Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2025

Definitive global law guides offering comparative analysis from top-ranked lawyers

Contributing Editor
Christian Schröder
Orrick

Chambers

Global Practice Guides

Cybersecurity

Contributing Editor

Christian Schröder

Orrick

2025

Chambers Global Practice Guides

For more than 20 years, Chambers Global Guides have ranked lawyers and law firms across the world. Chambers now offer clients a new series of Global Practice Guides, which contain practical guidance on doing legal business in key jurisdictions. We use our knowledge of the world's best lawyers to select leading law firms in each jurisdiction to write the 'Law & Practice' sections. In addition, the 'Trends & Developments' sections analyse trends and developments in local legal markets.

Disclaimer: The information in this guide is provided for general reference only, not as specific legal advice. Views expressed by the authors are not necessarily the views of the law firms in which they practise. For specific legal advice, a lawyer should be consulted.

Content Management Director Claire Oxborrow
Content Manager Jonathan Mendelowitz
Senior Content Reviewer Sally McGonigal, Ethne Withers, Deborah Sinclair and Stephen Dinkeldein
Content Reviewers Vivienne Button, Lawrence Garrett, Sean Marshall, Marianne Page, Heather Palomino and Adrian Ciechacki
Content Coordination Manager Nancy Laidler
Senior Content Coordinators Carla Cagnina and Delicia Tasinda
Content Coordinator Hannah Leinmüller
Head of Production Jasper John
Production Coordinator Genevieve Sibayan

Published by
Chambers and Partners
165 Fleet Street
London
EC4A 2AE
Tel +44 20 7606 8844
Fax +44 20 7831 5662
Web www.chambers.com

Copyright © 2025
Chambers and Partners

INTRODUCTION

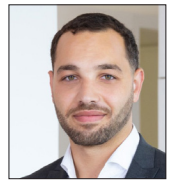
Contributed by: Christian Schröder and Odey Hardan, **Orrick**

Orrick is a global law firm dedicated to serving the technology and innovation, energy and infrastructure, finance, and life sciences and healthtech sectors. With more than 1,100 lawyers across 25+ markets worldwide, Orrick provides forward-looking, pragmatic advice on transactions, litigation, and compliance matters. As one of the world's leading tech law firms, cybersecurity and privacy are central to Orrick's practice. The firm has 15 cybersecurity and privacy-focused partners and over 50 specialised lawyers, making it one of the strongest data protection practices in the market, recognised by Chambers Global, US, and Europe. Orrick helps clients navigate the complex cybersecurity and privacy legal landscape, managing global compliance matters, cyber incidents, litigation, and regulatory investigations. They maximise data value, address global privacy requirements, and reduce security risks. Whether clients are managing compliance challenges, licensing data, or acquiring new companies, Orrick offers forward-thinking solutions to address data challenges.

Contributing Editor

Christian Schröder is a partner in Orrick's Düsseldorf office and leads the firm's Cyber, Privacy & Data Innovation Group in Europe. He collaborates with team members across the USA, EU, and Asia to support global clients. Christian specialises in data-focused laws, including cybersecurity, privacy compliance, incident response, data licensing, AI, and regulatory investigations. He advises on internal and external data transfers, product launches, and privacy requirements for connected cars. Christian maintains strong relationships with German and EU data protection authorities, effectively defending clients in investigations. Recognised by Chambers as a top practitioner, he is a noted thought leader in privacy law.

Co-Author



Odey Hardan is an associate in Orrick's Cyber, Privacy & Data Innovation Group. He provides comprehensive advice on data law and EU digital law, offering strategic guidance to clients and representing them before regulatory authorities and in court proceedings. Prior to joining Orrick, Odey served as a research assistant focusing on European law, authoring several academic papers. During his doctoral studies, he specialised in European, international, and data protection law.

INTRODUCTION

Contributed by: Christian Schröder and Odey Hardan, **Orrick**

Orrick, Herrington & Sutcliffe LLP

Heinrich-Heine-Allee 12
40213 Düsseldorf
Germany

Tel: +49 211 3678 7316
Email: cschroeder@orrick.com
Web: www.orrick.com

Introduction to the Cybersecurity Guide

In recent years, cybersecurity has become a paramount concern for legal professionals, policymakers, and businesses. The increasing frequency and sophistication of cyberattacks have prompted jurisdictions worldwide to enact comprehensive legal frameworks to protect digital infrastructures and ensure the safety of personal and non-personal data.

The recent wave of cybersecurity regulations reflects a global recognition of the critical importance of safeguarding digital assets. These regulations have significant implications for businesses. They underscore the necessity for comprehensive risk management strategies, accountability at the highest levels of management, and the implementation of rigorous security measures across all sectors.

One of the primary implications of these regulations is the heightened accountability placed on organisational leadership. With the mandate for senior executives to oversee cybersecurity measures, laws aim to ensure that cybersecurity is prioritised at the strategic level. This shift in responsibility requires a cultural change within organisations, where cybersecurity is integrated into the core business strategy rather than treated as a peripheral IT issue.

Furthermore, the emphasis on incident reporting and transparency has profound implications for how organisations handle data breaches and cyber incidents. Timely reporting to regulatory authorities and affected parties is not only a legal obligation but also a critical component of maintaining trust and credibility. Organisations must develop clear protocols for incident response and communication to comply with these requirements.

The focus on supply chain security and the resilience of critical infrastructures highlights the interconnected nature of modern digital ecosystems. Cybersecurity cannot be viewed in isolation; it requires an inclusive approach that involves stakeholders across the supply chain. This interconnectedness of services necessitates that organisations conduct thorough assessments of their third-party relationships and implement stringent security controls to mitigate risks.

The European Union (EU) has implemented a series of directives and regulations aimed at enhancing the security of its digital market.

One of the cornerstone laws in the EU's cybersecurity framework is the Network and Information Security Directive (NIS2). The NIS2 Direc-

Contributed by: Christian Schröder and Odey Hardan, **Orrick**

tive applies to companies in sectors deemed critical and listed in Annex I and II of the Directive, including digital infrastructure and certain manufacturing industries. Specifically, it affects entities such as internet node operators, DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, and providers of publicly accessible electronic communication services. Additionally, digital service providers like online search engines, online marketplaces, and social networks, as well as manufacturers of electrical equipment, data processing devices, medical devices, and those in the machinery and automotive industries, are also covered. This directive sets out obligations for essential and important entities, such as digital service providers and operators of critical infrastructure, to implement risk management measures, conduct regular cybersecurity audits, and report significant incidents to national authorities. By holding management bodies accountable for compliance, NIS2 ensures that cybersecurity is prioritised at the highest levels of organisational leadership.

In addition to NIS2, the EU has introduced the Digital Operational Resilience Act (DORA), which targets the financial sector. The regulation addresses the critical role of information and communication technologies (ICT) in the financial sector, the vulnerabilities to cyber threats, and the dependencies on external service providers. DORA requires financial entities and critical ICT providers to establish comprehensive ICT risk management frameworks and mandates regular testing of digital operational resilience. This framework should address ICT risks and ensure high digital operational resilience. It must include strategies, policies, procedures, protocols, and applications necessary to protect all information and ICT assets. The principle of proportionality and a risk-based approach are emphasised in DORA, requiring the framework to be tailored to the company's processes and technical means. To maintain a high level of protection, financial entities must continuously test their digital operational stability. They must develop a programme to assess their defensive readiness, identify vulnerabilities, and implement corrective measures. Tests should be conducted by independent internal or external parties, with sufficient resources provided to avoid conflicts of interest.

The Cyber Resilience Act (CRA) further complements the EU's cybersecurity framework by addressing the security of products with digital elements. The CRA imposes life cycle security obligations on manufacturers, importers, and distributors, requiring them to conduct cyber-risk assessments, manage vulnerabilities, and report security incidents to the European Union Agency for Cybersecurity (ENISA) within specified timeframes. By focusing on the security of digital products, the CRA aims to mitigate vulnerabilities and enhance user trust in the digital marketplace. The draft CRA complements other legislation like NIS2. It applies to all products connected to other devices or networks, with some exclusions such as open-source software and certain regulated services (eg, medical devices, aviation, and cars).

One of the key challenges in cybersecurity regulation is the harmonisation of standards across jurisdictions. While the EU has made strides in creating a unified cybersecurity framework, achieving global consensus remains a complex task. Differences in legal systems, regulatory approaches, and levels of technological development can hinder efforts to establish common standards. However, international co-operation and dialogue are essential to overcoming these

Contributed by: Christian Schröder and Odey Hardan, **Orrick**

barriers and creating a cohesive global cybersecurity strategy.

Another challenge lies in the integration of emerging technologies, such as artificial intelligence (AI) and the Internet of Things (IoT), into existing cybersecurity frameworks. These technologies offer tremendous potential for innovation but also introduce new vulnerabilities that must be addressed. The EU's AI Act, for example, sets standards for the design and operation of AI systems to ensure they are resilient to errors and secure against unauthorised alterations. As technology continues to evolve, legal frameworks must be adaptable to accommodate new developments and address emerging threats.

Public-private partnerships also play a crucial role in enhancing cybersecurity. By collaborating with private sector entities, governments can leverage the expertise, resources, and innovation of industry leaders to strengthen cybersecurity defences. These partnerships facilitate the sharing of best practices, threat intelligence, and technical expertise, leading to more resilient digital infrastructures.

In the EU, initiatives such as the European Cybersecurity Organisation (ECSO) and the European Cybersecurity Competence Centre (ECCC) exemplify the importance of public-private collaboration. These organisations bring together stakeholders from government, industry, and academia to promote research, innovation, and capacity building in cybersecurity. By fostering a collaborative approach, the EU aims to create a secure digital environment that supports economic growth and protects citizens' rights.

