ashurst

2023-2030 Australian Cyber Security Strategy

Response to Cyber Security Strategy Discussion Paper

Introduction

Ashurst welcomes the opportunity to provide a submission in response to the Expert Advisory Board's consultation on the 2023-2030 Australian Cyber Security Strategy Discussion Paper.

As part of the consultation process, we are encouraged by the development of a forward-looking strategy for Australia. Future reform should pivot towards building systemic cyber resilience into the ecosystem. In the following pages, we have outlined areas for consideration and further discussion.

In a changing world, our vision at Ashurst is to be a highly progressive global law firm. For over 200 years we have advised corporates, financial institutions and governments on their most complex transactions, disputes and projects. We offer the reach and insight of a global network, combined with our knowledge and understanding of local markets.

At Ashurst, we help our clients build cyber resilience and effective cyber risk management through a combination of legal, risk advisory and programme delivery teams. We provide end-to-end, whole-of-life-cycle expertise across cyber, data and privacy issues.

> "Future reform should pivot towards building systemic cyber resilience into the ecosystem"

Having advised on some of Australia's most high-profile cyber incidents, we have unique insights and expertise that can improve how organisations prepare for and respond to high-impact cyber incidents, at executive and Board level.

The views expressed in this submission are made on a general basis in relation to the 2023-2030 Cyber Security Discussion Paper. In proposing broadly legal, operational and regulatory measures, we have taken a balanced approach, taking into account the needs of Australian business, government, the economy and all Australians.

We have provided responses to a select group of questions outlined in the Discussion Paper, and welcome any further questions or discussion.


"protected":
"verified":
"followers_
"friends_
"listed_
"favourites_
"statuses_
"created_at":
"utc_offset":
"time_zone":
"geo_enabled":

Q1

What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

Public and private organisations of all sizes and across industries are now key stakeholders in Australia's national security and are at the cyber security frontier. This national security imperative should drive closer collaboration, information sharing and investment between government and industry.

Investment in cyber security is a clear priority for the Australian Government, and has finally made its way to the top of the agenda for Australian corporates, both large and small. Future reform no longer needs to target raising awareness of the threat, but should pivot towards building systemic cyber resilience into the ecosystem. The Australian Government needs to play a key role in building this resilience.

The 2023-2030 Australian Cyber Security Strategy must address the imminent threat within our existing ecosystem. Industry and government must be incentivised to invest in:

- **Business transformation to reduce exposure:** for example, through data minimisation measures and the implementation of more robust systems such as Digital ID.
- **Uplifting operational security:** including scaling security and resilience capability in a way that improves the network using shared learnings and insights, avoids the need for organisations to reinvent the wheel, and reduces and shares cost burdens.
- **Building a resilient ecosystem focused on incident response and recovery:** an ecosystem which acknowledges the reality that cyber incidents will remain a threat, but which is designed to promote a speedy recovery and ensure minimum consequential harm.
- **Designing regulation and enforcement for resilience:** ensuring our enforcement environment is calibrated to have a positive impact on cyber security and does not discourage engagement with agencies and regulators.

Our submission outlines a number of legal, regulatory and operational measures designed to mitigate the impact and scale of cyber incidents, while strengthening Australia's cyber resilience.

The 2023-2030 Australian Cyber Security Strategy must address the imminent threat within our existing ecosystem. Industry and government must be incentivised to invest in:

1. Business transformation to reduce exposure
2. Uplifting operational security
3. Building a resilient ecosystem focused on incident response and recovery
4. Designing regulation and enforcement for resilience

Q2

What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

Data retention and minimisation

Industry and government are subject to a wide range of data retention requirements that are challenging to understand – and are often misunderstood. The result is that Australian organisations often retain data for longer than necessary. This makes us attractive to cyber threat actors and exposes personal, sensitive and commercial information.

The benefits of retaining information must now be balanced against the risks of retaining it, and the costs of keeping it secure.

Government can act by clarifying and simplifying the complex, and often overlapping, regulatory regimes that impose data retention obligations on the public, quasi-public and private sectors. We see many organisations struggle with document retention obligations that apply across vast numbers of data sets, with differing retention periods often attached to very specific pieces of data. At the same time, regulators are encouraging organisations to rethink their retention practices for certain data, such as personal information.

We need to pivot away from the historical approach that asked "how can the data be retained" to ask "should the data be retained". This requires a review of legal provisions relating to the retention of any data across the public and private sectors, and could form part of the review of legal provisions requiring the retention of personal information under Proposal 21.6 of the Privacy Act Review Report issued by the Attorney General's Department, which proposes a review of all legislation that requires the retention of personal information to determine if it is appropriately balanced against the risks of holding significant volumes of personal information.

