Cyber Resilience: Managing Cyber Risk for Sustainable Prosperity

David Gerber, Partner, Clayton Utz and Lachlan Gell, Lawyer, Clayton Utz consider ASIC's recent focus on cyber risk management and cyber resilience

INTRODUCTION

On 21 April 2016 the Prime Minister, the Hon Malcolm Turnbull MP, launched Australia's new $230 million Cyber Security Strategy. Although the strategy has a focus on protecting Australian public sector organisations from cyber threats, it also addresses the importance of cyber security and cyber resilience in the private sector. The strategy emphasises that it is the responsibility of businesses themselves, and not the government, to ensure that they are able to manage effectively cyber security threats. Under the heading 'raising the bar', the strategy proposes that: "[s]elf-regulation and a national set of simple, voluntary guidelines co-designed with the private sector will help organisations improve their cyber security resilience." [1]

The strategy emphasises that it is the responsibility of businesses themselves, and not the government, to ensure that they are able to manage effectively cyber security threats.

To this end, the Government proposes to introduce an online "cyber threat sharing portal" for all businesses to share and collaborate on threats. It will also provide voluntary "health checks" to ASX 100 listed businesses, enabling them to better understand their cyber security status and how they compare to similar organisations.

Although the strategy stresses the importance of organisations strengthening their cyber defences and sharing information, it does not provide detail as to how cyber resilience ought to be improved. Over the last year, the Australian Securities and Investments Commission (**ASIC**) has, however, released reports which give this guidance. ASIC's reports explain how businesses can review and update their cyber-risk management practices.

This article provides an overview of ASIC's focus on cyber risk and cyber resilience. It sets out a step-by-step guide to assessing cyber resilience, summarises ASIC's practical guidance and lists questions that a board of directors may wish to ask when reviewing the organisation's risk management framework. It also examines briefly the government's recent proposal to introduce a mandatory cyber breach reporting regime. The authors conclude that cyber security and resilience will be key to sustainable prosperity in the information age.

CYBER RISK AND THE IMPORTANCE OF CYBER RESILIENCE

Every day we create and share information electronically as a fundamental part of doing business. The risks of doing so are numerous and increasing. They can lead to loss of data and serious privacy breaches, system shutdowns or even electronic blackmail and extortion. The impact of cyber risks can be significant - practically, legally and financially. Beyond the immediate costs to resolve cyber issues affecting systems and data, there can be profound impacts on reputation and potentially liability to third parties.

There is a growing recognition of the widespread risk to Australian businesses of all sizes of cyber-attacks and data breaches.[2] ASIC has released reports aimed at increasing awareness among Australian businesses of cyber risk and the importance of cyber resilience. These reports also indicate that the issue of cyber risk is now firmly on the regulatory agenda and should be front of mind for companies and their directors in almost all sectors of the economy, but most notably those regulated by ASIC's licensing regimes.

WHAT SHOULD ORGANISATIONS BE DOING TO MANAGE CYBER RISK?

In March 2015, ASIC released a report titled "Cyber Resilience: Health Check".[3] The report recommended that regulated entities review and update their cyber-management practices. ASIC suggested a health check on "cyber resilience" which ASIC defines as the ability to prepare for, respond to and recover from a cyber-attack.

The "health check" encourages businesses to take a number of specific actions, including:

1. to identify and monitor cyber risks;
2. to actively monitor trends in cyber risks and adapt to new cyber risks as they arise;
3. to let their customers and clients know if their personal data has been compromised;
4. to take responsibility for improving their cyber resilience;
5. to consider using the NIST Cybersecurity Framework[4] to help the business develop cyber resilience

1 Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy* (April 2016), p. 35.