For legal professionals, navigating the complexities of cybersecurity law requires a deep understanding of both the regulatory landscape and the technical aspects of cybersecurity. The path forward involves balancing innovation with regulation, ensuring that legal frameworks are both comprehensive and adaptable to emerging threats. By focusing on the implications of recent regulations and adopting forward-thinking strategies, governments and organisations can enhance their cybersecurity defences and protect their digital assets.

AUSTRALIA

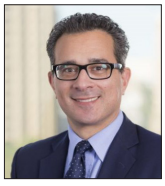
Law and Practice

Contributed by:
Dennis Miralis and Jack Dennis
Nyman Gibson Miralis

Contents

Nyman Gibson Miralis is a market leader in all aspects of general, complex and international criminal law and is widely recognised for its involvement in some of Australia's most significant cases. The firm's team in Sydney has expertise in dealing with complex national and international cybercrime investigations and advising individuals and businesses who are the subject of cybercrime investigations. Its expertise includes dealing with law enforcement requests for information from foreign jurisdictions, challenging potential extradition proceedings as well as advising and appearing in cases where assets have been restrained and confiscated worldwide.

Authors



Dennis Miralis is a partner at Nyman Gibson Miralis and a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional investigations and criminal prosecutions. His areas of expertise include cybercrime investigations, anti-bribery and corruption, global tax investigations, proceeds of crime, anti-money laundering, worldwide freezing orders, national security law, INTERPOL Red Notices, extradition and mutual legal assistance law. In 2021 Dennis was awarded a certificate of completion for the "Cybersecurity: The Intersection of Policy and Technology" programme, January 2021, John F. Kennedy School of Government at Harvard University, Executive Education.

Jack Dennis is a senior criminal defence lawyer who practises in international and domestic criminal, corporate and tax law at Nyman Gibson Miralis. His international criminal work includes transnational criminal and regulatory investigations, liaising with foreign legal and regulatory bodies, as well as advising clients on matters concerning international public law. Domestically, Jack has advised on a range of criminal issues and investigations, including white-collar crime, fraud, sanctions, INTERPOL, extraditions and national security. He also has significant international, corporate and tax experience, having advised on cross-border transactions and disputes involving foreign and domestic corporations and individuals, across the software, financial services and crypto industries.

Nyman Gibson Miralis

Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 292 648 884
Email: dm@ngm.com.au
Web: www.ngm.com.au

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

On 22 November 2023 the Australian government released the 2023-2030 Australian Cyber Security Strategy (the "Strategy"), with the aim of strengthening Australia's cyber defences and supporting people and businesses to be resilient to and recover quickly from cyber-attacks.

Alongside the Strategy was the 2023-2030 Australian Cyber Security Strategy: Action Plan (the "Action Plan") setting out three "Horizons", which culminate in Horizon 3 with Australia as a leader of the global frontier in developing cyber technologies and adapting to risk and opportunities. Currently, Australia is in the final year of Horizon 1 ("Strengthen our foundations") whereby it is aiming to address critical gaps, build protections and support "initial cyber maturity uplift", with the government setting itself up for Horizon 2 ("Expand our search") come 2026, which aims to scale cyber maturity across the whole economy, make investments and grow a diverse cyber workforce.

The government has grounded its vision in six "shields" or "layers of defence" comprising the businesses and citizens, safe technology, world-class threat sharing and blocking, protected critical infrastructure, sovereign capabilities, and resilient region and global leadership. It has set out in its Action Plan different actions and objectives for each shield, some of which can be seen through recent reform and others not.

Notwithstanding 2025 is the final year of Horizon 1, it is also the first year that the Action Plan is set to be reviewed; and with the Federal election to take place by May 2025, there may be some changes to the strategy, purposes and actions to come.

1.2 Cybersecurity Laws

Australia has a broad system of federal, state and territory-based laws which govern data protection, cybersecurity and cybercrime.

Data Protection

Entities dealing with personal information in Australia should also be aware of their obligations with respect to:

- the Privacy Act 1988 (Cth) (the "Privacy Act"), which regulates the handling of personal information by "APPs entities" pursuant to the Australian Privacy Principles (APPs);

- the Digital ID Act 2024 (Cth) (the "Digital ID Act"), which is intended to embed safeguards for digital ID services and data in addition to the Privacy Act;
- privacy legislation enacted at the state and territory level;
- the My Health Records Act 2012 (Cth) (the "My Health Records Act"), which imposes specific obligations for health information collected and stored in Australia's national online health database (in addition to the Privacy Act);
- state and territory health records legislation enacted in NSW, Victoria (Vic) and the Australian Capital Territory (ACT); and
- federal, state and territory surveillance legislation, which regulates video surveillance, computer and data monitoring, GPS tracking and the use of listening devices on individuals.

Further definitions and details on the Privacy Act are set out in **6.1 Cybersecurity and Data Protection**.

Cybersecurity

Cybersecurity laws in Australia are primarily governed under sector-specific federal laws, and include the following.

- Critical infrastructure: this sector is regulated under the Security of Critical Infrastructure Act 2018 (Cth) (the "SOCI Act"), which imposes registration, reporting and notification obligations on owners and operators of critical infrastructure and empowers the Australian government to gather information and issue directions where there is a risk to security. More details are in **2. Critical Infrastructure Cybersecurity**.
- Telecommunications: this sector is regulated by dual legislation, being:
  (a) the Telecommunications Act 1997 (Cth) (the "Telecommunications Act"), which imposes security and notification obligations on Australian telecommunications providers and empowers the Australian government to gather information and issue directions; and
  (b) the Telecommunications (Interception and Access) Act 1979 (Cth) (the "TIA Act"), which prohibits the interception of communication and access to stored communication data, except for certain law enforcement and national security purposes.
- Corporate: corporations generally are regulated under the Corporations Act 2001 (Cth) (the "Corporations Act"), which is highly relevant to the cybersecurity space. For example, the director's duty to exercise "care and diligence" (Section 180) is equally relevant here.
- Financial services: certain financial, insurance and superannuation entities are regulated through standards, including the Prudential Standard CPS 234 on Information Security (CPS 234), issued by the Australian Prudential Regulation Authority (APRA). Additionally, entities in the financial services have specific obligations under the Corporations Act, such as adequate risk management systems to hold a financial licence (Section 912A).

There are additional laws that are highly relevant to the cybersecurity space that are less sector-specific, such as consumer law, specifically the Competition and Consumer Act 2010 (Cth) (the "Consumer Act") which addresses consumer affairs, including consumer data protection and cyberscams.

Cybercrime

Overlaying the above are various cybercrime offences in Australia at the federal, state and ter-

ritory levels. These offences broadly encompass two categories:

- offences that are directed at computers or other devices and involve hacking-type activities; and
- cyber-enabled offences where such devices are used as a key component of the offence, including in online fraud, online child abuse offences and cyberstalking.

Federally, cybercrime is criminalised under Parts 10.6 and 10.7 of the Schedule to the Criminal Code Act 1995 (Cth) (the "Criminal Code"), which set out a variety of offences with maximum penalties ranging from fine-only through to life imprisonment.

Organisations should note that in addition to the Criminal Code:

- the TIA Act also makes it a federal offence for an individual to (without authorisation) intercept or access private telecommunications without the knowledge of those involved; and
- state and territory laws criminalise computer offences similar to those criminalised under the Criminal Code (eg, Part 6 of the Crimes Act 1900 (NSW) provide for multiple computer offences regarding unauthorised access, modification or impairment of restricted data and electronic communications).

Australian states and territories also have their own criminal laws which govern cybercrime offences.

Other Laws

Areas that are also related to cybersecurity include:

- the Broadcasting Services Act 1992 (Cth) (the "Broadcasting Act") regulates broadcasting services through internet and other means in Australia and enables the creation of industry codes of practice regulating the content of such services;
- the Online Safety Act 2021 (Cth) (OSA) establishes complaint systems for cyberbullying of children, non-consensual sharing of intimate images, cyber-abuse of adults, and the online/social media availability of content that would be subject to broadcasting classifications (restricted or age 18 years and over);
- The Spam Act 2003 (Cth) (the "Spam Act") prohibits the use of electronic communications for the purpose of sending unsolicited marketing materials to individuals; and
- The Do Not Call Register Act 2006 (Cth) (the "DNCR Act") prohibits unsolicited telemarketing calls being made to phone numbers registered on a Do Not Call Register.

1.3 Cybersecurity Regulators

Australia has a range of federal, state and territory regulators and agencies which deal with cybersecurity.

The overarching government agencies are:

- the Department of Home Affairs (DoHA); and
- the Australian Signals Directorate (ASD).

The key regulators and enforcement bodies include:

- the Office of the Information Commissioner (OAIC);
- the Critical Infrastructure Centre (CIC);
- the Australian Communications and Media Authority (ACMA);
- the Australian Securities and Investments Commission (ASIC);

- the Australian Prudential Regulation Authority (APRA); and
- the Australian Competition and Consumer Commission (ACCC).

Specifically in relation to criminal enforcement, the following regulators are key:

- the Australian Federal Police (AFP);
- the Commonwealth Director of Public Prosecutions (CDPP);
- the Australian Security Intelligence Organisation (ASIO);
- the Australian Transaction Reports and Analysis Centre (AUSTRAC); and
- the Australian Criminal Intelligence Commission (ACIC).

Each of the above are addressed below.

Overarching Government Agencies

DoHA

The DoHA is the lead government department for cyberpolicy. The DoHA develops cybersecurity and cybercrime law and policy, implements Australia's national cybersecurity strategy and responds to international and domestic cybersecurity threats and opportunities, including in the areas of critical infrastructure and emerging technologies. The DoHA also has responsibility for cybersecurity and cybercrime operational agencies including the AFP, ACIC, AUSTRAC, and ASIO.

