Law Council
OF AUSTRALIA

Office of the President

15 March 2024

Cyber Strategy Unit
Department of Home Affairs
PO Box 25
Belconnen ACT 2616

By email: AusCyberStrategy@homeaffairs.gov.au

Dear Cyber Strategy Unit

2023–2030 Australian Cyber Security Strategy: Legislative Reforms

The Law Council is grateful for the opportunity to make a submission in response to the Department of Home Affairs' Consultation Paper *2023–2030 Australian Cyber Security Strategy: Legislative Reforms*.

I am pleased to enclose the Law Council's submission, which has been informed by contributions from the Law Society of New South Wales and the Law Institute of Victoria. The Law Council is also grateful to its Business Law Section for its advice in the preparation of this submission.

If you require further information or clarification, please contact Mr Nathan MacDonald, Deputy General Manager of Policy on [redacted] or at [redacted]

Yours sincerely

[redacted]

Greg McIntyre SC
President

Law Council
OF AUSTRALIA

Australian Cyber Security Strategy: Legislative reforms

Department of Home Affairs

15 March 2024

Telephone +61 2 6246 3788
Email mail@lawcouncil.au
PO Box 5350, Braddon ACT 2612
Level 1, MODE3, 24 Lonsdale Street,
Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.au

Table of contents

About the Law Council of Australia

The Law Council of Australia represents the legal profession at the national level; speaks on behalf of its Constituent Bodies on federal, national, and international issues; promotes and defends the rule of law; and promotes the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts, and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world. The Law Council was established in 1933, and represents its Constituent Bodies: 16 Australian State and Territory law societies and bar associations, and Law Firms Australia. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Law Society of the Australian Capital Territory
- New South Wales Bar Association
- Law Society of New South Wales
- Northern Territory Bar Association
- Law Society Northern Territory
- Bar Association of Queensland
- Queensland Law Society
- South Australian Bar Association
- Law Society of South Australia
- Tasmanian Bar
- Law Society of Tasmania
- The Victorian Bar Incorporated
- Law Institute of Victoria
- Western Australian Bar Association
- Law Society of Western Australia
- Law Firms Australia

Through this representation, the Law Council acts on behalf of more than 104,000 Australian lawyers.

The Law Council is governed by a Board of 23 Directors: one from each of the Constituent Bodies, and six elected Executive members. The Directors meet quarterly to set objectives, policy, and priorities for the Law Council. Between Directors' meetings, responsibility for the policies and governance of the Law Council is exercised by the Executive members, led by the President who normally serves a one-year term. The Board of Directors elects the Executive members.

The members of the Law Council Executive for 2024 are:

- Mr Greg McIntyre SC, President
- Ms Juliana Warner, President-elect
- Ms Tania Wolff, Treasurer
- Ms Elizabeth Carroll, Executive Member
- Ms Elizabeth Shearer, Executive Member
- Mr Lachlan Molesworth, Executive Member

The Chief Executive Officer of the Law Council is Dr James Popple. The Secretariat serves the Law Council nationally and is based in Canberra.

The Law Council's website is www.lawcouncil.au.

Acknowledgements

This submission is informed by contributions from the Law Society of New South Wales and the Law Institute of Victoria. The Law Council is also grateful to its Business Law Section for its advice in the preparation of this submission.

Executive summary

1. The Law Council welcomes the opportunity to provide a response to the Department of Home Affairs' *2023–2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper* (the **Consultation Paper**).

2. The 2023–2030 Australian Cyber Security Strategy plays a critical role in identifying the key principles and challenges emerging from the parallel proposals, reforms and review processes taking place in relation to privacy, data protection and cyber security regulation across the economy.

3. The Law Council emphasises the need to ensure proportionality, consistency, and certainty within the regulatory landscape. Regulatory and procedural certainty is critical in the aftermath of a cyberattack where the timeframe to make decisions and to respond appropriately is significantly constrained.

4. The Law Council has primarily focussed on proposals in the Consultation Paper as they relate to information sharing in the wake of a cyber incident, especially Measure 2 (ransomware reporting) and Measure 3 (limited use obligations). In responding to these proposed measures, the Law Council has sought to achieve a balance between incentivising disclosure through requirements that are easily applied and understood without unnecessary regulatory burden, while providing entities with assurances that information shared will be used effectively to add value by providing better protections for Australian citizens and businesses.

