IIS Partners

REFORMS TO IMPROVE THE RESILIENCE OF AUSTRALIA'S CRITICAL INFRASTRUCTURE

What businesses need to know about amendments to the *Security of Critical Infrastructure (SOCI) Act 2018* (Cth)

By Mike Trovato and Sascha Hess

July 2022

Reforms to the Security of Critical Infrastructure (SOCI) Act are being implemented

Critical (and vulnerable) infrastructure

Australia's dependency on and the vulnerability of essential services has been on display in recent years. We have experienced issues ranging from grocery supply shortages [1], heavily strained hospital services [2], to soaring fuel [3] and electricity prices [4].

In addition to being vulnerable to natural disasters and consequences of the global COVID-19 pandemic, digital transformations and growing interconnectivity have made critical infrastructure a valuable cyber target. In Australia, recent examples of ransomware crippling operations include a meat producer [5], transport company [6], and hospital [7]. Malicious actors have also compromised the parliamentary network [8] and the Bureau of Meteorology (BOM) [9]. The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) reported that approximately one quarter of reported incidents in 2020-21 were associated with critical infrastructure [10].

Is Australia's critical infrastructure sufficiently resilient? The answer can be found in *Australia's Cyber Security Strategy 2020* report which called for strengthening the protection of critical infrastructure across a wide range of sectors [11].

The reforms to the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act) are one of several legislative frameworks either under review or already in force. *Australia's Cyber Security Strategy 2020* report and discussion paper laid out several interdependent and concerted efforts, including reviews of interconnected legislative frameworks such as the *Privacy Act 1988* (Cth) (Privacy Act), *Corporations Act 2001* (Cth), Australian Consumer Law and, of course, the SOCI Act [12].

The updates to the SOCI Act aim to raise the bar on resilience for Australia's critical infrastructure and reduce the likelihood of data breaches that either cause harm to Australians or are leveraged as part of targeted attacks against critical infrastructure.

Impactful legislative changes

The SOCI Act has expanded to cover 11 sectors from the previous four sectors and added cyber-related obligations. Essentially, the Act requires regulated entities to:

- allow the government to assist and intervene as part of a serious security incident response
- register and report on critical infrastructure assets
- report cyber incidents promptly
- implement and annually report on an adequate Risk Management Program
- fulfill additional enhanced cyber obligations if assets are declared a 'system of national significance'.

Holistic and robust risk management systems should create the bulk of SOCI compliance as a by-product and minimise any compliance burden

Government assistance applies to all 11 critical infrastructure sectors but 'positive security obligations' (PSOs) are 'switched-on' and adjusted with rules for the 22 specified asset classes. At this stage, there are two PSOs that can be switched on:

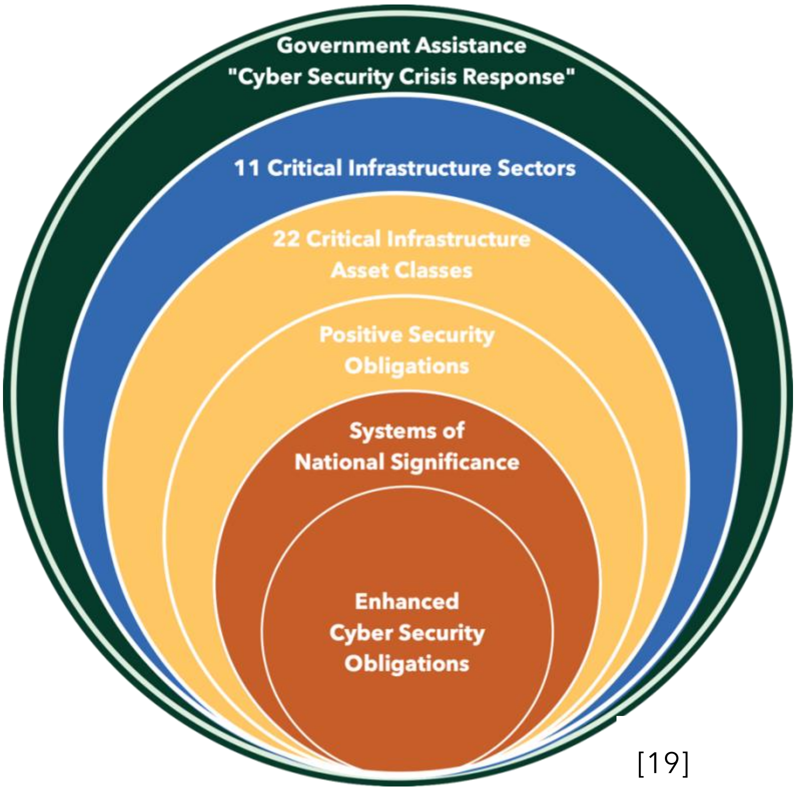
1. a requirement to provide ownership and operational information of critical assets to the Register of Critical Infrastructure Assets, and
2. a requirement to report cyber incidents to the ACSC.

