Perspectives on **Cyber Risk 2020**

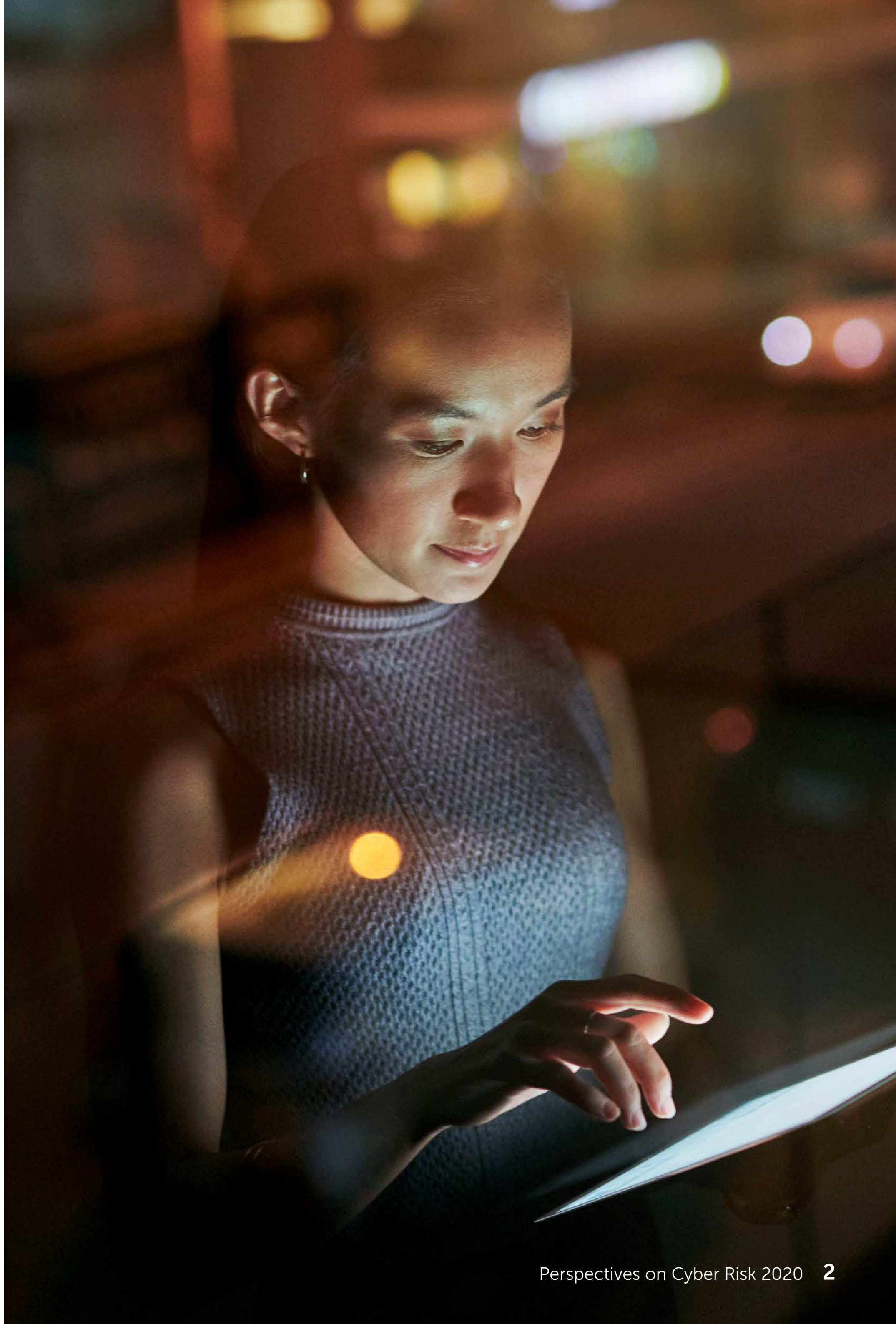
minterellison.com

MinterEllison

Contents

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

Paul Kallenbach, Partner; Susan Kantor, Senior Associate; Margaret Gigliotti, Senior Associate; Gary Yang, Lawyer.



Methodology

MinterEllison's fifth annual cybersecurity survey was completed by more than 120 legal counsel, Chief Information Officers, Chief Operating Officers, Data Protection / Privacy Officers, Board members, IT specialists and risk managers of ASX 200 and private companies, government agencies and not-for-profit organisations.

Just over half of our respondents came from organisations with more than 1,000 staff.

As in 2019, we issued the same survey to all participants. Participants responded to questions about cybersecurity roles, responsibilities and attitudes within their organisations.

The survey was conducted during November 2019. 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.

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

As in previous years, in Perspectives on Cyber Risk 2020, we review the cyber risk challenges that have arisen over the past 12 months, analyse the cyber survey responses received, and consider what the next 12 months may hold.

However, 2020 has brought with it some significant new challenges, and we cannot overlook the additional risks currently facing all organisations as a consequence of COVID-19. In addition to clear and present health, economic and logistical challenges, it is important that organisations do not underestimate elevated cyber risks resulting from the pandemic.

These cyber risks are manifesting in a number of ways. Cyber criminals are already seeking to take advantage of the fraught global situation by establishing malicious websites that purport to offer public health information but instead access users' personal details, by distributing ransomware or other malware using disguised COVID-19 related emails, SMS messages and phone calls (including by impersonating the World Health Organisation and government authorities).

In these uncertain times, it is understandable that individuals will feel more vulnerable and anxious to keep themselves updated with the latest public information. This may make them more susceptible to malicious messages or social engineering attacks. As highlighted later in our Report, personnel who inadvertently succumb to phishing attacks continue to be a key source of cyber incidents.