This would be separate from the recent independent review of the mandatory data retention regime under the *Telecommunications (Interception and Access) Act 1979* (Cth), and the independent reviews and holistic reform of electronic surveillance legislative powers which are also being undertaken.

Government can also play an active role in incentivising the destruction or de-identification of data in the public and private sectors by:

1. Reviewing data retention obligations through a cyber-risk management lens, and balancing those risks against policy objectives that require retention of that information
2. Encouraging ecosystem changes that reduce the need to collect and retain personal and higher-risk information
3. Encouraging secure storage and data transfer solutions and obligations in cases where collection and retention of higher-risk information is necessary

Q2 continued

This may involve, for example, leveraging the Commonwealth Digital Transformation Agency's Hosting Certification Framework for secure data transfer and deletion frameworks, or developing domestic certification mechanisms to support the implementation of standardised secure data transfer and deletion frameworks.

Reformulating data retention and deletion requirements would benefit from broader consultation with industry to address the practical and operational challenges that will arise.

Identity information

We can progressively reduce Australia's exposure to data breaches by taking a risk-based approach to building resilience to protect the higher-risk data that is most valuable to threat actors.

Measures could include:

- **Reducing the amount of identity information collected and retained** by reviewing current law and practice on verification of identity, and either removing the requirements where they are unnecessary or introducing and encouraging the uptake of more robust verification methods, such as Digital ID.
- **Making identity information less valuable** by implementing more robust systems such as Digital ID with the aim of ensuring that government identifiers and identity documents cannot be used for identity fraud.
- **Identifying other higher-risk information and implementing strategies to reduce its value**, such as changes in payment systems which may reduce the value of stolen credit card and bank account details.
- **Adopting an industry risk-based review**, such as undertaking a review of how the Australian medical system (including hospitals, practitioners, insurers and government agencies) collects and stores our most sensitive medical information.

We can progressively reduce Australia's exposure to data breaches by taking a risk-based approach to building resilience to protect the higher-risk data that is most valuable to threat actors by:

1. Reducing the amount of identity information collected and retained
2. Making identity information less valuable
3. Identifying other higher-risk information and implementing strategies to reduce its value
4. Adopting an industry risk-based review

Q2(a)

What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

A combination of mandatory operational cyber security standards that are embedded across legislation, regulation and regulatory guidance is necessary, but a "one-size fits all" approach is unlikely to be effective and standards should evolve over time to be industry- and asset-specific.

Government should consider the following reforms to help organisations to strengthen their cyber resilience:

Industry-specific risk management rules

Setting a broad-based minimum standard for all organisations is only the starting point. Industry-specific risk management rules under the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act) will foster cyber security maturity in our most critical sectors by:

- addressing risks that are more prevalent in a specific industry sector (such as operational technologies and network segregation in the utilities sector, and critical third party risk in the financial services sector);
- providing guidance and clarity on the expected levels of maturity (rather than minimum levels of maturity) for each sector and for asset classes/scales within each sector;
- deduplicating the effort involved in demonstrating compliance across multiple regulatory agencies, by cross-referencing industry regulations and standards;
- providing guidance on appropriate standards for service providers in core areas of cyber expertise;
- providing guidance and standards that uplift organisations' capability to respond effectively across 8 key response domains: strategic crisis management, business continuity, communications and notifications, customer support, data breach response, third party service providers, regulatory investigation and strategic recovery planning; and
- encouraging industry collaboration, information sharing and benchmarking that will improve industry-wide resilience over time.

Government should consider the following reforms to help organisations to strengthen their cyber resilience:

1. Industry-specific risk management rules
2. Regulatory guidance and cooperation on industry contingency and response planning
3. Support for SMEs
4. Incentivising standards compliance

Q2(a) continued

Regulatory guidance and cooperation on industry contingency and response planning

The Government's recent announcements regarding industry "war games" is most welcome. Improving industry-level preparedness will help organisations to uplift their capability to respond to a cyber attack. In particular, the role of Government should include:

- working with industry groups to provide clarity, and to practise how government will respond and support in the event of a large-scale cyber incident;
- conducting industry-wide continuity planning to support communities in the event of a "worst case scenario" attack; and
- providing transparency, without breaching an organisation's confidentiality, regarding industry maturity levels, best practice and standards of readiness.

