JONES DAY | One Firm Worldwide®

WHITE PAPER

December 2020

Accountability for Cybersecurity in Australia—A Major Regulatory and Litigation Risk

There are showers, there are squalls, and there are storms. The growth in cybersecurity attacks in Australia, as in much of the world, is a storm and Australian companies need to batten down the hatches. In the period from 1 July 2019 to 30 June 2020 alone, the Australian Cyber Security Centre ("ACSC") responded to 2,266 cybersecurity incidents at a rate of almost six per day and the ACSC expects the true volume of malicious activity to be much higher.

When you consider the continued increase in cybersecurity attacks in Australia, it is unsurprising that cybersecurity has become a key policy issue for the Australian Government and is considered critical to Australia's national security, innovation and competitiveness.

This Jones Day *White Paper* considers the rise of cybersecurity risk for Australian companies, the increasing importance of cybersecurity and cyber resilience from the perspective of the Australian Government policy agenda and Australian regulators, particularly in the financial sector, and the ways in which Australian companies and their individual directors and officers will be held to account for cybersecurity issues moving forward. The paper concludes by addressing the steps companies, and individual directors and officers, should be taking to ensure they are adequately prepared for a cybersecurity incident and to avoid the potential legal, financial and reputational costs to firms.

TABLE OF CONTENTS

AUSTRALIAN POLICY DEVELOPMENTS IN RELATION TO CYBERSECURITY

Australia's Cyber Security Strategy ("CSS"), released in August 2020 by the Australian Government Department of Home Affairs, will see AU$1.67 billion invested over the next decade to advance and protect Australia's cybersecurity interests.[1] This is the largest ever investment in cybersecurity by a government in Australia.

Central to the CSS is the introduction of an enhanced legal framework[2] to protect critical infrastructure and systems of national significance, imposing security obligations across nine sectors: banking and finance; communications; data and cloud; defence; education, research and innovation; energy; food and grocery; health; space; transport and water.[3]

The enhanced legal framework includes a positive security obligation that will require designated firms and operators to meet sector-specific standards proportionate to their cybersecurity risk. The enhanced legal framework will also include additional government powers and capabilities, including to the power to request information and give directions. The Australian Government is seeking to fast-track the introduction of the enhanced legal framework.[4]

The Australian Government's focus on cybersecurity and resilience is also reflected in the regulatory priorities of the Australian Securities and Investments Commission ("ASIC") and the Australian Prudential Regulation Authority ("APRA").

ASIC's Interim Corporate Plan for 2020-21 sets out various actions ASIC intends to take in this area, including disrupting and deterring cyber misconduct and monitoring the cyber resilience of market participants and market infrastructure providers.[5] ASIC has also released guidance on cyber resilience for financial institutions.

APRA has made cyber resilience in the financial system one of its strategic priorities until 2024. One of the key strategic initiatives is the development of APRA's own Cyber Security Strategy for 2020 – 2024 which seeks to influence the financial system more broadly, including suppliers and providers that financial institutions rely upon.

Focus on Cybersecurity and Resilience for the Financial Sector

Whilst vital to companies in all sectors, there is an acute focus on cyber resilience and security in the financial sector. The sources of legal obligations for financial institutions in relation to cybersecurity are diverse and are often enforced by overlapping regulators.[6]

APRA Prudential Standard *CPS 234 Information Security* (CPS 234) is particularly significant in that it expressly sets out the measures APRA-regulated entities, including authorised deposit-taking institutions ("ADIs"), are expected to take in relation to information and cybersecurity, and imposes ultimate responsibility for information and cybersecurity on the board.[7] This includes requiring APRA-regulated entities to clearly define the information-security related roles and responsibilities of the board, senior management, governing bodies and individuals; to maintain an information security capability commensurate with the size and extent of threats to their information assets; to implement controls to protect their information assets commensurate with the criticality and sensitivity of those information assets; and to undertake systematic testing and assurance regarding the effectiveness of those controls.

In August 2020, we saw the first civil penalty proceedings filed by ASIC in relation to deficient cybersecurity systems in the Federal Court action against RI Advice Group Pty Ltd ("RI"), an Australian Financial Services ("AFS") Licensee. ASIC alleges that RI failed to implement (including by its authorised representatives) adequate policies, systems and resources which were reasonably appropriate to manage risk in respect of cybersecurity and cyber resilience. ASIC is seeking declarations that RI contravened the general obligations for AFS Licensees, pecuniary penalties and orders relating to compliance measures.

