ASIC
Australian Securities & Investments Commission

REPORT 429

Cyber resilience: Health check

March 2015

About this report

This report highlights the importance of cyber resilience to ASIC's regulated population.

It is intended to help our regulated population improve their cyber resilience by increasing their awareness of cyber risks, encouraging collaboration between industry and government, and identifying opportunities for them to improve their cyber resilience. It also aims to identify how cyber risks should be addressed as part of current legal and compliance obligations that are relevant to ASIC's jurisdiction.

About ASIC regulatory documents

In administering legislation ASIC issues the following types of regulatory documents.

Consultation papers: seek feedback from stakeholders on matters ASIC is considering, such as proposed relief or proposed regulatory guidance.

Regulatory guides: give guidance to regulated entities by:

- explaining when and how ASIC will exercise specific powers under legislation (primarily the Corporations Act)
- explaining how ASIC interprets the law
- describing the principles underlying ASIC's approach
- giving practical guidance (e.g. describing the steps of a process such as applying for a licence or giving practical examples of how regulated entities may decide to meet their obligations).

Information sheets: provide concise guidance on a specific process or compliance issue or an overview of detailed guidance.

Reports: describe ASIC compliance or relief activity or the results of a research project.

Disclaimer

This report does not constitute legal advice. We encourage you to seek your own professional advice to find out how the Corporations Act and other applicable laws apply to you, as it is your responsibility to determine your obligations.

Examples in this report are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

Contents

A Overview

Key points

The digital age is central to the economic growth and wellbeing of Australians. It brings both opportunities and challenges.

Over recent years, there has been significant growth in the number and severity of cyber attacks around the world.

Cyber resilience is the ability to prepare for, respond to and recover from a cyber attack. Resilience is more than just preventing or responding to an attack—it also takes into account the ability to adapt and recover from such an event.

We are seeking to assist our regulated population in their efforts to improve cyber resilience. It is critical that our regulated entities manage their cyber risks.

We have outlined some 'health check prompts' to help you consider your cyber resilience.

1 The digital age is central to the economic growth and wellbeing of Australians. It brings both opportunities and challenges.

2 The rapid growth in innovation and technological developments in financial markets and services have delivered substantial productivity improvements in markets, both in Australia and globally. However, the rise of e-commerce and widespread internet connectivity also expose individuals, businesses and the financial system to risks that criminals can exploit.

3 Cyber attacks are a major risk for our regulated population.

4 The electronic linkages between the financial system, including market participants and financial market infrastructure, mean that the impact of a cyber attack can spread quickly—potentially affecting the integrity and efficiency of global markets and trust and confidence in the financial system.

What is cyber resilience?

5 Cyber resilience is the ability to prepare for, respond to and recover from a cyber attack. Resilience is more than just preventing or responding to an attack—it also takes into account the ability to operate during, and to adapt and recover, from such an event.

6 For our purposes, cyber resilience is the intended outcome of cyber risk management and cybersecurity measures.

7 Customarily, organisations have focused on protection against cyber attacks. However, a resilience-based approach to cyber attacks is vital for organisations to better adapt to change, reduce exposure to risk, and learn from incidents when they occur.

8 It is in the interest of all businesses to improve their resilience to cyber risks. Due to business, technological and financial interconnectedness, improving the resilience of one organisation can be a small step in improving the cyber resilience of all.

Purpose of this report

9 This report highlights the importance of cyber resilience to ASIC's regulated population, to support investor and financial consumer trust and confidence and ensure that markets are fair, orderly and transparent.

10 The purpose of this report is to assist our regulated population improve their cyber resilience by:

(a) increasing awareness of cyber risks (see Section B and Appendix 1);

(b) encouraging collaboration between industry and government and identifying opportunities for our regulated population to improve its cyber resilience (see Section C); and

(c) identifying how cyber risks should be addressed as part of current legal and compliance obligations that are relevant to ASIC's jurisdiction (see Section D and Appendix 2).

11 This report also highlights the US National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) as a potentially useful cyber resilience resource for our regulated population, and one that may be particularly relevant for licensees: see Section C and Appendix 3 for further information.

12 This report is intended to complement work being done nationally and internationally to address cyber threats and risks, including the Australian Government's review of Australia's cybersecurity policy, led by the Department of the Prime Minister and Cabinet. This report is focused on the resilience of individual regulated entities against cyber attacks within their existing requirements.

13 We may update our work to complement any Australian Government policy initiatives that are developed once this review is finalised, or in light of any relevant international developments.