5. To this end, the Law Council makes the following key recommendations:

    - Compulsory reporting following a ransomware attack should be limited to situations where an entity has made a ransomware or extortion payment. Reporting on ransomware or cyber extortion attacks more generally should be managed through the limited use framework in Measure 3, subject to the changes recommended by the Law Council.
    - There should be clear statutory safeguards that preserve legal professional privilege and confidentiality in any documents provided following a ransomware attack. This includes ensuring material is exempt from disclosure under a subsequent freedom of information request.
    - Clarity is required on the role of 'no fault and 'no liability' protections in the context of instruments of crime and sanctions regimes, which may be inadvertently breached through a ransomware payment.
    - To adequately incentivise disclosure, information provided to the Australian Signals Directorate (**ASD)** and/or Cyber Coordinator should not be shared with regulators without the express consent of a disclosing entity.
    - There should be clear statutory safeguards that preserve legal professional privilege and confidentiality in any documents provided to the ASD and/or Cyber Coordinator under Measure 3. This includes ensuring material is exempt from disclosure under a subsequent freedom of information request.
    - If 'consequence management' is to be relied upon as a purpose for the sharing of incident information, this term should be clearly defined to cover a narrow set of circumstances.

6. The Law Council is grateful for the opportunities provided to engage directly with the Australian Government while preparing this submission.

Introduction

7. The Consultation Paper outlines nine proposed measures that seek to address identified gaps in the current legislative and regulatory framework for cyber security. These measures relate to:

    - Measure 1: Secure-by-design standards for Internet of Things devices
    - Measure 2: Ransomware reporting for businesses
    - Measure 3: Limited use obligations
    - Measure 4: A Cyber Incident Review Board
    - Measure 5: Data storage systems and business critical data
    - Measure 6: Consequence management powers
    - Measure 7: Protected information provisions
    - Measure 8: Review and remedy powers
    - Measure 9: Telecommunications sector security under the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**)

8. The focus of the Law Council's submission is on Part 1 of the Consultation Paper as it relates to proposed new cyber security legislation. In the time available, we have not had an opportunity to respond individually against each of the measures and have instead focussed primarily on the first four initiatives listed above.

9. In making this submission, the Law Council wishes to emphasise that, while there is a need for an overarching framework for cyber security regulation and response, any regulatory framework must be appropriately balanced so as not to unduly discourage innovation, and investment in innovation, in Australia.

Measure 1: Secure-by-design standards for Internet of Things devices

A mandatory cyber-security standard for consumer-grade smart devices

10. The Law Council supports efforts to enhance cyber security measures to safeguard both individuals and businesses that might be vulnerable to cyber threats. As such, the Law Council broadly agrees with the conclusion that there is a need to tighten the security and integrity of Internet of Thing (**IoT**) devices through the implementation of cyber security standards that will better protect consumers, particularly given that these smart devices are often developed with functionality as a priority and may lack important security features.

11. Despite potential challenges that may arise with enforcing mandatory standards, the Law Council agrees that defining and implementing basic security requirements for IoT devices is necessary to bolster consumer safety and device reliability. This perspective reflects the Law Council's support for initiatives aimed at strengthening cyber security protections, particularly for vulnerable individuals and businesses.

12. The implementation of a cyber security standard may result in distributors and manufacturers, especially larger scale manufacturers who are more likely to absorb the cost of regulation, to become incentivised to enforce compliance up and down the supply chain. This could prove positive as manufacturers and suppliers at all levels of the market are mandated to uphold a level of responsibility and accountability for threats and greater protection of consumers.

13. The Law Council agrees that tightening the security of IoT devices through this approach could help raise awareness of security safeguards associated with IoT devices, as well as building consumer confidence by improving the overall cyber security of these devices. This in turn may result in greater security overall for smart devices.

Types of smart devices to be covered by a mandatory cyber security standard

14. When considering the types of devices that should or should not be covered by a mandatory cyber security standard, it is useful to look at international examples given many manufacturers distribute their products globally. The United Kingdom has passed legislation which sets out the mandatory standards for IoT devices and regulating the products that it considers are to be included or excluded from mandatory standards.

15. As a relatively small technology market, Australia should have access to the same protections as its counterparts. If a mandatory scheme were implemented (with similar exception provisions), it is likely to force an uplift in standards across the industry globally. Consequently, the ability for smart devices that do not meet mandatory smart device standards to make their way into Australian consumer stores would be limited, and this in turn could have a chilling effect on manufacturers who fail to comply with the minimum standards.

