THE CYBER INVESTIGATIONS GUIDE

THIRD EDITION

Editors
Benjamin Powell and Shannon Togawa Mercer

The Cyber Investigations Guide

Third Edition

Editors

Benjamin A Powell

Shannon Togawa Mercer

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-80449-253-6

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

Anderson Mōri & Tomotsune

BCL Solicitors LLP

Clifford Chance US LLP

Cravath, Swaine & Moore LLP

Jones Day

K&L Gates LLP

Nyman Gibson Miralis

Ropes & Gray LLP

Wilmer Cutler Pickering Hale and Dorr LLP

Publisher's Note

The Cyber Investigations Guide is published by Global Investigations Review (GIR), the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature by providing an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its seventh edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation from discovery to resolution.

The Cyber Investigations Guide takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Cyber Investigations Guide* as the close-up.

The Cyber Investigations Guide is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

David Samuels
Publisher
May 2023

CHAPTER 10

Australia

Dennis Miralis, Lara Khider, Mohamed Naleemudeen and Arman Salehirad[1]

Key cybersecurity standards and requirements

Australia's cybersecurity legislative framework comprises of federal, state and territory-based laws. The key legislative instruments are the Privacy Act 1988 (Cth) (the Privacy Act) and the Security of Critical Infrastructure Act 2018 (Cth) (the SOCI Act). The framework also incorporates sector-specific legislation, including the My Health Records Act 2012 (Cth) and the Telecommunications Act 1997 (Cth).

The Privacy Act

On a federal level, the handling of data containing personal information is governed and protected under the Privacy Act. Schedule 1 of the Act contains 13 Australian Privacy Principles (APPs) and governs the standards, rights and obligations around the:

- collection, use and disclosure of personal information;
- an organisation or agency's governance and accountability;
- integrity and correction of personal information; and
- the rights of individuals to access their personal information.

---

1 Dennis Miralis is a partner, Lara Khider is a senior lawyer and Mohamed Naleemudeen Arman Salehirad are defence lawyers at Nyman Gibson Miralis. The authors would like to acknowledge the contributions of defence lawyer Lingwei Kong and paralegal George Papasavvas to the chapter.

'Personal information' is defined under the Privacy Act as 'information or an opinion about an identified individual or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not'.[2]

The Privacy Act imposes obligations on APP entities, which are generally defined as federal government agencies and private sector organisations with an annual turnover of more than A$3 million. Small businesses with a turnover of less than the A$3 million threshold may still be considered APP entities if they fall into an exception, which includes businesses that provide a health service and hold health information, sell or purchase personal information, or provide services to the federal government.[3]

APP entities are obliged to take 'reasonable steps' to implement policies, practices and systems to ensure compliance with APPs. The Privacy Act also requires mandatory reporting for certain APP breaches under the Notifiable Data Breach scheme. Under this scheme, the APP entity in breach must notify the affected individuals and the Office of the Australian Information Commissioner (OAIC).

The OAIC has developed a 'Privacy management framework', which contains a series of governance steps that APP entities should undertake to meet their privacy compliance obligations. The steps include embedding a privacy-compliant culture, establishing robust and effective privacy processes, evaluating privacy processes to ensure continued effectiveness and enhancing responses to privacy issues.[4]

Security of Critical Infrastructure Act

The SOCI Act creates a framework for the regulation and protection of critical infrastructure sectors and imposes registration, reporting and obligation requirements on owners and operators of critical infrastructure. As part of Australia's Cyber Security Strategy 2020, the Australian government introduced critical infrastructure law reforms with the aim of further actively defending Australia's critical infrastructure.[5]

---

2 Privacy Act 1988 (Cth), Section 6.

3 ibid., Sections 6(1), 6C and 6D.

4 Australian Government, Office of the Australian Information Commissioner (OAIC), 'Privacy management framework: enabling compliance and encouraging good practice' (4 May 2015) (https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/privacy-management-framework-enabling-compliance-and-encouraging-good-practice (last accessed 30 March 2023)).

5 Australian Government, Department of Home Affairs, *Australia's Cyber Security Strategy 2020* (Report, 6 August 2020), page 6.

