition to those imposed by the NDB scheme.

Lessons from the NDB scheme

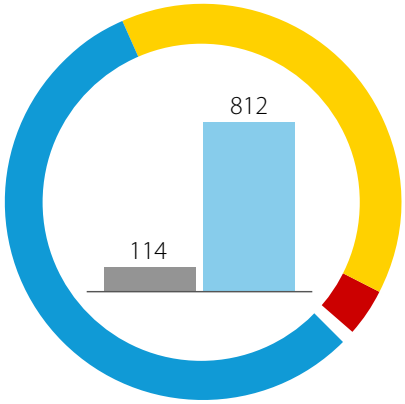
The NDB scheme introduced new obligations requiring organisations to notify the OAIC and affected individuals of certain data security breaches in addition to complying with the rules in the APPs, Part IIIA (credit reporting) and Tax File Number provisions.

It also imposes a positive duty on organisations to assess suspected, 'eligible' data breaches. The key rationale for the scheme is that, if an individual is at risk of serious harm because of a data breach involving their personal information, notification of the data breach can empower that person to take action to protect themselves and reduce or remove the risk of that harm actually occurring. The NDB scheme also helps to improve transparency for consumers and accountability for Australian businesses as well as enable the OAIC to understand and report on the causes of data breaches.

This means Australian organisations must consider how to prepare for a data breach and the steps that they will take if a data breach occurs.

A significant volume and wide variety of data breaches were reported under the NDB scheme in its first 10 months of operation. The previous 12 months of voluntary data breach notification saw only 114 data breaches reported to the OAIC, according to its Annual Report 2017-18. Since the start of the NDB scheme until the end of January 2019, a total of 812 data breaches were reported to the OAIC. Of those, 56.25% were attributable to malicious or criminal attacks (including phishing emails and malware), 39.25% to human error (including unauthorised disclosure of personal information, personal information sent to the wrong recipient, and the insecure disposal of personal information), 4.25% to system faults, and 0.25% to other issues.

Comparison of reported Data breaches



Data breaches in the last 12 months of the voluntary scheme

Data breaches in the first 12 months of the NDB scheme

56% Malicious or criminal attacks

39% Human Error

4% System error

**Total equals 99% due to rounding error*

Lessons from the NDB scheme continued

This increase in data breach reporting to the OAIC may indicate a greater accountability on the part of organisations in responding to data breaches. But it may also indicate that organisations are erring on the side of caution and notifying breaches that may not strictly qualify as 'eligible data breaches' under the NDB scheme.

So far, the sector with the highest number of data breaches notified under the NDB scheme is the health sector, with a total of 163 reported data breaches in 2018. (This figure does not account for data breaches relating to the MyHealth Record system, which is the subject of a separate annual report by the Australian Digital Health Agency at the end of each financial year.)

This statistic should also be considered in context, as health information that is subject to unauthorised access or disclosure is more likely to result in affected individuals suffering serious harm. Furthermore, there is no small business exemption under the Privacy Act for health service providers. This means there are many more smaller health service provider entities subject to the NDB scheme who may be more vulnerable to data breaches.

The financial services sector reported 119 data breaches, the second highest number of breaches in 2018. This is perhaps not surprising, given that financial services organisations are frequently a target of malicious and criminal attacks, due to the valuable (and therefore lucrative) types of personal information they hold. In September 2018, APRA urged the banks to upgrade legacy computer systems that are exposing the banks and their customers to risk.

It has become clear from the first 12 months of the NDB scheme that how an organisation delivers a data breach notification to affected individuals is crucial, as additional harm could be caused by a premature or inaccurate notification.

While the OAIC's role during the first 12 months of the NDB scheme has been, in part, to offer guidance in relation to compliance with the scheme, we expect that, going forward, the OAIC will require organisations to more carefully assess whether actual or suspected data breaches are 'eligible data breaches' before notifying. This is due to the OAIC's stated concern that its (limited) resources be directed to breaches where there is a serious risk of harm to affected individuals.

However, the concept of 'risk of serious harm' and its practical application remain a challenge for organisations that have been affected by a data breach.

We have set out some guidance on this issue on page 16.

How an organisation delivers a data breach notification to affected individuals is crucial, as additional harm may be caused by a premature or inaccurate notification.

Guidance for assessing the likelihood of 'serious harm'

DATA TYPE AND VOLUME
In assessing the likelihood of serious harm, the paramount consideration is the data that has been affected and the individuals to whom it relates. The greater the volume of data, the more varied the classes of data, the more sensitive the data, and the greater number of individuals affected – the greater the likelihood of serious harm.