ASIC's role

14 ASIC is Australia's integrated corporate, markets, financial services and consumer credit regulator. We contribute to Australia's economic reputation and wellbeing by ensuring that Australia's financial markets are fair, orderly and transparent, and underpinned by financial consumer and investor trust and confidence.

15 Our regulated population is at the frontline of cyber risk management. Many have proactive and sophisticated risk management practices to address cyber risks. The types of risks businesses face, and the efforts that they will need to undertake to ensure their cyber resilience, will depend on the nature, scale and complexity of their businesses.

16 However, given the breadth of our regulated population, ASIC has a role to play to ensure we are aware of cyber risks and to encourage risk-based and proportionate cyber-resilience management practices.

17 To promote cyber resilience, we intend to:

(a) monitor market developments;

(b) continue to engage with other Government departments to identify cyber risks and build cyber resilience;

(c) improve awareness of the importance of cyber resilience and increase the profile of the issues; and

(d) incorporate cyber resilience in our surveillance programs, where appropriate, across our regulated population.

18 We are considering providing a self-assessment tool based on the NIST Cybersecurity Framework that may be useful to our regulated population in assessing their cyber resilience.

19 ASIC is also responsible for promoting consumer protection in relation to the Australian financial system. As part of this responsibility, we provide information through ASIC's MoneySmart website (www.moneysmart.gov.au) to help financial consumers and investors better protect themselves from cyber risks.

Health check prompts

20 If you are an entity regulated by ASIC—particularly if you are a licensee[1]—you have legal and compliance obligations that may require you to review and update your cyber-risk management practices.

21 We have outlined some questions to help you consider your cyber resilience. These 'health check prompts' are set out Table 1. They summarise and build on a number of 'action points' included throughout this document that may help you improve your cyber resilience.

22 The prompts highlight issues to consider as part of general governance practices, and the specific ways you can identify, protect against, detect, respond to, and recover from, cyber risks.

23 More generally, we encourage all businesses to be aware of the cyber risks they face and take action to improve cyber resilience.

[1]For our purposes, this includes an Australian financial services (AFS) licensee, an Australian credit licensee (credit licensee), an Australian market licensee (market licensee), a clearing and settlement (CS) facility licensee or an Australian derivative trade repository (ADTR) licensee.

Table 1: Health Check Prompts

Have you considered …		
General context		
Governance	1. If your board and senior management are aware of your cyber risks?	You are encouraged to review the level of board and senior management oversight of your cyber risks, including how frequently risks are updated. Oversight should take into account your legal and compliance obligations and be proportionate to the cyber risks you face and the nature, scale and complexity of your business.
	2. Assessing your organisation against the NIST Cybersecurity Framework? See Action C1.	The NIST Cybersecurity Framework allows you to assess and manage your cyber resilience by assisting you to: • determine your current cybersecurity capabilities; • set goals for a target level of cyber resilience; and • establish a plan to improve and maintain cybersecurity and therefore cyber resilience. We encourage businesses—particularly where their exposure to a cyber attack may have a significant impact on financial consumers, investors or market integrity—to consider using the NIST Cybersecurity Framework to assess and mitigate their cyber risks or to stocktake their cyber-risk management practices. The NIST Cybersecurity Framework is risk based and scalable and can help you develop your cyber resilience in a proportionate way.
Identify	3. What information or business assets are essential to your organisation?	You may not have assessed what information, data or operational assets are essential to your business. This may include intellectual property, people or personnel information, financial information, trade secrets, strategic assets, or information. As part of your assessment, it is useful to maintain an up-to-date inventory of all systems, software and information assets (internal and external), catalogued according to the level of risk exposure associated with each.

Have you considered …		
Identify (cont.)	4. What cyber risks you are exposed to? See Actions B1 and B2.	The risks you are exposed to can determine what action you take to improve your cyber resilience. A cyber risk assessment could involve: • identifying cyber risks (threats and vulnerabilities) faced by a business; • measuring and communicating those risks internally' and • prioritising and implementing measures to mitigate the risks. Cyber risks evolve and change over time and require ongoing monitoring and assessment.
	5. The cyber resilience of vital third-party providers or clients?	Poor cyber resilience of your third-party providers, such as business partners, service providers, vital contractors and suppliers, customers and clients, or others in your supply chain may expose you to cyber risks. You may consider reviewing the cyber-risk management of third parties critical to your business continuity—including the cyber risks of outsourcing arrangements or cloud-based services.
	6. If cyber risks are well integrated into your normal business risk management and procedures?	You may want to assess whether you have adequate arrangements to identify, protect, detect, respond, and recover from cyber risks, and whether these form part of overall risk management, governance and business process change practices. This may include: • periodic risk assessments to assess, evaluate and manage cyber risks; • business continuity planning that takes into account cyber risks; and • processes for sharing information or collaborating on cyber intelligence, in order to ensure responses to cyber risks are driven by appropriate intelligence (see Health Check Prompts 11–12). You should take a proportionate approach to cyber resilience according to the cyber risks you face and the nature, scale and complexity of your business.