2 Commonwealth of Australia, *Financial System Inquiry Final Report* (November 2014), pp. 268-269.

3 Australian Securities and Investments Commission, Report 429 *Cyber Resilience: Health Check* (19 March 2015).

in a proportional way, particularly where their exposure to a cyber-attack may have a significant impact on financial consumers, investors or market integrity;

6. to report cybercrime and cybersecurity incidents to relevant government agencies;
7. to consider using a CREST Australia[5] approved member organisation to help test existing IT systems, processes and procedures to ensure that they respond well to cyber risks;
8. if it is regulated by ASIC, to mitigate cyber risks by, at a minimum, implementing the ASD's[6] four highest-ranked mitigation strategies;
9. if it is regulated by ASIC (and particularly, if a licensee), to address cyber risks as part of their legal and compliance obligations - including risk management and disclosure requirements;
10. if it is an AFS licensee, to review the adequacy of their risk management systems and resources to address cyber risks; and
11. depending on a company's risk profile, consider taking out cyber insurance.

In March 2016, ASIC issued a further report titled "Cyber resilience assessment report: ASX Group and Chi-X Australia Pty Ltd".[7] The report presents the findings of ASIC's cyber resilience assessments of Australia's major financial infrastructure providers. It also provides some examples of cyber resilience good practices implemented by a wider sample of organisations operating in the financial services industry.

In conducting its formal assessment of the ASX Group and Chi-X, ASIC identified the following practices as the most resilient or "adaptive" across the organisations:

- established information security policies are periodically reviewed and updated;
- cyber security roles are defined, communicated and understood at the senior management level;
- legal and compliance obligations are understood and managed;
- response and recovery plans are managed, communicated and tested on a periodic basis; and
- cyber events are communicated within the organisation to ensure ongoing awareness of threats.

The 2016 report also encourages organisations to recognise the growing threat of cyber security, and improve their cyber resilience preparedness. It encourages them to adopt a number of cyber resilience good practices. These include:

- ongoing board engagement with cyber strategy and board ownership of cyber resilience;
- governance practices that are responsive to a rapidly changing cyber risk environment;
- cyber risk management driven by routine threat assessment of both internal and third party sources such as cloud-based service providers;
- collaboration and information sharing with other industry members, security agencies and law enforcement; and
- creating an organisational culture of cyber awareness through training programs.

CYBER GUIDANCE

ASIC is also proposing to issue guidance on cyber resilience, which would include the following key concepts:

- the attention of the board and senior management is critical to a successful cyber resilience strategy;
- the ability to resume operations quickly and safely after malicious cyber activities is paramount;
- providers should make use of good-quality threat intelligence and rigorous testing;
- cyber resilience requires a process of continuous improvement; and
- cyber resilience cannot be achieved by a financial market provider alone, it is a collective effort of the whole ecosystem.

cyber security and resilience will be key to sustainable prosperity in the information age

ASIC expects that the Cyber Guidance will be finalised in the second half of 2016.

KEY QUESTIONS FOR AN ORGANISATION'S BOARD OF DIRECTORS

Of particular interest is the emphasis that ASIC places on the responsibility for cyber resilience as an issue for an organisation's board of directors and senior management. ASIC has encouraged company officers to address the following key questions when reviewing their risk management frameworks:

1. Are cyber risks an integral part of the organisation's risk management framework?
2. How often is the cyber resilience program reviewed at the board level?
3. What risk is posed by cyber threats to the organisation's business?
4. Does the board need further expertise to understand the risk?

4 The NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity issued by the National Institute for Standards and Technology.

5 Council of Registered Ethical Security Testers Australia.

6 Australian Signals Directorate.

7 Australian Securities and Investments Commission, Report 468 *Cyber resilience assessment report: ASX Group and Chi-X Australia Pty Ltd* (7 March 2016).

5. How can cyber risk be monitored and what escalation triggers should be adopted?
6. What is the people strategy around cybersecurity?
7. What is in place to protect critical information assets?
8. What needs to occur in the event of a breach?