Support for SMEs

If mandatory standards are to be imposed, the Government should reflect on the practicalities and likely impact on small and medium-sized organisations (SMEs). Government may want to consider putting measures in place to support compliance.

Incentivising standards compliance

Compliance with standards helps to manage business risk in the ordinary course, but regulation can increase the value of standards compliance and lead to widespread adoption. For example, access to a "safe harbour" or immunity from certain liability might be linked to compliance with standards.

Participants in Australia's Consumer Data Right may be relieved of certain liability in cases where they have complied with various mandatory requirements and standards. This approach has been criticised – in respect of the breadth of the immunity, as well as its binary nature. A similar liability framework has been proposed for Australia's Trusted Digital Identity Framework.

In both cases, participants are part of a larger security framework for which they are not solely responsible, and there is a strong national interest in encouraging participation in both the Consumer Data Right and the Trusted Digital Identity Framework. Each framework has mandated minimum standards and requirements, and each framework has "boundaries" that help distinguish general business risk from the risks incurred by participating in the framework.

The US Cyber Security Strategy includes a proposal to impose liability on software manufacturers if they fail to take reasonable precautions to secure their products and services. The US administration said in its draft report that it would work with Congress and the private sector to develop the language of such a Bill, which would include "an adaptable safe harbour framework" to protect companies that "securely develop and maintain their software products and services". Compliance with standards may serve as an objective measure of secure development and maintenance environments, even if security failures do occur.

Q2(b)

Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

The application of the SOCI Act is currently driven by whether or not an asset is a critical infrastructure asset. If the Government intends to approach data security as a threat to national security, then there are sound reasons to expand the remit of the SOCI Act to cover the customer data and systems of those critical infrastructure assets.

However, that still leaves a gap in relation to customer data and systems of those entities that are not caught by the SOCI Act. This is a key risk given that a number of recent cyber incidents were caused as a result of incursions into the supply chain, rather than the systems of the entity whose assets would otherwise have fallen within the scope of the SOCI Act.

The SOCI Act already applies directly to customer data and systems to the extent that they are critical data and storage processing assets, as well as indirectly if an entity responsible for a critical infrastructure asset has a data storage or processing service provided to it which relates to business-critical data. However, there is merit in expressly expanding the SOCI Act to deal with assets that are not, strictly speaking, data storage or processing assets, but which hold business-critical data – a likely scenario given that many organisations outsource some, if not all, of their IT systems.

We also believe it would be beneficial to engage with industry in order to clarify and provide additional sector-specific guidance on customer data and systems that fall within the scope of sector-specific asset definitions.

We are mindful of the potential for overlap with the *Privacy Act 1988* (Cth) and the *Telecommunications Act 1997* (Cth), which regulate the personal information held by the various entities falling within the ambit of that legislation. While the Privacy Act is also seeking to enhance the security and integrity of personal information, the focus of the SOCI Act is on managing national security risks. Again, if the approach is to classify the threat to data as a national security threat, then the SOCI Act would be a convenient vehicle to operationalise this approach, but the Government should consider how to minimise regulatory overlap in order to optimise compliance.

A key deliberate limitation of the SOCI Act is that assets will not be deemed critical infrastructure assets if, or to the extent that, the asset is located outside of Australia (section 2B). The Privacy Act, on the other hand, applies outside of Australia.

Introducing cross-sector regulation that will apply only to data and systems hosted in Australia could incentivise the offshoring of data. This could damage Australia's hosting industry and put organisations that choose to localise their data, or that are required to do so (e.g. state government entities), at a competitive disadvantage.

Mandatory onshoring of data may be an appropriate policy objective in certain cases, but such an intervention should be considered carefully as it may limit access to foreign suppliers and technologies that are important to critical sectors.

Q2(c)

Should the obligations of company directors specifically address cyber security risks and consequences?

Effective management of cyber security risks is a core concern for all directors and we believe it is effectively legislated as part of the existing duties imposed by the *Corporations Act 2001* (Cth) (Corporations Act). Obligations of company directors do not need to specifically address cyber security risks and consequences. In particular, the existing obligations already include:

- an overarching set of personal obligations on directors to ensure they have appropriate oversight of key risks, including a civil obligation in relation to care and diligence which requires directors to be mindful of, and properly manage, key business risks such as cyber security and the management of data (section 180 of the Corporations Act); and
- a requirement for directors to stay informed about, and apply an enquiring mind regarding, the organisation's activities, monitor its affairs and policies, test information put before them by management and proactively consider what other information they require. These obligations apply to a wide range of business risks, and include having appropriate systems in place to prevent and respond to cyber security incidents.