ACTUAL HARM
If there is evidence that actual harm has already occurred to some impacted individuals (for example, due to credit card fraud) the assessment process is simple – there is generally a likelihood of serious harm to all affected individuals. Organisations should promptly take remedial action (such as placing a watch on compromised credit cards) and notify all impacted individuals and the OAIC

CONTEXT
Context is crucial. Place yourself in the shoes of the affected individuals, and resist taking an organisation-centric approach in determining the likelihood of serious harm. A name and address may not give rise to harm in some contexts but may do so in others (for example, the location details of a person in a witness protection program). It is acceptable (and often advisable) to notify only those individuals who you assess to be at risk of serious harm.

NOTIFICATION IMPACT
Notification itself can cause harm, so take a thoughtful and measured approach to managing the notification process.

GUIDELINES
Familiarise yourself with the OAIC's useful guidance on assessing the risk of serious harm.

It is also clear from the first 12 months of the NDB scheme that:

- many organisations are still unsure about the timeframes that apply for reporting data breaches –the more prescriptive 72 hour timeframe under the GDPR has caused particular confusion; and
- for the increasing number of organisations who rely on third party cloud service providers or other vendors, it is not always clear who should take primary carriage for notifying a data breach to the OAIC and to affected individuals. This confusion was readily apparent in the PageUp data breach (discussed further on page 18).

The rise of data breach class actions

Class actions arising from data breaches have started to emerge.

These include:

- a class action commenced against New South Wales Ambulance, after a former contractor sold the workers compensation files of 130 former and current NSW Ambulance staff to solicitors. The outcome of this action could have a significant impact on breach of confidence and invasion of privacy claims in Australia, with the mooted introduction (at least in New South Wales) of a statutory cause of action for serious invasion of privacy (as was proposed by the Australian Law Reform Commission in its Serious Invasions of Privacy in the Digital Era Report in 2014);
- an expression of interest currently being circulated by an Australian law firm, for individuals who may have been affected by the PageUp data breach; and
- a complaint lodged with the OAIC against Facebook in relation to the Cambridge Analytica matter. This complaint is being pursued by litigation funder IMF Bentham.

These types of class actions follow from the experience in the United States, where Facebook, Equifax and Yahoo are all facing class action claims instigated by shareholders after data breaches resulted in a fall in the share prices of these companies.

The effect of the GDPR (discussed further on page 20), could also mean similar class actions brought in Europe, particularly given that the GDPR enables individuals to seek compensation for non-economic damages, such as embarrassment, distress and inconvenience.

Lessons from the PageUp data breach

The most significant data breach in Australia in the last 12 months, both in terms of impacted organisations and individuals and the effect on the cross-border regulatory landscape, was the PageUp data breach in May 2018.

PageUp Limited, an Australian online human resources services organisation, detected suspicious activity from a malicious threat actor in late May 2018. To comply with the stringent 72 hour timeframe for notifying the ICO under the GDPR, PageUp promptly notified the British regulator and client organisations in both Australia and the United Kingdom. The Australian Cyber Security Centre **(ACSC)** and the OAIC were also subsequently notified.

While PageUp was proactive in its notifications to the regulators and impacted client organisations, its Australian clients affected by the breach (and who had direct relationships with potentially impacted individuals) were faced with the challenge of what to do next. PageUp's forensic investigations into the data breach were incomplete, and it was unclear to its clients whether this was an 'eligible data breach' requiring notification to individuals under the NDB scheme.

The response from PageUp client organisations varied. Some elected to promptly notify affected individuals, despite PageUp's investigations being incomplete. Others awaited developments before notifying individuals in the weeks following PageUp's initial notification. Many others elected to notify after PageUp indicated that it intended to notify individuals directly.

While organisations no doubt had the best of intentions, their actions were inconsistent. The advice to affected individuals varied from organisation to organisation. Many individuals received multiple notifications with varying advice. First responders were criticised for a lack of insight. Those who waited were the subject of complaints due to their delay.