The two tranches of law reform enacted under the Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth) and the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth) came into force on 3 December 2021 and 1 April 2022, respectively. Under the reforms, the scope of the SOCI Act expanded to cover 11 critical infrastructure sectors and 22 classes of critical infrastructure assets. The reforms also introduced 'positive security obligations', requiring entities to manage the security and resilience of their critical infrastructure assets, including the extension of the obligation to report information in the register of critical infrastructure assets, mandatory cybersecurity incident notification obligations and obligations on certain entities to adopt and maintain a risk management programme.[6]

Sector-specific legislation

Entities dealing with personal information in Australia may also have obligations with respect to:

- the My Health Records Act 2012 (Cth) obligations for health information about individuals that is collected and stored in Australia's national online health database;
- the Telecommunications Act 1997 (Cth), which imposes security and notification obligations on Australian telecommunications providers and regulates the use of personal information; and
- federal, state and territory surveillance legislation regulating video surveillance, computer and data monitoring, tracking via the Global Positioning System and the use of listening devices on individuals.

Summary of breach notification rules

APP entities have an obligation under the Privacy Act to comply with the mandatory data breach notification regime.

Mandatory notification applies to data breaches involving personal information, credit reporting information, credit eligibility information and tax file numbers. An 'eligible data breach' occurs when the following requirements are met:

- there is unauthorised access to, unauthorised disclosure of, or loss of, the information that an organisation or agency holds;

6 Security of Critical Infrastructure Act 2018 (Cth), Parts 2, 2A and 2B, as amended by the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth).

- a reasonable person would conclude that the access, disclosure or loss would be likely to result in serious harm to any of the individuals to whom the information pertains; and
- the organisation or agency has not been able to prevent the likely risk of serious harm through remedial action.

'Serious harm' is not defined under the Privacy Act; however, the OAIC has provided examples of what may constitute serious harm. These examples include identity theft (which can affect an individual's finances and credit report) and financial loss through fraud (which is a likely risk of physical harm, serious psychological harm or serious harm to an individual's reputation).[7]

Generally, the regime requires the organisation or agency to assess whether a data breach is likely to result in serious harm within 30 days of the suspected event.

Unless an exception applies, if an APP entity has reasonable grounds to believe that there has been an eligible data breach of the entity, it must prepare, and provide the OAIC with, a copy of a statement as soon as practicable after the entity becomes aware of the breach. The statement must set out the following:

> *(a) the identity and contact details of the entity; and*
> *(b) a description of the eligible data breach . . . ; and*
> *(c) the kind or kinds of information concerned; and*
> *(d) recommendations about the steps that individuals should take in response to the eligible data breach . . .*[8]

Under Section 26WL of the Privacy Act, unless an exception applies, an APP entity must take reasonable steps to notify the contents of the statement provided to the OAIC either:

- to each individual to whom the relevant information relates; or
- to each individual who is at risk of serious harm from the eligible data breach.

If neither of the above is practicable, the APP entity must publish the statement on its website and take reasonable steps to publicise its contents.

---

7 Australian Government, OAIC, 'What is a notifiable data breach' (https://www.oaic.gov.au/privacy/your-privacy-rights/data-breaches/what-is-a-notifiable-data-breach (last accessed 30 March 2023)).

8 Privacy Act 1988 (Cth), Section 26WK(3).

If a data breach does occur but is not assessed as likely to result in serious harm, or where sufficient remedial action has been taken to eliminate the likelihood of serious harm, then there will not be an 'eligible' data breach and there is no requirement for the organisation or agency to notify affected individuals.

There are various exceptions to the requirement to notify affected individuals and (or) the OAIC of a data breach notification, including where:

- compliance by a law enforcement body would be likely to prejudice its enforcement-related activities;
- notification would be inconsistent with a Commonwealth secrecy provision; and
- the OAIC grants an exception (an APP entity would need to apply for such an exception).

Best practices for cyber incident response

All organisations should have a cyber incident response plan (CIR) to ensure an effective response and prompt recovery in the event of a cybersecurity incident. The OAIC recommends that all organisations, including small and medium-sized businesses, should adopt a CIR as malicious cyber activity against Australian entities is increasing in frequency, scale and sophistication.[9]

The OAIC has published a 'Cyber Incident Response Plan – Guidance & Template' and a 'Cyber Incident Response Readiness Checklist' to assist organisations in developing an effective CIR.[10] Organisations should note that this is a general framework for a CIR that must align with their own incident, emergency, crisis and business continuity arrangements, as well as jurisdictional and national cyber and emergency arrangements.[11] Organisations should also support personnel to fulfil their roles by outlining their responsibilities and all legal and regulatory obligations.