Under the SOCI Act amendments, 12 (banking; broadcasting; domain name systems; electricity; financial market infrastructure; food and grocery, freight infrastructure; freight services; gas; insurance assets; liquid fuel; and superannuation) of the identified 22 asset classes require further rules to be made to finalise the assets that are subject to the enhanced regulatory framework.

Apart from the Risk Management Program (RMP) obligations, the requirements outlined above are already in force for many assets classes. The RMP Rules and applicability are intended to be 'switched-on' next (though the timing is uncertain due to the recent change of Government).

Owners or operators of critical assets are privately notified and consulted in the case that their assets are declared a 'system of national significance' (SoNS). For these assets, a set of 'enhanced cyber obligations' can be requested, such as: providing incident response plans, participating in cyber security exercises, sharing vulnerability assessments, and providing additional access to system information.

The Cyber and Infrastructure Security Centre (CISC) provides useful resources on the relevant obligations for various industry sectors and asset classes at www.cisc.gov.au.


Government Assistance
"Cyber Security Crisis Response"
11 Critical Infrastructure Sectors
22 Critical Infrastructure Asset Classes
Positive Security Obligations
Systems of National Significance
Enhanced Cyber Security Obligations

[19]

Organisations should strive for compliance artefacts to be a by-product of their governance, risk and compliance (GRC) systems

Compliance as a by-product

Risk management is a basic and necessary part of running organisations and cyber security risks have been a key concern for both public and private sector organisations alike [13].

The intent of the Australian Government to strengthen corporate governance around cyber resilience is clearly articulated in the discussion paper *Strengthening Australia's cyber security regulations and incentives* [14] and was reinforced with Australia's first cyber case ruling against a company for failing to have 'adequate risk management systems to manage its cyber security risks' (*ASIC v RI Advice Group Pty Ltd* [2022] FCA 496) [15]. ASIC has since commented that it may enforce a firm's cyber security risk management obligations if it considers that these have not been met [16].

Regardless of regulatory obligations, it is clear why investing in robust risk management skills, tools and systems is important – the risk landscape is becoming more complex and dangerous with the progressive adoption of technology and rapidly rising cyber threat levels.

Organisations should strive for compliance artefacts to be a by-product of their governance, risk and compliance (GRC) systems and review their existing system to identify any adjustments that might reduce their additional reporting burden.

Additional resources may be required initially to meet the new SOCI Act obligations, particularly if the current Risk Management Program requires uplifting. Particular industries in need of enhancing GRC include those that are attractive targets for criminals and other threat actors, as well as those that have historically been slow to implement cyber security protections due to risk-discounting and overly cost-focused management. The enhanced legislation makes these GRC investments (such as cyber security tools) a requirement.

Registration and incident notification requirements are relatively easy to embed in existing processes. Specifically, the incident notification requirement is likely already implemented by organisations with existing assessment and notification mechanisms that address other regulations such as APRA's Prudential Standard CPS 234, Australian Privacy Act or EU General Data Protection Regulation. Reporting the same incident to multiple authorities may be required.

However, validating that an organisation's current Enterprise Risk Management System is producing the right evidence for the upcoming Risk Management Program Rules is likely to be more involved for the 'switched-on' asset classes.

The requirements echo longstanding and contemporary concerns alike, including a holistic all-hazard approach which includes people, supply chain risks and demonstrable governance over good risk management practices.

Organisations should consider implementing a governance framework that addresses all of their data, privacy, and security objectives cohesively

The proposed rules further require responsible entities to ensure that their Risk Management Program includes details on how the organisation complies with at least one of the listed standards or any equivalent cyber security framework.