16. Aligning Australia's regulatory approach with existing global cyber security norms may be an efficient way to ensure consistency in the quality and security of smart devices available in the domestic market, and could streamline compliance and simplify enforcement efforts.

Measure 2: Ransomware reporting for businesses

17. Under Measure 2, the Consultation Paper proposes to impose two new reporting requirements on relevant entities, namely where an entity:

    - is impacted by a ransomware or cyber extortion attack and receives a demand to make a payment to decrypt its data or prevent its data from being sold or released; or
    - makes a ransomware or extortion payment.

18. The Law Council acknowledges the importance of collecting specific details related to ransomware payment transactions and instances of cyber-attacks. This information is invaluable for tracing and effectively combating cybercrime—rendering this data critical to bolstering national cyber security defences. The Law Council's approach to ransomware reporting seeks to enhance the understanding of cyber threats at a national level, while alleviating the potential burden of compulsory reporting obligations on businesses while they are being impacted by an attack.

Reporting triggers

19. The comments below have specific regard to the potential difficulties in identifying the scope and nature of a ransomware or cyber extortion attack, and the competing challenges faced by entities at a highly stressful time in its ongoing operations. Based on these views, the Law Council recommends that reporting requirements relating to ransomware are simplified and limited only to situations where ransomware or extortion payments are actually made.

20. In the Law Council's view, information sharing in relation to cyber attacks at the point of identification (prior to any ransom being paid) is better dealt with through the limited use framework set out against Measure 3, subject to the comments made about that Measure below.

Types of entities

21. In seeking to minimise the potential regulatory burden caused by additional ransomware reporting obligations, the Consultation Paper notes:

> *… it may be appropriate to acquit the proposed ransomware reporting obligation through existing reporting obligations. In some cases, an entity may be subject to other incident reporting obligations that could collect the relevant information about a ransomware or cyber extortion incident. For example, approximately 1,000 Australian entities fall under the mandatory cyber incident reporting obligations under the SOCI Act.*[1]

22. In addition to considering consolidating the proposed new obligations with existing reporting obligations under the SOCI Act, consideration should also be given to consolidating, where possible, the proposed ransomware reporting obligations with existing reporting obligations under the Notifiable Data Breaches (**NDB**) Scheme and the *Privacy Act 1988*. The NDB Scheme and Privacy Act should inform both the types of entities captured by the new requirements, and the timeframes for reporting, in order to promote consistency in the relevant law and minimise regulatory burden.

23. Consideration of which entities should be subject to the reporting requirements under Measure 2 is somewhat complicated by the ongoing review of the Privacy Act. While the Government has 'agreed in principle' to removing the small business exemption from the Privacy Act, we note that this is subject to further consultation on the impact that removing the small business exemption would have.[2]

24. An effective ransomware reporting regime that is developed to accelerate law enforcement action, enhance whole-of-economy risk mitigation, and help tailor victim support services should be broadly applicable across the economy, and is ideally not limited to large entities only. Instead, the focus should be on the nature and sensitivity of the data held by, and stolen from, the business.

25. If the small business exemption is removed from the Privacy Act, it is suggested that the proposed ransomware reporting requirements for small businesses should be consistent with their other reporting requirements under the NDB Scheme and Privacy Act. However, subject to the outcome of the Government's further consultations with small businesses, consideration could also be given to introducing a more streamlined mandatory reporting process for small businesses, to reduce the regulatory burden of Measure 2.

Types of information

26. The Consultation Paper sets out various types of information that could fall within the Measure 2 reporting requirements, including:

- when the incident occurred, and when the entity became aware of the incident;
- what variant of ransomware was used (if relevant);

[1] Consultation Paper, 15.
[2] Australian Government, Government Response: Privacy Act Review Report, (September 2023), 6.

- what vulnerabilities in the entity's system were exploited by the attack (if known);
- what assets and data were affected by the incident;
- what quantum of payment has been demanded by the ransomware actor or cybercriminal, and what method of payment has been demanded;
- the nature and timing of any communications between the entity and the ransomware actor or cybercriminal;
- the impact of the incident, including impacts on the entity's infrastructure and customers; and
- any other relevant information about the incident or actor that could assist law enforcement and intelligence agencies with mitigating the impact of the incident and preventing future incidents.

27. While there may be value in having this information form part of the relevant reports, certain information, such as 'what assets and data were affected' and 'the impact of the incident', may be highly complex and can take significant time to fully ascertain. In some cases, it simply may not be possible to provide this information comprehensively within a short period, particularly if the timeframe for reporting is to align with, for example, the 72-hour timeframe to report cyber incidents under the SOCI Act.