By placing the ultimate responsibility of cyber risk management on the officers of a business, this regulator has made it clear that cyber resilience is not simply a matter of good practice but, essentially, is one of regulatory compliance.

this legislative reform is expected to increase further the focus on cyber risk management

MANDATORY BREACH NOTIFICATION REGIME

Although not mentioned in the Cyber Security Strategy, ASIC's reports are timely given the Government's recent proposal to introduce a mandatory data breach notification scheme for entities regulated by the Privacy Act. The proposed scheme will likely mean that significant data breaches receive heightened attention from both the Office of the Australian Information Commissioner (**OAIC**) and ASIC.

Organisations which are subject to the *Privacy Act 1988* (Cth) are currently required to protect personal information from misuse, interference and loss, unauthorised access, modification and disclosure under Australian Privacy Principle 11. However, they are not subject to a mandatory data breach notification requirement under the Privacy Act. They are obliged to minimise the likelihood that personal information within their possession could be compromised. The legislation does not yet require them to notify an individual or agency in the event of an actual or suspected security breach. This is expected to change.

In December 2015, the Federal Government released a discussion paper[8] and an exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*. The Bill, if passed, will require certain entities to notify "serious data breaches" to affected individuals and the Australian Information Commissioner as soon as practicable. A "serious data breach" is one that creates a "real risk of serious harm" to the affected individuals. This includes harm to reputation, economic and financial harm, and may include physical, psychological and emotional harm. Guidance is expected to be issued by the OAIC to help businesses comply with the requirement to identify where "serious data breaches" have occurred.

Under the proposed Bill, an organisation would be required to notify the Commissioner of the details of the serious breach; the compromised information; and any remedial steps that victims should take. Businesses that fail to comply with the provisions would risk enforcement action including civil penalties for serious or repeated infringements. Further, a business will also be found to have failed to comply with the notification obligations if it was not aware of a serious data breach, but reasonably should have detected it.

There is much to be said for the introduction of mandatory data breach notification legislation.[9] If an organisation has suffered a serious data breach, notification will give people the opportunity to reduce the impact of the breach (e.g. by cancelling credit cards or changing account passwords). It should also increase public confidence in the handling of consumer information as organisations are compelled to improve their data security procedures and policies.

For an organisation that has suffered a data breach, mandatory notification gives rise to potential reputational risk and cost. Put simply, when an organisation is faced with regulatory investigations and is obliged to take steps to notify customers of a data breach, it is likely to incur significant legal and other costs. This may include costs to defend regulatory action on behalf of a class of affected individuals or, depending on the circumstances of the data breach, potentially even a class action. They will likely also face increased media and other public scrutiny. Therefore this legislative reform is expected to increase further the focus on cyber risk management. It may also drive the market for cyber risk insurance policies. An individually tailored cyber insurance policy can be a valuable tool for managing these risks and costs.

CONCLUSION

ASIC has cautioned that the 'weakest link' is often the real measure of an organisation or industry's cyber resilience. The regulator suggests that organisations ensure good practices are in place for assessing cyber risk and driving continuous improvement.

Clearly, both ASIC and the government expect that an organisation's cyber resilience framework must evolve continuously to cope with the dynamic and unpredictable nature of cyber threats. It is therefore essential for businesses in the private sector to have a long-term and comprehensive commitment to cyber resilience to deal with the issue of cyber threats.

Like many business opportunities, cyber carries with it some risk. The organisations which manage most effectively their cyber security and build and maintain cyber resilience, will be best placed to extract the value from developing or disruptive technologies in a sustainable way.

DAVID GERBER (Partner) and LACHLAN GELL (solicitor) practise in the Insurance and Risk group at Clayton Utz.

8 Commonwealth of Australia, Attorney-General's Department, *Discussion paper - Mandatory data breach notification* (December 2015).
9 See Smyth, Sara N, "Does Australia Really Need Mandatory Data Breach Notification Laws - And If So, What Kind?" (2013) 22(2) *Journal of Law, Information and Science* 159.