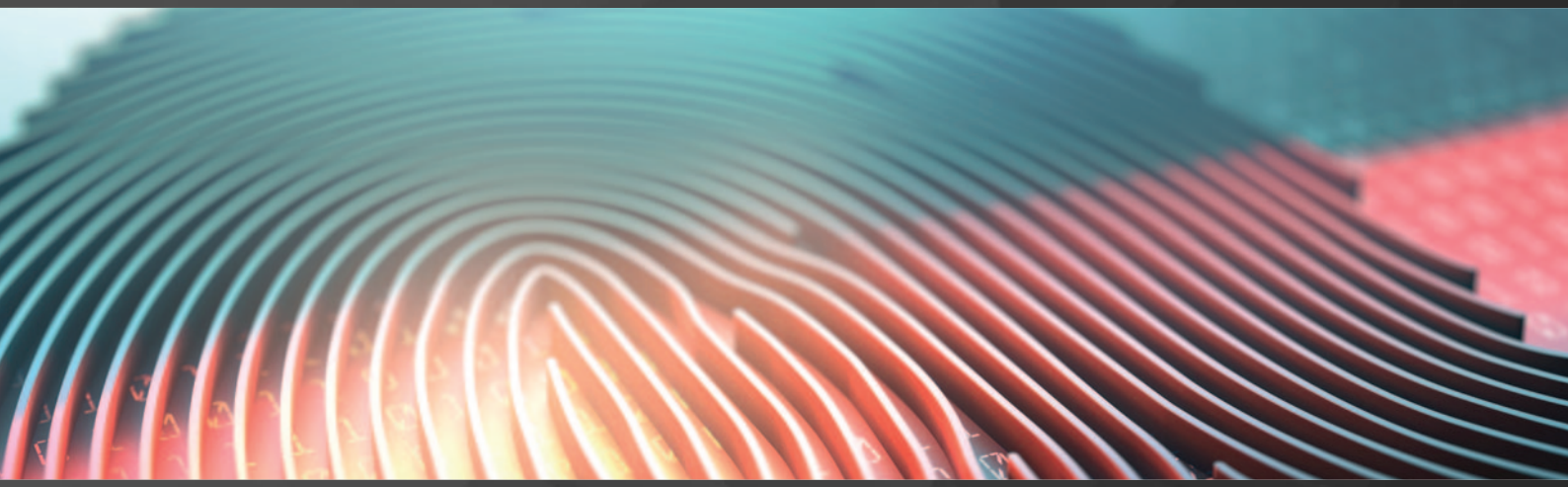
International Comparative Legal Guides



Cybersecurity 2020

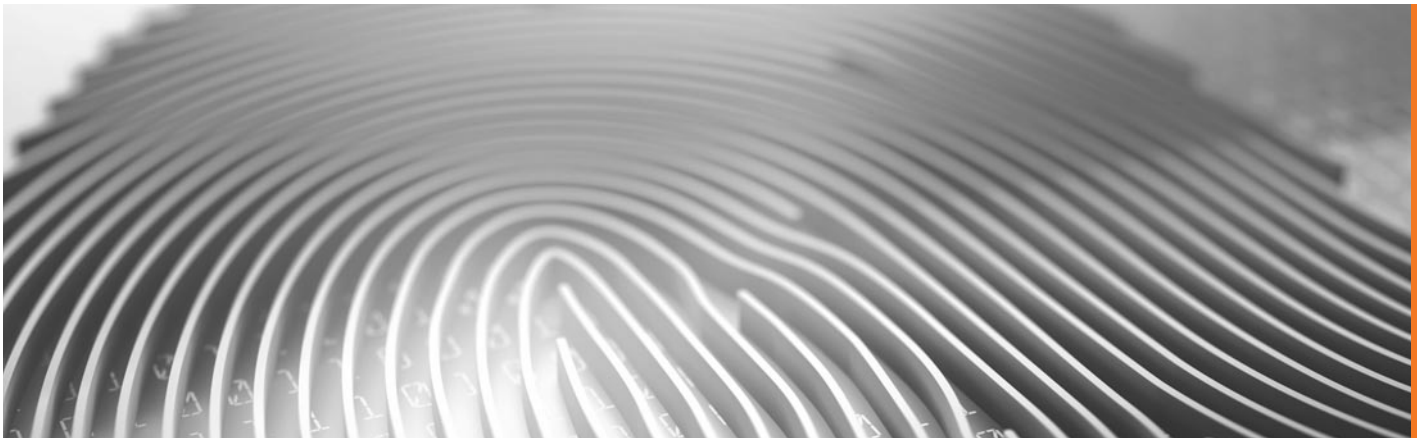
A practical cross-border insight into cybersecurity law