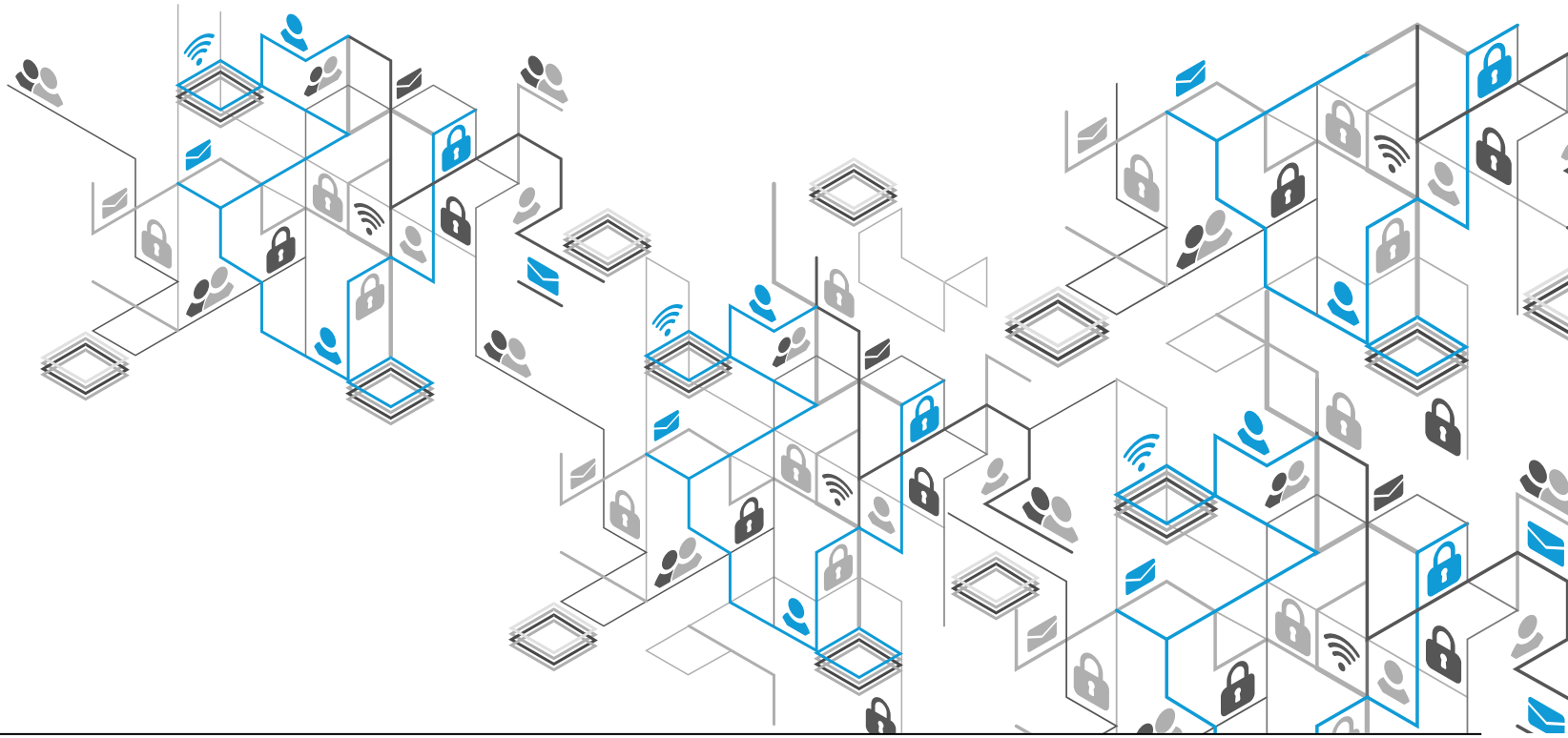
Cohesive guidance on the response finally came in the form of a joint statement between the OAIC, the ACSC and the Australian Government funded IDCARE. It confirmed that the compromised data on PageUp's systems had been accessed, not exfiltrated (ie not removed). The overall risk to affected individuals was assessed to be low.

PageUp subsequently implemented additional layers of security and risk management measures to prevent a repeat incident.

Lessons from the PageUp data breach

Organisations should consider the following lessons from the PageUp experience:

- Conduct a thorough cybersecurity audit of third party providers who will hold the organisation's personal information. Ensure that the contractual arrangements allow for ongoing periodic audits.
- The NDB scheme is designed so that only one organisation needs to notify the OAIC and affected individuals. Breach notification and related obligations under the NDB scheme should be addressed in contracts with third party providers to ensure that the parties' respective roles and obligations are clear in the event of a data breach.
- The NDB scheme only requires the notification of 'eligible data breaches', that is, breaches likely to cause serious harm to impacted individuals. See our guidance for making this assessment on page 16.