ASD, ACSC and CERT

The ASD is Australia's operational lead on cybersecurity and plays both a signals intelligence and information security role. The ASD undertakes cyberthreat monitoring and conducts defensive, disruption and offensive cyber-operations offshore to support military operations and to counter terrorism, cyber-espionage and serious cyber-enabled crime. The ASD also advises and co-ordinates operational responses to cyber-intrusions on government, critical infrastructure, information networks and other systems of national significance.

Within the ASD sits the Australian Cyber Security Centre (ACSC). The ACSC drives cyber-resilience across the whole Australian economy including with respect to critical infrastructure, government, large organisations and small to medium businesses, academia, NGOs and the broader Australian community. The ACSC provides general information, advice and assistance to Australian organisations and the public on cyberthreats and it collaborates with business, government and the community to increase cyber-resilience across Australia.

The ACSC also runs the Computer Emergency Response Team (CERT), which provides advice and support to industry on cybersecurity issues affecting Australia's critical infrastructure and other systems of national significance.

Other key government bodies

At this juncture, the following should also be noted.

- The Attorney-General's Department (AGD) advises government on cybersecurity policies and law, including in relation to human rights, privacy, protective security, international law, administration of criminal justice, and oversight of intelligence, security and law enforcement agencies.
- The Department of Defence (DoD) contributes to Australia's whole-of-government cybersecurity policy and operations and houses ASD; it also houses the Information Warfare Division, which develops information warfare

capabilities for the Australian Defence Force (ADF).
- The Department of Foreign Affairs and Trade (DFAT) advances Australia's international cyber-affairs agenda, which includes digital trade, cybersecurity, cybercrime, international security, internet governance and co-operation, human rights and democracy online, and technology for development.

Data Protection and Privacy

The OAIC is the federal privacy and information regulator with a range of functions and powers to investigate and resolve privacy complaints, enforce privacy compliance, make determinations and provide remedies for breaches under the notifiable data breach (NDB) scheme. The OAIC operates by reference to the Privacy Act, the My Health Records Act, the Telecommunications Act, the TIA Act, and recently the Digital ID Act.

The remedies range from enforceable undertakings to civil penalties of 2,000 penalty units (approximately AUD626,000); but may also involve imprisonment. Since December 2022, serious and repeated interferences with privacy may attract a penalty of up to:

- for entities, not body corporates – AUD2.5 million; or
- for body corporates – the greater of AUD50 million, three times the value of the benefit attributable to the conduct or 30% of the adjusted turnover for the relevant period.

There are also state and territory privacy commissioners which administer state and territory-based privacy and health information laws. These include:

- the NSW Information and Privacy Commission who administers, inter alia, the Privacy and Personal Information Protection Act 1998 (NSW) and Health Records and Information Privacy Act 2002 (NSW); and
- the Office of the Victorian Information Commissioner who administers the Privacy and Data Protection Act 2014 (Vic) and the Victorian Health Complaints Commissioner handles breaches of the Health Records Act 2001 (Vic).

Critical Infrastructure Cybersecurity

The CIC is part of the DoHA and is the federal regulator of the SOCI Act and certain provisions of the Telecommunications Act with powers to investigate, audit and enforce on compliance matters.

The CIC also has the ability to make recommendations to DoHA and the Home Affairs Minister on whether their information-gathering powers and directions powers should be exercised. The CIC also has enforcement powers which allows it to issue penalties for non-compliance that range from performance injunctions, enforceable undertakings, civil penalties of up to 250 penalty units (AUD78,250) or seek two years' imprisonment.

Telecommunications, Broadcasting and Marketing Cybersecurity

The ACMA is Australia's regulator for broadcasting, telecommunication and certain online content and provides licensing to industry providers. ACMA has specific regulatory powers under the Telecommunications Act, the TIA Act, the Spam Act, and the DNCR Act to investigate and resolve complaints and enforce compliance. In dealing with non-compliance, ACMA is empowered to issue warnings, infringement notices, enforceable undertakings and remedial directions. ACMA

is further able to cancel or impose conditions on licences and accreditations. ACMA also has the ability to commence civil proceedings or refer matters for criminal prosecution.

Additionally, the Office of the eSafety Commissioner (the "eSafety Commissioner") has powers to promote and regulate online safety with respect to telecommunications, broadcasting and other online industries. However, the eSafety Commissioner cannot investigate matters of cybercrime. Penalties range from takedown notices and blocking directions.

Corporations, Consumers and Financial Services Cybersecurity

The ASIC is Australia's corporate, market and financial services regulator, is empowered under the Corporations Act to investigate and bring actions against corporations, directors and officers for non-compliance with the Corporations Act, which, in some circumstances, may involve cybersecurity issues. It regulates publicly listed corporations under the Corporations Act and may investigate issues which touch on cybersecurity.

The APRA regulates certain finance, banking, insurance and superannuation entities and issued information security standards CPS 234. APRA has powers to supervise, monitor and intervene in matters of cybersecurity for regulated entities and has a range of enforcement powers to deal with breaches of its standards. Such powers involve APRA issuing infringement notices, providing directions or enforceable undertakings, imposing licensing conditions, disqualifying senior officials and commencing court-based action.

The ACCC is Australia's competition regulator and consumer protector, may, where appropriate, undertake enforcement action against breaches of the Consumer Act, including breaches involving cybersecurity, cybercrime and cyberscam issues. The ACCC additionally:

- administers the Consumer Data Right (CDR) regime;
- co-regulates (with OAIC) the Digital ID Act; and
- hosts the Scamwatch website which provides public information, alerts and access to complaints mechanisms on a wide range of consumer scams, including scams perpetrated online.

Also relevant for the financial sector is that OAIC regulates the aspects of the Privacy Act which deal with credit reporting obligations and the credit reporting code, which imposes certain conditions on entities that hold credit-related personal information.

Cybercrime

Cybercrime at the federal level is investigated and enforced by the AFP and prosecuted by the CDPP. The AFP have a dedicated cybercrime operations team comprising investigators, technical specialists and intelligence analysts who operate across multiple jurisdictions to conduct cyber-assessments and to triage, investigate and disrupt cybercrime.

More specifically:

- ACIC is Australia's national criminal intelligence agency – it has broad investigative and coercive powers and shares information between all levels of law enforcement;
- AUSTRAC is the domestic watchdog for Australia's anti-money laundering and counter-terrorism measures – it supports law

enforcement operations involving cybercrime financing; and
- ASIO investigates cyber-activity involving espionage, sabotage and terrorism related activities – ASIO also contributes to the investigation of computer network operations directed against Australia's systems.

State and territory-based police and prosecution agencies investigate, enforce and prosecute state and territory cybercrimes.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

Australia's critical infrastructure and assets are regulated through Commonwealth, state and territory legislation, with a particular emphasis on the SOCI Act. That said, there is broader legislation, such as the Privacy Act and Cyber Security Act, and more sector-specific legislation, such as the Telecommunications Act, that cannot be ignored.

SOCI Act (and TSSR)

The SOCI Act currently regulates certain assets across eleven sectors: communications, data storage and processing, financial services, energy, food and grocery, health and medical, higher education and research, space technology, transport, water and sewerage, and the defence industry. And from November 2025, telecommunications security obligations (which are currently under the Telecommunication Sector Security Reforms (TSSR)) will be moved into the SOCI, a change implemented by the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 (Cth) (the "2024 SOCI Amendment Act").

Notwithstanding recent reforms which clarified the SOCI Act, the exact parameters of the legislation are broad and complex, and extend to various participants in a supply chain including "responsible entities", "reporting entities", "direct interest holders", "managed service providers" and "operators". Some of these definitions are asset-specific, but for our purposes, it is important to note that a "responsible entity" is generally the entity that owns, is licensed or otherwise responsible for operating the asset.

Further, despite the imminent shift of the TSSR and its obligations to the SOCI Act, these obligations still remain in force and apply to the relevant infrastructure as is. The TSSR are applicable to carriers, carriage service providers and carriage service intermediaries.

Cyber Security Act

Additionally, there are cybersecurity obligations imposed on critical infrastructure under the Cyber Security Act where they constitute "a reporting business entity".

A "reporting business entity" is an entity that:

- is carrying on a business in Australia with an annual turnover for the previous financial year that exceeds the "turnover threshold for that year" (to be determined) but is not a Commonwealth body, State body, or responsible entity for a critical infrastructure asset; or
- a responsible entity for a critical infrastructure asset "to which Part 2B of the Security of Critical Infrastructure Act 2018 applies", which is defined in the rules or declaration – at the time of writing, these were prescribed in Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022 (the "SOCI Application Rules") and includes most infrastructure assets.

2.2 Critical Infrastructure Cybersecurity Requirements

The SOCI Act imposes requirements on owners and operators of assets across various fields. The exact requirements vary depending on the particular asset/industry; however, may include a requirement to:

- register with the Register of Critical Infrastructure Assets;
- provide ownership and operational information;
- notify the government of certain cyber-incidents;
- implement and comply with a critical infrastructure risk management programme (CIRMP); and
- if they have "business critical data" processed or stored by a third party on a commercial basis, they must take reasonable steps to notify that third party.

Further still, the SOCI Act and associated rules impose enhanced cybersecurity obligations on assets designated as "systems of national significance" (SoNS). These must be assets that are already considered a "critical infrastructure asset", but also that they are of "national significance". These designations are private and confidential so as to avoid publicising their significance to malicious actors. Reports indicate that over 200 systems have been designated to date.