Frameworks come to the rescue

While there are many cyber security frameworks to choose from, organisations should consider a framework that includes all of their data, privacy, and security objectives. Organisations may want to choose a primary framework and then add missing and localised components from other sources (e.g., Australian Privacy Principles (APPs), ACSC's Essential Eight, CPS 234). A possible framework to consider, even for industries outside of the energy sector, is the Australian Energy Sector Cyber Security Framework (AES CSF). The AES CSF combines elements from the NIST framework, Cybersecurity Capability Maturity Model, APPs and the Essential Eight.

The required annual compliance attestation of the Risk Management Program will also need to list the incidents that had a 'significant' or 'relevant' impact on one or more of an organisation's critical infrastructure assets and evaluate the effectiveness of the risk program considering the event.

Interestingly, the Explanatory Memorandum for the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* provides insights on what may be considered a 'significant' or 'relevant' impact [17]. While this clearly will vary between assets and across sectors, it does include considerations of events with an impact that has caused harm to customers or detrimentally impacted an organisation's information security, including theft or unauthorised access of, sensitive information or personal information.

This serves as a reminder that a privacy breach, particularly a Notifiable Data Breach under the Privacy Act may have a significant or relevant impact on critical infrastructure and should not be underestimated. The privacy breach experienced by Service NSW in 2020 [18] is a recent example of how devastating and damaging a breach can be to individuals (both customers and employees) as well as the associated financial cost and business disruption for the impacted entity.

Boards will want to ensure their Executives are accountable and responsible to deliver on the key requirements of the updated SOCI Act

Time to act

Organisations are well advised to stay abreast of the increasingly complex regulatory environment as the updated SOCI Act is just one piece of the Government's roadmap of reforms around privacy, data and security.

For entities responsible for critical assets, the PSOs are about to be 'switched on'. Now is a good time for these organisations to review their existing processes, incorporate the requirements and uplift their practices.

Boards will want to ensure their Executives are clearly accountable and responsible to deliver on these key requirements. Since Russia's attack on Ukraine, most Five Eyes countries have been delivering a strong message that cyber attacks and ransomware are coming – and to be prepared.

If the SOCI Act requirements are adequately addressed by organisations, this will have a positive effect on risk reduction. It would be an unenviable position for Boards and Executives to be in should any penny-pinching or risk discounting result in the need to consider paying a ransom to an attacker.

Please contact IIS Partners (contact@iispartners.com) if you would like to know more about the SOCI Act requirements or require assistance in uplifting your cyber security posture to address your risk and compliance obligations.

Key Questions for Boards and Executives

Boards:

- Do we have a comprehensive view on upcoming changes called out in the SOCI Act (as amended) that may impact our organisation?
- Is our organisation equipped to deal effectively with an increasingly complex cyber security regulatory environment?
- Is our current cyber security governance mechanism appropriate?
- Who is accountable for the cyber security risks and for their governance in our organisation?
- Do we have sufficient oversight of our SOCI readiness (e.g., compliance timelines, relevant incidents, key government interactions?)
- What evidence do we want and need as a Board to sign-off on the future annual cyber security attestation?

Executives:

- Have we defined our roles and responsibilities with regards to reviewing our SOCI readiness, addressing any gaps and implementing our operational model?
- Are there any areas where we must lift our capabilities? What is the right mix of in-house, external and on-demand capabilities?
- How do we best integrate SOCI requirements into our existing frameworks (e.g., business continuity, incident response, NIST CSF) and operating models (e.g., risk assessments, asset owners, shared security services)?
- What assets are in scope and how are they reflected in our current cyber resilience plans?
- Do we have the right mechanisms in place for the responsible Executives to provide the Board with the necessary evidence for future annual compliance attestation?
- Do we have the right level of reporting to keep our stakeholders up to date?

Bibliography

[1] F. Macau, “Supermarket shortages are different this time — here's how to respond and avoid panic,” 10 Jan 2022. [Online]. Available: https://www.abc.net.au/news/2022-01-10/how-to-deal-covid19-supermarket-supply-shortages/100744160. [Accessed May 2022].