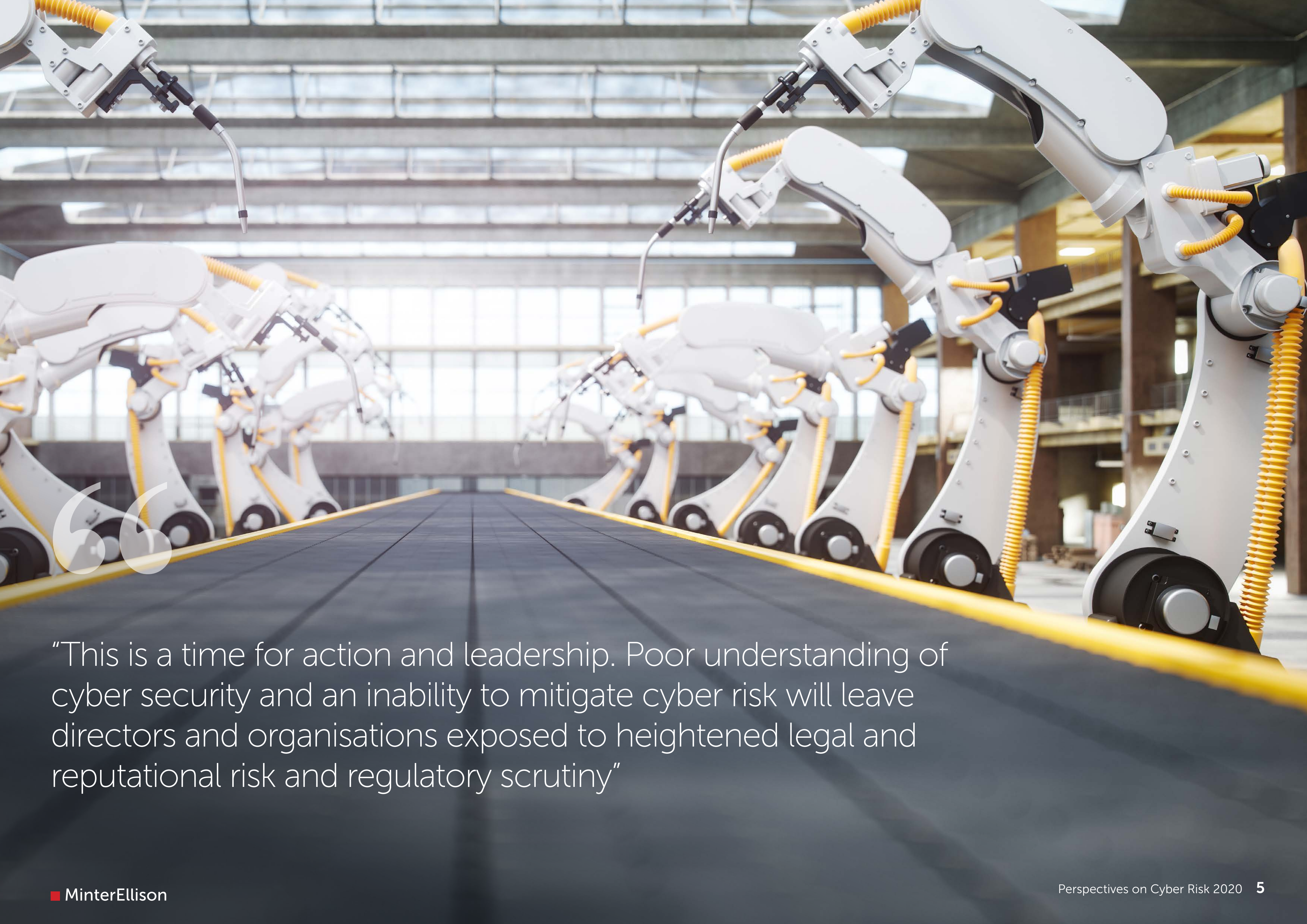
In addition, with so many organisations having moved to a work from home environment, in-house and external IT resources are more stretched than ever, and are being diverted to ensure that remote access connectivity can be maintained for staff. However, it remains critical to ensure that business as usual security processes are not degraded, leaving IT systems vulnerable to attack.

Moreover, with large numbers of workers now relying on their home networks and devices in order to access work resources, there are increased points of vulnerability for many organisations.

It is more important than ever that organisations continue to distribute cyber awareness information to their staff, to ensure heightened vigilance about the threat of phishing and other cyber attacks, and that IT security policies, processes and procedures are updated to take account of the far-reaching impact of COVID-19.

Some tips to protect yourself from COVID-19 related cyber attacks

- Do not reply, click on links or open attachments on suspicious or unsolicited emails
- Never respond to unsolicited SMS or calls that ask for personal or financial details — just press delete or hang up
- Think before you click on any links shared in Whatsapp, Facebook or other social media platforms
- Thoroughly research websites before providing your information or buying any products
- Scammers could also set up fake charities - carefully vet the organisation before you donate



“This is a time for action and leadership. Poor understanding of cyber security and an inability to mitigate cyber risk will leave directors and organisations exposed to heightened legal and reputational risk and regulatory scrutiny”

Looking back on 2019

During 2019, cyber attacks affected millions of individuals worldwide. These included large scale breaches in Australia, most notably the infiltration of the Australia National University's information systems by a sophisticated malicious actor, and the exposure of Landmark White's records on the 'dark web'.

As the frequency, sophistication and impact of cyber attacks continues to grow, so too does the stridency of the response by global privacy regulators – particularly against organisations which fail to implement basic security controls, leaving themselves and their customers vulnerable to attack. In the past 12 months, this has been reflected in record fines imposed by regulators, including a US$5 billion levied against Facebook by the US Federal Trade Commission and the UK Information Commissioner's Office's proposed £183.39 million fine against British Airways and £99 million fine against Marriott.

In 2020, the message to directors and management is clear: poor data security practices can impact not only the board room, but the bottom line. An insufficient understanding of cybersecurity and inability to mitigate cyber risk will leave directors and organisations exposed to heightened privacy and data security expectations of regulators and customers.

2019 was marked by fewer changes to privacy law affecting Australian organisations compared with 2018, which saw the introduction of both the Australian mandatory data notification laws, and the European General Data Protection Regulation **(GDPR)**. This has afforded a welcome opportunity for many organisations to consolidate and refine their privacy compliance and data protection activities.

The Australian banking sector, however, continues to grapple with evolving regulatory requirements. In 2019, banks continued to prepare for the implementation of the consumer data right (now delayed to July 2020), as well as new information security requirements imposed by the Australian Prudential Regulation Authority (APRA) under Prudential Standard CPS 234.

With CPS 234, APRA seeks to drive improvements in information security practices. These practices affect not only financial services sector organisations, but many of their suppliers, who must meet APRA's security standards in order to provide ICT services to their financial services customers.

It is also clear, following the release of the Australian Competition and Consumer Commission's **(ACCC's)** Digital Platforms Inquiry Final Report and the commencement of legal proceedings against HealthEngine and Google, that the ACCC is now focused on privacy and consumer data risks, and is determined to take on a proactive role in addressing deficient privacy and security practices.

Lessons to learn from 2019

There are important lessons for organisations arising from various publicly reported data breaches and enforcement action across the globe in 2019:

1. Implement and regularly test robust cybersecurity governance arrangements (including incident response and business continuity plans) – investment by management and allocation of resources is crucial.
2. Implement and regularly update technical controls, including by applying the Australian Signals Directorate's Essential Eight Maturity Model.
3. Ensure ongoing and regular training for staff on cybersecurity risks, especially regarding phishing emails and social engineering attacks.
4. Undertake thorough due diligence in relation to key suppliers' data handing and IT security practices and regularly audit those suppliers.
5. Implement arrangements to manage insider risks, including an appropriate level of monitoring and auditing of personnel.
6. Undertake thorough cybersecurity due diligence as part of proposed M&A transactions – know what you are buying.
7. Be aware of risks around de-identification of data, particularly with large data sets, and implement controls to limit the use and disclosure of de-identified data.

What's ahead?