A responsible entity for a SoNS may be required to:

- fulfil statutory response planning obligations;
- undertake a cybersecurity exercise (see **3.6 Threat-Led Penetration Testing**);
- undertake a vulnerability assessment (see **3.6 Threat-Led Penetration Testing**); and
- where the system is a computer or needs a computer to operate the system, undertake periodic reports, provide event-based reports or install software that transmits system information to the ASD.

It is also worth noting that the SOCI Act also includes:

- an information gathering power for the Secretary of the DoHA to monitor compliance; and
- a directions power for the Home Affairs Minister to direct regulated entities to do or not do a specified thing that is reasonably necessary to protect critical infrastructure from national security risks.

2.3 Incident Response and Notification Obligations

Mandatory Incident Reporting Obligations

SOCI Act

As mentioned above, the SOCI Act and associated rules impose reporting obligations on various entities.

Responsible entities must report cybersecurity incidents that have a significant or relevant impact on their asset. In other words, a "responsible entity" must make a report when it becomes aware of the following.

- A "cyber security incident" that "has had, or is having, a significant impact (whether direct or indirect) on the availability of the asset" – such a "significant impact" is defined as being where "the incident has materially disrupted the availability of [the] essential goods or service" in connection with which the asset is used to provide. The report must be made "as soon as practicable, and in any event within 12 hours, after the entity becomes aware". If the initial report is oral, then a writ-

ten report must be made within 84 hours after the oral report is given.
- A "cyber security incident" that "has had, or is having, or is likely to have, a relevant impact on the asset" – such a "relevant impact" is defined (for critical infrastructure assets) as a (direct or indirect) impact on the availability, integrity, reliability of the asset, or on the confidentiality of information about the asset, information stored on the asse or computer data constituting the asse. The report must be made "as soon as practicable, and in any event within 72 hours, after the entity becomes aware. If the initial report is oral, then a written report must be filed within 48 hours of the oral report.

A "cyber security incident" is the:

- unauthorised access to or modification of computer data or computer program;
- unauthorised impairment of electronic communications to or from a computer (but does not include "a mere interception of any such communication"); or
- unauthorised impairment of the availability, reliability, security or operation of computer data, a computer program or a computer.

Either of these reports must be given to the ASD (unless another relevant Commonwealth body is specified in the rules). Failure to make a report at all or in writing, or in the approved form, can each be punished by an AUD16,500 fine.

Cyber Security Act

Irrespective of whether the cybersecurity incident meets the above significance or relevance thresholds, most critical infrastructure assets (being "a reporting business entity") have additional reporting obligations under the Cyber Security Act.

In summary, there is an obligation to report to the ASD (or other designated Commonwealth agency) where:

- there is a cybersecurity incident that has had, is having, or could reasonably be expected to have a (direct or indirect) impact on a reporting business entity;
- an entity (the extorting entity) demands a benefit; and
- the reporting entity (or a third party on their behalf) makes the ransomware payment.

Such a report must be given with 72 hours of the reporting business entity becoming aware of the payment and must contain certain information.

A "cyber security incident" for these purposes broader than under the SOCI Act as it not only includes any such incident that falls within the scope of the SOCI Act, but is presumed to include any incident:

- involving unauthorised impairment of electronic communication to or from a computer (per the SOCI Act) including mere interception of any such communication; and
- where the incident is (actually or is reasonably expected to be) effected by means of "telegraphic, telephonic or other like service", if the incident (actually, probably, or it is reasonable to expect it) impeded or impaired "the ability of a computer to connect to such a service" or the incident (probably or is reasonably expected to have) prejudiced Australia's social/economic stability, defence or national security.

Voluntary Incident Reporting Obligations

The ACSC has a cyber-incident reporting portal through which critical asset owners are encour-

aged to voluntarily report cybersecurity incidents.

Any impacted entity carrying or a business in Australia or otherwise a responsible entity for critical infrastructure is now being statutorily encouraged to make voluntary reports to the NCS Coordinator under the Cyber Security Act, even where it is unclear if an incident is a cybersecurity incident.

Other Mandatory Reporting Obligations

Other reporting obligations under the SOCI Act for critical infrastructure assets include:

- taking reasonable steps to notify a third-party entity if that third party is processing or storing "business critical data" on a commercial basis;
- an ongoing obligation on a "reporting entity" to report a "notifiable event" in relation to an asset usually within 30 days after the event occurs, which relates to changes in the operational information and interest/control information in relation to "director interest holders", or the status of an entity as a reporting entity; and
- reporting if a hazard had significant relevant impacts on a critical infrastructure asset.

See additionally relevant obligations in **6.1 Cybersecurity and Data Protection**.

Criminal Offences

Related to infrastructure, Part 10.6 of the Criminal Code places obligations on providers of content or hosting services to notify the AFP as to the existence of material displaying "abhorrent violent conduct" (if occurring in Australia) and, in any event, to expeditiously remove or cease to host such material.

2.4 State Responsibilities and Obligations

The Australian government considers "the responsibility for ensuring the continuity of operations and the provision of essential services to the Australian economy and community" as being shared "between owners and operators of critical infrastructure, state and territory governments and the Australian Government".

Generally speaking, government bodies may also be captured within the scope of legislative regimes such as the Privacy Act, and therefore have the same (or similar) obligations as their private-sphere counterparts. However, the SOCI Act does not apply to the Commonwealth or a body corporate established under Commonwealth law unless so declared or prescribed.

The Australian government is responsible for the "final defence" of Australian infrastructure and cybersecurity. To this end, the SOCI Act grants the Minister last resort "government assistance measures" and powers where a cybersecurity incident relates to a declared national emergency, or else where there is a material risk that a cybersecurity incident has, is or will likely seriously prejudice the Australia's social or economic stability, defence or national security. These include the heavily circumscribed Ministerial power to request an authorised agency to intervene in relation to computer-related activities where an entity is unwilling or unable to respond to an incident.

Additionally, the Cyber Incident Review Board (CIRB) has been established as an independent statutory advisory body responsible for conducting no-fault, post-incident reviews of significant cybersecurity incidents in Australia. The CIRB post review report will contain recommendations to government and industry about actions

to prevent, detect, respond to or minimise the impact of future cybersecurity incidents of a similar nature.

In pursuit of national cohesion, the state authorities adopt the following approaches.

- The ACSC facilitates information and collaboration across private, public and NGO sectors to develop collective cyber-resilience and to respond to cyber-incidents. In this regard, the ACSC has commenced: a partnership programme, involving private, public, and NGO sectors, to enable information sharing and network hardening; and an alert service, which provides information on recent cyber threats as well as prevention and mitigation advice.
- The Joint Cyber Security Centres (JCSC) are state-based agencies which collaborate with organisations across the private, public and NGO sectors on cybersecurity and cybercrime threats and response options.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

Even for the financial sector, there is a patchwork of legislation covering the financial sector's operational resilience, leading to variation in scopes. This legislation includes the SOCI Act, the Corporations Act, the Banking Ac 1959 (Cth) and the Insurance Act 1973 (Cth).

Corporations Act

As a starting point, the Corporations Act imposes a duty to exercise "care and diligence" on all directors and officers of corporations (Section 180) which inherently involves considerations relating to cybersecurity resilience. But more specifically, the Corporations Act requires corporations holding financial licences to have adequate risk management systems (Section 912A).

CPS 234

On top of this, APRA's CPS 234 regulates information security standards for APRA-regulated financial, insurance and superannuation entities.

Other Legislation (SOCI Act and Cyber Security Act)

Additionally, other legislation and regulation applicable to sectors beyond the financial is equally relevant here. These include the SOCI Act, since the financial services and markets sector does fall within its scope, so as to include certain banking assets, superannuation assets, insurance assets and financial market infrastructure assets (see **2. Scope of Critical Infrastructure Cybersecurity**). Each of these are, in turn, defined and cover a range of assets owned or operated by entities with certain Australian market licensees, CS facility licensees, benchmark administrators, and more, but most with the underlying condition that the asset is "critical to the security and reliability of the financial services and markets sector".

Those that fall outside the scope of the SOCI Act may fall within the scope of the Cyber Security Act, which imposes reporting obligations on "reporting business entities". See **2. Scope of Critical Infrastructure Cybersecurity**.

3.2 ICT Service Provider Contractual Requirements

Information and communications technology (ICT) service providers are not expressly defined in Australia. However, legislation does address "data processing or storage" assets and providers. Such an asset may be considered itself

a critical infrastructure asset, separate to other critical infrastructure, and therefore fall within the scope of the SOCI Act.

Specifically, an entity that owns or operates a "data storage or processing asset" will be considered a responsible entity under the SOCI Act and their asset "critical" if:

- the entity wholly or primarily provides data storage or processing services that relate to "business critical data", being "personal information" (per the Privacy Act – see **6.1 Cybersecurity and Data Protection**) relating to at least 20,000 individuals, or otherwise information relating to any research and development, needed to operate, systems needed to operate, or risk management and business continuity in relation to a critical infrastructure asset;
- these services are provided to certain end-users, primarily either:
  - (a) the Commonwealth, a State, a Territory, or a body corporate established under such a Commonwealth, State or Territory law; or
  - (b) the responsible entity for a critical infrastructure asset;
- the entity knows that the asset is used by the above end-user; and
- the asset does not constitute another critical infrastructure asset.

Further, the 2024 SOCI Amendment Act clarified the SOCI Act so that it included secondary assets who hold business critical data relating to the primary asset. Notably, the intent behind these amendments is not to capture all non-operational systems holding business critical data; rather only those where vulnerabilities could significantly impact critical infrastructure assets. Examples of relevant operational data included network blueprints, encryption keys, algorithms, operational system code, and tactics, techniques and procedures.

The regulations may specifically exclude other such assets. See **2. Critical Infrastructure Cybersecurity** for their obligations and responsibilities.