The OAIC states that an organisation's CIR should include:

- developing a cybersecurity policy or strategy that outlines the organisation's approach to prevention, preparedness, detection, response, recovery, review and improvement;

---

9 Australian Government, Australian Cyber Security Centre (ACSC), 'Cyber Incident Response Plan' (July 2022) (https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-incident-response-plan (last accessed 30 March 2023)).

10 id.; and Australian Government, ACSC, *Cyber Incident Response Plan – Readiness Checklist* (July 2022) (https://www.cyber.gov.au/sites/default/files/2022-07/ACSC%20Cyber%20Incident%20Readiness%20Checklist_A4.pdf (last accessed 30 March 2023)).

11 'Cyber Incident Response Plan', op. cit. note 9.

- allocating and training staff, including a critical incident response team, to be involved in managing and responding to cyber incidents;
- documenting all critical assets, logging all incidents and tracking all technologies used to manage a response;
- creating processes to support the organisation in meeting its legal and regulatory requirements on cyber incident notification, reporting and response;
- engaging with third parties to assist in monitoring threats and assessing the organisation's technical systems and processes;
- maintaining a secure location to store data captured during an incident, which could be used as evidence of the incident and the adversary's tradecraft, and shared with third-party stakeholders if needed; and
- creating processes to conduct post-incident reviews after an incident.

The OAIC recommends the developed CIR be tested and reviewed regularly.

The Australian Cyber Security Centre (ACSC) has also published *Guidelines for Cyber Security Incidents* to assist organisations in responding to cybersecurity incidents.[12] These Guidelines provide steps that organisations should take when preparing for, responding to and recovering from cyber incidents. These steps include establishing an incident management policy, logging and analysing any suspicious user activity, and ensuring cybersecurity staff have access to sufficient data sources and tools.

The ACSC's *Strategies to Mitigate Cyber Security Incidents* publication also sets out several recommended measures for organisations in responding to cybersecurity incidents. The ASCS's strategies include monitoring or active defensive components, such as filtering email and web content, and frequent analysis of data.[13]

Optus data breach

The Optus data breach demonstrated that businesses without rigorous cyber practices can suffer data breaches and cybersecurity incidents that have a wide-scale impact on a state and its population.

---

12 Australian Government, ACSC, *Guidelines for Cyber Security Incidents* (Information Security Manual, 2 March 2023) (https://www.cyber.gov.au/sites/default/files/2023-03/04.%20ISM%20-%20Guidelines%20for%20Cyber%20Security%20Incidents%20%28March%202023%29.pdf (last accessed 30 March 2023)).

13 Australian Government, ACSC, *Strategies to Mitigate Cyber Security Incidents* (last updated February 2017) (https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Strategies%20to%20Mitigate%20Cyber%20Security%20Incidents%20%28February%202017%29.pdf (last accessed 30 March 2023)).

On 22 September 2022, Optus became the victim of a cyberattack that resulted in the disclosure of their customers' personal information.[14] Optus announced that a hacker had accessed the records of between 2.5 million and 9.7 million current and former customers.[15] In some cases, that data included driving licence, passport and Medicare details, putting customers at risk of fraud.

It was reported that cybercriminals were able to obtain personal data with relative ease as Optus's application programming interface (API) was not secured and did not require authorisation or authentication to access customer data.[16] In this instance, any user with knowledge and experience of using devices that directly connect to an information-exchange network could have accessed information on Optus's API.

Optus has been criticised for its poor cybersecurity processes and preparation, which has led to one of Australia's largest cyber incidents.[17] Systemic issues in Optus's preparation, including adequately securing its data and thorough logging of its API, are flagged as issues that should have been addressed. Optus was also noted to be struggling with a shortage of skilled cybersecurity professionals. However, Optus's response to the incident itself was effectively handled, as its incident response team was able to secure its systems and report the incident within a short timeframe.[18] Optus immediately engaged with cybersecurity experts to assist with securing the system and capturing data that could be used as evidence.

---

14 Australian Securities and Investments Commission, 'Guidance for consumers impacted by the Optus data breach' (https://asic.gov.au/about-asic/news-centre/news-items/guidance-for-consumers-impacted-by-the-optus-data-breach/ (last accessed 30 March 2023)).

15 Tory Shepherd, 'The biggest hack in history: Australians scramble to change passports and driver licences after Optus telco data debacle', *The Guardian* (1 October 2022) (https://www.theguardian.com/business/2022/oct/01/optus-data-hack-australians-scramble-to-change-passports-and-driver-licences-after-telco-data-debacle (last accessed 30 March 2023)).