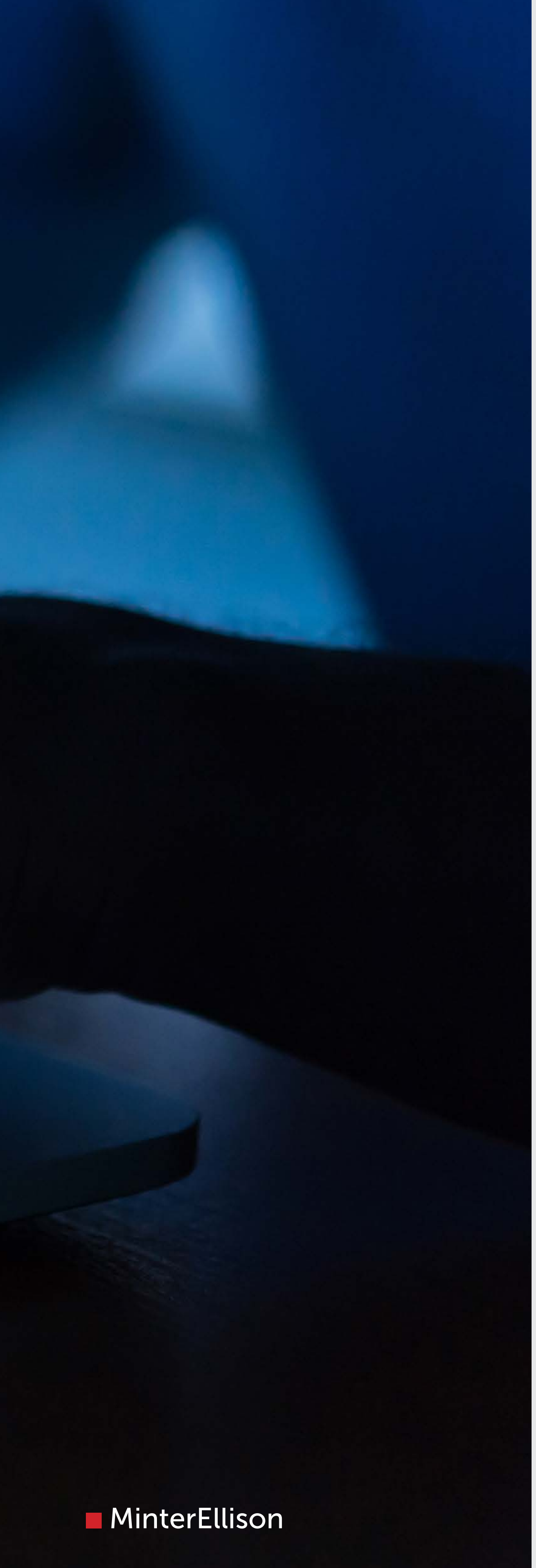
We can expect that cyber attacks will continue to become even more sophisticated. The ANU data breach exemplifies just how sophisticated malicious actors have become (and is further considered on page 14). The significant impact of large scale data breaches is already evident in 2020 following the ransomware attack on freight delivery company, Toll. In January, Toll was forced to temporarily shut down some of its IT systems following the attack, resulting in manual workarounds.

Despite these recent developments, individuals continue to share, and organisations continue to collect, an ever greater volume of data. The need for robust cybersecurity arrangements – particularly to maintain public trust in the handling of data by both public and private sector organisations – remains as important as ever.

Significantly, we await the outcome of Federal Court proceedings commenced in March 2020 by the Australian Information Commissioner against Facebook in connection with the Cambridge Analytica matter. In the six years since the civil penalty provisions under the Privacy Act took effect, this is the first time that the Commissioner has issued proceedings alleging that an organisation has committed serious or repeated interferences with privacy. If the Commissioner is successful, the action could result in the first civil penalty order imposed under the Privacy Act.

In the future, we can expect that the ACCC will play a more central role in the regulation of consumer-related data, including by taking enforcement action against organisations. Organisations should therefore take steps to ensure that their public-facing privacy and IT policies and statements do not include representations that are misleading or deceptive to, or that are likely to mislead or deceive, the public.

Another area of focus for the ACCC is the implementation of the Consumer Data Right **(CDR)**. On 20 December 2019, the ACCC announced that the introduction of the information-sharing obligations associated with the CDR in the banking industry had been delayed by six months, to allow for 'additional implementation work and testing to be completed and better ensure necessary security and privacy protections operate effectively'. ACCC Commissioner Sarah Court said '[r]obust privacy protection and information security are core features of the CDR and establishing appropriate regulatory settings and IT infrastructure cannot be rushed'.



The CDR regime

In the banking sector, the CDR (referred to as 'Open Banking') means that a customer of a bank – whether an individual or business – can request or give consent for their data to be shared with an accredited third party. The scheme is intended to offer customers clearer visibility of their data and, consequently, the ability to make more informed decisions, as well as to facilitate increased competition in the sector.

On 6 February 2020, the ACCC announced the commencement of the CDR Rules, and the Office of the Australian Information Commissioner subsequently released the CDR Privacy Safeguard Guidelines. The current challenge for the banking sector is to determine how it will implement the Rules and Guidelines, as well as the Consumer Data Standards, which are issued by Data61.

The legislation and rules that make up the CDR are complex, and we expect that organisations subject to the CDR will be grappling with how they will implement procedures and processes to operationalise them. A further consideration is that the same dataset held within an organisation could be subject to regulation under both the Privacy Act and CDR regime at different times, depending on the capacity in which the organisation, at any given time, is holding the data.

Importantly, if the data is CDR data, the CDR regime supersedes privacy laws. Therefore, the question for organisations is whether they should generally raise their compliance standards to meet the stricter CDR requirements at all times, or whether they should apply different standards at different times. An analogous dilemma arises in relation to the **GDPR**. Here, many global organisations have adopted a global compliance standard of GDPR requirements (which is, in general terms, stricter than most other privacy regimes, including Australia's), rather than taking a different approach in each jurisdiction in which they operate.

While there are advantages in streamlining an organisation's compliance approach, in some cases, there may be practical difficulties in adopting a single, higher standard. These include greater compliance costs, and the cultural and other changes that may be required within a global organisation in order to adopt the higher standard.

Although the CDR is being implemented initially in the banking sector, the government has already announced that, in due course, it will also apply to the energy and telecommunications sectors.

Following a period of consultation, the ACCC announced in August 2019 the preferred data sharing model in the energy sector (using the Australian Energy Market Operator as the gateway for making CDR requests and distributing information). This was determined to be the preferred model for energy operators, rather than the model of direct request and access in the banking sector, given the unique manner in which data is held across the energy industry.

In January 2020, the federal Treasurer announced the government's Inquiry Into Future Directions of the Consumer Data Right, and is seeking submissions from all sectors of the economy on a range of matters about the CDR, including how it can support the development of a safe and efficient digital economy. The Inquiry is currently due to report by September 2020.