3.3 Key Operational Resilience Obligations

There is no specific legislation for "digital operational resilience" for the financial sector as seen in the European jurisdictions; however, the objectives of enabling the financial sector to be or remain resilient in the face of serious operational disruption and prevent/mitigate cyberthreats are reflected in the patchwork of legislation.

SOCI

Specifically looking at the obligations under the SOCI Act for the financial sector, although financial business using or constituting critical infrastructure assets have the same incident reporting obligations already covered (see **2.3 Incident Response and Notification Obligations**), such services do not have the obligations to register as critical assets and to have a CIRMP under the SOCI Act (except where they are "payment services").

As an aside, a financial service can be classified as a SoNS under the SOCI Act, attracting the enhanced cybersecurity obligations.

Corporations Act

Notwithstanding the position under the SOCI Act, financial services are likely already required to be registered with APRA and/or obtain a form of financial service licensing; and in doing the latter, must, inter alia, provide their services

"efficiently and fairly" and have an adequate risk management program. Australian courts have already confirmed that such a risk management plan must ensure adequate cybersecurity and cyber-resilience measures are adequately implemented across its business.

CPS 234

APRA's CPS 234 requires APRA-regulated financial, insurance and superannuation entities to comply with legally binding minimum standards of information security, including by:

- specifying information security roles and responsibilities for the entities' board, senior management, governing bodies and individuals;
- implementing and maintaining appropriate information security capabilities;
- maintaining tools to detect and respond to information security incidents in a timely way; and
- notifying APRA of any material information security incidents.

These standards provide that an entity's board is ultimately responsible for information security and that the board must ensure that its entity maintains information security in a manner that is commensurate with the size and vulnerability of that entity's information assets.

APRA-regulated entities are required to externally audit their organisation's compliance with CPS 234 and report to APRA in a timely manner.

If organisations are non-compliant, they may be required to issue breach notices and create rectification plans. If organisations are unable to comply with the standards following this process, APRA may undertake a more formal enforcement process which may include enforceable undertakings or court proceedings.

Cyber Security Act

In addition to the reporting obligations under the CPS 234, certain responsible entities concerning "critical financial market infrastructure asset" (**2.1 Scope of Critical Infrastructure Cybersecurity Regulation**) also have ransomware reporting obligations under the Cyber Security Act (see **2.3 Incident Response and Notification Obligations**).

3.4 Operational Resilience Enforcement

As at the time of writing, there was no enforcement action against "data processing or storage" providers or other ICT services. In fact, there has been no enforcement action reported in relation to the SOCI Act.

According to CISC's Compliance and Enforcement Strategy published in April 2022, the CISC prioritises industry partnership and pursues a co-operative, educative and overall voluntary approach. Although it has a range of regulatory options available, it is yet to use any penalising enforcement action.

Depending on the breach, action against ICTs may also come from other regulators such as the OAIC.

3.5 International Data Transfers

Government Transfers

Although there are limits on the use of the cybersecurity information provided by reporting business entities under the Cyber Security Act and Intelligence Services Act 2001 (Cth), these limitations are unlikely to prevent the ASD, National Cyber Security Coordinator (NCS Coordinator) or CIRB from disclosing the information to foreign authorities or joint partnerships for particu-

lar purposes. For example, where information if voluntarily provided in relation to a significant cybersecurity incident, the NCS Coordinator disclose this information in "coordinating the whole of Government response" or otherwise to inform Commonwealth ministers; who may then disclose this information for a "permitted cyber security purpose" such as mitigating material risks that prejudice Australia's social/economic stability, defence or national security. This may include sharing and international transfers of information to foreign authorities or co-ordinated partnerships.

Market Transfers

Privacy Act

The primary legislation governing data transfers in Australia is the Privacy Act, which was relevantly amended by the Privacy and Other Legislation Amendment Act 2024 (Cth) (the "2024 Privacy Amendments") on 29 November 2024.

Prior to these amendments, international (cross-border) disclosures of personal information were addressed primarily by APP 8. This principle required APP entities to "take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles". What is "reasonable" depends on one's specific circumstances but will usually involve a contract incorporating the APPs and the Australian entities monitoring or at least assessing the overseas entity's systems. Importantly, APP 8 is not limited to where there is active transfer of data but rather extends to wherever data is accessible to an overseas entity (eg, stored on servers in Australia, but accessible by overseas entities).

The 2024 Privacy Amendments introduces an adequacy regime, meaning there is now a mechanism by which the Government can prescribe a "white list" of countries and binding schemes that are recognised as being on par with APP 8.

Consumer Data Right

In respect of data transfers more generally, Part IVD of the Consumer Act regulates the handling (including sharing) of CDR. The CDR was rolled out to the banking and energy sectors in 2020 and 2022 respectively. Although it was to continue into the superannuation, insurance and telecommunications sectors (and then into the non-bank lenders and Buy Now Pay Later products), the government paused the roll out in 2023, commissioned a report in August 2024 (which found that compliance costs exceeded initial estimates) and is now considering amendments to "reset" the CDR, involving the simplification of the customer consent progress and the encouragement of operational enhancements to reduce the barriers to participation in the CDR.

Prohibitions

Certain information is prohibited from being held or taken outside Australia, such as records held for the purposes of the My Health Record system. Breach of this prohibition could result in a maximum criminal penalty of five years imprisonment and AUD99,000; or a civil penalty of AUD495,000.

Cybercrime

For completeness, it should also be noted that unauthorised access to computer systems (hacking, forceable transfers, etc) is criminalised by both State and Federal legislation. For example, persons suspected of unauthorised access to computer systems are charged pursuant to Section 478.1 of the Criminal Code, which provides for the offence of "Unauthorised access to, or modification of, restricted data".

These offences have extraterritorial application, meaning that conduct undertaken outside Australia can still be charged and prosecuted under Australian law if:

- the crime involves conduct both inside and outside Australia;
- the crime results in harm within Australia;
- the offender is an Australian citizen, or a corporation incorporated in Australia; or
- the crime is related to another crime that occurred in Australia.

Other legislation

In addition to the above, the following existing and potential legislation is relevant to data transfers, including those that are cross-border.

- In December 2024, the Digital ID Act and the Digital ID (Transitional and Consequential Provisions) Act 2024 (Cth) commenced that, inter alia, restrict an accredited entity on the collection, use and disclosure of biometrics and other personal information. The Digital ID Rules are to also address the storing and transfer of information outside Australia and are expected to take the form of blanket prohibitions, with an exemption application process.
- The Australian Treasury's action has stalled since 2023 when it announced that a formal ban on "screen scraping" or "digital data capture" (ie, collection of displayed data for various uses) in the banking sector was being considered. There are continuing concerns of the protection of screen scraped data, and how existing legislation applies to its handling or transfers.

3.6 Threat-Led Penetration Testing

Threat-led penetration testing (TLPT) is the testing of systems by replicating the methods used by actual threat actors against. Generally speaking, TLPT is not a requirement in Australia.

Currently, only those critical infrastructure assets designated as a SoNS may be required to undertake:

- a "cyber security exercise", the purpose of which is to test the entity's ability to respond appropriateness, preparedness to respond appropriately, and ability to mitigate the relevant impacts, and thereafter prepare an internal report, which can in turn, be audited; and
- a vulnerability assessment, the purpose of which is to test system vulnerabilities to the relevant cybersecurity incident, and thereafter prepare a vulnerability assessment report.

TLPT is also a component of regulatory guidance (eg, ASD's best practices for deploying secure and resilient AI systems).

On the flipside, unsolicited/unauthorised penetration testing activity could be captured by Section 478.1 of the Criminal Code, which provides for the offence of "[un]authorised access to, or modification of, restricted data".

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

There is no specific legislation for cyber-resilience in Australia.

However, cyber-resilience requirements have legislative status across various contexts, including:

- the risk management programmes required by the legislation already discussed under the

SOCI Act for responsible entities of critical infrastructure assets (**2.2 Critical Infrastructure Cybersecurity**) and the Corporations Act for financial licensees (**3.3 Key Operational Resilience Obligations**);
- other obligations on certain responsible entities concerning TLPT-like requirements (**3.6 Threat-Led Penetration Testing**); and
- the data protection standards for various types of information such as "personal information" (**6.1 Cybersecurity and Data Protection**) and the healthcare sector (**6.3 Cybersecurity in the Healthcare Sector**).

Further, the Cyber Security Act provided a framework by which the Minister can prescribe mandatory rules for smart devices, which seeks to replace the 2020 voluntary Code of Practice: Securing the Internet of Things for Consumers. The details of the framework are still yet to enter into law, but it will apply to products that are either "internet-connectable" or "network-connectable", subject to certain exceptions relating to laptops, medical devices and cars. This framework will be primarily targeted towards manufacturers and suppliers of these devices.

4.2 Key Obligations Under Legislation

Cyber-resilience obligations are imposed on certain responsible entities of critical infrastructure asset by way of the Critical Infrastructure Risk Management Program, which must be adopted, reviewed and updated. The purpose of these programmes is to identify each hazard with a material risk and minimise, eliminate or mitigate that hazard (or its material risk). The relevant responsible entities and specific requirements for these programmes are set out in the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023.

In respect of smart devices, according to the CISC's explanatory document outlining the Cyber Security (Security Standards for Smart Devices) Rules, their cyber-resilience obligations will include mandatory obligations relating to passwords, procedures to report security issues, support period for security updates, as well as voluntary labelling schemes. However, the regulations are yet to be passed.

Other cyber-resilience obligations for critical infrastructure, the broader financial sector and others are discussed elsewhere in this chapter.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

There is no single legislation in Australia addressing broad-sweeping information technology and cybersecurity (ITC) certification procedures.