Lessons from the GDPR

On 25 May 2018, the GDPR replaced the previous European Union (EU) data protection regime.

Its purpose is to protect fundamental rights and freedoms of individuals in the EU when processing their personal data (wherever that may happen) and to enable the free movement of personal data within the EU. (A more detailed description of the GDPR is set out in our 2018 Report.)

EXTRATERRITORIAL APPLICATION

The GDPR has broad extraterritorial application. This means that Australian organisations of all sizes need to consider whether this new regime applies to them. Australian organisations are subject to the GDPR if they have an establishment in the EU, or, if they do not have an establishment in the EU, to the extent they offer goods and services to individuals in the EU, or monitor the behaviours of individuals, where that takes place within the EU.

In November 2018, the European Data Protection Board released for consultation a set of guidelines which provide further guidance for Australia businesses to assess whether they fall under the GDPR. In particular, the draft guidelines clarify that citizenship, residency or other legal status of an individual is irrelevant in determining the application of the targeting criteria; rather, the GDPR protects any natural person located in the EU irrespective of such factors.

Further, in respect to Article 3(2)(a) of the GDPR, which provides for extraterritorial application for offering goods or services to individuals in the EU, the guidelines confirm that the factors which, in combination, may amount to an organisation 'targeting' data subjects in the EU, include the following:

- Targeted advertising – paying a search engine operator to facilitate access to an organisation's website in an EU Member State;
- References to EU Member States – making explicit references to countries in the EU on the organisation's websites;
- International nature of activities – offering goods or services that are inherently of an 'international' nature (such as tourist activities);
- Language – using the language of an EU Member State, where that language is not relevant to customers in the home country;
- Currency – using the currency of an EU Member State, where that currency is not generally used in the home country;
- Domain name – using a website with the top level domain name of an EU Member State;
- Customer testimonials – using testimonials from a customer in an EU Member State to promote the goods and services;
- Contact information – providing a dedicated address or phone number to be reached from an EU Member State;
- Travel instructions – providing a description of how to travel from an EU Member State to the place where goods/services are provided; and
- Delivery – offering delivery of goods to an EU Member State.

REQUIREMENTS ABOVE AND BEYOND THE PRIVACY ACT

The key concepts that underpin the GDPR are broadly similar to the Privacy Act. However, some GDPR requirements go beyond those in the Privacy Act. Indeed, the OAIC in its Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation has confirmed that organisations impacted by the GDPR will need to implement additional compliance measures.

These include:

Restrictions on data processing – the requirement in Article 6 to have a 'lawful basis' for all data processing activities in relation to the data of EU individuals;

Consent – while consent under the APPs includes implied consent, the GDPR requires a higher standard of 'freely given, specific, informed and unambiguous consent';

Transfer to third parties and third countries – the GDPR limits the circumstances under which personal data can be transferred to a third party and to a third country outside the EU;

Additional rights – EU individuals are granted further rights in respect of their personal data, such as the 'right to be forgotten', the right to object to processing or to withdraw consent, the right to data portability, and the right not to be subjected to automated decision making and profiling;

Collection notices – EU individuals must be provided with a collection notice that includes the information prescribed in Articles 13 and 14 of the GDPR (which exceed the requirements of APPs 1.4 and 5.2);

Record keeping and PIAs – organisations must keep a record of their data processing activities (unless an exception applies) and undertake Data Privacy Impact Assessments in certain circumstances; and

Mandatory data breach notification – there are shorter timeframes for notifying the relevant EU supervisory authority of a suspected data breach (ie, 72 hours) and there is a positive obligation to notify unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. This lower threshold for the data breaches that must be notified is a key difference between the GDPR and the NDB scheme in the Privacy Act.

PENALTIES

The penalties for non-compliance with the GDPR are staggeringly high (up to 4% of worldwide annual revenue for 'data controllers') compared with Australia and other jurisdictions. Fines under the GDPR can also potentially be imposed across borders.

The first application of this was seen in October 2018 when the ICO issued a cross-border enforcement notice against Canadian company AggregateIQ. The company is alleged to have used personal data to target political advertising without notifying individuals of that use, in breach of the principles of transparency, limited purpose and data minimisation.

In addition, the French Data Protection Authority **(CNIL)** began an investigation into Google on the day the GDPR came into effect, in response to concerns that Google did not fully disclose how it collected and processed personal information. The CNIL subsequently found that Google had contravened the GDPR and imposed a fine of €50 million.

