14 April 2023

Mr Brendan Dowling
First Assistant Secretary
Cyber and Critical Technology Coordination Centre
Department of Home Affairs
Via webform.

Dear Mr Dowling,

RE: Australian Cyber Security Strategy 2023 – 2030

The FSC welcomes the opportunity to provide comment on the 2023-2030 Australian Cyber Security Strategy Discussion Paper (**the Strategy**).

The FSC and its members are supportive of risk-based, evidence backed measures that improve the cybersecurity landscape for Australians. Specifically, the FSC is supportive of the overall goal of making Australia the most cyber secure nation by 2030.

However, acknowledging the significant amount of work occurring across government that also impacts cybersecurity, for example, scams, privacy, and the Consumer Data Right, the FSC is calling on government to create an overarching strategic plan to provide industry certainty and ensure that measures implemented in one area are not incongruent with those implemented in another.

Industry is also calling for significant improvements to the information sharing landscape both from government to industry, between government agencies, and within and across affected industries. Reasonable measures that allow organisations to have access to and share information can significantly increase threat awareness and preparedness and encourages industry best practice.

Answers to specific questions are outlined below.

Summary of Recommendations

1. Measures in the Strategy should be evidence and risk-based ensuring a correct balance between important and necessary consumer protections and the need for legitimate cyber transactions to occur in a timely and efficient manner.
2. Government should take a leadership role in preparing Australian organisations for cyber incidents. This can be achieved through shared cyber-event scenarios, guidance resources, joint exercises, and information sharing.
3. The Australian Government should craft a cross-government ‘Scams, Fraud and Cybersecurity Strategy’ that brings together the work of various departments, agencies, and regulators in fields affecting online and economic crime.
4. The Department of Home Affairs should consider ways to mitigate potential issues relating to the proliferation of artificial intelligence from cloud computing services including exploring the feasibility of identity and/or background checks for the use of such service.
5. The Department of Home Affairs should institute a legislative ban on the payment of ransoms and extortion demands for businesses to demonstrate to would be actors that there is nothing

Financial Services Council Ltd
Level 5, 16 Spring Street
Sydney NSW 2000
E. info@fsc.org.au
W. fsc.org.au
ABN 82 080 744 163

to be gained from committing cyber-attacks in Australia.

6. The Department should consider necessary changes to the Privacy Act to better facilitate threat and information sharing from both government to industry, as well as between industry operatives.
7. There should be an obligation on organisations to fully cooperate with Government during an active cyber incident and organisations should be provided with assurances that information gleaned during that process will only be used for the purposes of responding to that cyber incident.
8. The Department should consider other barriers such as the AUSTRAC 'tipping off' provisions which hinder industry's ability to share information.
9. The Australian Government should consider mechanisms which would make it easier for organisations to report, update, and share cyber event information with multiple agencies from a single source.
10. The Department should institute a legislative requirement to report material data breaches and cyber-attacks.
11. The Department should ensure the Strategy adequately considers the threat of innovative technologies such as AI.

About the Financial Services Council

The FSC is a peak body which sets mandatory Standards and develops policy for more than 100 member companies in one of Australia's largest industry sectors, financial services. Our Full Members represent Australia's retail and wholesale funds management businesses, superannuation funds, and financial advice licensees.

The financial services industry is responsible for investing more than $3 trillion on behalf of over 15.6 million Australians. The pool of funds under management is larger than Australia's GDP and the capitalisation of the Australian Securities Exchange and is one of the largest pools of managed funds in the world.

Question 1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world?

Evidence and Risk-based Measures

The FSC is supportive of the overarching goal of the Strategy to make Australia the most cyber secure nation in the world by 2030. The FSC notes that to be the most cyber secure nation means that the country will have implemented well suited, evidence and risk-based measures that ensure an adequate balance between consumer protection methods and barriers to legitimate cyber transactions.

In the financial services context this means that cybersecurity measures implemented protect consumers and operators from cybersecurity threats and associated harms, such as fraud, whilst still maintaining sufficient flexibility to transact in an agile and time sensitive way. For example, funds management customers have expectations as to the speed and ease with which they can access and manage their funds, including their investments, and the FSC expects that being the most cyber secure nation in the world would not result in measures that unduly interfere with this customer experience.

Further, as operatives within the financial services sector range in size and sophistication, it is important that measures introduced to make Australia the most cyber secure nation in the world are reflective of the different risk profiles of individual organisations. Regulatory interventions are rarely successful when they are implemented with a one size fits all, risk agnostic approach.

Recommendation

1. Measures in the Strategy should be evidence and risk-based ensuring a correct balance between important and necessary consumer protections and the need for legitimate cyber transactions to occur in a timely and efficient manner.

Role of Government in Cyber Preparedness

The FSC believes that the Australian Government has a significant role to play in building up incident and response capabilities. This can be achieved through shared cyber-event scenarios, best practice guidance resources, joint exercises, and information sharing. These proactive measures will help organisations prepare for and respond to cyber incidents.