Third Edition

Featuring contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Boga & Associates
Christopher & Lee Ong
Cliffe Dekker Hofmeyr
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Faegre Baker Daniels
G+P Law Firm
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.
Iwata Godo
King & Wood Mallesons
Lee & Ko
Lee and Li, Attorneys-at-Law
LEĜA
Lesniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Ropes & Gray
SAMANIEGO LAW
Shardul Amarchand Mangaldas & Co.
Siqueira Castro – Advogados
Sirius Legal
Stehlin & Associés
Synch

ICLG.com



ISBN 978-1-83918-005-7
ISSN 2515-4206

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
www.iclg.com

Group Publisher
Rory Smith

Associate Publisher
James Strode

Senior Editors
Caroline Oakley
Rachel Williams

Deputy Editor
Hollie Parker

Creative Director
Fraser Allan

Printed by
Stephens & George
Print Group

Cover Image
www.istockphoto.com

Cybersecurity 2020

Third Edition

Contributing Editors:
Nigel Parker and Alexandra Rendell
Allen & Overy LLP

Strategic Partners

Expert Chapters

Country Q&A Chapters

ICLG.com

From the Publisher

Dear Reader,

Welcome to the third edition of *The International Comparative Legal Guide to Cybersecurity*, published by Global Legal Group.

This publication, which is also available at www.iclg.com, provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to cybersecurity laws and regulations around the world.

This year, there are three general chapters which provide an overview of key issues affecting cybersecurity, particularly from the perspective of a multi-jurisdictional transaction.

The question and answer chapters, which cover 32 jurisdictions in this edition, provide detailed answers to common questions raised by professionals dealing with cybersecurity laws and regulations.

As always, this publication has been written by leading cybersecurity lawyers and industry specialists, to whom the editors and publishers are extremely grateful for their invaluable contributions.

Global Legal Group would also like to extend special thanks to contributing editors Nigel Parker and Alexandra Rendell of Allen & Overy LLP for their leadership, support and expertise in bringing this project to fruition.

Rory Smith
Group Publisher
Global Legal Group

Australia


Dennis Miralis


Phillip Gibson


Jasmina Ceic

Nyman Gibson Miralis

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

In Australia, unauthorised access to computer systems is criminalised by both State and Federal legislation. In the Federal jurisdiction, hacking is criminalised under the Criminal Code Act 1995 (Cth) ("the Code"). Most commonly, persons suspected of engaging in cybercrime are charged pursuant to the Code, given its universal application in all States and Territories in Australia.

The recent report published by the Five Eyes intelligence alliance details the public availability of hacking tools and the worldwide proliferation of hacking practices. Hacking activity is carried out by both sophisticated organised crime syndicates as well as independent amateur perpetrators. The tools detailed fall into five categories: Remote Access Tools; Web Shells; Credential Stealers; Lateral Movement Frameworks; and Command and Control Obfuscators.

Persons suspected of unauthorised access to computer systems are charged pursuant to s. 478.1 of the Code, which provides for the offence of "Unauthorised access to, or modification of, restricted data". The offence is comprised of three elements of proof. The offence is committed if: a person causes any unauthorised access to, or modification of, restricted data; the person intends to cause the access or modification; and the person knows that the access or modification is unauthorised. The maximum penalty for a contravention of s. 478.1 of the Code is two years' imprisonment.

