s

Cybersecurity in Australia: End of Year Wrap Up (2023)

In brief

2023 has ended with a flurry of activity from Australian authorities and regulators that provides deep insights into Australia's current and emerging cyber threat environment and will heavily influence the development of Australia's cyber policy in the years to come.

We've pulled together key insights, important trends in the cyber threat landscape and recommendations for cyber risk management that should be of interest to all Australian businesses and directors moving into 2024 and beyond.

If you find this article useful, you may also enjoy reading our 2023 Year in Review on Australian AI regulatory developments.

Contents

Setting the Scene

Recent reports from Australian authorities and regulators provide deep insights into Australia's current and emerging cyber threat environment and will heavily influence Australia's cyber policy in the years to come, with wide-ranging implications for all Australian business and especially critical infrastructure providers, including the following key developments:

- On 1 November 2023, the **Department of Home Affairs** released the Cyber and Infrastructure Security Centre's (**CISC**) first Critical Infrastructure Annual Risk Review which highlights potential security risks to Australia's critical infrastructure providers in light of the threat and hazard categories in the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) and the Rules for Critical Infrastructure Risk Management Programs (**CIRMP**);
- On 14 November 2023, the Australian Signals Directorate (**ASD**) published its Annual Cyber Threat Report 2022–23 which highlights key trends in cyber security threats based on ASD's experience responding to over 1,100 cyber security incidents throughout FY 22-23 across a full cross-section of government and industry organisations;
- On 22 November 2023, Australia's Cyber Security Minister released the 2023-2030 Cyber Security Strategy which adds further context to the Australian cyber threat environment, highlights opportunities for Australian businesses and outlines new funding and 6 "cyber shields" designed to safeguard Australians from cyber threats, including several proposed legal reforms; and
- On 27 November 2023, Australian Prudential Regulation Authority (**APRA**) released its findings and recommendations based on a multi-year data risk management study with a selection of banks following its 100 Critical Risk Data Elements (**CRDE**) Pilot which sets out key data risk management recommendations for APRA-regulated entities in light of specific regulatory guidance in **CPG 235 Managing Data Risk** and data featuring as a key risk type in **CPS 234 Information Security** and more recently in **CPS 230 Operational Resilience**.

We take this opportunity to share key insights and themes from these reports, including important trends in the cyber threat landscape and recommendations for cyber risk management that should be of interest to all Australian businesses and directors moving into 2024 and beyond.

Overarching Themes and Recommendations

Growing threats in the cyber risk environment

Over the past year, there has been a significant increase in the frequency, cost, and severity of reported malicious cyber activity and data breaches.

Australian governments, critical infrastructure and businesses continue to be the targets of cybersecurity incidents and attacks. Critical infrastructure remains one of the key targets as these assets and networks hold sensitive information, maintain essential services, and often have high levels of connectivity with other organisations and critical infrastructure sectors. Government institutions and private businesses remain an enduring target for state actors seeking to extract sensitive and valuable data such as proprietary information, research, and personal information.

There are a multitude of risks and hazards for businesses to consider in the cybersecurity landscape. These range from unpatched vulnerabilities to the ability for attackers to move laterally between networks with the increasing interconnection of systems, through to sector interdependency that can compound the impacts of a single cyber-attack. While ransomware remains the most destructive threat, business email compromise, denial of service and data theft all cause significant impacts on Australian organisations. Existing risks in the threat environment are enhanced by growing cyber threats presented by emerging AI and Machine Learning applications, the billions of additional devices being connected to the internet as part of the Internet of Things, and the "most challenging geopolitical environment since the Second World War".

As cybercriminals constantly evolve their operations and tactics used, businesses must remain vigilant in relation to the cyber threat environment and potential hazards, and should continuously uplift their security practices to mitigate against existing and emerging risks that arise.

A key concern raised in recent cybersecurity reports is that data practices are often being performed as an additional standalone compliance exercise, rather than being consistently integrated into standard business activities, processes and practices.