Prior to ASIC's action against RI, regulatory enforcement action in relation to cybersecurity had been limited to investigating complaints made to the Office of the Australian Information Commission ("OAIC"). These OAIC investigations remain a regulatory risk, considering that the OAIC has a legislative mandate to investigate any complaint that an act or practice may be an interference with the privacy of an individual, or can initiate an investigation of its own volition.[8]

ASIC's recent Federal Court proceedings signal a more active regulatory and enforcement approach in relation to cybersecurity matters going forward, consistent with ASIC's broader "why not litigate" approach to enforcement. This would also be consistent with the Australian Government's policy agenda and the key actions under the CSS.

Potential Personal Liability of Directors and Officers in Relation to Cybersecurity

Directors and officers need to be conscious of their potential exposure to liability in relation to cybersecurity, including by failing to exercise reasonable care and diligence and by failing to disclose a cybersecurity incident in a timely manner.

Failure to Exercise Due Care and Diligence: Recognising and managing risk is a crucial part of directors' and officers' duty of care and diligence. The magnitude and prominence of cybersecurity risk for most companies, particularly companies dealing with sensitive data such as financial institutions, is such that all directors need to treat it as an essential element of the company's broader risk framework.

In the context of cybersecurity, exercising the duty of care and diligence requires directors and officers to have adequate oversight of a company's cyber risk management framework and to consider critically and on a continuing basis the types of information the company holds and the unique cybersecurity risks the company faces. One of the biggest challenges for directors in this regard is that cybersecurity can involve advanced concepts, has a high level of technicality and complexity and is constantly evolving. As such, being in a position to apply a critical mind to cybersecurity risks can require a level of technical knowledge over and above general business acumen.[9] This is of particular concern to directors whose previous commercial experience may not have equipped them with the skills necessary to identify and understand the unique cybersecurity risks a company faces.[10]

The technicality and complexity of cybersecurity may lead some directors to rely more heavily on management and technical experts to identify the risks and develop solutions than they would for other business processes. Whilst this may be reasonable in certain circumstances, directors will still be expected to "take a diligent and intelligent interest in the information available to him or her, to understand that information, and apply an enquiring mind to the responsibilities placed upon him or her".[11]

The complexity and volume of information received from management and other experts will also not be an excuse for failing to properly read and understand the issues. As Middleton J commented in *Australian Securities and Investments Commission v Healey* (2011) 278 ALR 618*:* "A board can control the information it receives. If there was an information overload, it could have been prevented. If there was a huge amount of information, then more time may need to be taken to read and understand it".[12]

Whether a decision concerning the management of cybersecurity risk could be protected by the business judgment rule in the *Corporations Act 2001* (Cth) (Corporations Act) is untested. Even if they are, reliance on the rule requires a director to reasonably inform themselves about the subject matter of the judgment and rationally believe the judgment is in the best interests of the company. Given the uncertainty as to the application of the business judgment rule and the historical difficulty in successfully invoking it, directors should proceed on the basis that it will not provide protection in relation to cybersecurity issues.

Failure to Disclose in a Timely Manner: A company's corporate disclosure obligations may be triggered if the company suffers a cybersecurity incident which has a material effect on operations or the value of the corporation.[13] If a company fails to disclose information about a cybersecurity incident in a timely manner, the company can be exposed to liability for a civil penalty[14] and/or a shareholder class action.[15] The incident itself may also be alleged to demonstrate that any previous positive statements or assurances made in annual reports, contractual negotiations, or other publicly available documents concerning cybersecurity were false, misleading or deceptive.[16]

Whilst the obligation to disclose primarily lies with the company itself, a director may be implicated if there is evidence that a director failed to exercise his or her duty of care and diligence by causing the disclosure failure or failing to prevent it, or if he or she has been in any way, by act or omission, directly or knowingly concerned in, or party to, the disclosure failures.[17]

Additional Considerations for Directors and Officers of Financial Institutions: Due to the greater cybersecurity risks faced in the financial sector and the enhanced legal and regulatory obligations imposed, directors and officers of financial institutions in Australia face heightened legal risk in this area.[18]

AFS Licensees have a number of general obligations under section 912A(1) of the Corporations Act which may by breached through a failure to have an adequate cybersecurity risk management framework in place including obligations to comply with financial services laws (which would include CPS 234 for APRA regulated entities), to have adequate resources (including financial, technological and human resources) to provide the financial services, and to have adequate risk management systems.[19]

If an AFS Licensee is alleged to have breached any of its general obligations, a director may be implicated if there is evidence that the director failed to exercise his or her duty of care and diligence by causing or failing to prevent the AFS Licensee from breaching its general obligations. Moreover, a director may be found personally liable if he or she has been in any way, by act or omission, directly or knowingly concerned in, or party to, the AFS Licensee's breaches of its general obligations.[20]