Denial-of-Service attacks

Denial-of-Service attacks ("DoS attacks") or Distributed Denial of Service attacks ("DDoS attacks") are criminalised by s. 477.3 of the Code, which provides for the offence of "Unauthorised impairment of electronic communication". The offence is comprised of two elements. The offence is committed if a person causes any unauthorised impairment of electronic communication to or from a computer and the person knows that the impairment is unauthorised. The maximum penalty for a contravention of s. 477.3 of the Code is 10 years' imprisonment.

Phishing

Phishing, being a form of online fraud, is criminalised under the Code in instances where the victim is said to be a Commonwealth entity. When the victim is a member of the public, charges are brought under parallel State or Territory legislation.

Commonwealth fraud prosecution encompasses a wide variety of offending conduct, including phishing-style offences which would affect a Federal government body. Depending on the subsequent financial gain or loss suffered subsequent to the activity, the below charges are available:

- S. 134.2(1) – obtaining a financial advantage by deception.
- S. 135.1(1) – general dishonesty – obtaining a gain.
- S. 135.1(3) – general dishonesty – causing a loss.
- S. 135.1(5) – general dishonesty – causing a loss to another.

For the charge to be proven, the prosecution must establish that the accused obtains or causes a financial advantage, gain or loss by way of deception or dishonesty. The maximum penalty for each offence is 10 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The infection of IT systems with malware is criminalised by s. 478.2 of the Code, which provides for the offence of "Unauthorised impairment of data held on a computer disk etc.". The offence is comprised of three elements. The offence is committed if: a person causes any unauthorised impairment of the reliability, security or operation of data held on a computer disk, a credit card or another device used to store data by electronic means; the person intends to cause the impairment; and the person knows that the impairment is unauthorised. The maximum penalty is two years' imprisonment.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Possession or use of hardware, software or other tools used to commit cybercrime is criminalised by s. 478.3 of the Code, which provides for the offence of possession or control of data with intent to commit a computer offence. The offence is comprised of two elements. The offence is committed if: a person has possession or control of data; and the person has that possession or control with the intention that the data be used, by the person or another person, in committing an offence against Division 477 of the Code or facilitating the commission of such an offence. The maximum penalty for a contravention of s. 478.3 of the Code is three years' imprisonment.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity crime, and in particular identity fraud offences, are criminalised by Division 372 of the Code. Particular acts that are criminalised include dealing in identification information, dealing in identification information that involves use of a carriage service, possession of identification information and possession of equipment used to make identification information. The offence of "Dealing in identification information that involves use of a carriage service" is most relevant to cybercrime. It is criminalised by s. 372.1A of the Code and is comprised of four elements. The offence is committed if: a person deals in identification information; the person does so using a carriage service; the person intends that any person will use the identification information to pretend to be, or to pass the user off as, another person (whether living, dead, real or fictitious) for the purpose of committing an offence or facilitating the commission of an offence; and the offence is an indictable offence against the law of the Commonwealth, an indictable offence against a law of a State or Territory or a foreign indictable offence. The maximum penalty is five years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft is criminalised by s. 478.1 of the Code. As the offence is committed if a person modifies restricted data, modification is defined in the Code as the alteration or removal of the data held in a computer, or an addition of the data held in a computer, the unauthorised copying of data from a computer would contravene the offence provision.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Part 10.6 of the Code creates offences related to telecommunication services. They include offences relating to dishonesty with respect to carriage services and interference with telecommunications.

Failure by an organisation to implement cybersecurity measures
See the discussion below in relation to corporate governance.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Extended geographical jurisdiction applies to offences under Part 10.7 of the Code (Divisions 477 and 478).