However, ITC-relevant certification provisions are relevant to the SOCI Act. Specifically, where a responsible entity holds a certain "certificate of hosting certification (strategic level)" that relates to its critical infrastructure asset, that entity is exempt from needing a critical infrastructure risk management programme. This certificate must be issued under a scheme that is administered by the Commonwealth and known as the hosting certification framework.

At the time of writing, this framework was only available to data centre providers and cloud service providers; and approximately 11 data centre facilities and 14 cloud services were certified.

For additional context, since 30 June 2022, all government contracts for hosting services must

be with certified service providers. However, this policy requirement is not restricted to "strategic level" certification per the SOCI Act. Under this framework, there are three certification "strategic", "assured" and "uncertified". Depending on a government department's risk profile and data set, they may contract with a "Certified Assured Service Provider".

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

The Privacy Act

Scope

Federally, data containing personal information is protected under the Privacy Act, which regulates the handling of this information by "APPs entities".

At this juncture, it is important to note two definitions.

- "Personal information" under the Privacy Act is defined broadly as information or an opinion about an identified or reasonably identifiable individual. It is not required to be true or recorded in a material form. Personal information also includes "sensitive information", which includes information or opinions on an individual's race, ethnicity, politics, religion, sexual orientation, health, trade associations and criminal records. Sensitive information is often afforded a higher level of protection than other personal information.
- "APP entities" are, subject to some exceptions, federal government agencies, private sector organisations with an annual turnover of over AUD3 million and smaller entities with data-intensive business practices (including private health providers, businesses that sell or purchase personal information and service providers to the federal government).

Schedule 1 of the Privacy Act contains 13 APPs, which are minimum standards for processing and handling personal information by APP entities. The Privacy Act also requires mandatory reporting for certain APP breaches under the NDB scheme. Breaches of the Privacy Act may result in investigation and enforcement action by the OAIC.

Reporting obligations (the NDB scheme)

The NDB scheme requires APP entities to notify both affected individuals and the OAIC where there are reasonable grounds to believe that an "eligible data breach" has occurred. In short, as per Section 26WE(2) of the Privacy Act, an "eligible data breach" occurs where:

- there is unauthorised access to/disclosure of personal information and a reasonable person would conclude that this "would be likely to result in serious harm to any of the individuals to whom the information relates"; or
- personal information is lost in circumstances where a reasonable person would conclude that unauthorised access to/disclosure of it is likely to occur and, were it to occur, it "would be likely to result in serious harm to any of the individuals to whom the information relates".

However, Section 26WF of the Privacy Act creates an exception to reporting such an incident, where the entity in question takes remedial action to ensure that the breach does not cause serious harm to the individuals concerned.

Notably, specific data breaches related to certain health records are excluded from this scheme and are to be addressed under Section 75 of the

My Health Records Act (see **6.3 Cybersecurity in the Healthcare Sector**).

The ACSC provides an overarching definition for cybersecurity events in its Guidelines for Cyber Security Incidents. In these Guidelines, a cybersecurity event is "an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security". While there is no general legislative definition of a cybersecurity event, the SOCI Act, at Section 12M, provides a limited, more complex definition.

Statutory tort

Also, it is important to note here that the 2024 Privacy Amendment introduced a statutory tort for serious invasions of privacy, giving individuals a route to seek redress for privacy harms in the courts.

State and Territory Reporting Obligations

There are also schemes at the state/territory level. For example, both NSW and Queensland had introduced mandatory notification of data breach schemes via, respectively, the Privacy and Personal Information Protection Amendment Act 2022 (NSW) (entered into force 28 November 2023) and Information Privacy and Other Legislation Amendment Act 2023 (Qld) (commencement date to be set by proclamation). These largely mirror the federal scheme.

Other Reporting Obligations

There is other relevant legislation for data protection and reporting obligations, including in relation to certain health records (see **6.3 Cybersecurity in the Healthcare Sector**), financial sector (**3. Financial Sector Operational Resilience**) and critical infrastructure assets (**2. Critical Infrastructure Cybersecurity**).

6.2 Cybersecurity and AI

At the time of writing, there is no AI-specific regulation on AI; however, there is a patchwork of laws regulating critical infrastructure, privacy, consumer protection, data security and more that all touch on aspects of AI development and use.

Further, Australia has voluntary instruments, including:

- ethical frameworks, including the Australia's AI Ethics Principles, that has been supplemented on 15 June 2023 by NAIC's Implementing Australia's AI Ethics principles: A selection of responsible AI practices and resources; and
- a voluntary AI Safety Standard released on 5 September 2024, comprising practical guidance in the form of ten "AI guardrails".

Similarly, regulators ASD, in conjunction with foreign authorities such as the U.S. National Security Agency's Artificial Intelligence Security Center, has published guidance on deploying, engaging with and developing AI systems. Further, the ASD has endorsed the Cybersecurity Performance Goals (CPGs) developed by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST).

6.3 Cybersecurity in the Healthcare Sector

Reporting Obligations

Certain data breaches relating to My Health Record information or the system itself are to be reported under Section 75 of the My Health Records Act (rather than through the NDB scheme under the Privacy Act).

Section 75 of the My Health Records Act requires a report where there has (actually or potentially) been unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record or the (actual or potential) compromise of the security or integrity of the My Health Record. Such a report must be made to the relevant system operator and/or the OAIC. Subsequently, all "affected healthcare recipients" must also be notified of the compromise or unauthorised disclosure.

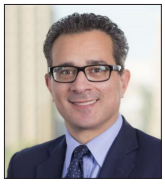
Other than those data breaches to which the My Health Records Act applies, medical data would generally be personal information and covered by the federal NDB scheme (see **6.1 Cybersecurity and Data Protection**).

Trends and Developments

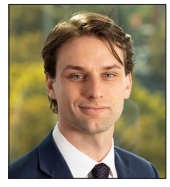
Contributed by:
Dennis Miralis and Jack Dennis
Nyman Gibson Miralis

Nyman Gibson Miralis is a market leader in all aspects of general, complex and international criminal law and is widely recognised for its involvement in some of Australia's most significant cases. The firm's team in Sydney has expertise in dealing with complex national and international cybercrime investigations and advising individuals and businesses who are the subject of cybercrime investigations. Its expertise includes dealing with law enforcement requests for information from foreign jurisdictions, challenging potential extradition proceedings as well as advising and appearing in cases where assets have been restrained and confiscated worldwide.

Authors



Dennis Miralis is a partner at Nyman Gibson Miralis and a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional investigations and criminal prosecutions. His areas of expertise include cybercrime investigations, anti-bribery and corruption, global tax investigations, proceeds of crime, anti-money laundering, worldwide freezing orders, national security law, INTERPOL Red Notices, extradition and mutual legal assistance law. In 2021 Dennis was awarded a certificate of completion for the "Cybersecurity: The Intersection of Policy and Technology" programme, January 2021, John F. Kennedy School of Government at Harvard University, Executive Education.



Jack Dennis is a senior criminal defence lawyer who practises in international and domestic criminal, corporate and tax law at Nyman Gibson Miralis. His international criminal work includes transnational criminal and regulatory investigations, liaising with foreign legal and regulatory bodies, as well as advising clients on matters concerning international public law. Domestically, Jack has advised on a range of criminal issues and investigations, including white-collar crime, fraud, sanctions, INTERPOL, extraditions and national security. He also has significant international, corporate and tax experience, having advised on cross-border transactions and disputes involving foreign and domestic corporations and individuals, across the software, financial services and crypto industries.

Nyman Gibson Miralis

Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 292 648 884
Email: dm@ngm.com.au
Web: www.ngm.com.au

Introduction

Since releasing the 2023-2030 Australian Cyber Security Strategy (the "CS Strategy") on 22 November 2023, the Australian government has pursued sweeping reforms to address the gaps in cybersecurity. The government aims to become "a world leader in cybersecurity by 2030"; however, the effectiveness of these actions and reforms still remains to be seen. For 2025, the actual impact of the 2024 reforms remains to be seen in the still-patchwork style legislative landscape and the Australian government continues to play catch-up with both technology and other countries as it with an eyes the "frontier".

The CS Strategy is aimed at strengthening Australia's cyberdefences and supporting people and businesses to be resilient to and recover quickly from cyber-attacks. Grounded in the 2023-2030 Australian Cyber Security Strategy: Action Plan (the "Action Plan"), the CS Strategy is planned out across three "Horizons" targeting six "shields" or "layers of defence". Currently, Australia is in the final (albeit second) year of Horizon 1 ("Strengthen our foundations") whereby it is aiming to address critical gaps, build protections and support "initial cyber maturity uplift", with the government's performance target being 75% of department-led activities to be on track. The government is setting itself up for Horizon 2 ("Expand our search") come 2026, which aims to scale cyber maturity across the whole economy, make investments and grow a diverse cyber workforce.

In its pursuit of the cyber frontier, the Australian government introduced the Cyber Security Bill 2024 (Cth) as part of the Cyber Security Legislative Package 2024, involving a number of updates to existing legislation. This bill is Australia's first standalone cybersecurity legislation, but reflects largely what has been seen in the UK, Europe and other jurisdictions. This reform occurred in a long line of changes that have preceded 2024. Overall, 2024 can be categorised as another year of change for the cybersecurity space, illustrating the fast pace of the technologies and malicious actors, the delayed yet quickening pace of the government, and the inherent but necessary gap between implementation and enforcement to accommodate the slow adoption of these laws and regulation throughout many industries.

Despite the success of law enforcement, such as Operation Cronos, cyber vulnerabilities are becoming more and more critical, as demonstrated by ransomware attacks such as against UnitedHealthGroup in February 2024 or even

software upgrades gone wrong as in the case of CrowdStrike-Microsoft Outage in July 2024. Attacks by state-sponsored and independent actors are only set to increase. And the importance of effective cybersecurity laws and protections is becoming ever-more critical.