Findings of our 2019 cyber risk survey

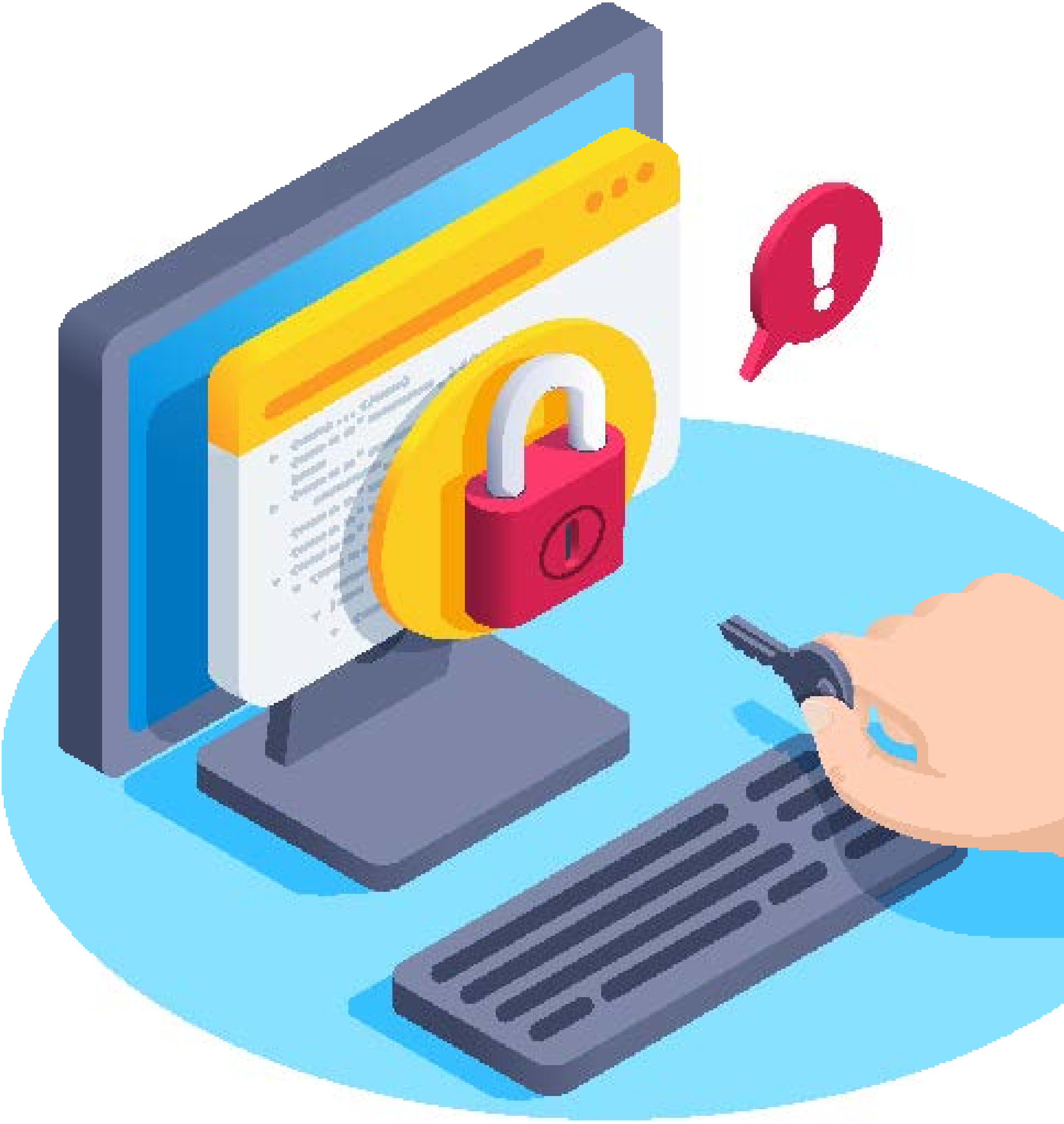
In late 2019, we conducted our fifth annual cybersecurity survey to understand the level of awareness of and importance that organisations place on cyber risk.

Finding #1: The more you know, the more you realise you don't know

In previous surveys conducted between 2016 and 2018, there had been a year-on-year increase in the number of respondents who identified themselves as having a 'very good understanding' of their organisation's exposure to the risk of cyber attacks. However, this year marks the first year in which there was a decline in this response, falling from 35% of respondents last year to just 20% this year.

Does this mean that organisations have become less knowledgeable about the risks of cyber attacks over the past 12 months? We think this unlikely. Rather, this year's decline may reflect an acknowledgment by respondents of the increasingly complex and ever-evolving nature of cyber risk, and of the need to continually augment their understanding of a dynamic cyber risk landscape.

It is critical for organisations to recognise the need for adaptation, learning and change. Failure to do so can lead to complacency and vulnerability.



Findings of our 2019 cyber risk survey

Finding #2: Testing cybersecurity and data incident response plans is critical

In our latest survey, we saw a significant increase in the number of organisations which have been subject to more than five cyber attacks that have compromised their systems or data in the past 12 months – from 5% in 2018 to 14% in 2019. There has also been a corresponding decrease in the number of organisations which have not suffered such an attack, from 63% in 2018 to 38% in 2019. A majority of our survey respondents have experienced some form of compromising cyber attack in the past year.

These results reflect the increase in the volume of cyber attacks that organisations are experiencing, as well as the evolving nature of cyber risk – meaning that even vigilant organisations may suffer multiple attacks.

It is pleasing, however, to see an increase, albeit a small one, in the number of respondents who told us that their organisation regularly tests their data incident response plans. This signals a growing awareness by organisations of the need to continually improve and enhance their approach to cyber risk, as the volume and complexity of cyber attacks continue to increase. More recently, COVID-19 has put business continuity plans in the spotlight, with cyber risk and digital resouces a significant part of this.

Finding #3: Cyberattacks which rely on social engineering are still the most prevalent

Among our survey respondents, the most prevalent form of cybersecurity incident resulted from social engineering, with 50% of incidents involving a phishing incident (whether via email or telephone) and a further 21% involving an email compromise (such as invoice fraud). Of the other identified types of incidents, only 3% comprised denial of service attacks, while 13% involved ransomware.

This finding is consistent with the Office of the Australian Information Commissioner's (**OAIC's**) 2019 Insights Report in relation to Australia's Notifiable Data Breach scheme, which found that 'phishing and spear phishing continue to be the most common and highly effective methods by which entities are being compromised'. The most recent statistics published (covering 1 July through 31 December 2019) continue to reflect this position. Of all malicious attacks reported to the OAIC during that period, 44% involved some form of phishing attack. These findings demonstrate that, no matter how robust an organisation's technical security, the element of human error will always exist. Unfortunately, it only takes one individual within an organisation to follow a malicious link, or to provide information they ought not have, to expose their organisation (and potentially organisations with which they electronically interact) to cyber risk.

Given the prevalence of phishing and other social engineering related attacks, we were pleased to see that, of the organisations which told us they had been affected by a cybersecurity incident, 60% provided additional staff training and communication as a consequence. As criminals become more sophisticated in their phishing and social engineering techniques, organisations must arm their employees with critical tools (including regular staff training and communication) to defend themselves and their workplace.

The Australia National University (ANU) cyber incident in 2019 (discussed on page 14) is a recent example of a sophisticated phishing attack.

Recently, artificial intelligence (**AI**) techniques have been deployed to conduct cyber attacks. For example, in early 2019, AI-based software was used to impersonate the voice of a chief executive of a UK-based energy company, defrauding the company of €220,000. The number of such attacks is likely to grow as the sophistication of AI-based systems continues to evolve.

Findings of our 2019 cyber risk survey

Finding #4: Uptake in the usage of AI and big data is at its early stages, but there is an increasing awareness of potential privacy implications

The potential for AI and big data to reshape organisations and industries has been a frequent topic of discussion in the media over the past 12 months. However, at least for our respondents, the media hype is not yet reflected in the implementation of AI and big data solutions within their organisations. Our survey results disclosed only a modest increase – from 15% last year to 21% this year – in organisations currently using an AI or big data solution. Around 10% (about the same as last year) said they planned to implement such a solution in the next 12 months.