A person will not commit offences under that Part unless: the conduct constituting the alleged offence occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; or the conduct constituting the alleged offences occurs wholly outside Australia and a result of the conduct occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; or the conduct constituting the alleged offence occurs wholly outside Australia and at the time of the alleged offence, the person is an Australian citizen or at the time of the alleged offence, the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory; or all of the following conditions are satisfied: the alleged offence is an ancillary offence; the conduct constituting the alleged offence occurs wholly outside Australia; and the conduct constituting the primary offence to which the ancillary offence relates, or a result of that conduct, occurs, or is intended by the person to occur, wholly or partly in Australia or wholly or partly on-board an Australian aircraft or an Australian ship.

Australia is also a signatory to the *Council of Europe Convention on Cybercrime* (the Budapest Convention), a multilateral instrument intended to facilitate intergovernmental cooperation in the regulation, investigation and enforcement of cybercrime. Chapter III of the treaty makes provision for cooperation among Parties "to the widest extent possible". Cooperation is not limited with respect to cybercrime (offences against and by means of computers) but also includes any example of crime involving electronic evidence. Increasingly, Australian government agencies are operating as part of cross-border investigations, often working collaboratively with their international counterparts in parallel investigations.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The *Crimes Act 1914* (Cth) prescribes the sentences applicable to breaches of Federal legislation, such as the Code. Relevant matters for consideration on sentence are set out as a non-exhaustive list of factors under s. 16A of the Crimes Act 1900 (Cth). Matters that generally will mitigate a penalty include the timing of any guilty plea, the offender's character, the offender's prior record, assistance provided by the offender to the authorities and the offender's prospect of rehabilitation and likelihood of reoffending. Notification would be a matter that could be taken into account by a sentencing court as a factor of mitigation.

A number of the offences particularised above cannot be "attempted"; they must actually be committed. For example, a person cannot attempt to commit the offence of "Unauthorised access, modification or impairment with intent to commit a serious offence".

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

A number of criminal offences may arise in relation to cybersecurity or the occurrence of an Incident, although they are best understood as tangential or ancillary to cybersecurity or the occurrence of an Incident. For example, there have been prosecutions for offences such as blackmail where an offender has used material obtained as a result of a breach of confidence to blackmail the owner by threatening to release that material online.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The following laws in New South Wales relate to cybersecurity: the *Privacy Act* (Cth) ("Privacy Act"); the *Crimes Act 1914* (Cth); the *Security of Critical Infrastructure Act 2018* (Cth); the *Criminal Code 1995* (Cth); and the *Telecommunications (Interception and Access) Act 1979* (Cth).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The *Security of Critical Infrastructure Act 2018* (Cth), which commenced on 11 July 2018, seeks to manage national security risks of sabotage, espionage and coercion posed by foreign entities. The Act was implemented as a response to technological changes that have increased cyber connectivity to critical infrastructure. 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". The Act applies to approximately 165 specific assets in the electricity, gas, water and ports sectors.

The Act establishes a Register of Critical Infrastructure Assets, empowers the Secretary of the Department of Home Affairs with an information-gathering power (whereby certain information can be requested of direct interest holders, responsible entities and operators of critical infrastructure assets) and a Minister has the power to issue a direction to an owner or operator of critical infrastructure assets to mitigate national security risks.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

See generally the answer to question 4.3 below in respect of the NDB Scheme.

The Australian Securities and Investments Commission ("ASIC") provides guidance to Australia's integrated corporate markets, financial services and consumer regulator, and provides guidance to organisations through its "cyber reliance good practices". The good practices recommend, *inter alia*, periodic review of cyber strategy by a board of directors, using cyber resilience as a management tool, for corporate governance to be responsive (i.e. keeping cybersecurity policies and procedures up to date), collaboration and information sharing, third-party risk management and implementing continuous monitoring systems.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

See the answer to question 4.3 below.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

See the answer to question 4.3 below.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Subject to the restrictions in the Applicable Laws (such as the Privacy Act), organisations are permitted to voluntarily share information related to an Incident or potential Incidents with a regulatory or other authority and other private sector or trade associations.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

See the answer to question 4.3 below.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

See the answer to question 4.3 below.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Office of the Australian Information Commissioner ("OAIC") is an independent statutory agency within the Attorney-General's Department. The OAIC has three functions; namely, privacy functions conferred by the Privacy Act, freedom of information functions, such as reviewing the decisions made by agencies and ministers pursuant to the *Freedom of Information Act 1982* (Cth), and government information policy functions conferred by the *Australian Information Commissioner Act 2010* (Cth).