The obligation to protect key organisational data and ensure cyber security resilience forms part of directors' existing obligations.

Even without a new mandatory duty, directors may be liable, through the use of the "stepping stones" mechanism, if they do not exercise due care and diligence in relation to cyber security matters, particularly where the company is in breach of the law. It is not necessary to impose new forms of director liability whenever a new issue emerges.

While there is a need to ensure directors and executive management are accountable, this accountability must be balanced against the negative effects on directors' sentiment and their willingness to serve on Boards (or even continue business in Australia), as well as the costs of compliance and professional indemnity insurance.

However, many directors recognise that cyber security is a complex area of risk to govern, and not all Boards will feel fully equipped to do so. Directors have a responsibility to ensure they have the appropriate skills and access to expertise; however the Government can support them to improve their management of cyber security through a number of initiatives and mechanisms including:

- uplifting the crisis management capabilities of directors, by promoting government-led simulations across major high-risk sectors;
- updating and improving regulatory guidance, particularly given the limited precedents and existing case law relating to specific cyber security issues and directors' duties;
- ensuring the consistency and frequency of the threat intelligence reports that directors have access to by improving intelligence sharing, and engaging directly with industry and the non-executive director community, particularly in terms of critical infrastructure assets;
- providing targeted guidance, through mechanisms such as the Essential Eight and cyber policy forums, on the various levels of cyber expertise that a Board may require access to (internally or externally); and
- continuing to support and sponsor forums that can consistently demonstrate to a Board "*what good looks like*".

Q2(f)

Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?

This is a complex question. While the clear policy objective in prohibiting the payment of ransoms is to undermine the ultimate business model enjoyed by cyber criminals, there are a series of unintended consequences that could flow from doing so.

For example, any prohibition on ransom payments would necessarily require certain exceptions in certain circumstances, such as threat to life and/or safety. We can reasonably anticipate that cyber criminals will move to exploit the circumstances that give rise to any exceptions. This could lead to an unintended escalation in the nature of attacks and may encourage cyber criminals to target our most vulnerable Australians.

Instead, Government could consider a range of measures which, when taken together, make the payment of a ransom unnecessary in most circumstances.

Ensuring that not paying a ransom is the most viable option

Many organisations that pay a ransom do so as "a matter of last resort", yet organisations continue to pay. Both government and industry have an interest in ensuring that not paying a ransom is always the *most viable option* for an organisation. The following measures could be implemented to support organisations in making the decision to not pay.

Introducing legislation to protect directors from liability if they do not pay

Australian directors currently face a dilemma: in some circumstances directors may form a view that paying the ransom is necessary to protect the business and comply with their directors' duties. Creating this aligned incentive to pay is a key strategy of threat actors.

Government should consider introducing a safe harbour in the form of a defence against any subsequent action by regulators in relation to the incident for those organisations that comply with notification provisions.

The defence would not be available in circumstances where the organisation has been negligent. The organisation would need to be able to demonstrate that it has taken reasonable care to prepare for, and mitigate the impact of, the cyber incident (e.g. by compliance with any mandatory standards).

Government could consider a range of measures which, when taken together, make the payment of a ransom unnecessary in most circumstances

1. Introducing legislation to protect directors from liability if they do not pay the ransom
2. Additional support for SMEs
3. Improving how government and industry can work together to support impacted individuals and limit harm

Q2(f) continued

Additional support for SMEs

SMEs are less likely to have sophisticated cyber defence, resilience and recovery capabilities. They can lack the funds necessary to invest in adequate business continuity arrangements, and the forensic and cyber security resources to effectively respond during and after an attack.

Government has an important role to play in supporting SMEs by improving access to quality advice, support and expertise. This could include, for example, scaling affordable and effective resilience and back-up tools, providing tax incentives and grants to enable SMEs to improve their cyber maturity, as well as financial assistance for cyber response services in specific circumstances.

Improving how government and industry can work together to support impacted individuals and limit harm

The work done by the Australian Government and industry following the recent spate of cyber incidents to allow the sharing of data has demonstrated the benefits of targeted intervention and institutional cooperation in reducing the potential for identity theft and fraud.

The introduction of measures such as the Digital ID should drive down post-incident remediation costs, reduce the inconvenience of replacing identity documents, and limit attacks over time as the value of stolen personal data is reduced.

Government should also introduce legislation that clearly prohibits individuals and organisations from accessing, benefiting from or publishing personal and/or stolen data on the Dark Web.