Of those organisations employing AI or big data solutions, there was a significant increase in the number that have undertaken a privacy or security impact assessment in relation to the implementation of such technology, from 32% last year, to 53% this year.

This is particularly important for AI and big data projects, which by their nature rely on large data sets. As the digital threat environment has become more sophisticated, these data sets have proven to be attractive targets for unscrupulous actors (both external and internal).

There is an increased focus by regulators and the public on the ethical implications of AI and big data. Many of these implications are privacy-related, including, for example, the ramifications of the improper use of AI and big data in re-identifying information as personal information, and the use of flawed or biased algorithms in policing and other sensitive contexts.

The use of AI and machine learning technology has attracted recent media attention in the case of Clearview AI, an application owned by a private company that has collected more than three billion publicly available images from the internet and uses machine learning to create biometric templates to match those images to individuals. The use of Clearview AI by law enforcement agencies in Australia and overseas has garnered criticism from privacy advocates due to the lack of transparency and accountability in the way the tool is used, and the lack of privacy protections in place. Proponents of the technology maintain that it has been successful in identifying criminals and securing convictions. However, Digital Rights Watch and other privacy advocate groups, both in Australia and overseas, have called for a moratorium on the use of facial recognition technologies until regulatory frameworks for their use have been implemented.

Concurrently, the Australian Human Rights Commission released its Human Rights and Technology Discussion Paper in December 2019, seeking submissions on its 29 preliminary recommendations to protect and enhance human rights in the context of technological advances (particularly AI), including the regulation of AI-influenced decision making. At this stage, it remains to be seen whether new AI regulation will be introduced in Australia. However, with this context in mind, it is important for organisations to prudently approach the implementation of AI and big data solutions.

To this end, privacy impact assessments are recommended by the OAIC for any project involving the handling of personal information to determine compliance with privacy legislation and alignment with public privacy expectations. These assessments are particularly important for projects involving AI and big data solutions, which often deploy ground breaking technologies of significant power and potential, but also ingest vast amounts of data and pose new privacy challenges for organisations. For those starting new projects, incorporating 'privacy by design' elements, such as de-identifying data where possible, can go some way to mitigating the reputational and financial risks that serious data breaches can pose.

The past year has seen the publication of Artificial Intelligence: Australia's Ethics Framework, a framework by CSIRO's Data61 to guide the proliferation of AI in Australia in accordance with a set of ethical principles. This is a useful resource for organisations considering implementing AI or big data solutions.

Findings of our 2019 cyber risk survey

Finding #5:
Less than 60% of organisations have assessed whether GDPR applies

This year, our survey asked for the first time whether organisations had assessed the applicability of the EU GDPR. Only 58% of respondents said they had considered whether it applies to their organisation, while 12% of organisations had not considered its applicability, and 24% of respondents were unsure.

The GDPR is the European Union's privacy law, which came into effect in May 2018, and which can apply directly to Australian organisations. Though many of the privacy requirements are similar to those found in the Privacy Act 1988 (Cth), there are a number of concepts which are unique to the GDPR (such as data 'processors' and 'controllers'). Compliance with the Australian privacy laws alone will not meet an organisation's GDPR obligations. In particular, data breach notification obligations are stricter under the GDPR than under Australian privacy laws.

As such, it is recommended that organisations (especially those with a physical presence in the EU or those offering goods and services in the EU) assess whether the GDPR applies to them.

Our survey results disclose that a significant number of surveyed organisations are yet to assess the applicability of the GDPR. With its significant penalties for non-compliance (of up to 4% of annual global turnover or €20 million, whichever is higher), and the ACCC and the Australian Government flagging their increased appetite for GDPR-style privacy reform (discussed below), it is important that Australian organisations understand whether the GDPR applies to them, and, if so, whether their current privacy and data protection policies and practices meet the requisite standards.

Lessons learned from high profile Australian data breaches over the last 12 months

The impact of high profile cyber attacks in Australia has been significant this year, and there are important lessons that can be learned from them.

Australia National University

In June 2019, ANU publicly announced that it had suffered a cyber attack, which had only been discovered two weeks prior. This was despite a malicious actor gaining unauthorised access to its enterprise systems in November 2018. ANU disclosed that the malicious actor had accessed an unknown quantity of information dating back up to 19 years, affecting approximately 200,000 individuals.

ANU took the unprecedented step in Australia of publishing an 'Insight Report' of the incident on 2 October 2019. The Report highlighted that the actor used a variety of sophisticated methods in order to obtain credentials and network access, including a number of sophisticated spear phishing emails. Unlike traditional phishing methods, the emails sent throughout the organisation did not require user interaction. In other words, even though the emails were only previewed (without being opened), the malicious code contained in the emails still allowed for credentials to be sent to external web servers. The Insight Report also explained there had been approximately a two week delay between identifying the attack and the notification to allow time for ANU to take remediation steps prior to the announcement, including to mitigate the effects of ongoing attempts to regain unauthorised access to ANU systems (either by the original actor, or by others).

The Insight Report helpfully included a number of lessons for other organisations. The successful use of phishing by the actor highlights the need to invest in regular cybersecurity awareness training and education across all organisations. The sophisticated nature of these emails also suggests a need for greater understanding of phishing, including new ways in which information can be compromised and the technical measures that organisations need to implement to mitigate against this.

Lessons learned from high profile Australian data breaches over the last 12 months

LandMark White

In May 2019, LandMark White (LMW), Australia's largest independent property valuation firm, announced that it had suffered a second data breach, following its announcement of an earlier breach in February 2019. In both cases, thousands of company documents were posted online – either to the dark web (in the first attack) or to US sharing platform, Scribd (in the second attack). Although the compromised documents were not confidential in nature (insofar as the information contained could be found by alternate means, e.g. through a title search), the breach severely impacted LMW's reputation, with devastating results. LMW voluntarily entered a trading halt following the announcements, and its CEO resigned from the company. In addition, LMW's key clients – major Australian banks – immediately suspended the use of LMW's services. Collectively, these events contributed to a loss of $15.1 million in FY19, and LMW was forced to raise equity through a rights issue in order to continue trading. In December 2019, LMW announced that it was re-branding to 'Acumentis' in an effort to start afresh.

Unlike some of the other significant data breaches that have occurred over the last 12 months, the incident did not arise due to a sophisticated attack. Instead, it was the work of an inside IT contractor, who has since been charged with a number of offences and remains in custody.

Public media reports suggest that at least 15 senior employees and contractors of LMW knew that the network was vulnerable before the incidents occurred – highlighting the critical importance of strong and effective board-level cyber governance.