In relation to its privacy functions, the OAIC has the power to commence investigations, conduct privacy performance assessments, request an entity to develop an enforceable code, direct an agency to give the OAIC a privacy impact assessment about a proposed activity or function and recognise external dispute resolution schemes to handle privacy-related complaints.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

See the answer to question 4.3 below.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The OAIC reported that, in response to Commissioner-initiated investigations, enforceable undertakings were accepted by three Australian Privacy Principles ("APP") entities over the 2017–2018 period, namely the Australian Red Cross Blood Service, Precedent Communications Pty Ltd and the Department of Health.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There are presently no laws in Australia which prohibit the use of a Beacon or near-field communication technology.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are presently no laws in Australia which prohibit the use of Honeypot technology or similar autonomous deception measures.

Honeypots are a cybersecurity tool used by both public and private agencies to detect network attacks.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There are presently no laws in Australia which prohibit the use of Sinkhole technology. The malicious use of Sinkhole methods to steer legitimate traffic away from its intended recipient may, however, constitute an offence under s. 477.3 of the Code.

Sinkholes can be lawfully used as a defensive practice for research and in reaction to cyber-attacks. In this capacity, Sinkholes are a tool used by both public and private agencies.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice varies across different business sectors in New South Wales. The Notifiable Data Breaches ("NDB") Scheme, for example, only requires not-for-profit businesses with an annual turnover of more than AUD $3 million to report data breaches.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Part IIIA of the Privacy Act specifically regulates the handling of personal information about individuals' activities in relation to consumer credit, including the types of personal information that credit providers can disclose. All credit reporting bodies (defined in ss 6 and 6P as a business that involves collecting, holding, using or disclosing personal information about individuals for the purposes of providing an entity with information about the creditworthiness of an individual) are subject to Part III.

Part 13 of the Telecommunications Act 1997 (Cth) regulates carriers and carriage service providers in their use and disclosure of personal information. Part 5-1A of the Telecommunications (Interception and Access) Act 1979 (Cth) requires providers of telecommunications services in Australia to collect and retain specific types of data for a minimum period of two years and must comply with the Privacy Act in relation to that data.

See generally the answer to question 4.3 below for more information. The NDB Scheme in Part IIIC of the Privacy Act requires the telecommunications and financial services sectors to take steps to secure personal information. These sectors must notify individuals whose personal information is involved in a data breach that is likely to result in serious harm, and must also notify the OAIC.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

A failure by a company to prevent, mitigate, manage or respond to an Incident may result in breaches of provisions of the *Corporations Act 2001* (Cth). The *Corporations Act 2001* (Cth) imposes duties on directors to exercise powers and duties with the care and diligence that a reasonable person would. A director who ignores the real possibility of an Incident may be liable for failing to exercise their duties with care and diligence.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Presently, the Applicable Laws do not require companies to designate a CISO, establish a written Incident response plan or policy, conduct periodic cyber risk assessments or perform penetration tests or vulnerability assessments.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

In February 2018, the Privacy Amendment (Notifiable Data Breaches) Act 2017 amended the Privacy Act to require APP entities to, as soon as practicable, provide notice to the OAIC and affected individuals of an "eligible data breach", where there are reasonable grounds to believe that an "eligible data breach" has occurred. This process is called the Notifiable Data Breaches Scheme.

Eligible data breaches arise when: there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds; this unauthorised disclosure of personal information, or loss of personal information is likely to result in serious harm to one or more individuals; and the entity has not been able to prevent the likely risk of serious harm with remedial action. Indicators such as malware signatures, observable network vulnerabilities and other 'red-flag' technical characteristics may represent reasonable grounds for an APP entity to form a belief that an eligible data breach has occurred.