16 John Davidson, 'All Optus customers can do is hope', *The Australian Financial Review* (26 September 2022) (https://www.afr.com/technology/all-optus-customers-can-do-is-hope-20220925-p5bku9 (last accessed 30 March 2023)).

17 Stephen Withers, 'Optus breach casts spotlight on cyber resilience', ComputerWeekly.com (29 September 2022) (https://www.computerweekly.com/news/252525513/Optus-breach-casts-spotlight-on-cyber-resilience (last accessed 30 March 2023)).

18 Paul Smith, 'Inside the Optus hack that woke up Australia', *The Australian Financial Review* (22 December 2022) (https://www.afr.com/technology/inside-the-optus-hack-that-woke-up-australia-20221123-p5c0lm (last accessed 30 March 2023)).

Following the cyberattack, there has been a paradigm shift in viewing the corporation's role as a custodian of personal information on behalf of customers. The Australian Information Commissioner, Angelene Falk, noted that the 'regulatory framework needs to shift the dial to place more responsibility on organisations who are the custodians of Australians' data, to prevent and remediate harm to individuals caused through the handling of their personal information'.[19]

Cybersecurity and incident response trends

Australia continues to struggle against rising rates of cybercrime.

The Australian Signals Directorate (ASD) in its annual cyber threat report for 2021–2022 stated that the ACSC had received more than 76,000 reports of cybercrime.[20] This was a 13 per cent increase from the previous financial year. The ACSC stated that the most commonly reported cybercrimes were online fraud (26.9 per cent), online shopping (14.4 per cent), online banking (12.6 per cent) and investment (12.2 per cent).

There was also a rise in the average cost of cybercrimes reported by businesses. In 2021–2022, the cost of reported cybercrime was more than A$39,000 for small businesses, A$88,000 for medium businesses and more than A$62,000 for large businesses.[21]

Ransomware attacks remain the most destructive cybercrime threat, having have increased in Australia by nearly 500 per cent since the start of the covid-19 pandemic. Several high-profile ransomware attacks have resulted in millions of Australians' data being published online.[22] These attacks targeted large institutions, including telecommunications, medical and financial services providers.

During this recorded period, the ASCS responded to more than 1,100 cybersecurity incidents.[23] The ASCS noted that a majority of these incidents could have been avoided by adequate CIR.

---

19 Australian Government, OAIC, 'OAIC updated statement on Optus data breach' (29 September 2022) (https://www.oaic.gov.au/updates/news-and-media/oaic-updated-statement-on-optus-data-breach (last accessed 30 March 2023)).

20 Australian Signals Directorate, ACSC, *ACSC Annual Cyber Threat Report, July 2021 to June 2022* (4 November 2022), page 11 (https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf (last accessed 30 March 2023)).

21 ibid., page 24.

22 Australian Government, OAIC, 'Cyber security incidents impact data breach risk' (1 March 2023) (https://www.oaic.gov.au/newsroom/cyber-security-incidents-impact-data-breach-risk (last accessed 30 March 2023)).

23 'Cyber Incident Response Plan', op. cit. note 9.

Australian businesses' CIR shortcomings can be partially attributed to shortages of cyber skills.[24] The need for cybersecurity experts has increased because of surging cybercrime and cyber risks. Industry groups believe that the country's shortfall in cybersecurity professionals will hit 30,0000 unfilled positions by 2026. However, recruiting these professionals will be a challenge as Australia will have to compete with more developed markets in the United Kingdom, the United States and Canada.

Regulatory considerations

High-profile data breaches and the rise in cybercrime have intensified the focus on Australia's regulatory issues.

The OAIC regulates data protection and privacy in Australia.[25] The OAIC has powers under the Privacy Act to investigate, resolve complaints, make determinations and provide remedies for breaches under the Notifiable Data Breach (NDB) scheme. These remedies range from enforceable undertakings to civil penalties.[26] The OAIC reported that, between 2021 and 2022, it finalised 14 privacy determinations.[27] The outcomes of these determinations included apologies, records being amended and compensation being paid. Infrequently, the OAIC also uses enforceable undertakings to enforce future compliance with the Privacy Act.