There may be additional consequences for directors and officers of ADIs under the Banking Executive Accountability Regime ("BEAR") by virtue of BEAR's interaction with CPS 234. BEAR requires ADIs to provide APRA with accountability maps which allocate the roles and responsibilities of accountable persons across the ADI and its subsidiaries. An accountable person is a person in a senior executive position with actual or effective management or control of the ADI, or the management or control of a substantial part of the ADI group's operations.[21]

If an individual director or officer is assigned responsibility for cybersecurity under CPS 234, which may include oversight responsibility, BEAR will impose accountability obligations on that person to take reasonable steps to identify and manage cybersecurity risks, including having:

- Appropriate governance, control and risk management in relation to cybersecurity;
- Safeguards against inappropriate delegations of responsibility in relation to that matter; and
- Appropriate procedures for identifying and remediating problems that arise or may arise.[22]

Similar to the duty of care and diligence, the reasonable steps a person could take to meet his or her accountability obligations under BEAR must be considered in terms of that person's functions or responsibilities. For example, a non-executive director in an oversight role may be expected to take different actions from an officer in order to prevent matters arising that would adversely affect the prudential reputation or prudential standing of the ADI.[23]

If a director or officer breaches his or her accountability obligations under BEAR to take reasonable steps to identify and manage cybersecurity risks, he/she may be disqualified from being or acting as an accountable person.[24]

Whilst BEAR currently only applies to ADIs, the regime is expected to soon be replaced by the Financial Accountability Regime ("FAR"), which will extend the accountability obligations under BEAR to all APRA-regulated entities. Accordingly, directors and officers of all APRA regulated entities should be aware of the potential personal consequences which may arise once FAR has been implemented, by virtue of FAR's expected interaction with CPS 234.[25]

CUSTOMER AND SHAREHOLDER CLASS ACTIONS AS A CYBERSECURITY ACCOUNTABILITY MECHANISM

Wherever there is the potential for high profile incidents and crises impacting a company's operations and reputation, there is class action risk.

We have written about the expected rise in "data breach" class actions by customers in a previous Jones Day *White Paper.*

Whilst there have been a handful of class actions investigated and filed on behalf of persons whose data has been comprised as a result of a data breaches, thus far there has been little litigation in Australia commenced by shareholders against companies or their directors and officers for deficient cybersecurity systems and cybersecurity incidents.

We continue to expect a rise in class actions in relation to data breaches and cybersecurity incidents and anticipate that, as this class action area develops, we may also see individual directors and officers personally joined as defendants to these actions for strategic reasons. This trend is being observed in the United States where there have been at least seven class actions brought against directors and officers of major U.S.

companies in connection with cyber incidents,[26] which, not surprisingly, have generally related to unauthorised access of customers' financial data.[27]

CYBERSECURITY GOVERNANCE AND RISK MANAGEMENT

Given the potential legal consequences for companies as a result of a cybersecurity incident, including those for directors and officers personally, companies need to ensure their boards and management team are equipped to critically assess cybersecurity risks and the adequacy of their cybersecurity risk management framework. There are a number of steps companies can take to achieve this objective, including:

- Developing a clear, comprehensive and dynamic cybersecurity agenda for the board which may include establishing a cybersecurity sub-committee;
- Assessing the composition of the board and the skill and expertise of individual directors and officers, and considering how to address any gaps in expertise, including by providing education and training;
- Ensuring officers within the business who have been assigned responsibility for cybersecurity are sufficiently experienced and have a direct line to the board;
- Establishing clear communication protocols for reporting cybersecurity information to the board, which may include appropriate dashboards and metrics relating to cybersecurity controls; and
- Engaging external experts to review and challenge the information presented to the board by management.

When designing, implementing and maintaining a cybersecurity risk management framework, boards should always consider the various sources of cybersecurity legal obligations of the company and its directors and officers, and the extensive regulatory guidance which has been issued by domestic and, where applicable, foreign regulators. Boards should also ensure that the company is meeting the relevant global standards, such as those developed by the National Institute of Standards and Technology, the IOSCO Board and Cyber Task Force and/or the International Organisation for Standardisation and International Electrotechnical Commission.