The OAIC expects APP entities to conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm.

The notification to the OAIC and to the affected individual must include the identity and contact details of the organisation, a description of the data breach, the kinds of information concerned and recommendations about the steps individuals should take in response to the data breach.

A failure to comply with the notification obligations can result in the imposition of substantial civil penalties. A serious or repeated interference with privacy attracts a fine of 2,000 penalty units, currently AUD $420,000.00. The maximum penalty that a court can order for a body corporate is five times the amount listed in the civil penalty provision, currently a maximum of AUD $2.1 million.

The Privacy Act also confers a number of additional enforcement powers on the OAIC, including accepting an enforceable undertaking, bringing proceedings to enforce an enforceable undertaking, making a determination, making orders that the APP entity must redress any loss or damage suffered by the complainant and that the complainant is entitled to payment of compensation for such loss or damage, bringing proceedings to enforce a determination, delivering a report to the responsible Minister and seeking an injunction.

Under the Privacy Act, an APP entity is defined as an "agency" or "organisation". "Agency" includes a Minister, a Department, and most government bodies; and "organisation" means an individual, a body corporate, a partnership, any other unincorporated association or a trust that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

In the performance of its role as an Australian intelligence and security agency, and through its use of foreign signals intelligence and offensive cyber operations, the Australian Signals Directorate ("ASD") may also detect security weaknesses or vulnerabilities in technology that are unknown to the vendor and that may pose a threat to Australians and Australian systems. The ASD will disclose these vulnerabilities only in circumstances where disclosure is determined to be in the Australian national interest.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

The Australian Privacy Principles contained in schedule 1 of the Privacy Act provide for the manner in which APP entities must handle and use personal information. There are 13 privacy principles, covering: open and transparent management of personal information; anonymity and pseudonymity; collection of solicited personal information; dealing with unsolicited personal information; notification of the collection of personal information; the use or disclosure of personal information; direct marketing; cross-border disclosure of personal information; adoption, use or disclosure of government-related identifiers; quality of personal information; security of personal information; access to personal information; and the correction of personal information. The APPs are not prescriptive, and an APP entity must consider how the principles apply to its own situation.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Australian common law does not recognise a general right of privacy. The equitable cause of action for breach of confidence may provide a remedy for invasions of privacy. Traditionally, the elements are that information must be confidential, information must have been imparted in circumstances importing an obligation of confidence and there must be an unauthorised use of that information. The current doctrine of breach of confidence does not currently entertain cases of wrongful intrusion, as opposed to cases of wrongful disclosure of confidential information.

The Privacy Act regulates the way Commonwealth agencies handle personal information. A person may obtain an injunction in the Federal Circuit Court against a Commonwealth agency that engages in, or proposes to engage in, conduct that is in breach of the Privacy Act. An action cannot be brought against an individual acting in their own capacity. A person may apply to the Court for an order that an entity pay compensation for loss or damage suffered by the person if a civil penalty has been made against the entity, or the entity is found guilty of an offence under the Privacy Act.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

No relevant civil proceedings have been brought by individuals in relation to an Incident. Given the evolution of the doctrine of breach of confidence, it is likely such cases will be forthcoming.

Investigations conducted by the OAIC most commonly result in out-of-court outcomes. For example, a joint investigation conducted by the Australian Privacy Commissioner and the Privacy Commissioner of Canada into a highly publicised hacking breach of confidential data held by online adult dating service Ashley Madison, resulted in an enforceable undertaking being entered into by the company pursuant to s. 33E of the Privacy Act.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