28. Accordingly, the Law Council suggests that any proposals under Measure 2 should account for the practical difficulty in providing a complete snapshot of ransomware attacks in a limited timeframe and should allow for further information to be subsequently furnished by victims of ransomware attacks as it becomes known.

29. In addition, there may be further complications where legal advice forms part of the incident response to a ransomware attack. The proposed reporting structures will need to address the professional obligations of confidentiality and matters relating to legal professional privilege that attach to communications in those circumstances, including through clear statutory safeguards that preserve legal professional privilege and confidentiality in any documents provided. A fuller discussion on this point is in our response to Measure 3 below.

30. Finally, it will be important to explicitly address the evidentiary status of any notifications, reports and related communications in any litigation, prosecutions or investigations that may be triggered by a given incident. Material provided should be exempt from disclosure under a subsequent freedom of information (**FOI**) request or a subpoena, summons, notice to produce, or notice requiring non-party disclosure. Legislation should also make it clear that the information provided remain 'confidential' for other relevant purposes, such as (for listed entities) ASX Listing Rule 3.1A.2.

'No fault' and 'no liability' protections

31. The Department has sought views on the extent to which the proposed 'no fault' and 'no liability' principles would encourage entities to report ransomware attacks. While there is merit in adopting a no fault and no liability approach, further clarification is required regarding how, in practice, these principles would interact with entities' existing legislative and regulatory obligations in dealing with a relevant cyber incident. For example, it is not clear how information reported under Measure 2 would be treated under the Commonwealth FOI regime.

32. The Law Council is supportive of the 'no fault' and 'no liability' protection principles as outlined in the Consultation paper as a means of providing assurance to entities in the reporting process.

33. However, the Law Council seeks clarity on the overlap between the proposed 'no fault' and 'no liability' regime and potential penalties arising from ransomware payments amounting to breaches of instruments of crime regimes under various State and Territory criminal legislation, or where a payment is deemed to contravene laws prohibiting payments to sanctioned organisations. The Law Council believes greater clarity is needed as to whether this regime will provide adequate protections for potential breaches of sanctions laws or instruments of crime legislation, noting the potential for ransomware payments to find their way to sanctioned entities.

Recommendations

- **Reporting requirements following a ransomware attack should be limited to situations where an entity has made a ransomware or extortion payment. Reporting on ransomware or cyber extortion attacks more generally should be managed through the limited use framework in Measure 3, subject to the changes recommended by the Law Council.**
- **There should be clear statutory safeguards that preserve legal professional privilege and confidentiality in any documents provided following a ransomware attack. This includes ensuring material is exempt from disclosure under a subsequent freedom of information request.**
- **Clarity is required on the role of 'no fault and 'no liability' protections in the context of instruments of crime and sanction regimes that may be inadvertently breached through a ransomware payment.**

Measure 3: Limited use obligation

Sharing and use of information

34. Measure 3 proposes to establish a legislated 'limited use' obligation for the ASD and the National Cyber Security Coordinator (**Cyber Coordinator**) in respect of cyber incident information they receive. The intention of these restrictions is to encourage greater industry engagement with government during and following a cyber incident.

35. Under the proposed limited use obligation, information shared with ASD or the Cyber Coordinator would be limited to 'prescribed cyber security purposes' defined in legislation, and could not be used by regulatory agencies for investigative or compliance action. The Consultation Paper provides a range of permitted possible uses that may constitute prescribed cyber security purposes.[3]

36. The Law Council is concerned to ensure that information provided to ASD or the Cyber Coordinator is treated confidentially, and has strong reservations about a 'limited use' approach as this may disincentivise organisations from voluntarily reporting in an open and timely manner. Any ability for information provided to ASD or the Cyber Coordinator to be disclosed to regulators, private litigants or the public may lead to a reticence to share that information, even despite the Consultation Paper indicating that information could not be used for investigations or compliance.

37. We note that the Consultation Paper seeks to clearly delineate between the limited 'use' of relevant information and the 'sharing' of such information. It states:

[3] Consultation Paper, 20.