The OAIC's regulation and enforcement have been criticised for being weak and ineffective. The OAIC has provided limited compensation to claimants in privacy determinations, opting to penalise businesses with low fines or an order to issue an apology.[28] Further, the regulator has been hesitant to utilise

24 Max Mason, 'Cyber skills shortage to "hit 30,000 in four years"' *The Australian Financial Review* (13 September 2022) (https://www.afr.com/technology/cyber-skills-shortage-to-hit-30-000-in-four-years-20220912-p5bhde (last accessed 30 March 2023)).

25 Privacy Act 1988 (Cth) s 27.

26 Australian Government, OAIC, 'Privacy regulatory action policy' (last updated December 2022) (https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/privacy-regulatory-action-policy (last accessed 30 March 2023)).

27 Australian Government, OAIC, *Annual Report 2021-22* (28 September 2022), page 39 (https://www.oaic.gov.au/__data/assets/pdf_file/0021/23097/OAIC_annual-report-2021-22_final.pdf (last accessed 30 March 2023)).

28 Australian Government, OAIC, 'Privacy determinations' (https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/privacy-determinations (last accessed 30 March 2023)).

its civil penalty provisions. The OAIC's shortcomings have contributed to the weak regulatory environment that has resulted in businesses either avoiding their compliance obligations or failing to understand their obligations.[29]

However, the OAIC's powers have been increased by legislative amendments that came into effect in November 2022. In response to the high-profile data breaches, the government passed the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, which amended the Privacy Act. The amendments provided the OAIC with the following greater enforcement powers:

- The OAIC can request information from an entity regarding its compliance with the NDB scheme or following an actual or suspected data breach of that entity.
- If an entity engages in conduct that causes an interference with the privacy of an individual, the OAIC can make determinations requiring the relevant entities to prepare and publish more detailed statements, including a description of the conduct and the steps to be taken to ensure the conduct is not repeated or continued.
- The OAIC can issue infringement notices for non-compliance with requests for information.
- The ability of the OAIC to share information with other enforcement bodies, including foreign data protection authorities, has been enhanced.
- The OAIC is empowered to publish certain information if it is in the public interest to do so.

The amendments also increased the maximum penalty for serious and repeated interferences with privacy to an amount not more than the greater of A$50 million, three times the value of any benefit obtained through misuse of the information in question, or 30 per cent of the entity's annual Australian turnover. The government has also substantially increased funding to the OAIC.[30]

---

29 Australian Government, Attorney-General's Department, *Privacy Act Review – Report 2022*, page 260 (https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf (last accessed 30 March 2023)).

30 Australian Government, OAIC, 'OAIC welcomes additional Budget funding' (26 October 2022) (https://www.oaic.gov.au/newsroom/oaic-welcomes-additional-budget-funding2 (last accessed 30 March 2023)).

There is likely to be an increase in the OAIC's regulatory and enforcement action as a result of its increased powers and funding, coupled with the public appetite for government action against non-compliant entities following the high-profile data breaches.

In light of the OAIC's increased powers, it would be prudent for businesses to take steps to ensure that its cybersecurity risk management and controls satisfy the Privacy Act and APP requirements. The OAIC's privacy management framework helps businesses to satisfy their continuing compliance obligations.[31] The framework is drafted in general terms to accommodate the varying sizes, services and resources of entities, and includes steps such as:

- assigning staff with responsibility for managing privacy;
- developing and maintaining processes around the handling, collecting and disposing of personal information;
- regular monitoring and reviewing of privacy processes, policies and notices; and
- engaging external assessors and auditors to assess the privacy and risk management processes and systems.

A further increase of the OAIC's powers may be on the horizon. On 16 February 2023, Australia's Attorney-General released *Privacy Act Review – Report 2022*, which includes 116 proposals for reforming the Privacy Act.[32] This Report includes several proposals that would enhance the OAIC's regulatory and enforcement powers, including new civil penalties, new powers concerning investigations, public inquiries and determinations and a shorter timeframe for entities to report eligible data breaches to the OAIC.[33]

The Report also proposes that the OAIC should publish guidance to assist businesses to understand and implement their obligations and understand the thresholds for enforcement actions and consequences for non-compliance.

---

31 Australian Government, OAIC, 'Privacy management plan template' (16 May 2016) (https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/privacy-management-plan-template (last accessed 30 March 2023)).

32 *Privacy Act Review – Report 2022*, op. cit. note 29.

33 ibid., pages 252–303.

Litigation considerations

Civil claims by individuals

Individuals who have suffered loss or damage because of a business's cyber breach or data breach have minimal avenues to pursue a direct right to action. The Privacy Act is silent on this matter. Therefore, there has been minimal private litigation in Australia against companies and their directors by individuals for data security incidents and breaches.