Practical insights for risk mitigation

Key steps Australian organisations can take now to build cyber resilience include to:

- Implement a best practice cyber security framework like ASD's 'Essential Eight';
- Manage supply chain risks by clearly articulating cybersecurity expectations in contractual agreements with suppliers, and conducting comprehensive assessments of supplier cybersecurity posture, product accesses, and risks related to foreign control or interference.
- Prioritise the adoption of secure-by-design and secure-by-default products in procurement processes, and closely scrutinise the security controls of any new software, hardware, or Operational Technology before it is purchased (as well as the vendor's approach to patching and ongoing security).
- Regularly test cyber security detection, incident response, business continuity and disaster recovery plans. This includes practicing cyber incident response plans (e.g. via table top exercises) and treating a cyber incident as a 'when' not 'if' scenario in risk and business continuity planning.
- Implement robust cybersecurity measures for remote work solutions and conduct regular audits. Verify adherence to policies ensuring secure system usage, legal compliance, and protection of sensitive data.
- Train staff on cyber security matters, including by ensuring individuals implement good cyber hygiene practices such as enabling multi-factor authentication (MFA), utilising strong and unique passphrases, regularly updating software, backing up critical files, staying vigilant against phishing and scams, and reporting cybercrime incidents promptly.
- Confirm that operational technology and IT systems are, or can be, effectively segmented to prevent attackers from moving laterally between networks and reduce the risk of service interruptions during cyber incidents.

In more detail:

1. ASD Cyber Threat Report 2022-23

The Annual Cyber Threat Report published by the ASD (**ASD Report**) highlights the persistent challenged posed by malicious cyber activity and indicates that cyber-attacks have continued to increase in frequency, cost and severity.

Growing threats in the cyber risk environment

Key findings include:

- a 23% year-on-year increase in the number of reported cybercrimes (to approximately 94,000).
- a 14% rise in average cost of cybercrime per report, with averages reaching $46,000 for small businesses, $97,000 for medium businesses and $71,000 for large businesses;
- email compromise, business email compromise fraud, and online banking fraud are the top 3 reported cybercrimes for businesses. Additionally, state-sponsored cyber groups (actors conducting activity on behalf of a state) and hackers have increased assaults on Australia's critical infrastructure, businesses and homes;
- by sector, the Federal Government overwhelmingly had the highest number of reported cyber security incidents (30.7%) followed by state and local government (12.9%), possibly due to the heightened reporting obligations for government sectors compared to others. The professional, scientific and technical services sector was next (6.9%), with the information media and telecommunications sector falling out of the top five reporting sectors to seventh place (4.2%); and
- ongoing challenges for cybersecurity include complex information and communications technology (ICT) supply chains and advances in fields such as artificial intelligence.

Key cyber security trends in FY 2022-23 include:

- one in five critical security vulnerabilities were exploited by malicious cyber actors within 48 hours of public disclosure of a patch or mitigation advice being available. This means that 80% of vulnerabilities and exposures were exploited more than 48 hours after the patch or mitigation advice was published;
- Australian critical infrastructure was targeted via increasingly interconnected systems. Operational technology connected to the internet and into corporate networks provided opportunities for malicious cyber actors to attack these systems. Australian networks regularly experienced both opportunistic and deliberate malicious cyber activity, and a range of malicious cyber actors showed the intent and capability needed to compromise vital systems;
- State-based actors focused on critical infrastructure as part of ongoing information gathering campaigns or disruption activities. Cyber operations are increasingly the preferred means for state actors to conduct espionage and foreign interference, with government and critical infrastructure networks targeted as part of information-gathering campaigns or disruption activities across the globe; and
- cybercriminals continued to adapt tactics and seek new ways to extract maximum payment from victims and minimise their risk.

Practical insights for risk mitigation

In light of the cyber threat landscape, the ASD Report encourages Australian organisations to take additional steps to build cyber resilience, including by:

- implementing a best practice cyber security framework like ASD's Essential Eight;
- understanding and mapping their networks and maintain an asset registry to help manage devices on all networks, including OT;
- prioritising secure-by-design or secure-by-default products, and closely scrutinising the security controls of any new software, hardware, or OT before it is purchased as well as the vendor's approach to patching and ongoing security; and
- regularly practising their cyber incident response plans (e.g. via table top exercises) and treating a cyber incident as a 'when' not 'if' scenario in risk and business continuity planning.

2. Australia's 2023-2030 Cyber Security Strategy

The Cyber Security Strategy (**Strategy**) released by Australia's Cyber Security Minister is a roadmap intended to aid in realising the government's vision of becoming a "world leader in cyber security by 2030" and is described as a "whole-of-nation endeavour" to undermine cybercrime business models and put Australians in a strong position to respond effectively to cyber-attacks. The Strategy is supplemented by the 2023-2030 Australian Cyber Security Action Plan (**Action Plan**), which details the key initiatives that will commence over the next two years to begin the implementation of the Strategy.