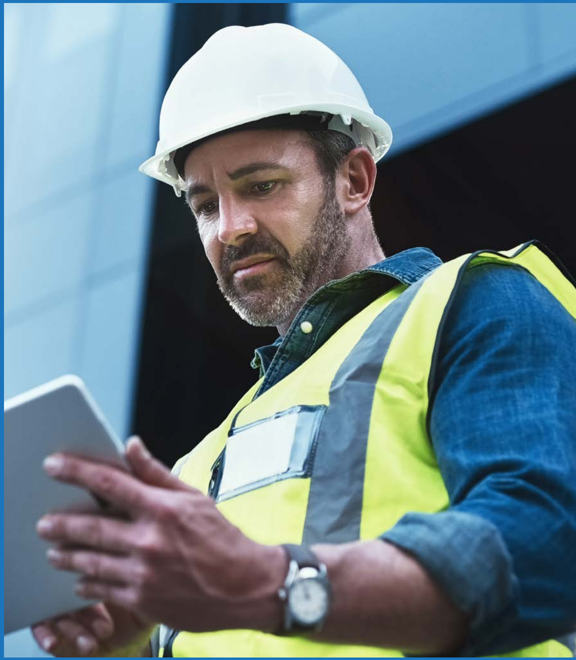
Victorian public hospitals

In October 2019, a number of regional hospitals in Victoria were subject to a ransomware attack, which blocked access to several major systems. In an attempt to contain the infection, the impacted hospitals disconnected a number of their IT systems (including patient records, booking and management systems).

The attack resulted in the facilities having to resort to manual systems to maintain health and other services.

This attack follows an audit released by the Auditor-General in May 2019, which exposed the vulnerability of patient data stored in Victoria's public health system. The report also found that staff awareness of data security was low, increasing the likelihood of successful phishing by malicious actors.

In the OAIC's 2019 Insights Report and again in the six monthly report on data breaches between 1 July and 31 December 2019, the OAIC concluded that the highest number of notifiable data breaches have occurred in the health sector. Between 1 July 2019 to 31 December 2019, 43% of these breaches were found to be the result of human error, as opposed to the average of 32% for all other sectors. These results highlight the need for organisations that handle health and other sensitive information to implement robust cybersecurity and cyber resilience measures.



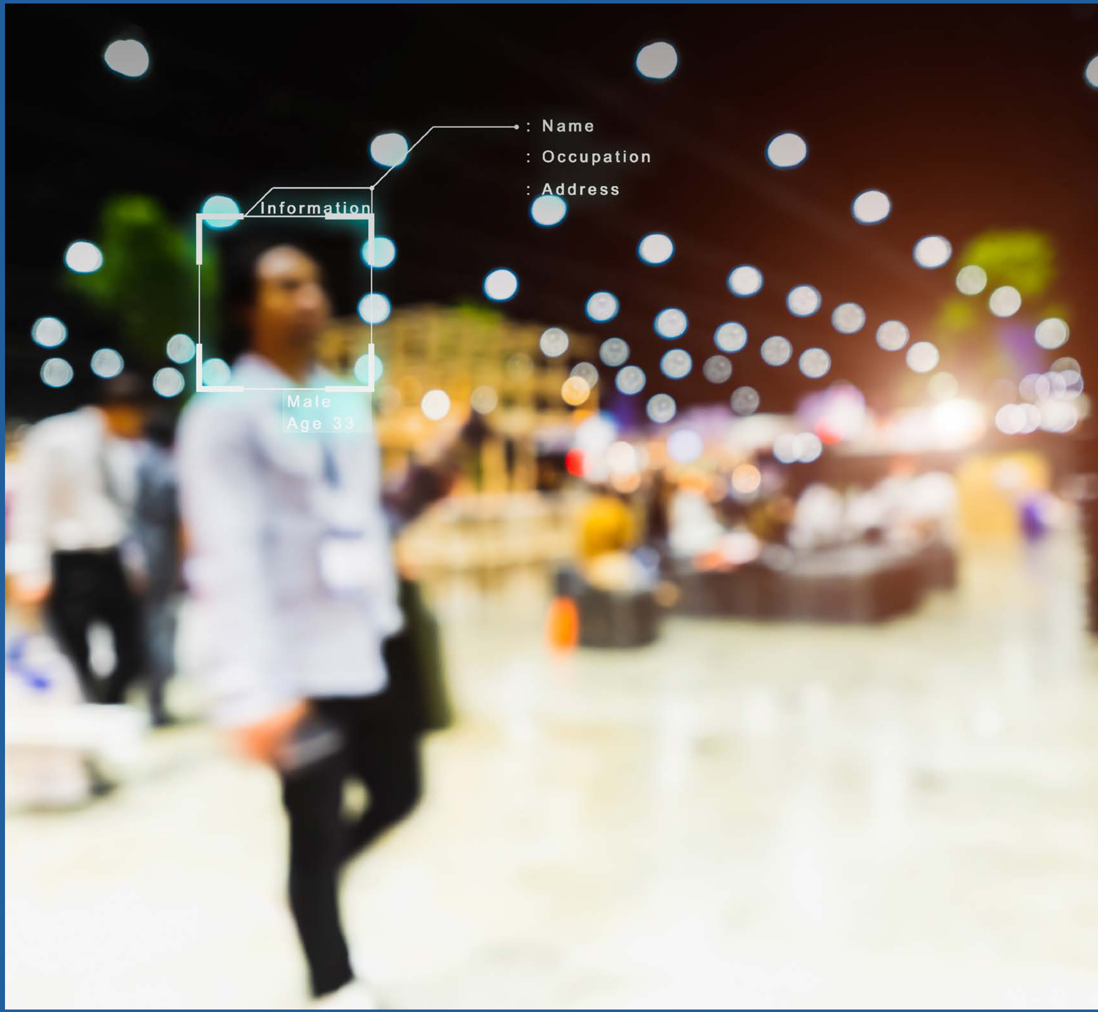
Lessons learned from high profile Australian data breaches over the last 12 months