In 2019, the Australian Competition and Consumers Commission highlighted that the minimal litigation is a result of individuals not having appropriate avenues to pursue private action.[34]

The Australian Attorney-General's *Privacy Act Review – Report 2022* proposed a direct right of action for individuals who have suffered loss or damage as a result of interference with their privacy.[35] The proposed action would allow individuals to seek compensation in the Federal Court or the Federal Circuit Court. The recommendation is to compensate individuals who suffer loss or damage directly as a result of an organisation's contravention of its data protection obligations. The report also recommended the introduction of a statutory tort for serious invasions of privacy that are intentional or reckless.[36] Under the proposal, individuals may claim damages for emotional distress even if the invasion of privacy did not cause actual damage.

Class actions

There has been minimal class action litigation activity in Australia concerning cyberattacks. This is because there is no specific personal statutory right or cause of action for a claimant to make a claim in respect of a cyber breach or data breach. Therefore, claimants will likely have to rely on common law causes of action, including the tort for breach or invasion of privacy.

The High Court of Australia, in *Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd*,[37] rejected recognising a general right in Australia and a corresponding tort for a breach or invasion of privacy. However, this issue is likely to be

34 Australian Government, Australian Competition & Consumer Commission, *Digital Platforms Inquiry – Final Report* (June 2019), page 478 (https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf (last accessed 30 March 2023).

35 *Privacy Act Review – Report 2022*, op. cit. note 29, page 272.

36 ibid., page 286.

37 *Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd* [2001] 208 CLF 199.

tested again in the Australian courts by the class action litigations concerning the respective data breaches of telecommunications provider Optus and healthcare provider Medibank Private, which are likely to unfold during the coming year.

Optus is currently being investigated by the law firms Maurice Blackburn and Slater and Gordon for potential class action lawsuits.[38] These investigations follow Optus data being breached following a cyber incident, with the personal information of millions of Australians being compromised. On 11 October 2022, the OAIC opened an investigation into Optus over the data breach.[39]

Medibank data breach

In October 2022, Medibank Private was targeted in a cyberattack. The cyber-criminals accessed and published 200 gigabytes of data containing the personal details of 9.7 million current and former customers.

The company is now facing four separate class action lawsuits, with Baker and McKenzie being the most recent firm to file a class action.[40] The class actions allege that Medibank breached the privacy of its customers by failing to adequately protect the personal and health information of its current and former customers.[41]

The data included personal information such as current and former customers' personal details, policy numbers and claims data.[42] The latter included details of where medical services were received and codes relating to diagnoses and procedures.

---

38 Kate Austin, et al., 'A step into the breach – will the Optus incident give rise to more data breach class actions?' (Allens, 12 October 2022) (https://www.allens.com.au/insights-news/insights/2022/10/a-step-into-the-breach-will-the-optus-incident-give-rise-to-more-data-breach-class-actions/ (last accessed 30 March 2023)).

39 Australian Government, OAIC, 'OAIC opens investigation into Optus over data breach' (11 October 2022) (https://www.oaic.gov.au/newsroom/oaic-opens-investigation-into-optus-over-data-breach (last accessed 30 March 2023)).

40 Josh Taylor, 'Medibank class action launched after massive hack put private information of millions on dark web', *The Guardian* (16 February 2023) (https://www.theguardian.com/australia-news/2023/feb/16/medibank-class-action-launched-data-breach-private-information-dark-web (last accessed 30 March 2023)).

41 Colin Kruger, '"Case closed": Medibank faces heavy fines as hackers dump customer data', *The Sydney Morning Herald* (1 December 2022) (https://www.smh.com.au/business/companies/case-closed-medibank-hackers-release-massive-data-file-20221201-p5c2pu.html (last accessed 30 March 2023)).

42 Josh Taylor, 'Medibank hackers announce "case closed" and dump huge data file on dark web', *The Guardian* (1 December 2022) (https://www.theguardian.com/australia-news/2022/dec/01/medibank-hackers-announce-case-closed-and-dump-huge-data-file-on-dark-web (last accessed 30 March 2023)).

The AFP stated that a Russian hacking group was responsible for the cyberattack.[43] The AFP Commissioner said that the group was responsible for various cybercrime incidents and was run like a business supported by affiliates and associates.