Guidance for company directors from Australian regulators

For company directors seeking to comply with their responsibilities in relation to cyber security, ASIC encourages an assessment of their company's cyber security threats and vulnerabilities to understand what, where and how data is held.

This process allows directors to understand the cyber risks their organisation faces, and direct resources to the appropriate management of its cyber resilience. ASIC's Cyber Resilience Good Practices Guide, released in October 2018, provides a useful starting point, together with ASIC's Report 429 Cyber Resilience Health Check, which remains relevant even several years after its publication.

Our survey shows that the overwhelming majority of surveyed organisations have actioned the OAIC's recommendation to develop a data breach response plan as part of their cyber resilience preparedness. While this is a good start, it is not in itself sufficient. Organisations must also regularly test and update their plans and supplement this valuable document with playbooks, checklists and other support resources to facilitate an efficient and effective response to a data breach.

Employee training and awareness remains a key issue. As discussed on page 9, according to the OAIC, human error remains the second largest cause of notifiable data breaches.

While awareness is key, organisations should also prioritise creating a culture of openness, so that employees feel there is a 'safe space' for reporting and escalating actual or suspected data breaches.

Organisations should also conduct regular risk assessments on bring your own devices (BYOD), remote access and the use of cloud-based services, to ensure that risks are appropriately identified and managed. This is particularly important for employee mobile phone use, given the growth in malicious phone porting and 'SMiShing' over the past 12 months.

Finally, while cyber security, privacy risk management and compliance clearly remain a challenge for many organisations, there is ample opportunity for organisations to differentiate their offerings through prioritising privacy and security. Apple has been an early adopter of privacy as a marketing tool, most recently illustrated by use of prominent banner advertising at CES 2019 (the world's largest innovation convention) to promote its focus on privacy.