Growing threats in the cyber risk environment

The Strategy calls out growing cyber threats presented by emerging AI and Machine Learning applications, the billions of additional devices being connected to the internet as part of the Internet of Things, and the "most challenging geopolitical environment since the Second World War". It also highlights opportunities presented by the challenging cyber environment, and intends to:

- help support small and medium businesses to strengthen their cybersecurity;
- encourage access to more well-paid cybersecurity jobs for Australians; and
- support Australia to play an important role in developing new security-enhancing products that could be exported around the world.

The Government's roadmap

In addition to AUD$2.3 billion of funding for existing cyber initiatives, the Government has committed AUD$586.9 million to implement the goals outlined in the Strategy, focused around six "cyber shields" designed to safeguard Australian businesses and citizens from cyber threats:

- Shield 1: strong businesses and citizens;
- Shield 2: safe technology;
- Shield 3: world-class threat sharing and blocking;
- Shield 4: protected critical infrastructure;
- Shield 5: sovereign capabilities; and
- Shield 6: resilient region and global leadership.

For each "cyber shield", the Strategy and Action Plan outlines the Government's desired outcomes and the initiatives it will take in order to reach these, including some interesting initiatives from a technology and cyber security legal perspective.

Highlights include plans to:

- legislate a "no-fault, no-liability" ransomware reporting obligation for businesses to encourage information sharing;
- build a ransomware playbook to provide clear guidance to businesses and citizens on how to prepare for, deal with, and recover from ransom demands;
- clarify the Government's expectations for cyber governance by Australian businesses;
- establish a new no-fault post-incident review mechanism for conducting lessons-learned reviews of significant cyber incidents;
- simplify mandatory cyber incident reporting processes;
- legislate a "limited use" obligation for ASD and the Cyber Coordinator to limit how information businesses share can be used by other Australian Government entities including regulators;
- clarify the scope of critical infrastructure regulation; and
- pressure-test critical infrastructure to identify vulnerabilities and build playbooks for incident response.

More generally, key actions proposed under the Strategy and Action Plan include:

Initiative	Proposed actions
Shield 1: Strong businesses and citizens *Focuses on support for businesses and individuals to strengthen their cyber resilience*	
Support small and medium businesses to strengthen their cyber security	• Create a cyber "health check" program for small and medium businesses to access free cyber maturity assessment
Work with industry to break the ransomware business model	• Work with industry to co-design options for a mandatory "no fault, no liability" ransomware reporting obligation for businesses to report ransomware incidents and payments
Provide clear cyber guidance for businesses	• Provide industry with additional information on cyber governance obligations under current regulation • Co-design with industry options to establish a Cyber Incident Review Board to conduct no-fault incident reviews to improve our cyber security
Make it easier for Australian businesses to access advice and support after a cyber incident	• Simplify incident reporting by considering options to develop a single reporting portal for cyber incidents to make it easier for affected entities to meet their regulatory reporting obligations
Shield 2: Safe technology *Aims to improve the safety of smart technologies*	
Ensure Australians can trust their digital products and software	• Adopt international security standards for consumer grade smart devices by working with industry to co-design a mandatory cyber security standard • Co-design a voluntary labelling scheme to measure the cyber security of smart devices, developed through consultation with industry and aligned to international exemplars • Co-design a voluntary cyber security code of practice for app stores and app developers to clearly communicate expectations of cyber security in software development and incentivise enhanced cyber security in consumer apps.
Protect our most valuable datasets	• Review Commonwealth legislative data retention requirements, including through implementation of the Government's response to the Privacy Act Review, reforms to enable use of Digital ID, and the National Strategy for Identity Resilience. • Work with industry to design a voluntary data classification model to help industry assess and communicate the relative value of their data holdings in a consistent way.
Shield 3: World-class threat sharing and blocking *Aims to create a whole-of economy threat intelligence network and scale threat blocking capabilities*	
Share strategic threat intelligence with industry	• Establish the Executive Cyber Council as a coalition of government and industry leaders to improve sharing of threat information across the whole economy. • Continue to enhance the ASD's existing threat sharing platforms to enable machine-to-machine exchange of cyber threat intelligence at increased volumes and speeds. These platforms will enable a framework within which industry-to-industry and government-to-industry cyber threat intelligence can be exchanged.
Shield 4: Protected critical infrastructure *Aims to better protect Australia's critical infrastructure*	
Clarify the scope of critical infrastructure regulation	• Align telecommunication providers to the same standards as other critical infrastructure entities by moving security regulation of the telecommunications sector from the Telecommunications Sector Security Reforms (TSSR) in the *Telecommunications Act 1997* to the SOCI Act • Clarify the regulation of managed service providers under the SOCI Act and delegated legislation. • Consult with industry on clarifying the application of the SOCI Act to ensure critical infrastructure entities are protecting their data storage systems where vulnerabilities to those systems could impact the availability, integrity, reliability or confidentiality of critical infrastructure
Strengthen cyber security obligations and compliance for critical infrastructure	• Activate enhanced cyber security obligations for Systems of National Significance–- including requirements to develop cyber incident response plans, undertake cyber security exercises, conduct vulnerability assessments, and provide system information to develop and maintain a near real-time threat picture.
Shield 5: Sovereign capabilities *Aims to grow and professionalise Australia's cyber workforce*	
Grow and professionalise our national cyber workforce	• Reform the migration system to increase Australia's competitiveness and attract highly skilled migrants to expand the cyber security workforce.