Boards need to ensure that cybersecurity risk is integrated into the broader risk framework and that exposures are recognized and assessed for impact based on clearly defined metrics such as response time, cost and legal or compliance implications. This may also require recalibrating certain internal policies and procedures to address the full scope of cybersecurity risks. For example, a company's AML/CTF and sanction program may need to be updated to incorporate the risks of ransomware incidents and associated payments.[28]

To effectively monitor cybersecurity risk, boards need to invest in adequate IT infrastructure and technology. Companies at the forefront of good practice are using intelligence-driven monitoring solutions to deal with this challenge, such as Security Information and Event Management ("SIEM") technologies that enable the detection and alert of anomalous activity. Data analytics can also be used to integrate sources of threats and associated risks into a single view of the threat landscape in real time.

To ensure effective controls are in place, a board should satisfy itself that there is sufficient investment in staff awareness training and education (including for contractors) given its prominence as a source of risk—and because a collective effort against cybersecurity risks will better serve an organisation. Boards should also be satisfied there is adequate spending on technology to ensure core systems are resilient to threats.

To respond effectively to a cybersecurity incident, boards need to be satisfied there has been a sufficient level of scenario planning and testing and that response plans are valid and up to date, including with third-party suppliers. The board should also be satisfied that response teams, including the IT, cybersecurity, compliance, risk and legal functions, are adequately resourced and trained. The research demonstrates that there are substantial long-term cost savings from having tested and tried response plans and adequately resourced response teams.[29]

To ensure the ongoing adequacy of a company's cyber risk management framework, the board needs to regularly engage a third party to independently and objectively assess whether the framework is meeting the objectives set by the board. This

is particularly important given the rate of change in the cybersecurity risk landscape, and the speed at which a business can be severely compromised (potentially within hours).

Finally, cyber insurance also plays an important role in the management of these risks. A cyber insurance policy can help offset the costs relating to the management of a cybersecurity incident, court costs, remediation and regulatory fines, as well as extortion liability and network security liability. Cyber insurance providers can also contribute to the management of cyber risk by promoting awareness, by encouraging measurement of risk and by providing incentives for risk reduction. In assessing a company's application for cyber insurance, providers will expect to see the company's cybersecurity risk management framework and evidence that it is following global standards.

FOUR KEY TAKEAWAYS

1. With the increasing frequency, sophistication and impact of incidents, cybersecurity has become a key policy issue for the Australian Government and is considered critical to Australia's national security, innovation and competitiveness. The government's focus on cybersecurity is also reflected in ASIC and APRA's regulatory priorities.

2. Whilst vital to all companies, there is an acute focus on cyber resilience and security in the financial sector. ASIC's recent Federal Court proceedings against an AFS Licensee alleging deficient cybersecurity systems signals a more active regulatory and enforcement approach in relation to cybersecurity matters going forward.

3. Directors and officers could be found personally liable for a cybersecurity incident by failing to exercise reasonable care and diligence and/or by failing to disclose a cybersecurity incident in a timely manner. It is only a matter of time before we see more litigation in this area in Australia.

4. Companies need to ensure their boards and management team are equipped to critically and continually assess cybersecurity risks and the adequacy of their cybersecurity risk management framework, including regularly obtaining probative and independent assurance.

AUTHORS

Tim L'Estrange
Melbourne/Sydney
+ 61.3.9101.6820
+ 61.2.8272.0561
tlestrange@jonesday.com

Adam Salter
Perth
+ 61.8.6214.5720
asalter@jonesday.com

Lisa M. Ropple
Boston
+ 1.617.449.6955
lropple@jonesday.com

Maria Yiasemides
Sydney
+ 61.2.8272.0770
myiasemides@jonesday.com

Daniel Moloney
Melbourne
+ 61.3.9101.6828
dmoloney@jonesday.com

Drew R. Broadfoot
Perth
+ 61.8.6214.5721
dbroadfoot@jonesday.com

Isabel G. Roney
Melbourne
+ 61.3.9101.6815
ironey@jonesday.com

ENDNOTES

1 See Australian Government Cyber Security Strategy 2020, 28-29.

2 The enhanced legal framework proposed in the CSS will build on the *Telecommunication and Other Legislation Act 2017* (Cth) and the *Security of Critical Infrastructure Act 2018* (Cth).

3 The CSS also sets out a plan to make legislative changes which will set a minimum cybersecurity baseline across all sectors of the economy. The Government intends to consult with businesses on multiple legislative reform options, including the role of privacy, consumer and data protection laws; duties for company directors and other business entities; obligations on manufacturers of internet devices.