Many organisations would also benefit from further consistent guidance on the expertise required to navigate the life cycle of a large ransomware attack. The rapid rise in attacks has contributed to the high growth of cyber response advisory services, which are variable in quality, consistency and efficacy. We have seen cases where ineffective or unqualified advisers contributed to a premature decision to pay a ransom. Government should continue to work closely with cyber response organisations to mature this important capability across the nation.

Mandatory notification of ransomware demands

Government should consider introducing mandatory notification of ransom demands on a confidential basis. Reporting will enable the Government to effectively monitor, and respond to, the changing risk profile of the cyber threat environment over time.

Time and again, we have learned that intelligence sharing and access to data in the context of a cyber incident can shift the dial, enabling organisations to minimise the impact of an incident and protect themselves against future attacks.

The notification should include:

- information about the attack, the threat actor and the ransom demand;
- a risk assessment of the impact of the incident (including the impact on systems, the organisation, individuals and other key third parties);
- an analysis of the potential impact of paying the ransom;
- an assessment of whether the risks identified can be adequately mitigated by not paying;
- details of any relevant issues that may impact a national security interest; and
- a summary of the outcomes.

Confidential statistical analysis should be provided regularly to help industry prepare for attacks.

The method and timing of mandatory notification should be carefully considered by the Government, and could be directly tied to any cyber incident response support available to the target. Government should also consider whether additional educational resources, benchmarking and information sharing about best practice are required to support organisations to effectively respond in the event of a cyber incident.

"Government should also introduce legislation that clearly prohibits individuals and organisations from accessing, benefiting from or publishing personal and/or stolen data on the Dark Web."

Q2(f) continued

Cyber insurance reforms

A healthy cyber insurance market is a vital part of building a resilient ecosystem that is resistant to shocks and allows organisations to recover. Insurance should be considered a means of protecting more Australians.

Cyber insurance is expensive and has been less available in recent years, but there are signs of recovery in the cyber insurance market with more insurers offering cover and recent significant year-on-year premium increases tapering off. The underwriting requirements of insurers with respect to the insured's own cyber resilience are also becoming more manageable. However additional exclusions are also being introduced, for example Lloyd's of London now requires its market insurers to exclude coverage for state-sponsored cyber attacks.

Much of the cyber insurance purchased by Australian insureds is provided by non-Australian insurers, which moves risk away from Australia.

Government should consider introducing measures to support the availability and affordability of cyber insurance for SMEs to cover an insured's own damage and loss (first party loss cover), and the insured's liability to others (liability cover) arising from a cyber event.

Further, a ban on insurers providing coverage for ransom payments by insureds will, over time, have a direct and significant impact on the number and scale of ransomware attacks against Australians. This approach has successfully disincentivised other ransom-based criminals but is not without risks, which will need to be carefully managed. For example:

- the burden of payment would move from the insurer to the insured; however, over time, this is likely to drive down the price of the average ransom payment and further disincentivise threat actors; and
- insurers may not cover the resulting ongoing business interruption loss of the insured and any increased liability of the insured to third parties.

We note that insurers dislike ransom payments and are aware that payment can encourage future cyber attacks and ransom demands. Insurers are monitoring this risk and taking steps to discourage cyber criminals.

Government should consider liaising with the insurance industry to explore measures whereby claims against, and payments under, cyber insurance are made subject to certain conditions. For example, France is introducing a measure which requires notification of cyber incidents to authorities within 72 hours in order for the target to be able to claim against its insurance policy.

Q2(f)(i)

What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

As we have indicated in our submission on question 2(f), this is a complex question.

Balancing the policy objectives that will undermine the ultimate business model enjoyed by cyber criminals against the possible series of unintended consequences that could flow from strict prohibition is challenging.

Large organisations are already demonstrating that they will not pay ransoms. Medibank established a high-water mark for non-payment with a focus on navigating support for customers, operational and reputational risks. Many organisations are now actively reviewing their ransom response plans and pre-emptively deciding they will not pay a ransom to secure stolen data. This requires a significant uplift in the depth and breadth of data breach response planning and in strategic crisis management capabilities.

A strict prohibition on ransomware payments, in the absence of other measures designed to strengthen the ecosystem, could cause harm to small and medium-sized businesses. When targeted, they may fail without additional support. We need a policy response that will allow Australian businesses to survive in circumstances where they do not pay.

"We need a policy response that will allow Australian businesses to survive in circumstances where they do not pay."