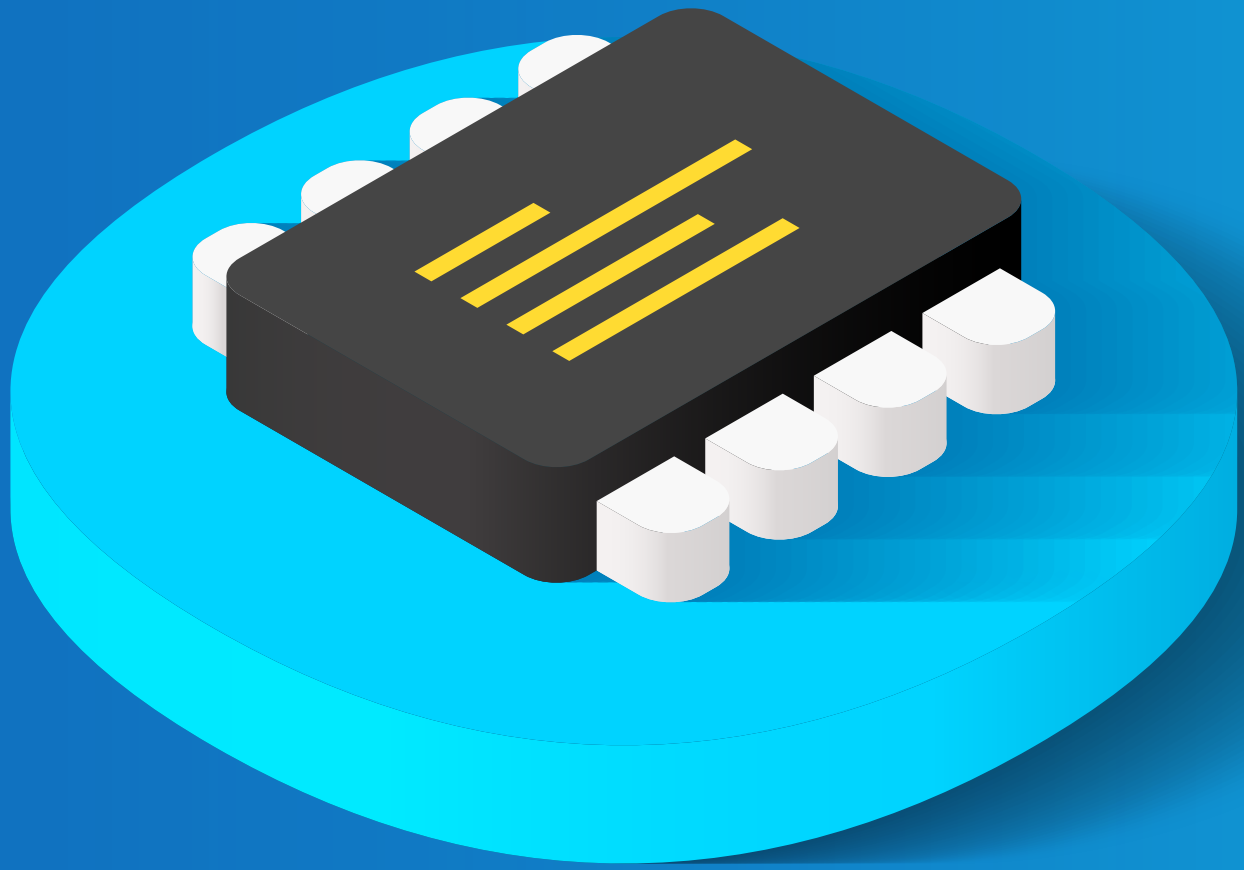
TOP TIPS FOR DIRECTORS

- Regularly review, test and update data breach response plans (involving directors and management in this process).
- Implement employee training and awareness at all levels.
- Conduct regular risk assessments on BYODs, remote access and the use of cloud-based services.
- Consider how a 'privacy positive' approach can be used as a differentiator.

Part three

Looking ahead

As we navigate the challenges of the fourth industrial (digital) revolution, we find ourselves at the crossroads of current and developing data-related rights: information privacy rights, consumer rights, intellectual property rights, and human rights.



Looking ahead

The growth and use of, as well as value in, AI, big data, the Internet of Things **(IoT)**, autonomous vehicles **(AVs)**, blockchain technologies, smart cities, the use of apps, and increased cyber security threats, mean that the security of data, as a right and as an asset, as well as a liability and a cost, has taken on increased significance.

Data is also challenging to regulate, particularly because it is dynamic and moves at speed through an increasingly interconnected and interjurisdictional supply chain.

Our interaction with the world as we go about our daily lives and our access to the products and services we rely on every day, now depend on the continued exchange of data. This brings with it significant benefit, but also risk. Regular, day-to-day activities like driving and shopping can expose individuals to cyber risk, and organisations need to be vigilant to ensure consumers are both informed and protected.

Events in the last 12 months, including the Cambridge Analytica scandal, and closer to home, concerns about the MyHealth Records system and its hesitant uptake, demonstrate a heightening in community expectations as to how organisations collect, use, process and manage data. Prudent organisations must move beyond mere compliance to using privacy and data protection as a key differentiator.

Meeting these heightened expectations will require the development of robust data governance and risk management frameworks. The consumers' interest must lie at the very heart of these frameworks.

These increasing consumer expectations are occurring against a backdrop of persistent cyber threats. Criminals are becoming even more sophisticated, and have seen the impact that interference with core infrastructure and essential services can have, as demonstrated by the drone incident at London's Gatwick airport in December 2018, and the compromise of the New South Wales Early Warning Network in January 2019.

While organisations grapple with these challenges, they will also need to make sense of and implement arrangements for data-related laws introduced to support security and law enforcement (such as Australia's 'decryption' laws and metadata retention laws).

Furthermore, they will need to deal with government identity records (such as health records and the national facial recognition scheme) and the 'long arm' reach of the GDPR.

AI and big data

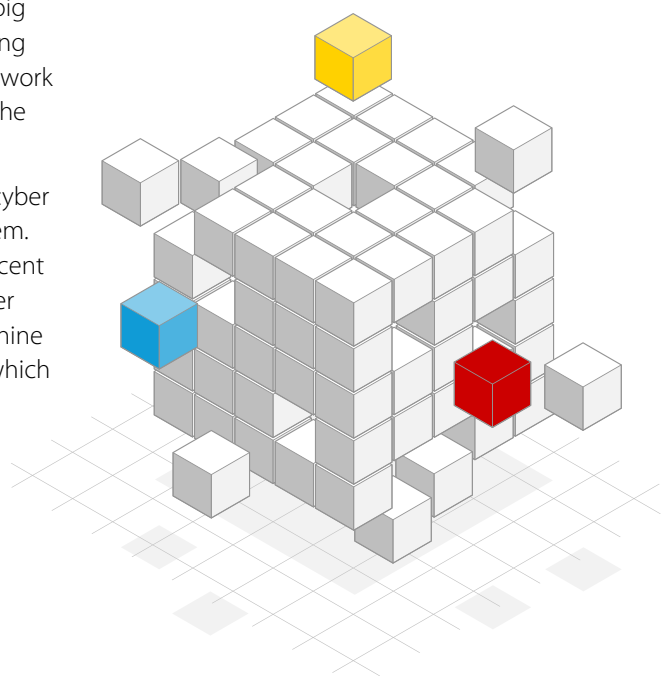
The use of 'big data' is not new and in many cases has become routine. However, machine learning and the development of AI is driving the collection of data, and the ways in which it is being used, beyond the limitations of the current global regulatory framework.