> *It is important that any limited use obligation does not preclude ASD and the Cyber Coordinator from sharing appropriate information with other agencies—including law enforcement, national security, intelligence agencies and regulators. The proposed model of a 'limited use' obligation would restrict the use of cyber incident information, but not the sharing of this information*.[4]

38. While the distinction is acknowledged between the sharing and use of information, the Law Council recommends restrictions against both. Importantly, and as pointed out in the Consultation Paper, a regulator would still be able to contact organisations directly to compel information from an entity, and entities will need to continue to meet reporting obligations.[5] For example, if ASIC sought information (and is aware of the event) it may issue a notice under section 33 of the *Australian Securities and Investments Commission Act 2001* (Cth) and information could be elicited through an examination under section 19.

39. Under this preferred model, information obtained by the ASD or the Cyber Coordinator would only be available to regulators with the express consent of the disclosing entity. The Law Council is concerned that anything less than this will not achieve the policy objective of incentivising timely and open disclosure in the wake of a cyber attack.

Protection of privileges and confidentiality

40. A further concern of the Law Council is to ensure that disclosure requirements to the ASD or Cyber Coordinator do not have the effect of abrogating privileges that might otherwise be attached to material, whether it be the privilege against self-incrimination or legal professional privilege. In relation to the latter, entities will be reluctant to share information with the ASD or Cyber Coordinator where such disclosure is considered to be a waiver of legal professional privilege.

41. At the very least, it should be made clear that confidential disclosure to the ASD or the Cyber Coordinator does not result in a waiver of any privilege that subsists in any documents. This would likely require specific legislative preservation of legal professional privilege together with a model that places strict confidentiality obligations on privileged material.

42. Finally, it will be important to reassure entities that information provided to the ASD or Cyber Coordinator will not be accessible to thirds parties through channels such as FOI. It is understood that, while the ASD is exempt from the *Freedom of Information Act 1982* (Cth), without legislative change, material provided to the Cyber Coordinator could be subject to the FOI framework. In the Law Council's view, information disclosed should be clearly recognised as confidential and exempt from FOI disclosure, as well as disclosure to regulators without the consent of the disclosing organisation.

43. Unless a disclosing organisation is provided with comfort that voluntary disclosures to ASD and the Cyber Coordinator will not be harmful to the organisation's interests, the measure will not be effective to encourage disclosures.

---

[4] Ibid, 21
[5] Consultation Paper, 21.

Recommendations

- **To adequately incentivise disclosure, information provided to the ASD and/or Cyber Coordinator should not be shared with regulators without the express consent of a disclosing entity.**
- **There should be clear statutory safeguards that preserve legal professional privilege and confidentiality in any documents provided to the ASD and/or Cyber Coordinator under Measure 3. This includes ensuring material is exempt from disclosure under a subsequent freedom of information request.**

Measure 4: A Cyber Incident Review Board

44. The essential purpose of the proposed Cyber Incident Review Board (**CIRB**) appears to be to conduct no-fault, post-incident reviews of cyber incidents and to promote collective cyber security by publicly sharing findings and best practice guidance. The Consultation Paper notes that the CIRB is not a law enforcement, intelligence or regulatory body, and its proposed functions should not be regulatory.

45. To be effective, this proposal would require a high level of coordination between the CIRB and a large number of federal and state agencies operating within the law enforcement, national security, privacy and data law spheres. This may pose considerable practical difficulties. There is also a risk that carving out certain information, so as not to prejudice or interfere with ongoing legal or regulatory activities, may result in an incomplete picture of the relevant cyber incident, or lead to significant delays in the CIRB carrying out an incident review. Ultimately, the utility of the CIRB's incident reviews is largely contingent on its ability to perform its functions in a timely and accurate manner.

46. With the above comments in mind, concerns have been raised with the Law Council regarding the potential overlap with existing regulatory bodies and fears of introducing further bureaucratic layers without clear benefits. It will be important for the CIRB, if implemented, to be structured so as not to duplicate the functions of other regulatory bodies, or impact transparency and collaboration between regulators and immediate incident responders.

47. To this end, the Law Council considers that the remit of the CIRB should be on general and systemic issues, noting that the US equivalent investigations have been about a particular criminal group, or an identified software vulnerability. Investigations into specific cyber incidents would likely require or result in judgements of responsibility, accountability or consequences, which should be outside the role of the CIRB.

48. Further, we also note that the proposed CIRB is, itself, likely to become a high priority target for cyber threat actors, particularly given its proposed information gathering powers. Accordingly, it would be critical that the CIRB is equipped with industry leading information security controls and standards (and ensures each of its members meet these standards) and is appropriately resourced to ensure it maintains highly robust cyber security measures.