More information about the importance of better information sharing is detailed below.

Recommendation

2. Government should take a leadership role in preparing Australian organisations for cyber incidents. This can be achieved through shared cyber-event scenarios, guidance resources, joint exercises, and information sharing.

Question 2. What legislative or regulatory reforms should Government pursue to enhance cyber resilience across the digital economy?

Consistent Strategy

The FSC is concerned that given the significant scope of work occurring across government in relation to scams, fraud, and cybersecurity, there is potential for government to create excess and conflicting regulation. For this reason, the FSC is calling on government to provide a 'Scams, Fraud, and Cybersecurity Strategy' that brings together the work of all of the various departments, regulators, and agencies under a suite of common goals.

While the FSC and its members are supportive of the overall aims of the Strategy, it is important to note that there is a significant amount of work occurring across government that have varying impacts on cybersecurity. This includes the work happening in various agencies to do with fraud and scam mitigation, work on the Consumer Data Right, the Privacy Act Review, as well as critical infrastructure regulation. Each agency or department may also be engaged in department-specific workstreams that affect different parts of the industry in different ways.

The FSC is concerned that regulation created in silos will not result in good outcomes for consumers or for industry and create a chaotic set of regulations, significantly increasing the compliance burden. For example, changes to cybersecurity regulation may result in changes to the way identity data is collected, used and stored, whilst changes implemented to mitigate scams and fraud may call for significantly increased identity data collection and storage. Regulation that is not harmonised will create confusion for organisations and will ultimately result in poor consumer outcomes.

The FSC believes that an overarching government strategy for scams, fraud and cybersecurity will be beneficial to government agencies, regulators, organisations, and consumers in understanding the vision of the Government in protecting consumers from the harms of online and economic crime.

This scams, fraud, and cybersecurity strategy could also have the added benefit of considering some of the key privacy and data issues that currently prevent the sharing of threat information between government and industry by harmonising privacy regulations with the Government's goals in relation to scams, fraud, and cybersecurity. See below for further information on information sharing.

Recommendation

3. The Australian Government should craft a cross-government 'Scams, Fraud and Cybersecurity Strategy' that brings together the work of various departments, agencies, and regulators in sectors affected by online and economic crime.

Cloud Services Artificial Intelligence

Cloud service providers provide artificial intelligence (**AI**) and machine learning tools as a service as part of their cloud offerings. Anyone can sign up and get access to these powerful tools which then have the potential to be mis-used. These tools can be easily utilised by criminals to conduct frauds, scams, or for cyber-attacks.

The Department should consider this as a potential area of future weakness as AI becomes more and more sophisticated and used in daily life. As a minimum, cloud services that offer AI tools should verify user identities and monitor the usage for responsible use of AI.

Recommendation

4. The Department of Home Affairs should consider ways to mitigate potential issues relating to the offering of artificial intelligence from cloud computing services including exploring the feasibility of identity and/or background checks for the use of such service.

Payment of Ransoms

The FSC is supportive of prohibiting the payment of ransom and extortion demands of cyber criminals by organisations, insurers, and government. This is a sensible outcome to achieve the goal of becoming the most cyber secure nation by 2030. An unequivocal legislative prohibition on the payment of ransoms by organisations would flag to cyber hackers that there is nothing to be gained through an act of interference in Australia.

The FSC believes there should, however, be an exemption from the legislative prohibition for small businesses. This is due to the materiality of data that would likely be stolen from larger enterprises. Naturally these organisations are a bigger target for cyber criminals and the consequences of a data breach more significant. Similar exemptions already exist in other areas such as privacy law.

The ability to pay ransoms may result in firms not taking their obligations as to cybersecurity seriously and can create competitive issues where smaller firms who are unable to pay ransoms are unable to compete with larger firms who can and will pay the ransom. The cybersecurity focus in Australia should be risk-based prevention, as opposed to post-event mitigation measures (such as the payment of ransoms) which serve to further encourage future cyber-attacks.

The FSC is supportive of the principle of the current legislative framework that all but prohibits payment of ransoms as the funds would be knowingly paying criminals for their crimes, or to terrorist groups. It is not suitable, from a principles perspective, to allow for the payment of ransoms where firms know that the funds being transmitted will simply be used to further inflict harm on Australians or others around the world.

Recommendation

5. The Department of Home Affairs should institute a legislative ban on the payment of ransoms and extortion demands for businesses to demonstrate to would be actors that there is nothing to be gained from committing cyber-attacks in Australia.

Question 7. What Can Government Do to Improve Information Sharing with Industry on Cyber Threats.

Intra-industry and Government Information Sharing

The FSC is supportive of improved opportunities for threat and general information sharing. Increased information from government and between industries could have a significant impact on an organisation's ability to respond and prepare for threats. Further consideration needs to be given to activity in other areas of government, such as privacy regulation, to help break down the barriers to communication that currently restrict information sharing practices.