	• Provide guidance to employers to target and retain diverse cyber talent, with a focus on barriers and biases that dissuade under-represented cohorts – specifically women and First Nations people – from entering and staying in the workforce.
Shield 6: Resilient region and global leadership *Aims to build cyber resilience in the and uphold international cyber law standards*	
Support a cyber-resilient region as the partner of choice	• Pilot options to protect the Asia Pacific region at scale by partnering with Australia's regional neighbours and the private sector to leverage industry solutions to protect more people, systems and data from cyber threats.
Shape, uphold, and defence international cyber rules, norms and standards	• Uphold and improve the framework of responsible state behaviour in cyberspace, including how international law applies and best practice implementation of norms. • Work with international partners to deter and respond to malicious cyber activity, including publicly attributing and imposing sanctions on those who carry out or facilitate significant cyber incidents where there is sufficient evidence and it is in Australia's interests to do so.

Next steps and key timelines

The Strategy will be delivered across three "horizons", being:

- **Horizon 1 (2023-2025)**, which will focus on addressing critical gaps in Australia's "cyber shields", building better protections for Australia's most vulnerable citizens and businesses, and supporting improved cyber maturity uplift;
- **Horizon 2 (2026-2028)**, which will focus on scaling cyber maturity across the whole economy, through investments in the broader cyber ecosystem and growth of a diverse cyber workforce; and
- **Horizon 3 (2029-2030)**, which will aim for Australia to "advance the global frontier of cyber security", through leading the development of emerging cyber technologies capable of adapting to new risks and opportunities across the cyber landscape.

3. Critical Infrastructure Annual Risk Review

In the first Critical Infrastructural Annual Risk Review (**Review**), the Federal Government highlights key security risks that had an impact on Australia's critical infrastructure in the preceding 12 months, as well as those likely to arise in 2024.

The Review is framed around the four key hazard categories relevant to critical infrastructure as set out in the SOCI Act and CIRMP:

1. cyber and information security hazards;
2. personnel hazards;
3. physical security and natural hazards; and
4. supply chain hazards.

Growing threats in the cyber risk environment

Key threats to Australia's critical infrastructure security identified in the Review include:

- **Sector interdependency:** modern critical infrastructure systems are highly interconnected, exhibiting a "creeping dependency". As a result, this interconnection between sectors can escalate the impact of disruptions. This means that a disruption in one sector can have widespread consequences.
- **Cyber / information:** malicious cyber activities pose a significant threat to a wide range of critical infrastructure. Cyber actors are looking to exploit systemic weaknesses in systems to obtain valuable sovereign research and gain insights into Australia's social, economic, or technological vulnerabilities. The convergence of operational technology, information technology, and the Internet of Things has created an environment for cyber actors to move laterally through systems to reach their target, essentially providing greater avenues for exploitation.
- **Supply chains:** Australia's critical infrastructure heavily depends on international supply chains, with most critical components sourced from overseas providers. Critical infrastructure sectors have few contingencies to manage long-term shortages from foreign or single-source suppliers, which makes Australia vulnerable to supply chain changes, disruptions, malfunctions or sudden demand spikes. Failure, acquisition of, or foreign interference from, a vendor with critical intellectual property, original equipment, or software could significant impact Australia's critical infrastructure operation s. It is important to understand where critical components and services come from, and have adequate contingencies in place.