Q6

How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

The Commonwealth Government plays a central role in fostering cyber security best practice through its regulatory and law enforcement role, but equally important is the example that it sets for private sector and state government entities. It is critical that Commonwealth Government departments and agencies adopt and demonstrate best practice in their own operations.

Importantly, by modelling cyber security best practice, departments and agencies can achieve the dual outcome of enabling efficient and effective protection of sensitive government data holdings, and acting as an accelerator for the broader cyber security ecosystem in Australia (refer to our submission on question 18).

Measures to better demonstrate and deliver cyber security best practice

Under the *Public Governance, Performance and Accountability Act 2013* (Cth) (the PGPA Act), responsibility for the proper use of public resources, including protecting them from cyber security threats, rests with each accountable Commonwealth Government department and agency.

This framework is further supported by regulations, including the Commonwealth Procurement Rules (CPRs), which already expressly require Commonwealth Government entities to consider and manage cyber security risk in their procurement activities. Policy guidance on how to implement management of cyber security best practice has been issued in the Protective Security Policy Framework (PSPF), the Information Security Manual, and in further extensive publications made available by the Australian Cyber Security Centre (ACSC).

Many Commonwealth Government departments and agencies have implemented additional cyber security management processes and procedures to demonstrate best practice in their own specific operational context. In our role over many years as a trusted adviser to the Commonwealth Government, we have had the opportunity to see the good work that various departments and agencies are undertaking in this area.

However, the area of cyber security best practice is rapidly evolving and there are significant operational barriers to the ability of Commonwealth Government departments and agencies to achieve and deliver cyber security best practice.

Best practice in procurement processes

Cyber security risk management needs to be more clearly embedded into procurement processes within Commonwealth Government departments and agencies. The CPRs and the PSPF clearly highlight the need for cyber security risk management of supply chains when conducting procurement, but in practice this is difficult for departments and agencies to implement.

The establishment of collaborative and trusted relationships with key suppliers is of critical importance to the proper management of cyber security risk in procurement. However, this can be difficult for departments and agencies to achieve when balanced against the other obligations in the CPRs, which require them to encourage competition, be non-discriminatory, and facilitate accountability and transparency. In many cases, past practice by departments and agencies has focused on shifting the legal risk in respect of cyber security risk management to suppliers, without engaging in the deeper strategic-level supplier collaborations that are required to address practical risks and implement effective mitigations.

We encourage the Commonwealth Government to further consider how guidance and training can be provided to assist departments and agencies in balancing these considerations while striving to achieve best practice in procurement processes.

Q6 continued

Availability of cyber security resources

Departments and agencies also have difficulty in accessing appropriate cyber security risk management expertise in a timely manner. While some are developing their own well-managed and capable cyber security resources, others do not have a similar level of access. This severely inhibits the ability of all departments and agencies to deliver on best practice in individual projects.

Inflexible regulations

An aspect of cyber security risk that we have identified in our submission on question 2 is that existing regulations requiring long periods of data retention also act to increase the risk of a data breach.

In the government context, some of our clients have expressed particular concerns in relation to the operation of inflexible regulations that require them to retain sensitive information (including personal information) beyond the useful operational life of that information.

A specific example is the *Archives Act 1983* (Cth), which exempts Commonwealth Records from the obligation to destroy personal information under the Privacy Act. Although there is a case for retention of significant records of national importance, the exceptions applied via the Archives Act are extremely broad. In some cases retention of personal information (in records not designated as national archives) is required for in excess of 100 years. There are a myriad of other examples of overlapping and complicated data retention obligations across the public and quasi-public sectors that are likely to make departments and agencies retain information for longer than necessary.

Greater coordination between departments and agencies

Many Commonwealth Government departments and agencies are proactive in developing a strong cyber security posture, but more coordination and assistance is required to ensure all departments and agencies have the resources and experience required to appropriately manage these risks.

This does not require a centralised approach. The achievements of departments and agencies need to be leveraged and enhanced to ensure all departments and agencies have an equal opportunity to deliver on cyber security best practice and serve as a model for other entities.

This requires a holistic assessment of systems and processes, including the legal terms on which Commonwealth Government departments and agencies contract, to ensure they appropriately allocate risk and reflect the practicalities of a cyber security ecosystem that is shared by many stakeholders.

Q8

During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD)/Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

The primary barrier to the early sharing of information with government during or immediately following an attack is the paucity of available information. Organisations operate in an "information vacuum" for a considerable period of time.

Breaking down barriers to open cooperation and trust

The primary objective of post-incident response should be to minimise the potential harm flowing from an incident.