4 See Protecting Critical Infrastructure and Systems of National Significance: Consultation Paper August 2020.

5 ASIC's Interim Corporate Plan for 2020-21

6 The sources include the general obligations of Australian Financial Services Licensees under the *Corporations Act 2001* (Cth), the accountability obligations of authorised deposit-taking institutions under the Banking Executive Accountability Regime in Part IIAA of the *Banking Act 1959* (Cth); APRA Prudential Standard CPS 234 *Information Security* ; the *Privacy Act 1988* (Cth) (including the Australian Privacy Principles in Schedule 1); and the Australian Consumer Law and Consumer Data Right, both enacted in the *Competition and Consumer Act 2010* (Cth).

7 See also APRA's prudential practice guides CPG 234 Information Security and CPG 235 Managing Data Risk.

8 *Privacy Act 1988* (Cth) s 40.

9 K Manwaring and P Hanraham, 'BEARing Responsibility for Cyber Security in Australian Financial Institutions: The Rising Tide of Directors' Personal Liability' (2019) 30 Journal of Banking and Finance Law and Practice 20, 36.

10 K Manwaring and P Hanraham, 'BEARing Responsibility for Cyber Security in Australian Financial Institutions: The Rising Tide of Directors' Personal Liability' (2019) 30 Journal of Banking and Finance Law and Practice 20, 36-37.

11 *Australian Securities and Investments Commission v Healey* (2011) 278 ALR 618 [20].

12 *Australian Securities and Investments Commission v Healey* (2011) 278 ALR 618 [229].

13 These include the continuous disclosure obligations for listed companies, the disclosure requirements for directors reports, and disclosure documents. If the Privacy Act applies to the organisation, and the cybersecurity incident constitutes an eligible data breach under the Privacy Act (i.e. the data breach is likely to result in serious harm to any of the individuals to whom the information relates), it must be reported to the OAIC and affected individuals.

14 *Corporations Act 2001* (Cth) s 674; ASX Listing Rules r 3.1.

15 Shareholder class actions for disclosure failures are most commonly brought under sections 1041E – 1041H of the Corporations Act.

16 K Manwaring and P Hanraham, 'BEARing Responsibility for Cyber Security in Australian Financial Institutions: The Rising Tide of Directors' Personal Liability' (2019) 30 Journal of Banking and Finance Law and Practice 20, 40.

17 *Corporations Act 2001* (Cth) s 79(c).

18 K Manwaring and P Hanraham, 'BEARing Responsibility for Cyber Security in Australian Financial Institutions: The Rising Tide of Directors' Personal Liability' (2019) 30 Journal of Banking and Finance Law and Practice 20, 2.

19 *Corporations Act 2001* (Cth) ss 912(1).

20 *Corporations Act 2001* (Cth) s 79(c).

21 Revised Explanatory Memorandum, Treasury Laws Amendment (Banking Executive Accountability and Related Measures) Bill 2017 (Cth) [1.92].

22 *Banking Act 1959* (Cth) s 37CB.

23 Revised Explanatory Memorandum, Treasury Laws Amendment (Banking Executive Accountability and Related Measures) Bill 2017 (Cth) [1.118].

24 *Banking Act 1959* (Cth) 37J(1).

25 The Government previously advised that it expects to introduce legislation implementing FAR at the end of 2020. In May 2020, the Government announced a six month deferral to the implementation of commitments associated with the Royal Commission. Those measures that the Government had indicated would be introduced into the Parliament by 30 June 2020, will now be introduced by December 2020. Similarly, those measures originally scheduled for introduction by December 2020 will now be introduced by 30 June 2021.

26 Class actions have been brought against Yahoo (now Altaba), TJX Companies, Wyndham, Target, Home Depot, Wendy's and Heartland Payment Systems.

27 K Manwaring and P Hanraham, 'BEARing Responsibility for Cyber Security in Australian Financial Institutions: The Rising Tide of Directors' Personal Liability' (2019) 30 Journal of Banking and Finance Law and Practice 20, 432.

28 On 1 October 2020, the US Treasury's Financial Crimes Enforcement Network (FinCEN) provided financial institutions with guidance on ransomware trends, red flags and reporting, and sharing of information to help in identifying and handling ransomware-related transactions. We have written about FinCEN's guidance and how ransomware attacks have increased money laundering and sanction risks faced by financial institutions both as targets of ransomware attacks and as potential intermediaries in facilitating ransomware payments in a previous Jones Day *Alert*.

29 From a sample of 500 companies globally, IBM found that the average total cost of a breach for companies with adequate incident response plans and teams was US$1.23 million less than for companies that had neither an incident response team nor an incident response plan (IBM Security, 'Cost of Data Breach Report,' (2019) *IBM Security* 1, 9).