In December 2022, the OAIC commenced an investigation into Medibank's practices in handling personal information in relation to the cyberattack. The OAIC said its investigation 'will focus on whether Medibank took reasonable steps to protect the personal information [it] held from misuse, interference, loss, unauthorised access, modification or disclosure'.[44]

The OAIC also stated that Medibank may be liable for civil penalties of up to A$2.2 million for each contravention if its investigation finds serious and (or) repeated interferences with privacy in contravention of Australian privacy law.[45] The results of the investigation are yet to be published.[46]

Notable civil action

The Federal Court matter of *Australian Securities and Investments Commission v. RI Advice Group Pty Ltd*[47] was a significant enforcement action. It is likely to see an expansion of the Australian Securities and Investments Commission's (ASIC) minimum requirements for a corporation's cybersecurity governance and cyber resilience framework.

On 5 May 2022, the Federal Court made declarations that RI Advice Group Pty Ltd (RI Advice), an Australian financial services licensee, breached its licence obligations to act efficiently and fairly when it failed to have adequate risk management systems to manage its cybersecurity risks.[48]

The finding came after nine cybersecurity incidents occurred involving authorised representatives of RI Advice between June 2014 and May 2020. The incidents resulted in the potential compromise of confidential and sensitive personal information of several thousand clients and other persons.

---

43 See https://www.afp.gov.au/news-media/media-releases/statement-afp-commissioner-reece-kershaw-medibank-private-data-breach (last accessed 30 March 2023).

44 Australian Government, OAIC, 'OAIC opens investigation into Medibank over data breach' (1 December 2022) (https://www.oaic.gov.au/newsroom/oaic-opens-investigation-into-medibank-over-data-breach (last accessed 30 March 2023)).

45 'OAIC opens investigation into Optus over data breach' op. cit. note 39.

46 'OAIC opens investigation into Medibank over data breach', op. cit. note 44.

47 *Australian Securities and Investments Commission v. RI Advice Group Pty Ltd* [2022] FCA 496.

48 ibid., paragraphs 27–28.

ASIC argued that under Section 912A of the Corporations Act 2001 (Cth), the 'core obligations' for an Australian financial services licence holder extended to cybersecurity, which required licence holders to have adequate strategies, frameworks, policies and other processes in place to manage cybersecurity and cyber resilience risk for itself and its network of authorised representatives.[49] ASIC demonstrated that RI Advice had not met these obligations based on the cyber incidents between June 2014 and May 2020.

The Honourable Justice Helen Rofe recognised that it is impossible to eliminate all cybersecurity risks, but that directors and officers must materially reduce the risk 'through adequate cybersecurity documentation and controls to an acceptable level'.[50] Adequate steps for cybersecurity and cyber resilience include identifying relevant risks in the course of providing services, adequate documentation and controls, and being informed technical experts in the area.

The matter was resolved through consent orders that required RI Advice to engage a cybersecurity expert to identify and implement what, if any, further measures are necessary to adequately manage cybersecurity risks across RI Advice's authorised representative network. RI Advice was also ordered to pay A$750,000 towards ASIC's costs.[51]

The Federal Court's declarations are likely to shape future enforcement action by ASIC and other regulators. Therefore, directors and officers should ensure that they are implementing adequate steps to control cybersecurity and cyber resilience risks by:

- identifying and understanding the risks that affect their company and industry;
- developing adequate documentation, controls and risk management systems with the assistance of technical experts;
- routinely engaging with a technical expert to assess and continually improve the risk management processes and controls; and
- having an incident response plan to minimise any damage caused by a successful data breach.

This is particularly important to directors and officers with a statutory obligation to manage risks.

49 ibid., paragraph 5.

50 ibid., paragraph 58.

51 ibid., paragraph 5, Order 6.

Types of threats and threat actors

Criminal, nation state, insider (intentional and accidental)

Criminal

The ACSC has identified cybercriminals as the most prominent threats to Australia's cybersecurity.

In 2021–2022, cybercriminals most commonly targeted individuals through methods such as online banking and shopping compromise.[52] Business email compromise[53] (BEC) trended towards targeting high-value transactions, such as property settlements. BEC was also used to target the personal information and login details of high-level users in businesses.

Cybercrime-as-a-service is an increasing cybercrime threat to Australia. This system encompasses an ever-increasing range of purchasable tools, services and information used to facilitate cybercriminal operations. The ACSC reported that this service has lowered the barrier to entry for individuals, allowing individuals with limited experience and access to sophisticated devices to engage in cybercrime.[54]

The Optus data breach was part of a string of high-profile attacks on Australian businesses by cybercriminals.[55] These incidents have resulted in millions of Australians having their personal information and data illegally accessed and published in forums.