Open cooperation and trust between the target of a cyber attack and the Australian Signals Directorate (ASD)/ACSC is essential. Confidence that open engagement with the ASD/ACSC will not prejudice the target is key to that cooperation and trust.

In our experience, the risk of prejudicing future regulatory action, together with reputational and media management risks, currently discourages open cooperation and engagement during a cyber incident. This risk dynamic places additional strain on organisations during the immediate crisis, and can be an unhelpful distraction when organisations need to focus on more critical harm reduction measures.

A clear separation of regulators is necessary between those responsible for supporting organisations in the event of an attack, and those responsible for investigating post-attack.

The urge for transparency reduces harm, but means organisations will sometimes get it wrong

Transparency surrounding a cyber incident is important. It enables individuals to protect themselves and ensures that markets are adequately informed. But the wider benefits of transparency can be significantly undermined if there is an associated risk that any transparency may have legal or regulatory repercussions. This risk is particularly acute during the initial stages of a cyber incident when the information is in a state of flux.

Organisations in the early stages of an incident will not be in a position to get it right every time – it is simply not possible given the scale and complexity of many attacks. The benefits and reduction in harm that stems from transparency during an attack are eroded when organisations are penalised, by regulators or through litigation, for not being entirely accurate in their initial reporting.

Streamlining regulatory engagement and post-incident investigation

Government should consider implementing a framework with a key focus on post-incident harm reduction and recovery. A priority of the framework should be operational simplicity.

The framework needs to:

- clearly identify the agencies responsible for incident response and recovery;
- ensure that information shared with those agencies is kept strictly confidential, and will not be used for enforcement or other purposes; and
- encourage agencies with enforcement powers to engage with targets of cyber attacks as they would in any other regulatory investigation, making use of already extensive information gathering powers. Targets should not be disadvantaged by cooperating.

This approach would streamline the post-incident response by reducing the number of regulators initially involved, and would encourage greater cooperation and transparency between the target of a cyber attack and the assisting agency.

Q18

Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

Procurement by the Commonwealth Government is already used in a number of areas as a lever to support and encourage policy outcomes. These measures need to be implemented consistently with the PGPA Act, CPRs and Australia's international trade obligations.

Although it is possible to implement a procurement-connected policy as a lever to support and encourage departments and agencies to use the skills of Australian cyber security firms, we would encourage the Commonwealth Government to consider this a secondary measure. Rather, we encourage the adoption by departments and agencies of best practice cyber security procurement and risk management approaches as an industry multiplier to promote viable paths to market.

As discussed in our response to question 6, procurement is critical to the Commonwealth Government's supporting and encouraging the adoption of best cyber security practice across both private and public sector organisations. Rather than introducing specific procurement policy levers, the Australian Government itself acts as a powerful industry multiplier by ensuring that Commonwealth Government departments and agencies are exemplary in their management of cyber security risks when conducting procurements.

The Commonwealth Government can promote awareness of best practice by leading best practice, and by encouraging other private sector and state government organisations to follow suit. Further, this approach adds to the growing pool of trained cyber security professionals through their direct experience of Commonwealth Government-led procurement processes.

Each of these factors assists in promoting viable paths to market for Australian cyber security firms, and in building capacity and expectation in other industry sectors which Australian cyber security firms will be able to exploit as global industry leaders.

"We encourage the adoption by departments and agencies of best practice cyber security procurement and risk management approaches as an industry multiplier to promote viable paths to market."

We appreciate the Expert Advisory Board providing industry participants with the opportunity to provide input on the development of the 2023-2030 Australian Cyber Security Strategy.

Key Contributing Authors

John Macpherson
Head of Cyber
Risk Advisory
T: [redacted]

Amanda Ludlow
Partner
Digital Economy Transactions
T: [redacted]

Renée Green
Global Expertise Counsel
Cyber & Data Risk
Digital Economy Transactions
T: [redacted]