There is wide acknowledgment that AI and big data may benefit society by increasing the rapidity of processing, supporting decision-making, improving efficiency, and creating new methods and solutions in fields such as health, medical care, scientific research, education, sustainable development, agriculture, transport and security. However, these benefits must be balanced against the significant challenges that AI and big data pose for business and consumers. These include increased cyber risk resulting from holding ever larger volumes of data, the matching and re-identification of data held within, or shared between organisations and the re-purposing of data for unintended uses.

In response to these risks, organisations, such as Microsoft, IBM and Google, have published a set of guiding AI ethical principles, as has the International Conference of Data Protection & Privacy Commissioners' (CDPPC), in its Declaration on Ethics And Data Protection In Artificial Intelligence (released in October 2018). Common themes across these ethical principles include fairness, transparency, accountability and governance, and the protection of privacy rights. By developing and publishing these principles, major technology companies have publicly committed to comply not only with their privacy obligations at law, but also to adopt an ethical, transparent and accountable approach to the use of AI.

Organisations that are adopting AI and big data solutions should consider developing their own governance and ethical framework to guide decision making in relation to the use of this technology.

Finally, while AI can help guard against cyber attacks, it can also be used to launch them. Organisations should be aware of the recent increase in the use of AI to conduct cyber and identity attacks, and the use of machine learning tools to craft phishing attacks which can be undertaken on a greater scale, across jurisdictions, anonymously, and with increasing sophistication.



Smart cities, AVs, block-chain, the IoT, and mobile technology and devices

Plans for smart cities, the development of AVs, and the increasing use of blockchain and IoT technologies, are all part of an emerging global internet-based system that seamlessly integrates multiple data collection devices that collect, store, process and share data, largely about individuals.

Data collection devices include everything from driverless AVs, to everyday health-related devices and wearables that monitor and track our wellbeing, to surveillance cameras, beacons and other devices that monitor and track individuals.

The promise of these systems, in terms of collecting and processing data, should be considered by organisations from a holistic perspective, to ensure that ethical, consumer, privacy, governance and cyber risks are also considered.

For example, the ethics of the use and programming of AVs is currently the subject of much debate. In order to perform their driverless tasks, AVs must be connected with other automated vehicles and infrastructure, as well as to mobile and other devices, if they are to talk to the environment around them.

As a result, like other forms of IoT-connected technology, AVs are constantly receiving, exchanging and relying on data shared with other AVs and devices.

As more devices and infrastructure are connected to the Internet in this way, the potential for issues to arise in relation to the collection, storage, processing and sharing of this data, including the risk of large scale cyber incidents, escalates.

How can organisations prepare to adopt new technologies and the accompanying challenges?

A key theme emerging from the adoption of these new technologies is the need to implement robust data governance arrangements and strategies to manage and protect data.

The law cannot keep up with the pace of technological change. It is therefore incumbent on organisations to develop their own baseline rules and frameworks to meet community, consumer, market and regulator expectations. These rules and frameworks should be established with a customer-centric approach to data use. The question to ask, in relation to data collection, use and processing, is not simply 'can we?' Rather, organisations should ask themselves:

- why are we doing this?
- will it benefit our business in the long run?
- what is the benefit to our customers?
- what is the potential privacy, social and reputational impact, both positive and negative?

PRIVACY IMPACT ASSESSMENTS

An important element of data governance arrangements is the need for organisations to undertake privacy impact assessments **(PIAs)** and other security and internal assessments when considering the adoption and use of new technologies.

As discussed on page 8, our survey shows that only 32% of respondent organisations planning to implement AI and big data solutions, have completed PIAs or security risk assessments.

An iterative approach may need to be adopted when undertaking these assessments, as technology and projects are often developed in an 'agile' environment. However, rushed or unplanned adoption of new technology and AI solutions and products, without proper assessment, can expose organisations to significant risk.