- **Physical:** espionage and foreign interference targeting Australia's critical infrastructure has the potential to compromise the physical security of critical infrastructure. All critical infrastructure providers may be targets for espionage and foreign interference (such as submarine cable landing stations that connect Australia to the rest of the world). Adversaries can utilise a range of tactics, including cyber operations, human intelligence, and data aggregation to infiltrate these systems. Systems may be intentionally targeted to spread misinformation and disinformation and erode public trust in the delivery of services. Misinformation and disruption may be spread to undermine confidence in the government's ability to deliver services. Grey zone attacks and foreign influence on corporate boards further add the complexity of the risks.
- **Natural hazards:** the increasing number and intensity of severe weather events, coupled with the unpredictability of climate-related risks, will create challenges for critical infrastructure providers. The interdependency between sectors will amplify the downstream impacts of natural hazards, requiring longer recovery periods.
- **Personnel:** personnel with access to, and privileged knowledge of, critical infrastructure, pose a significant vulnerability to critical assets and services. Disgruntled employees and insiders recruited by foreign actors are attractive targets for exploitation. The increased connectivity of work and personal devices, exacerbated by remote working trends, has created greater ease for insiders to remove data and provide access to third parties undetected. While vulnerability arises from high turnover of staff, there has also been increased leaking of sensitive information on online chat forums.

  The Review Identified that risk levels are very likely to increase during periods of heightened geopolitical tensions, as a result of infrastructure remaining an enduring target of interest for threat actors seeking to cause harm.

Future trends

Looking forward, the Review identifies the following areas of risk that are likely to have a heightened impact on Australia's critical infrastructure:

- rapid deployment of new technologies (such as generative AI);
- ongoing supply chain disruption leading to increased costs and delays;
- worsening staff shortages across all critical infrastructure sectors in the medium term;
- an increase in extreme weather events; and
- persistent cyber disruption with potential for larger and more disruptive breaches.

Practical insights for risk mitigation

To mitigate cybersecurity risks, key steps the Review indicates that critical infrastructure providers should take include:

- ensure separation of information technology and operational technology to limit the risk of cyber actors moving laterally through systems to reach their target (e.g. infiltrating the IT environment to gain access to the OT environment, where they can cause major disruptions to operational technology);
- acknowledge they are a high-interest target and that threat actors may seek out weaknesses in their systems to obtain valuable insights into Australia's economic and technological capabilities;
- carefully consider interdependencies with other critical infrastructure providers that may also be targets for threat actors, analyse cascading and compounding effects of a potential impact event and ensure this is reflected in the CIRMP;
- analyse supply chains to understand where critical components and services come from, limit the amount of sensitive data vendors have access to and ensure appropriate access controls are included in their arrangements with vendors; and
- educate personnel on contact reporting and security of personal and corporate devices given their increased risk of exposure to foreign actors including while travelling and be attentive in relation to online employee activity and dark web activity which may be targeting their personnel.

4. APRA multi-year data risk management study

APRA embarked on a multi-year pilot study with a selection of banks to gain insights into the status of data risk management. APRA's focus on data risk has intensified over the years due to the utility of quality data as a valuable asset for boards, management, and businesses for informed decision-making and improved business performance. As the cost of poorly managed data can have lasting negative impacts, APRA has highlighted that data management must be an ongoing area of focus for boards, management and businesses.