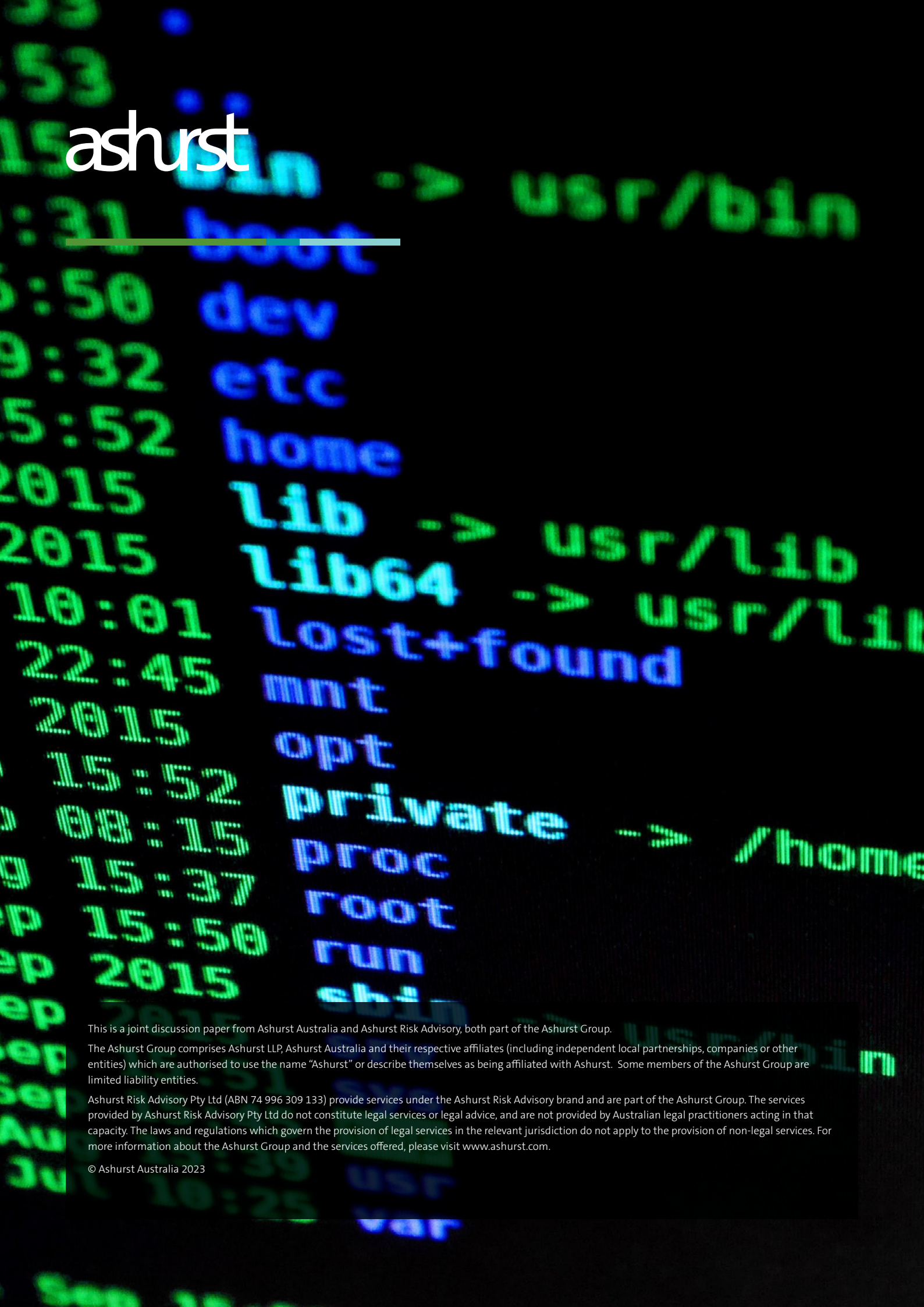
Andrew Hilton
Expertise Counsel
Digital Economy Transactions
T: [redacted]

Mathew Baldwin
Partner
Digital Economy Transactions
T: [redacted]

Miriam Kleiner
Partner
Legal Governance
T: [redacted]

Rehana Box
Partner
Insurance, Corporate Transactions
T: [redacted]

John Moore
Director
Risk Advisory
T: [redacted]



This is a joint discussion paper from Ashurst Australia and Ashurst Risk Advisory, both part of the Ashurst Group.

The Ashurst Group comprises Ashurst LLP, Ashurst Australia and their respective affiliates (including independent local partnerships, companies or other entities) which are authorised to use the name "Ashurst" or describe themselves as being affiliated with Ashurst. Some members of the Ashurst Group are limited liability entities.

Ashurst Risk Advisory Pty Ltd (ABN 74 996 309 133) provide services under the Ashurst Risk Advisory brand and are part of the Ashurst Group. The services provided by Ashurst Risk Advisory Pty Ltd do not constitute legal services or legal advice, and are not provided by Australian legal practitioners acting in that capacity. The laws and regulations which govern the provision of legal services in the relevant jurisdiction do not apply to the provision of non-legal services. For more information about the Ashurst Group and the services offered, please visit www.ashurst.com.