[2] ABC News, “Victoria's hospital and ambulance system under record pressure, data shows,” ABC News, 22 April 2022. [Online]. Available: https://www.abc.net.au/news/2022-04-30/victorias-hospital-and-ambulance-system-under-record-pressure/101028042. [Accessed 14 June 2022].

[3] D. Mercer, “Hip pocket pain at the bowser as fuel above $2 a litre prompts pleas from motoring groups,” ABC News, 24 May 2022. [Online]. Available: https://www.abc.net.au/news/2022-05-24/calls-for-more-help-as-fuel-soars-past-2-dollars-a-litre/101091962. [Accessed 14 June 2022].

[4] D. Mercer, “Australia on the 'precipice' of a UK-style energy crisis as soaring costs push retailers out,” ABC News, 1 June 2022. [Online]. Available: https://www.abc.net.au/news/2022-06-01/australia-on-brink-of-energy-crisis/101115924. [Accessed 14 June 2022].

[5] N. Beilharz and D. Claughton, “JBS Foods pays $14.2 million ransom to end cyber attack on its global operations,” ABC News, 10 June 2021. [Online]. Available: https://www.abc.net.au/news/rural/2021-06-10/jbs-foods-pays-14million-ransom-cyber-attack/100204240. [Accessed 14 June 2022].

[6] C. Osborne, “Logistics giant Toll Group hit by ransomware for the second time in three months,” ZDNet, 6 May 2020. [Online]. Available: https://www.zdnet.com/article/transport-logistics-firm-toll-group-hit-by-ransomware-for-the-second-time-in-three-months/. [Accessed 14 June 2022].

[7] J. Hendry, “Victorian hospitals go offline after ransomware attack,” IT News, 1 October 2019. [Online]. Available: https://www.itnews.com.au/news/victorian-hospitals-go-offline-after-ransomware-attack-531696. [Accessed 14 June 2022].

[8] D. Wroe and C. Uhlmann, “Federal MPs' computer network hacked in possible foreign government attack,” SMH, 8 February 2019. [Online]. Available: https://www.smh.com.au/politics/federal/federal-mps-computer-network-hacked-forcing-passwords-to-be-changed-20190208-p50wgm.html. [Accessed 14 June 2022].

[9] A. Greene, “Bureau of Meteorology hacked by foreign spies in massive malware attack, report shows,” ABC News, 12 October 2016. [Online]. Available: https://www.abc.net.au/news/2016-10-12/bureau-of-meteorology-bom-cyber-hacked-by-foreign-spies/7923770. [Accessed 14 June 2022].

[10] Australian Cyber Security Centre, “Annual Cyber Threat Report 1 July 2020 to 30 June 2021,” 15 September 2021. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21. [Accessed 15 June 2022].

[11] Department of Home Affairs, "Australia's Cyber Security Strategy 2020," 6 August 2020. [Online]. Available: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf. [Accessed 15 June 2022].

[12] Department of Home Affairs, "Strengthening Australia's cyber security regulations and incentives," 3 July 2021. [Online]. Available: https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf. [Accessed 20 June 2022].

[13] World Economic Forum, "The Global Risks Report 2022," World Economic Forum, 2022.

[14] Department of Home Affairs, "Strengthening Australia's cyber security regulations and incentives," 2021. [Online]. Available: https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf. [Accessed 30 June 2022].