The High Court in *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 sanctioned the recognition of a tort of invasion of privacy. Judge Hampel in the case of *Doe v ABC* (2007) VCC 281 imposed liability in tort for the invasion of the plaintiff's privacy. Such reasoning may apply to an action in relation to an Incident.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations are permitted to take out insurance against Incidents in Australia. This includes breaches of the Privacy Act.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limits specifically targeted at losses associated with Incidents. Numerous entities offer insurance for data breach, business interruption, email forgery, ransomware attacks, costs of rebuilding an IT system, theft of crypto-currencies and legal fees associated with the investigation of Incidents. Coverage is governed generally by the *Insurance Act 1973* (Cth), the *Insurance Contracts Act 1984* (Cth), the *Corporations Act 2001* (Cth) and the common law.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

At the Commonwealth level, the *Surveillance Devices Act 2004* (Cth) makes provision for the use of surveillance devices by Federal law enforcement officers.

The *Workplace Surveillance Act 2005* (NSW) (and uniform legislation in all other Australian States and Territories) restricts the use of both overt and covert forms of surveillance of an employee by employers and other members of the public. Surveillance can include computer surveillance. Significant penalties are imposed for breaches of the Act, including imprisonment.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

On 13 December 2017, the Treasury Laws Amendment (Whistleblowers) Bill 2017 (Cth) was introduced in Parliament. The Bill repeals the former whistleblower regime and creates a revised and consolidated whistleblower protection regime in the Corporations Act 2001 (Cth) and a whistleblower protection regime in the Taxation Administration Act 1953 (Cth).

The level of protection afforded to whistleblowers by the new law has been strengthened in a number of key areas including:

- strengthening the requirement of confidentiality of a whistleblower's identity;
- ensuring that persons, including regulators, cannot be required to disclose the identity of a whistleblower to a court or tribunal without a court order;
- strengthening the immunities provided to whistleblowers and ensuring that they are not subject to any civil, criminal or administrative liability following the provision of a qualifying disclosure; and
- broadening the prohibition against victimisation of whistleblowers and increasing the relevant penalties for instances of victimisation.

A qualifying disclosure can be made for information concerning misconduct, including criminal conduct or breach of legal obligation in relation to a regulated entity or related corporate entity.

The regime does not limit but, conversely, facilitates the reporting of cyber risks, security flaws, Incidents or potential Incidents to which there is an element of corporate culpability.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

A number of well-established legal investigatory powers are deployed by law enforcement authorities when investigating an Incident. These powers can include the issuing of search warrants, the seizure of IT equipment for forensic analysis, decryption (whether at encrypted or decrypted data points) and the compulsory examination of suspects in certain circumstances.

The ASD assumes responsibilities for defending Australia from global threats and advances its national interests through the provision of foreign signals intelligence, cybersecurity and offensive cyber operations as directed by the Australian Government. One of the express strategic objections of the ASD is to provide advice and assistance to law enforcement. To this end, the ASD can collaborate with the Federal, State and Territory police forces in relation to matters of national interest, including emerging areas such as cyberterrorism.

See the answer to question 8.2 below for statutory notices which can be issued by law enforcement agencies to access data held by designated communications providers.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

On 8 December 2018, the Federal Parliament passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. The Act provides for the facilitation of covert access to data for the purposes of disrupting and investigating criminal activity, as well as establishing a framework to facilitate lawful assistance from communications providers.

The legislation allows various Australian law enforcement and intelligence agencies to make a Technical Assistance Notice ("TAN"), ordering designated communications providers to provide data or assistance in relation to criminal investigations or matters of security. This may include access to encryption keys or provision of decrypted data. Similarly, Technical Capability Notices ("TCN") can

be issued, mandating that a designated communications provider establish new capability to intercept and decrypt communications that would otherwise be encrypted or inaccessible.

The above notices may be issued in a broad variety of circumstances, including the enforcement of criminal laws and laws imposing pecuniary penalties, either in Australia or in a foreign country, or if it is in the interests of Australia's national security, Australia's foreign relations, or Australia's national economic well-being.

A designated communications provider, including an individual employed or acting on behalf of such providers, who has been compelled to provide data or assistance under a computer access warrant and fails to do so, may face up to 10 years' imprisonment, a fine of up to 600 penalty units (currently AUD $126,000) or both.