This information sharing should occur not just between government and industry but cross industry as well, as often a cyber threat does not affect a single industry or sector. The ability for superannuation funds, funds management firms, and financial advice providers to be able to share threat and logistic information with other concerned industries such as banking, telecommunications, and digital platforms cannot be understated.

Similarly, to receive threat information from government organisations such as AUSTRAC would help prepare organisations for potential threats and make them more adaptative at locating threats when they occur.

Recommendation

6. The Department should consider necessary changes to the Privacy Act to better facilitate threat and information sharing from both government to industry, as well as between industry operatives.

The legal framework should facilitate effective cooperation with appropriate government entities during a cyber incident. However, those organisations should be confident that any information provided during that process will only be used for the purposes of responding to the relevant cyber incident and will not be used against them later for other regulatory proceedings.

One of the barriers to information sharing is concerns that sharing information about a cyber incident may be used against an organisation in later legal proceedings or regulatory action. In the heat of a cybersecurity incident, open sharing and collaboration is key, however, there may be some hesitation from organisations where there is a risk that any admissions made in the immediate processes of trying to stop a cyber-attack may be used against them either through government action or other legal processes, such as class action lawsuits.

The FSC recommends the Government place an obligation to provide detailed information about cyber incidents in real time to appropriate government agencies but equally assure organisations that that information will only be used for its intended purpose.

Recommendation

7. The legal framework should facilitate effective cooperation with Government during an active cyber incident and organisations should be provided with assurances that information gleaned during that process will only be used for the purposes of responding to that cyber incident.

Another potential deterrent to information sharing are the AUSTRAC 'tipping off' provisions which prevent organisations from discussing suspicious matter reports (SMRs). These reports are submitted by organisations to combat money laundering and terrorism financing and other serious economic crimes. The tipping off provisions mean that organisations essentially cannot discuss the submission of these SMRs for fear that it may alert the subject of the report to the potential investigation by law enforcement. Although this goal is reasonable, Government should find a way to harmonise this with the need for threat and information sharing to occur, ideally in real time, between industry operatives and government agencies to better protect Australians from cyber threats.

Recommendation

8. The Department should consider other barriers such as the AUSTRAC 'tipping off' provisions which hinder industry's ability to share information.

Threat Reporting Between Agencies

Currently, participants within the financial services industry may have multiple agencies that cyber events may need to be reported to. For example, cyber threats may need to be reported to multiple agencies because the organisation is an APRA regulated entity and/or a provider of critical infrastructure. The information required to be reported between agencies may have significant overlap but may also need to be reported at different times due to differences of reporting mandate triggers such as levels of threat and escalation.

For this reason, the FSC believes that the government should create better synergies for reporting of a single cyber threat to multiple agencies. A single place to report threats, where the information can be entered, updated, and sent to key agencies efficiently would significantly assist organisations in meeting their regulatory obligations whilst providing consistent and timely information.

Recommendation

9. The Australian Government should consider mechanisms which would make it easier for organisations to report, update, and share cyber event information with multiple agencies from a single source.

Question 9. Would expanding the existing regime for notification of cyber security incidents improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

The FSC is supportive of mandatory reporting of material cybercrime, including ransom and extortion demands. A materiality threshold is important because both organisations and

governments can get bogged down in cyber threats and events that are insignificant or fleeting, creating unnecessary burden for industry and muddying the waters of genuine and pressing threats.

Mandated reporting, combined with increased and more effective information sharing will improve the overall threat preparedness landscape by ensuring that current access and extortion methods are known to all industry participants.

Mandatory reporting will also have the added benefit of encouraging increased focus on cybersecurity preparedness and ensuring that all organisations are implementing appropriate data security controls to mitigate the risk of cyber-attacks.

Mandatory reporting should be applied uniformly across all businesses, irrespective of the scale or revenue of the business.

As noted above, any mandated reporting should be able to be done in a way that can be integrated across agencies in an efficient way. Threat reporting should also be able to be easily and regularly updated where an organisation experiences an escalation in a cybercrime activity.

Recommendation

10. The Department should institute a legislative requirement to report data breaches and cyber-attacks.

Question 19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

The Strategy should be adaptive and forward looking in its approach to cybersecurity. This includes having a strong horizon scanning approach to analysing ways in which new and emerging technologies may be used to conduct cyber-attack activity in the future.

For example, the emergence in the last year alone of artificial intelligence (**AI**) technology that is capable of believably mimicking human thinking, behaviour, and mannerisms poses a significant future threat to Australia's cybersecurity and considerably increases the threat of fraud and scam activity.

Recommendation

11. The Department should ensure the Strategy adequately considers the threat of innovative technologies such as AI.

Yours Sincerely,

Financial Services Council