Practical insights for risk mitigation

Based on its findings from the study, APRA recommends that businesses enhance their data management practices by:

- **Establishing Unified Data Governance:** entities are encouraged to implement a unified data strategy within a robust data governance framework. The study showed organisations that established a "data office" for centralised coordination demonstrated consistent implementation and progress in governing data. Set definitions and parameters allowed consistent data activities across teams, making data management practices part of everyday operations.
- **Defining roles and responsibilities:** entities should provide clarity on roles and responsibilities of personnel within the organisation, ensuring clear ownership of critical data elements and processes throughout the data lifecycle.
- **Simplifying Technology Landscape:** entities are encouraged to simplify the technology and data architecture environment by adopting improved platform solutions and decommissioning legacy assets. The study noted that participants were shifting away from traditional structured approaches for storing and processing data that is better suited to meeting complex business requirements, with a focus on improving the quality of data and increasing linkages between data points.
- **Identifying Critical Data Elements:** entities should recognise critical data elements and establish a consistent set of data controls to ensure data integrity. To meet increasing data requirements, participants in the study adopted the concept of "data as a product", leveraging data domains to create ready-to-use datasets that were accessible throughout the organisation. These datasets were equipped with controls to maintain data quality, ensuring trusted and purpose-fit data for analysis, visualisation, and reporting.
- **Monitoring Data Quality:** entities should implement mechanisms for ongoing monitoring of data quality and prompt remediation of errors. The study identified that effective management of data risks showed a strategic approach to identifying, assessing, and remediating data issues, while addressing their root causes, often through strategic technological solutions.
- Integrating Data Management into Risk Frameworks: entities should seamlessly integrate data management risk considerations into broader risk management frameworks. The study identified that establishing better connections between data issues and Governance, Risk and Compliance (GRC) systems provided a comprehensive understanding of data risk and helped identify investment drivers across the organisation.

Where to from here?

From a litigation perspective, the heightened focus on cybersecurity and data protection is likely to cause an upward trend in cyber related disputes and investigations, including:

1. prosecutions led by the Australian Securities and Investments Commission (**ASIC**);
2. class actions on behalf of persons directly impacted by a data breach; and
3. class actions on behalf of shareholders who claim to be impacted indirectly by the data breach.

We expect litigation in this area to increase should Australia adopt a direct right of action for serious data breaches under Australia's Privacy Act (which does not exist under Australia's current laws).

We have already observed the beginnings of this trend, with four large scale data breach related matters having been commenced in the Federal Court of Australia and the Supreme Court of Victoria in the last year, each involving group members in the many millions.

Common themes among the class actions include assertions of non-compliance with privacy laws and regulations, and misleading conduct with respect to representations as to data security, meaning that cyber related class action risk is most concentrated for

entities storing significant amounts of data, and/or those trading subject to the restraints of the Australian Consumer Law. The resolution of these class actions and the associated risk for directors remains uncertain, given the Court's approach to the determination of questions as to liability and compensation, particularly in relation to the entitlement to compensation for distress and anxiety caused by a data breach, will be tested again in connection with some of these cases.

In the regulatory space, ASIC has signalled an escalation in the regulation of privacy and data protection, in addition to the prosecution for cybersecurity failures. Of particular concern to directors, ASIC announced in September 2023 that it considers that ensuring 'good cyber risk management' is in place, forms part of directors' duty to act with care and diligence under section 180 of the *Corporations Act 2001 (Cth)*. ASIC cautioned that boards that fail to prioritise cyber are exposing themselves to the (potential) risk of enforcement action by ASIC.

Relatedly, penalties under the Privacy Act or serious or repeated infringements on the privacy of an individual have also increased, indicative of the Government's broader attitude towards cybersecurity failures.

We are also witnessing an increase in the activity of the Office of the Australian Information Commissioner (**OAIC**), which on 19 October 2023 reported a 34% increase in privacy complaints. During 2022-23 alone, the OAIC launched significant investigations into a number of major corporations in relation to several massive data breaches affecting over half of the Australian population. Privacy Investigations were also opened into the personal information handling practices of a number of retailers, focusing on the companies' use of biometric technology.

The above matters each point to a busy year ahead in 2024 for cybersecurity related disputes and investigations.

Contact Us

Paul Forbes
Partner
paul.forbes
@bakermckenzie.com

Ryan Grant
Partner
ryan.grant
@bakermckenzie.com

Adrian Lawrence
Partner
adrian.lawrence
@bakermckenzie.com

Anne Petterd
Partner
anne.petterd
@bakermckenzie.com

Jarrod Bayliss-McCulloch
Special Counsel
jarrod.bayliss-mcculloch
@bakermckenzie.com

Simone Blackadder
Special Counsel
simone.blackadder
@bakermckenzie.com

Tayler Wright
Senior Associate
tayler.wright
@bakermckenzie.com

Thank you to Saad Rao, Kirsten Foley and Liz Grimwood-Taylor for your assistance in preparing this alert.