Sensitive information

49. While the CIRB's role includes making public recommendations, the Consultation Paper contemplates including a mechanism to ensure that certain sensitive

information relating to cyber incidents remains appropriately confidential. For example, the Consultation Paper notes:

> *Potential safeguards to protect sensitive information could include granting the CIRB powers to provide confidential reports to Government and producing redacted reports for public consideration.*[6]

50. In this regard, guidance may be gleaned from existing legislation relating to independent reviews. For example, Part 2A, Division 4 of the *Health Administration Act 1982* (NSW), which relates to root cause analysis in the NSW public health system, sets restrictions on the types of incidents that can be reviewed[7] and what information can be disclosed by an incident reviewer,[8] and prohibits information being given in evidence or advice, or reports from the review being admitted in evidence.[9]

Measure 6: Consequence management powers

51. Concerns have been expressed to the Law Council about the broad use of the term 'consequence management' in the Consultation Paper. In addition to Measure 6, the term is used as an exception to the proposed 'limited use' of information provided to the ASD or Cyber Coordinator, however it is undefined in the Consultation Paper. It may be that there is a reliance on the description of consequence management as contained in from the ASD's *Cyber Incident Management Arrangements for Australian Governments* report which states:

> *'Consequence management relates to the second and subsequent order effects from cyber security incidents. It requires government and industry to work together to identify and mitigate the secondary harms that may result from a cyber security incident. In the most severe instances, this could include 'real world' impacts requiring the activation of emergency management arrangements, such as the NCM and, in cyber crises, the NSR and CCT.*
>
> *Consequences that could arise from a cyber security incident could include:*
>
> - *disruptions to government and the provision of government services, including those delivered both in-person (e.g., front-line health care) or online (e.g., government payment systems);*
> - *disruptions to critical infrastructure, critical goods and the provision of essential services upon which the community relies, including those owned or operated by governments (e.g., energy, water and sewerage) or by the private sector (e.g., airports, medical supplies, freight networks); and*
> - *large scale data breaches of government or personal identity data and subsequent criminal activity, which might require the re-issuing of credentials and increased levels of security applied to compromised identities.*[10]

---

[6] Ibid, 28.
[7] *Health Administration Act 1982* (NSW) s.21M.
[8] Ibid, s.21N
[9] Ibid, ss.21O and 21P.
[10] Australian Signals Directorate, *Cyber Incident Management Arrangements for Australian Governments* (14 Oct 2022), 3.

52. At the same time, consequence management is a term that is used in the context of compliance and risk management frameworks. For example:

    - In the context of Australian Prudential Regulation Authority (**APRA**) *Prudential Standard CPS 511* (Remuneration), APRA-regulated entities are required to maintain remuneration arrangements that appropriately incentivise individuals to prudently manage the risks they are responsible for, and that there are appropriate consequences for poor risk outcomes. Clause 20(d) of the Standard defined 'consequence management' as the approach to managing performance, risk and conduct outcomes, which may include downward adjustments to variable remuneration.
    - The Australian Financial Markets Association's *Consequence Management Standard* outlines that an internal Consequence Management Policy may include (but is not limited to): employee manuals, code of conduct, procedures to be adopted, appropriate workplace behaviour and employment/workplace relations. The standard also outlines that the consequences for an employee should be determined in accordance with the seriousness of the incident of misconduct and their culpability.

53. In light of the above examples, consequence management could be interpreted as not just managing downstream impacts of a cyber breach, but also in managing consequences for organisations and individuals who may have suffered a cyber security breach—not just in terms of remuneration but liability. This is particularly important as the Consultation Paper seeks to reserve the right for information to be disclosed to regulators for consequence management. While the information cannot be used for investigation or compliance, that does not prevent the regulator from obtaining the information (that it knows about) in a different way.

54. The Law Council suggests that a less ambiguous term would be preferable, or if 'consequence management' is retained, that it be given a narrow definition such as the one in section 45(1) of the *Emergency Management Act 2013* (Vic) which defines the term to mean:

> *'… the coordination of agencies, including agencies who engage the skills and services of non-government organisations, which are responsible for managing or regulating services or infrastructure which is, or may be, affected by a major emergency.'*

55. This approach would make it clear that consequence management is not about imposing obligations or addressing consequences, but around coordination of responses to an incident.

Recommendation

- **If 'consequence management' is to be relied upon as a purpose for the sharing of incident information, this term should be clearly defined to cover a narrow set of circumstances.**