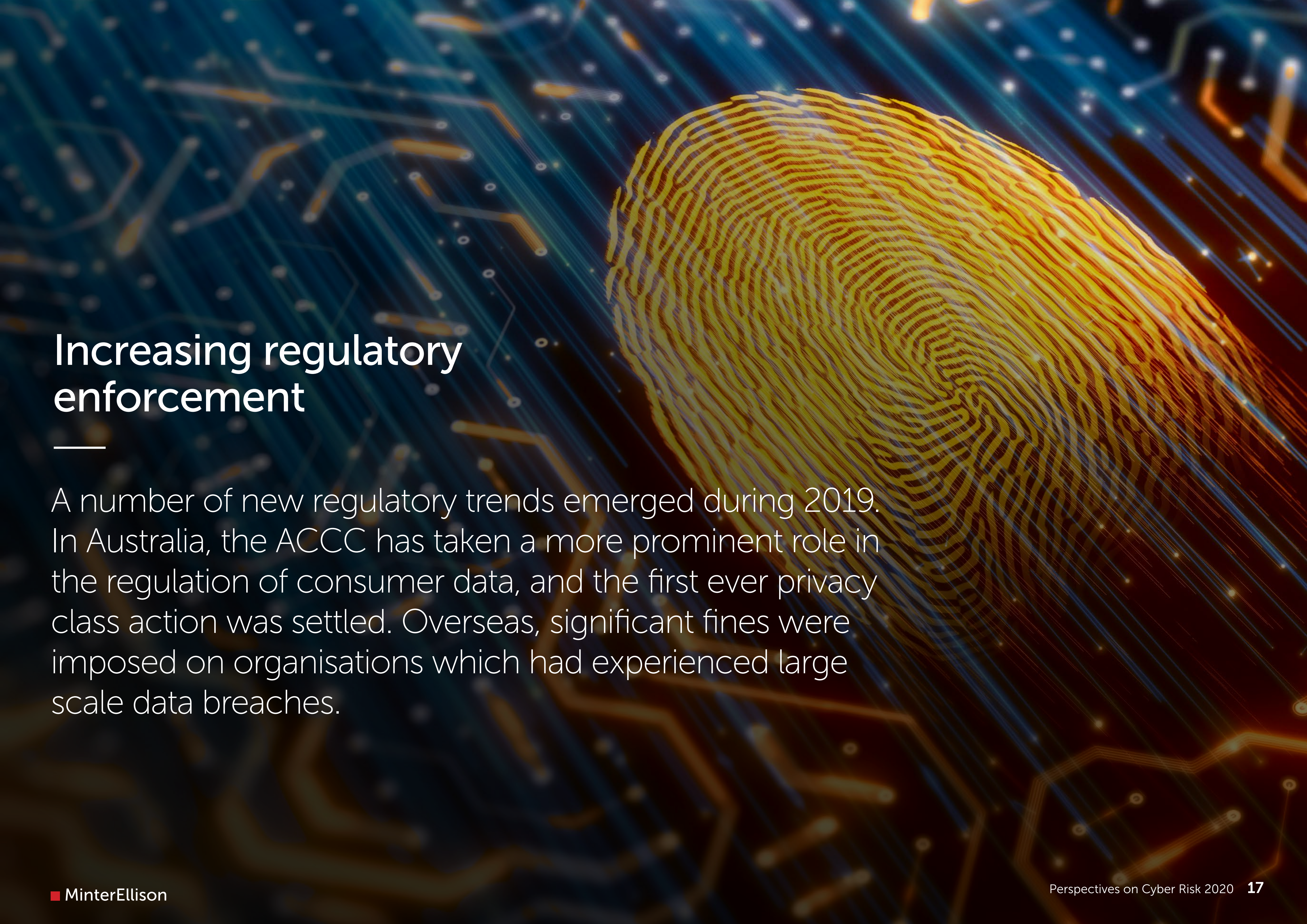
Myki

In August 2019, the Office of the Victorian Information Commissioner (OVIC) published its report on the release of myki data by Public Transport Victoria (PTV) of around 1.8 billion records of historical transport users' activity to Data Science Melbourne for a Data Hackathon. PTV released the dataset on the basis that, according to PTV, the information was de-identified and did not relate to individuals.

However, OVIC found that, because the data was released to the Data Hackathon participants without any restrictions on the use or onward disclosure of the data, and because there were a number of ways in which the data could be re-identified (as described in separate reports prepared by Data61 and academics at the University of Melbourne), it was reasonably possible to determine the identity of a substantial portion of the individuals whose travel movements were included in the dataset.

This incident is a timely reminder of the increasing difficulty organisations face in effectively de-identifying data. While the de-identification of data has, until now, been relied upon as a means of protecting data and enabling it to be used for secondary purposes, recent advances in AI and data analytics tools, combined with the increasing size of datasets, means that de-identification is increasingly difficult to achieve.





Increasing regulatory enforcement

A number of new regulatory trends emerged during 2019. In Australia, the ACCC has taken a more prominent role in the regulation of consumer data, and the first ever privacy class action was settled. Overseas, significant fines were imposed on organisations which had experienced large scale data breaches.

Australia

On 9 March 2020, the Australian Information Commissioner issued proceedings against Facebook Inc and Facebook Ireland Limited in relation to the "This is Your Digital Life" App, which allegedly sold personal information to Cambridge Analytica in relation to the users and 'friends' of users who installed the App. The Commissioner alleges that Facebook did not adequately inform individuals about the way their personal information could be disclosed (including their friends' information), or take reasonable steps to protect the security of the personal information from unauthorised disclosure. The case is highly significant, as it could result in the first ever civil penalty being imposed under the Privacy Act. At the time of writing of this report, Facebook has not filed a defence.

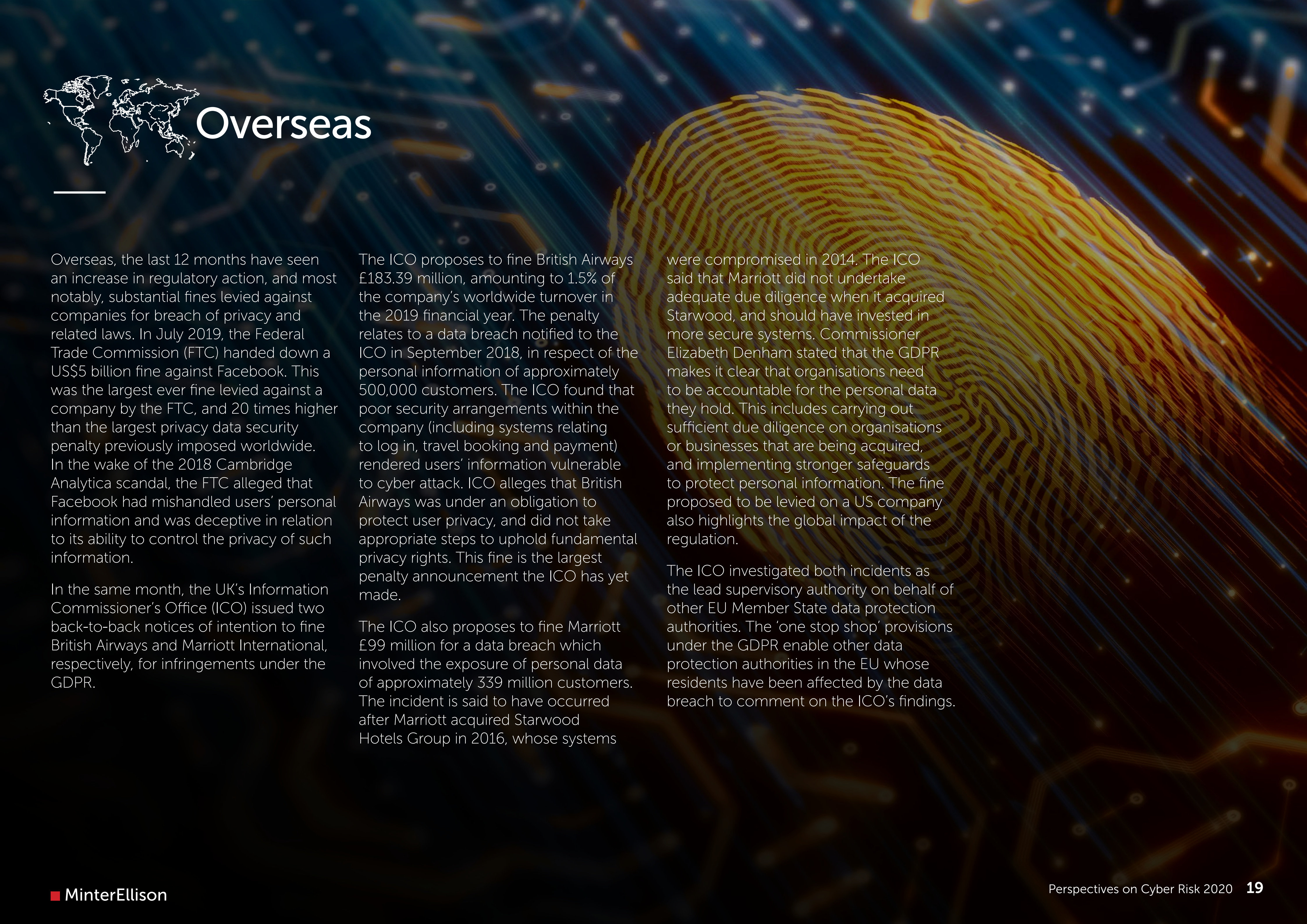
In July 2019, the ACCC published the Final Report of its 'Digital Platforms Inquiry' which examined the impact of digital platforms (including social media and search engines) on the supply of news and journalistic content. It also explored the implications of this for advertisers, content creators and consumers. The Report included recommendations to strengthen requirements under the Privacy Act relating to the collection and use of consumer data. In particular, it highlighted the importance of obtaining consent for different purposes of data collection, use and disclosure. In December 2019, after an extensive consultation period, the government published its response to the ACCC's recommendations, including amendments to the Privacy Act to strengthen penalties, as well as a broader review of the Privacy Act, which is to occur over the course of 2020-21.