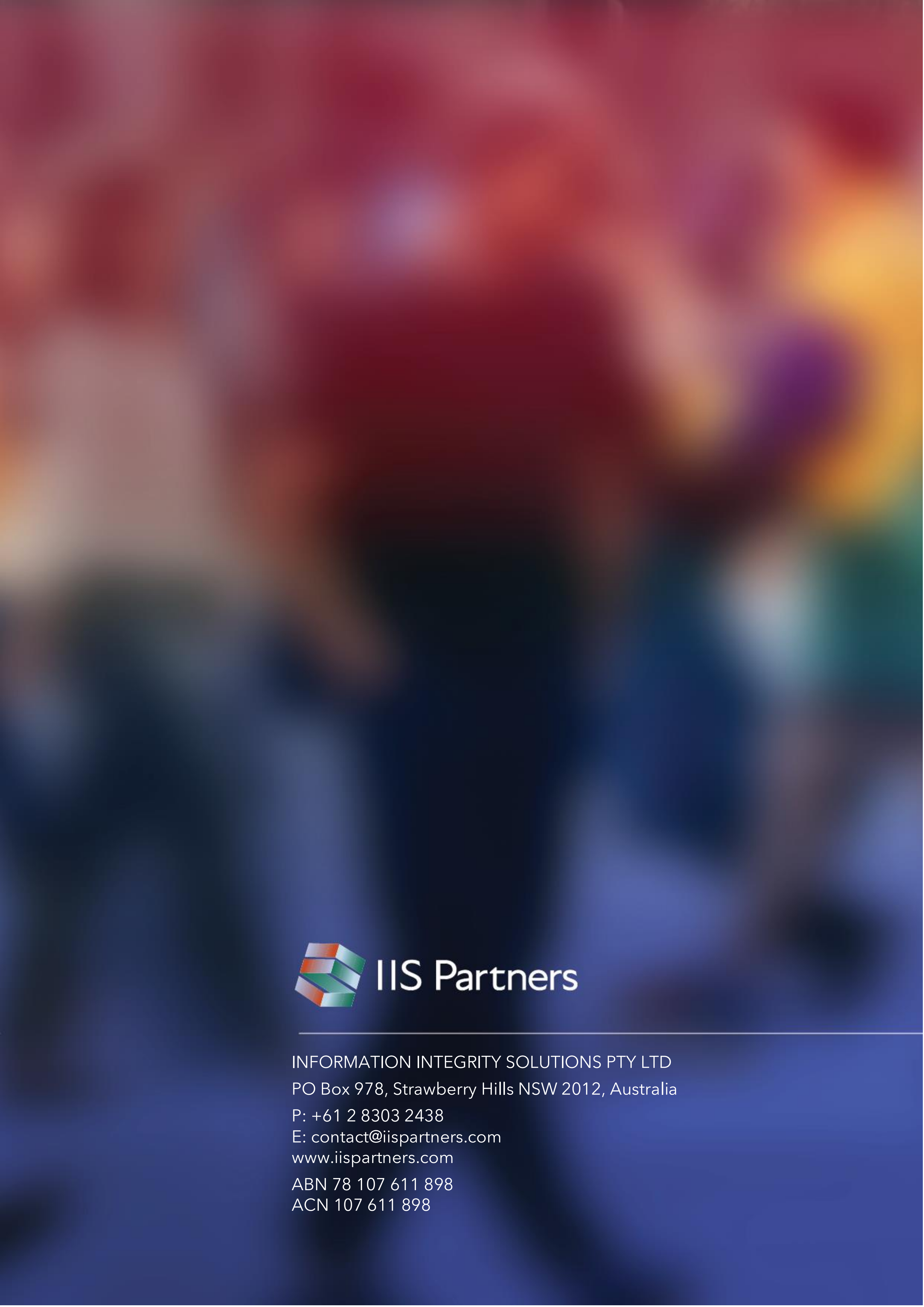
[15] ASIC, "Court finds RI Advice failed to adequately manage cybersecurity risks," 5 May 2022. [Online]. Available: https://asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-104mr-court-finds-ri-advice-failed-to-adequately-manage-cybersecurity-risks/. [Accessed 14 June 2022].

[16] G. Yanco, "Cyber safety a company culture matter," ASIC, 10 June 2022. [Online]. Available: https://asic.gov.au/about-asic/news-centre/articles/cyber-safety-a-company-culture-matter/. [Accessed 15 June 2022].

[17] *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, Explanatory Memorandum,* 2022.

[18] IIS Partners, "SNSW Data Breach – Post Incident Report," 16 December 2020. [Online]. Available: https://www.iispartners.com/s/DCSSNSWDataBreachPIRReport16122020Final.pdf. [Accessed 20 June 2022].

[19] Department of Home Affairs, *Protecting Critical Infrastructure and Systems of National Significance Security of Critical Infrastructure Act 2018 Part 2B – Notification of cyber security incidents,* Industry Awareness Session, 2022.



IIS Partners

INFORMATION INTEGRITY SOLUTIONS PTY LTD
PO Box 978, Strawberry Hills NSW 2012, Australia
P: +61 2 8303 2438
E: contact@iispartners.com
www.iispartners.com
ABN 78 107 611 898
ACN 107 611 898