How can organisations prepare to adopt new technologies and the accompanying challenges? continued

DATA SHARING

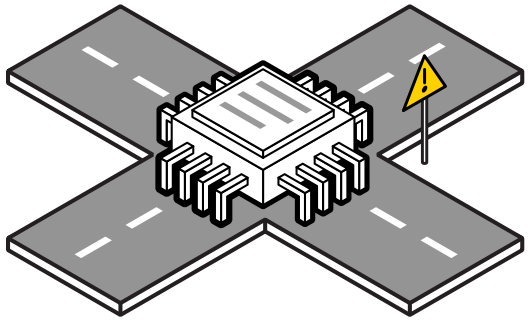
We expect to see an increase in the number and types of organisations that are entering into arrangements to share data and apply AI tools to these 'mega' datasets, in order to gain greater insights into customer behaviours and trends.

However, organisations should not overlook the need to have in place appropriate data sharing agreements that protect the confidentiality and intellectual property rights in the data as well as in their data analytics techniques and solutions.

CYBER RESILIENCE

Finally, as cyber criminals (whether individuals, organised crime syndicates, terrorist groups or nation states) are becoming more sophisticated in their attacks, the need for organisations to have well-developed and well-practised cyber security arrangements, supported by appropriatedly skilled staff, is more critical than ever.

Ultimately, the approach to privacy governance, data protection, ethics, consumer-centricity and cyber resilience, is established within the culture of an organisation – and it is the responsibility of the organisation's leadership to set and continually reinforce this.



...we find ourselves at the crossroads of current and developing data-related rights: information privacy rights, consumer rights, intellectual property rights, and human rights.

Conclusion

In our emerging data driven world, as we experience the fourth (digital) industrial revolution, there will be ongoing tension between the many new opportunities for business and collaboration, and the increased privacy risks and cyber threats that individuals and organisations face.

Big data, AI and other emerging technologies offer enormous potential as well as significant risk , particularly as cyber criminals use these technologies to develop new capabilities.

In an environment of increasing regulation, it is more important than ever for organisations to carefully consider their cyber readiness and take action where required.

This means:

developing, and implementing a cyber resilience strategy which is regularly updated

developing and implementing tailored data breach response, business continuity and disaster recovery plans, which are regularly tested and updated

regularly training all staff (not just IT staff) in order to embed a culture of cyber awareness and data protection across the organisation, and to ensure that everyone understands their roles and responsibilities in the event of a cyber incident

undertaking privacy impact and security assessments when planning to adopt AI, big data solutions, or other new technologies

developing governance and ethical guidelines and frameworks for the use of data having regard to the prevailing technological, regulatory and business environment

capturing lessons learned and monitoring global developments in privacy and data protection to continually assess and improve the organisation's cyber posture.

To discuss how these data protection and privacy developments might affect your organisation, please contact our team.

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.

Understand how GDPR applies to your business and ensure compliance across the data life cycle

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 award winning Safetrac online compliance system).

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.

Our team

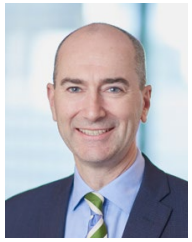
Paul Kallenbach
Partner
T +61 3 8608 2622
M +61 412 277 134

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

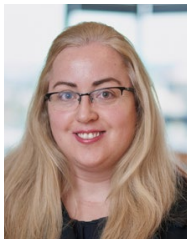
Anthony Lloyd
Partner
T +61 2 9921 8648
M +61 411 275 811

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



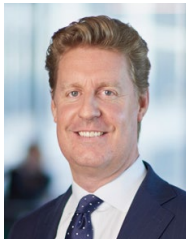
Leah Mooney
Special Counsel
T +61 7 3119 6230
M +61 421 587 950

John Fairbairn
Partner
T +61 2 9921 4590
M +61 410 475 96**5**

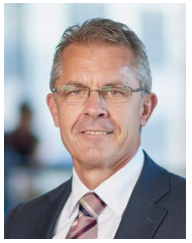
Vanessa Mellis
Special Counsel
T +61 7 3119 6101
M +61 434 658 811

Lisa Jarrett
Partner
T +61 8 8233 5501
M +61 448 880 530

Christina Graves
Special Counsel
T +61 2 6225 3349
M +61 2 62251349



Stephen Craike
Partner
MinterEllison Consulting
T +61 2 9921 8888
M +61 415 592 802



Simon Lewis
Partner
MinterEllison Consulting
T +61 2 9921 8609
M +61 418 320 011