A month after the ACCC published its final report, it initiated proceedings in the Federal Court against online health booking platform HealthEngine for misleading and deceptive conduct relating to the publication of patient reviews and ratings, and the sharing of patient information with third parties. The ACCC alleges that HealthEngine provided personal information of over 135,000 patients to private health insurance providers for a fee, without disclosing to consumers that it would do so. HealthEngine is accused of misleading patients into thinking their information would be kept by HealthEngine and not provided to third parties.

In October, the ACCC took further action in relation to consumer data, initiating proceedings against Google by alleging the company made misleading representations to users with Android phones about the collection of personal location data. It alleges that, in doing so, Google has 'collected, kept and used highly sensitive and valuable personal information about consumers' location without them making an informed choice'. Google is accused of misleading consumers when it made on-screen representations about the data that was collected, and how it was used. In particular, Google had indicated that location data would only be collected and used for the consumer's use of Google services. However, the data was in fact used by Google for a number of purposes unrelated to the consumer's use of these services.

Transparency and inadequate disclosures surrounding the collection and use of personal information were a major focus in the ACCC's Digital Platforms Inquiry, and remain a top priority according to ACCC Chair, Rod Sims. These proceedings are also a timely reminder for organisations to regularly review and update their privacy and IT security policies to ensure they do not contain potentially misleading statements. These actions, together with the ACCC's Digital Platform Inquiry report, signal a trend towards consumer-focused regulation and privacy reform in Australia.

Finally, to round out 2019, in December, it was announced that the Supreme Court of New South Wales had accepted the settlement of the first ever privacy class action in Australia. The proceedings date back to 2017, when employees of New South Wales Ambulance alleged that a former contractor of the organisation had sold the workers compensation files of 130 current and former NSW Ambulance staff to solicitors. The sum of $275,000 will be allocated between 108 class members. Other proposed class actions (in relation to the 2018 PageUp and Facebook Cambridge Analytica data breaches) have not proceeded.



Overseas

Overseas, the last 12 months have seen an increase in regulatory action, and most notably, substantial fines levied against companies for breach of privacy and related laws. In July 2019, the Federal Trade Commission (FTC) handed down a US$5 billion fine against Facebook. This was the largest ever fine levied against a company by the FTC, and 20 times higher than the largest privacy data security penalty previously imposed worldwide. In the wake of the 2018 Cambridge Analytica scandal, the FTC alleged that Facebook had mishandled users' personal information and was deceptive in relation to its ability to control the privacy of such information.

In the same month, the UK's Information Commissioner's Office (ICO) issued two back-to-back notices of intention to fine British Airways and Marriott International, respectively, for infringements under the GDPR.

The ICO proposes to fine British Airways £183.39 million, amounting to 1.5% of the company's worldwide turnover in the 2019 financial year. The penalty relates to a data breach notified to the ICO in September 2018, in respect of the personal information of approximately 500,000 customers. The ICO found that poor security arrangements within the company (including systems relating to log in, travel booking and payment) rendered users' information vulnerable to cyber attack. ICO alleges that British Airways was under an obligation to protect user privacy, and did not take appropriate steps to uphold fundamental privacy rights. This fine is the largest penalty announcement the ICO has yet made.

The ICO also proposes to fine Marriott £99 million for a data breach which involved the exposure of personal data of approximately 339 million customers. The incident is said to have occurred after Marriott acquired Starwood Hotels Group in 2016, whose systems were compromised in 2014. The ICO said that Marriott did not undertake adequate due diligence when it acquired Starwood, and should have invested in more secure systems. Commissioner Elizabeth Denham stated that the GDPR makes it clear that organisations need to be accountable for the personal data they hold. This includes carrying out sufficient due diligence on organisations or businesses that are being acquired, and implementing stronger safeguards to protect personal information. The fine proposed to be levied on a US company also highlights the global impact of the regulation.

The ICO investigated both incidents as the lead supervisory authority on behalf of other EU Member State data protection authorities. The 'one stop shop' provisions under the GDPR enable other data protection authorities in the EU whose residents have been affected by the data breach to comment on the ICO's findings.

MinterEllison's cybersecurity 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

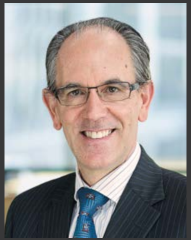
including assisting with cyber risk advice coverage issues, and strategic management of notifications and claims arising from cyber risk losses.

Get in touch with us

Paul Kallenbach
Partner
M +61 412 277 134
E paul.kallenbach@minterellison.com

Susan Kantor
Senior Assosciate
M +61 407 545 091
E susan.kantor@minterellison.com

Anthony Lloyd
Partner
M +61 411 275 811
E anthony.lloyd@minterellison.com



Anthony Borgese
Partner
M +61 400 552 665
E anthony.borgese@minterellison.com

Amanda Story
Partner
M +61 423 439 659
E amanda.story@minterellison.com

Cameron Oxley
Partner
M +61 417 103 287
E cameron.oxley@minterellison.com

Leah Mooney
Special Counsel
M +61 421 587 950
E leah.mooney@minterellison.com

John Fairbairn
Partner
M +61 410 475 965
E john.fairbairn@minterellison.com

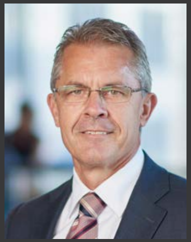
Vanessa Mellis
Special Counsel
M +61 434 658 811
E vanessa.mellis@minterellison.com

Lisa Jarrett
Partner
M +61 448 880 530
E lisa.jarrett@minterellison.com

Nicholas Pascoe
Partner
M +61 403 857 529
E nicholas.pascoe@minterellison.com

Christina Graves
Special Counsel
M +61 2 62251349
E christina.graves@minterellison.com

Stephen Craike
Partner
MinterEllison Consulting
M +61 415 592 802
E stephen.craike@minterellison.com



Simon Lewis
Partner
MinterEllison Consulting
M +61 418 320 011
E simon.lewis@minterellison.com

Ashish Das
Partner
MinterEllison Consulting
M +61 424 289 204
E ashish.das@minterellison.com

minterellison.com

MinterEllison