Threat Landscape

Victim typologies

The Australian Signals Directorate's (ASD) Annual Cyber Threat Report for 2023-24 (the "ASD 2023-24 Report") confirmed that the "top 5" sectors reporting cyberthreats remained the same as FY2022-23: federal government, state/local governments, healthcare, and tied fifth were education, professional/scientific services, utility services and information/telecommunications services. Yet vulnerabilities beyond these sectors cannot be understated.

The ASD 2023-24 Report flagged that the ASD responded to 11,000 cybersecurity incidents and received over 87,400 cybercrime reports (which was, in fact, a drop of 7%). The crime trends differ amongst targets:

- for individuals, self-reported cybercrimes comprised identify fraud (26%), online shopping fraud (15%) and online banking fraud (12%);
- for businesses, it was email compromise (20%), online banking fraud (13%) and business email compromise fraud (13%); and
- for critical infrastructure, it was compromised accounts or credentials (32%), malware infection (excluding ransomware) (17%), and compromised asset, network or infrastructure (12%).

With the government's focus primarily being on critical infrastructure, there remains a growing concern that small businesses are low-hanging fruit: vulnerable, ill-prepared, and are being increasingly targeted. Yet, most small businesses are exempt from basic statutory obligations such as the Privacy Act 1988 (Cth) (the "Privacy Act"). Immediate resourcing and compliance costs must be weighed against costs and damage of potential attacks.

Increasing efficiency of attacks

Attacks are becoming more efficient and sophisticated. This capacity strengthening is due, in part, to AI; however, such developments may also assist countermeasures. In recognition of this double-edged sword, the ASD has published resources for businesses and government, including Best Practices for Deploying Secure and Resilient AI Systems.

Similarly, the ASD recently confirmed that 2023 saw a rise in zero-day vulnerabilities (ie, exploitation of an unknown vulnerability, which developers have had "zero days" to address). Overall, this emphasises the need for the proactive "stance of 'when' not 'if' a cybersecurity incident will occur", as well as a pre-emptive approach such as with the secure by design principles.

State-sponsored attacks

Regulators noticed:

- state-sponsored actors targeting supply chain compromises;
- PRC state-sponsored actors' "increasingly emerging" living off the land (LOTL) techniques, "pre-positioning" themselves on or adjacent to critical infrastructure networks "for disruptive effects rather than traditional cyber espionage operations"; and
- Russian-sponsored actors adapting their operations to match industry shifts to cloud-based infrastructure.

State-sponsored cyber-operations are set only to increase with growing geo-political tensions, including the competition in the Indo-Pacific. Aswe continue to see sanctions, states may co-opt actors and state hacking itself to supplement revenue streams.

Other risks/vulnerabilities

Overall, it is important to acknowledge that the vulnerabilities are not only from external malicious actors. Incidences that occurred in 2024 highlight other critical focus points, such as the following.

- Insider threats: in October 2024, Qantas confirmed that two contractors working for Air India SATS company had allegedly accessed at least 800 customer booking details and diverted their frequent flyer points. As this India SATS provides services to a lot of airlines across the OneWorldAlliance, the true extent of the issue may never be known.
- Software issues: in July 2024, CrowdStrike released an update that caused worldwide outages of certain programs.

Legislative and Regulatory Reform

In 2024, the Australian government passed the Cyber Security Act package, introducing a range of new legislative reforms; some of which are explored below. Overall, these changes pave the way for better-informed government actions as well as increased enforcement actions to raise the general standard of Australian businesses across the board.

SOCI Act

The Security of Critical Infrastructure Act 2018 (Cth) (the "SOCI Act") regulates the critical infrastructure assets identified across eleven sectors, and was amended in November 2024 by the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 (Cth) (the "SOCI Amendment Act").

The SOCI Amendment Act included:

- crucial clarifications on the status of data storage systems;
- amendments to what is protected information, as well as exemptions to the prohibitions on the use and disclosure of such information; and
- new regulatory powers for "seriously deficient" Critical Infrastructure Risk Management Programs (CIRMP).

The shared-responsibility for and complexities of a single business' CIRMP and cybersecurity overall is demonstrated by the media's coverage of the back-and-forth between Delta Air Lines and CrowdStrike after the former commenced proceedings against the latter for damages caused by the CrowdStrike-Microsoft outage in July 2024. Delta claimed, inter alia, that CrowdStrike "cut corners, took shortcuts, and circumvented the very testing and certification processes it advertised"; while CrowdStrike retorted that Delta has had a "slow recovery away from its failure to modernise its antiquated IT infrastructure". Both businesses and service providers have responsibilities under a capable CRIMP. It remains to be seen if this specific matter progresses further.

The importance of reviewing and properly implementing these changes is only increased by the continued stance taken by the Department of Home Affairs (DoHA) under its performance targets. Target 8 comprises that 100% of instances of identified non-compliance with obligations in the SOCI Act will be subject to a compliance action within 90 days. The precise "compliance

action" will be determined by CISC's Compliance and Enforcement Framework "and the published regulatory posture". Watch this space.

Cyber Security Act

The Cyber Security Act was an Australian-first: legislation specifically aimed at cybersecurity. It introduced standards for smart devices, new reporting obligations, and also established two new roles:

- the National Cyber Security Coordinator (NCSC) responsible for co-ordinating whole-of-government action in response to significant cybersecurity incidents, policies and capabilities; and
- the Cyber Incident Review Board (CIRB), an independent advisory body that will undertake reviews of certain cybersecurity incidents on a no-fault basis.

Information-gathering routes under the Cyber Security Act include:

- obligatory ransomware reporting: see below;
- CIRB compulsive powers: the CIRB has the power to compel information and documents from entities believed to be "involved in a cyber security incident" (subject to a request for information having been made); and
- voluntary reporting: see below.

Information-gathering: ransomware reporting

2021-22 research suggests only one in five Australians are reporting ransomware attacks to authorities. This statistic undoubtedly needs updating with the increased prevalence of attacks and access to technology.

The Cyber Security Act mandated reporting when ransomware payments (or other benefits) are demanded for certain entities. This obligation joins the ranks of a slowly growing set of confined reporting obligations. This currently includes those imposed on critical infrastructure assets in respect of certain cybersecurity incidents (irrespective of ransomware payments) under the SOCI Act; on APRA-regulated entities in respect of material information security incidents. Outside these regimes, the Australian government relies on their own detection of such incidents, and more likely, voluntary reporting.

This ransomware obligation is just one more confined patch in Australia's patchwork of obligations. This obligation is imposed only on a "reporting business entity", which is defined by reference to the Australian business' previous year's turnover (the number undetermined at writing) or by being specific critical infrastructure assets. Therefore, the true extent to which these new obligations will be felt across Australian businesses (beyond critical infrastructure) remains to be determined (by the yet-to-be-published rules). The threshold will likely be determined with reference to the cybersecurity threat landscape as well as the compliance capabilities, costs and other burdens on Australian businesses. Speculatively, this may match the threshold under the Privacy Act, so as to include small businesses. This set-up grants the Australian government flexibility to adjust obligations according to the perceived needs but will likely result in a gap in the obliged reporting where there is a ransomware. That is without even acknowledging that these obligations only arise where there is a "ransom" demanded in the first place (albeit irrespective of the type of benefit, not only payments; and also irrespective of actual payment of the demand).

This piece is just one of many that makes up the puzzle of Australia's cybersecurity and attempts to balance several aspects including security,

compliance burden and costs. Nevertheless, it will likely still see a lot of incidents pass under the radar, leaving a widespread and fertile ground for malicious actors to test ransomware largely undetected and non-ransomware cyber-incidents more generally. With no safe harbour protections and heightening reputational concerns over breaches, an over-reliance on voluntary reporting may be insufficient.

Use of reports and other data shared

A key premise of Australia's strategy in obtaining information on incidents is to better understand vulnerabilities/targets, methods and techniques, and ultimately generate tools and strategies to proactively and reactively respond to future incidents. Australia has sought to increase the open and frank communications of ransomware reporting by restricting the use of the information. These purposes primarily relate to responding to, mitigating or resolving cybersecurity incidents. How far these express purposes extend may be the subject of future proceedings.

Taking a closer look at ransomware reporting, the Act implements "limited use" obligations on the bodies who receive the information (primarily or secondarily). In doing so, the Act excludes the use of the information for investigations or enforcement action unless it is a contravention of the reporting obligations themselves or a law attracting "a penalty or sanction for a criminal offence". This prevents the information from being used in most regulatory enforcement actions, but leaves the entities exposed to criminal law provisions. While individuals (including directors) may be able to rely on the privilege against self-incrimination where criminal law issues become live, the business entity itself is unlikely to have such protections given corporate entities do not have such a privilege under Australian law. Public suggestions of including a safe harbour provision were dismissed by the Australian government. In fact, the government expressly stated the intention was not to "shield a reporting entity from legal liability" or "to restrict law enforcement […] from gathering this information through another passage using their own existing powers" raising the concern of secondary methods of obtaining the obligatorily shared information by even civil regulators. This may complicate compliance with this obligation, particularly should the Australian government rely on criminal sanctions (alone or as alternatives to civil penalties) to enforce cybersecurity legislation.

There are expanded protections for any information voluntarily provided to the NCSC concerning an actual or potential cybersecurity incident, with Section 42 rendering such information inadmissible in criminal proceedings (except very specific circumstances) and any "proceedings for breach of any other Commonwealth, State or Territory law (including the common law)". Yet, these protections do not prevent authorities from obtaining the information via other methods and relying on it thereafter.