The Australian Federal Police (AFP) announced that it was working with overseas law enforcement to identify the offenders behind the attack and to protect the Australian community.[56] The AFP also launched Operation Hurricane to identify the cybercriminals behind the Optus breach and protect Australians from identity fraud. The operation includes a joint partnership between law

52 Australian Government, Australian Signals Directorate, ACSC, *ACSC Annual Cyber Threat Report – July 2021 to June 2022* (4 November 2022), page 23 (https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf (last accessed 30 March 2023)).

53 Business email compromise is a type of phishing attack that targets organisations, with the aim of stealing money or critical information.

54 *ACSC Annual Cyber Threat Report – July 2021 to June 2022*, op. cit. note 47, page 39.

55 'The biggest hack in history: Australians scramble to change passports and driver licences after Optus telco data debacle', op. cit. note 15.

56 Australian Federal Police, 'AFP working with overseas law enforcement on Optus breach' (26 September 2022) (https://www.afp.gov.au/news-media/media-releases/afp-working-overseas-law-enforcement-optus-breach (last accessed 30 March 2023)).

enforcement, the private sector and industry to combat the growing threat of cybercrime. On 6 October 2022, the AFP announced the arrest of one person involved in the cyberattack.[57]

Nation state

Australia as a state faces threats from various actors, including other states, cybercriminal groups and individuals.

The Australian Signals Directorate (ASD) stated in its annual report that Australia is targeted by persistent cyber espionage, which is often conducted or directed by foreign intelligence services.[58] The head of the ASD, Rachel Noble, expressly stated that espionage is driven by 'state-based actors who are sophisticated and capable and they have enormous amounts of money and people to put at this endeavour'.[59]

In response to Russia's invasion of Ukraine, the ACSC and counterpart agencies in the United States, Canada, the United Kingdom and New Zealand (collectively the Five Eyes) released a joint cybersecurity advisory titled 'Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure'.[60]

The government has also publicly criticised China and Iran for using cyber warfare against Australia and its allies. In July 2021, Australia joined the United States, the United Kingdom and other countries in levelling accusations at China's Ministry of State Security for exploiting Microsoft Exchange vulnerabilities that

57 Nick Bonyhady, 'Teenager arrested for alleged scam on Optus victims as government lets telco share data,' *The Sydney Morning Herald* (6 October 2022) (https://www.smh.com.au/technology/banks-to-get-optus-customers-identification-data-after-cyberattack-20221005-p5bnes.html (last accessed 30 March 2023)).

58 *ACSC Annual Cyber Threat Report – July 2021 to June 2022*, op. cit. note 47.

59 Matthew Knott, 'Cybercrime gangs combining with nation-states in "profound" new trend' *The Sydney Morning Herald* (4 November 2022) (https://www.smh.com.au/politics/federal/cybercrime-gangs-combining-with-nation-states-in-profound-new-trend-20221103-p5bv7h.html (last accessed 13 April 2023)).

60 Joint Cybersecurity Advisory: AA22-110A, 'Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure' (20 April 2022) (https://www.cyber.gov.au/acsc/view-all-content/advisories/russian-state-sponsored-and-criminal-cyber-threats-critical-infrastructure (last accessed 30 March 2023)).

brought down thousands of computer networks worldwide. A few months later, Australia was part of a joint Five Eyes advisory in November 2021 that confirmed the exploitation of these vulnerabilities by an Iranian state actor.[61]

Insider (intentional and accidental)

In the past few years, data breaches caused by insiders have tended to result from accidental actions.

The ASCS reported that in 2021–2022, the majority of significant incidents arose in organisations that have a lack of or insufficient patching (i.e., outdated software and operating systems).[62] Cybercriminals used targeted forms of phishing such as BEC to take advantage of businesses' practices and systems.

61 Joint Cybersecurity Advisory: AA21-321A, 'Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities' (17 November 2021) (https://www.cyber.gov.au/sites/default/files/2021-11/AA21-321A-Iranian_Government-Sponsored_APT_Cyber_Actors_Exploiting_Microsoft_Exchange_and_Fortinet_Vulnerabilities.pdf (last accessed 30 March 2023)).

62 *ACSC Annual Cyber Threat Report – July 2021 to June 2022*, op. cit. note 47.