S. 3LA of the *Crimes Act 1914* (Cth) also provides law enforcement authorities a mechanism by which a person must provide information or assistance that is reasonable and necessary to allow a constable to: access data held in, or accessible from, a computer or data storage device that is on warrant premises or that has been moved to a place for examination under subsection 3K(2) of the *Crimes Act 1914* (Cth); copy data held in, or accessible from, a computer or storage device; and convert into documentary form, or another form intelligible to a constable, data held in, or accessible from, a computer or data storage device, or data held in a data storage device to which the data was copied, or data held in a data storage device removed from warrant premises under subsection 3L(1A) of the *Crimes Act 1914*.

Acknowledgment

The authors would like to thank Damien Mahon, Solicitor, for his invaluable contribution to the writing of this chapter. Damien assists the Partners on international criminal law cases and cross-border investigations.

Dennis Miralis is a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional regulatory investigations and prosecutions. His areas of expertise include cybercrime, global investigations, proceeds of crime, bribery and corruption, anti-money laundering, worldwide freezing orders, national security law, Interpol Red Notices, extradition and mutual legal assistance law. Dennis advises individuals and companies under investigation for economic crimes both locally and internationally. He has extensive experience in dealing with all major Australian and international investigative agencies.
Full biography: https://ngm.com.au/our-team/dennis-miralis-partner-defence-lawyer/.

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: dm@ngm.com.au
URL: www.ngm.com.au

Phillip Gibson is one of Australia's leading criminal defence lawyers, with over 30 years of experience in all areas of criminal law. Phillip has significant experience in transnational cases across multiple jurisdictions, often involving: white-collar and corporate crime; asset forfeiture; money laundering and proceeds of crime; extradition; mutual legal assistance; Royal Commissions; bribery and corruption; and ICAC and Crime Commission matters. He has extensive experience in dealing with all major Australian and international investigative agencies.
Full biography: https://ngm.com.au/our-team/phillip-gibson-partner-specialist-defence-lawyer/.

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: pg@ngm.com.au
URL: www.ngm.com.au

Jasmina Ceic is an accomplished criminal trial advocate. She advises and acts in complex criminal law matters at all levels of the court system, with a specialist focus on serious matters that proceed to Trial in the Superior Courts, as well as conviction and sentence Appeals heard in the Court of Criminal Appeal. She has represented and advised persons and companies being investigated for white-collar and corporate crime, complex international fraud and transnational money laundering.
Full biography: https://ngm.com.au/our-team/jasmina-ceic-senior-associate/.

Nyman Gibson Miralis
Suite 8, Level 2
154 Marsden Street
Parramatta NSW 2150
Australia

Tel: +61 2 9633 4966
Email: jc@ngm.com.au
URL: www.ngm.com.au

Nyman Gibson Miralis is an international award-winning criminal defence law firm based in Sydney, Australia. For over 50 years it has been leading the market in all aspects of general, complex and international crime, and is widely recognised for its involvement in some of Australia's most significant criminal cases.
Our international law practice focuses on cybercrime, white-collar and corporate crime, transnational financial crime, bribery and corruption, international money laundering, international asset freezing or forfeiture, extradition and mutual legal assistance law.
Nyman Gibson Miralis strategically advises and appears in matters where transnational cross-border investigations and prosecutions are being conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide.

Working with international partners, we have advised and acted in investigations involving the USA, Canada, the UK, the EU, China, Hong Kong, Singapore, Taiwan, Macao, Vietnam, Cambodia, Russia, Mexico, South Korea, British Virgin Islands, New Zealand and South Africa.

www.ngm.com.au

NYMAN GIBSON MIRALIS
Criminal Defence Lawyers and Advisors est. 1966

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Law
Business Crime
Cartels & Leniency
Class and Group Actions
Competition Litigation
Construction & Engineering Law
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investments
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Sanctions
Securitisation
Shipping Law
Telecoms, Media and Internet Laws
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by global legal group