Online Safety Act

Surpassing the ranks of Russia's ban of Discord and the United States' (incredibly short) ban of TikTok, Australia passed a world-first age restriction on social media platforms for those under 16 years by introducing the Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth). The obligation is to take "reasonable steps" to prevent age-restricted users from having an account, but will impose restrictions on the kind of information that can be collected and how this information is stored, used and protected. Specific platforms are still to be confirmed, but the government initially intends to include Snapchat, TikTok, Facebook, Instagram

and X; while excluding messenger, online gaming, health and educational-focused services. Any platforms where an "account" is not needed (eg, Youtube) will not be caught.

Privacy Act

On 28 September 2023, the Australian government published its response to the Attorney-General's Department's Privacy Act Review Report (the "Review"). The Review contained 116 proposals to amend the current Privacy Act 1988 (Cth) (the "Privacy Act") to better align Australia's privacy laws with global standards of information privacy protection.

Of the 116 proposals in the Report, the government has "agreed" to 38 proposals and "agreed in-principle" to 68 others.

A year later, and Australia has seen the first tranche of resulting reforms. The Privacy and Other Legislation Amendment Act 2024 (Cth) took effect on 10 December 2024, and:

- introduces a new tort for serious privacy invasions;
- expands Office of the Information Commissioner's (OAIC) enforcement powers, including information-gathering powers concerning actual or suspected eligible data breaches;
- introduces the long-awaited automated decision-making requirements;
- introduces an adequacy regime (a "white list") specifying jurisdictions with which Australian companies may more freely share data;
- criminalises doxing; and
- clarifies that APP11 of the APPs (Australian Privacy Principles) (ie, APP entities must take active measures to ensure the security of personal information it holds) includes both technical (eg, IT expertise) as well as more general organisational training.

The Attorney-General's Department has indicated that it will start consulting on the second tranche of privacy reforms soon, which will likely reflect the remaining proposals that were "agreed", and potentially those "agreed in-principle".

Reflections on the Anti-Encryption Legislation

In a world-first initiative, the Telecommunications (Assistance and Access) Act 2018 (Cth) granted the Department of Home Affairs the power to request or compel assistance from telecommunications providers and technology companies in accessing encrypted communications, such as Technical Assistance Requests (TARs).

According to evidence from the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in 2020, the Australian Security Intelligence Organisation (ASIO) has issued "fewer than 20" TARs, the AFP has issued eight, and the New South Wales Police Force has issued 13. At this point, these requests were (reportedly) complied with on the most part (if not all).

Since then, the ASIO Director has stated that "encryption damages intelligence coverage" in all priority counter-terrorism and counter-espionage cases; but instead of flagging an increased use of these powers, has called for "tech companies to do more […] to give effect to the existing powers and to uphold existing laws". This tact calls into question the utility of the powers and authorities' capacities to properly wield them.

Responses, Investigations and Enforcement

Sanctions

On 23 January 2024, Australia imposed a cyber sanction under the Autonomous Sanctions Act 2011 (Cth) on Russian national Aleksandr Ermakov for his role in the compromise of Medibank Private in 2022. This sanction was the first such

use of the significant cyber-incidents sanctions regime established on 21 December 2021.

Since then, four more individuals have been added to the list for their involvement in LockBit and Evil Corp cybercrime groups.

Financial sanctions under the Sanctions Act now make it a criminal offence, punishable by up to ten years' imprisonment and heavy fines, to provide assets to designated individuals or to use or deal with his assets, including through cryptocurrency wallets or ransomware payments. The designated persons are also banned from travelling to or remaining in Australia.

Although ransomware payments are not illegal, the juncture between cyber sanctions and ransomware payments requires further consideration. Currently, the Department of Foreign Affairs and Trade (DFAT) encourages all such payments to be reported (mandatorily or voluntarily), and states that such disclosure "would be taken into account in any decision to pursue any enforcement or compliance action".

The crossover between cybersecurity and sanctions has continued to increase. DFAT has identified in their Advisory Note – Democratic People's Republic of Korea (DPRK) information technology (IT) workers (14 December 2024) a recent tactic by the Democratic People's Republic of Korea (DPRK) to deploy thousands of information technology professionals to seek remote employment (posing as non-DPRK nationals) to illicitly finance the DPRK and circumvent sanctions. At a time when many industries are looking to establish cybersecurity structures and compliant procedures, more and more are hiring or outsourcing these services (some reports suggest 76% of leading global businesses do so), potentially making them more vulnerable (eg, accessible, desperate) to other legal risks.

ASIC mandate

In November 2023, the chairperson of the Australian Securities and Investments Commission (ASIC), Joe Longo, stated that ASIC's priority for 2024 would be addressing governance and breach of directors' duties following the results of ASIC's 2023 Cyber Pulse Survey. As a snapshot, the survey found significant gaps in Australia's corporate security, with:

- 44% of participants failing to manage cyber-risks posed when dealing with third parties;
- 58% of participants having limited or no capability to adequately protect confidential information;
- 33% of participants not having a cyber-incident response plan; and
- 20% of participants not having adopted cybersecurity standards.

This was speculated to include ASIC prosecuting directors or officers for breaches of directors' duties concerning cybersecurity breaches. However, there was limited outward action on this front in 2024.

Nevertheless, a change may be afoot. At the ASIC Annual Forum on 14 November 2024, the ASIC deputy chairperson, Sarah Court, confirmed ASIC is "considering a range of matters where we consider [financial services and credit] licensees may have not adequately prepared for [cybersecurity] events". There, Court announced that ASIC's 2024 priority of action against financial service licensees who fail to comply with reporting obligations was out, to make way for ASIC's new 2025 priority of action against financial service and credit licensee's failures to have adequate cybersecurity protections. One

would expect this new priority will build on the 2022 Federal Court decision of ASIC v RI Advice Group Pty Ltd [2021] FCA 1193.

This change signals a potentially bigger shift. Data breaches and cybersecurity issues have generally been regulated from a privacy perspective by the Office of the Australian Information Commissioner (OAIC). This area may be a hot spot to watch for regulator "pile-ons".

CISC audits

The Cyber and Infrastructure Security Centre (CISC) considered 2022-2023 a learning and familiarisation period with the introduction of the Security of Critical Infrastructure (Application) Rules 2022. Then, in 2024, the CISC shifted its compliance focus from one primarily of education and awareness raising (2023-24) to a balance of education/awareness and compliance activities (2024-25). The SOCI Compliance Regulatory Posture was updated. In making this shift, the CISC conducted a limited series of trial audits with certain responsible entities "to test our processes for determining industry compliance with SOCI Act obligations". The CISC has also announced that a formal audit programme to evaluate compliance with SOCI obligations will commence in 2024-2025.

2024 marked the first year that responsible entities (under the SOCI Act) were required to file annual reports per the SOCI (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 (CIRMP).

OAIC determination and guidance on facial recognition

On 19 November 2024, the OAIC published a determination finding that retail chain Bunnings breached the Privacy Act 1988 (Cth) through its practices of automatically monitoring CCTV footage, processing imagery of individuals' faces, and storing the same on databases against allegedly known violent customers. This determination is a major development in facial recognition technology and biometric data under Australian law, and was also accompanied by new guidance, "Facial recognition technology: a guide to assessing the privacy risks".

Industry programs

Industry-wise, an increasing number of sector and government partners are choosing to participate in ASD programs, including the ASD-Microsoft initiative to connect ASD's Cyber Threat Intelligence Sharing platform with Microsoft's Sentinel platform.

Joint advisories and investigations

Internationally, Australia is pursuing a co-ordinated approach with its allies in the field of cybercrime where there have been co-ordinated international investigative and law enforcement efforts, resulting in the simultaneous sanctioning of entities. This was seen in 2024 with Operation Cronos, a co-ordinated law enforcement action against the LockBit ransomware group and comprising Australia, the UK, the USA, France and many more.

In addition to simultaneous sanctioning, the international partnerships also result in joint advisories, often seen in respect of Australian-viewed state-sponsored malicious actors. For example, the ASD continues to work with partners to highlight evolving state-sponsored cyber-actors, such the PRC-sponsored Volt Typhoon, APT40, and Integrity Technology Group, Russia's Unit 29155, and Iranian cyber-actors generally.

Another notable joint-operation appears to have involved the ASD and its international partners in identifying a "botnet" comprising 260,000

compromised devices controlled and managed by PRC's state-sponsored Integrity Technology Group since as early as mid-2021 world-wide. Although uncovering these actions is incredibly useful in strengthening cybersecurity, the authorities appear to have been able to do little more than release a joint advisory encouraging exposed device vendors, owners and operators to update and secure their devices. This example illustrates a government's reliance on industry and individuals in dealing with identified threats, at least when it comes to state-sponsored threats – if not beyond.

On the Horizon

Looking towards the future, there are reforms and threats emerging, both old and new.

Legislative changes are on the table such as tranche 2 of the Privacy Act amendments, as are regulations with the public consultation processes concerning the Cyber Security Act rules to take place by February 2025; but the formal and informal transitional periods of 2023-2024 are coming to an end. There have been noticeable shifts in regulatory approaches, as regulators' powers expand (eg, OAIC), their focuses shift to cyberspace (eg, ASIC), and their public approaches start firming into one of enforcement (eg, CISC). Even government agencies are set to adopt new approaches, with DoHA intending to create a new Technology Strategy and Cyber Security Strategy.

The year of 2025 is scheduled to be the end of Horizon 1, yet there appears to be much more foundational work to occur and gaps in Australia's cybersecurity to be addressed. With the Action Plan to be reviewed and the Federal election to take place by May 2025, the stage is set for significant changes in the strategy, purposes and actions across the board.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com