Have you considered …			
Identify (cont.)	7.	The level of awareness of cyber risks within your business?	Cyber risks can arise from within the business and you may want to review how well informed your staff are of your policies and procedures, and encourage good practices for cyber risk management. Good practices can include: • using strong passwords and changing them periodically; • logging out of systems when they are not in use, particularly when using remote access; and • raising awareness of the types of cyber attacks that may occur, and how to report them.
Protect	8.	Reviewing and updating your information security policies and procedures? See Action C6.	You may not have updated your information security policies and procedures to incorporate the latest standards. You can draw on a range of recognised strategies and standards, including the: • Australian Signals Directorate (ASD) *Strategies to mitigate targeted cyber intrusions*, particularly the four highest-ranked mitigation strategies, which address around 85% of common cyber risks; • International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) information security standards: – ISO/IEC 27001 *Information technology—Security techniques—Information security management systems—Requirements*; and – ISO/IEC 27002 *Information technology—Security techniques—Code of practice for information security management*; • Information Systems Audit and Control Association's (ISACA) Control Objectives for Information and Related Technology (COBIT 5); and • Payment Card Industry Security Standards Council's Payment Card Industry Data Security Standard.

Have you considered …		
Protect (cont.)	9. Testing your existing information technology (IT) systems, processes and procedures for cyber resilience? See Action C5.	You may not have tested your existing IT systems, processes and procedures recently to ensure they respond well to cyber risks. You can consider whether your policies and procedures are: • designed to allow you detect and respond to cyber attacks; • embedded in any new projects or new and upgraded systems; and • monitored and updated to reflect new or changed cyber risks as they arise. You may want to use a Council of Registered Ethical Security Testers (CREST) Australia approved member organisation to assist you.
	10. If you have sufficient resources to deal with the cyber risks, including properly trained staff (employees and contractors)?	Your investment in cyber resilience may depend on the type of risks you face, the nature, scale and complexity of your business and your legal and compliance obligations. As part of considering the resources you may require, consider updating or renewing appropriate education and training for employees and contractors.
Detect	11. If you have monitoring processes and procedures to detect a cyber attack?	Monitoring processes and procedures can be critical in the process of alerting you to and identifying any cyber attacks. The benefits of monitoring processes may include detecting signs of cyber attacks within your systems, on your websites or among external providers. This could include: • any anomalous activity occurring on your systems (e.g. unauthorised access to restricted applications or data, or unusually high accesses to certain data); • irregular behaviour by users in your websites; or • abnormal external service provider activity.
	12. How you should engage with other businesses and government? See Actions C2, C3, 0 and C5.	We encourage you to collaborate with others within your industry and with the Australian Government to share and improve your cyber intelligence. Businesses can also seek access to specialist resources and skills on cyber resilience, including from government. CERT Australia also provides resources: see Health Check Prompt 26.

Have you considered …		
Respond	13. If your response planning is adequate?	Response plans can be more effective where they are documented, communicated to relevant internal and external stakeholders, and regularly updated. In preparing response plans, you may consider incorporating specific scenarios in them that may be tested on a periodic basis, to allow you to review and update your response plans based on this testing.
	14. How you would notify law enforcement and other businesses of a cyber attack? See Actions C2 and C3.	If you are a small-to-medium-sized business, the Australian Cybercrime Online Reporting Network (ACORN) allows you to securely report cyber attacks that may be in breach of Australian law. If you are a large business, the Australian Cyber Security Centre (ACSC) through CERT Australia allows you to securely report cybersecurity incidents to Government. Reporting instances of cyber attacks to ACORN and ACSC will help you and our law enforcement agencies to better combat the growing threat of cyber attacks in Australia.
	15. How you would notify your customers or clients of a breach of their personal data? See Action B4.	To build and maintain investor and financial consumer trust and confidence, it is important to notify individuals—such as your employees, customers or clients—if there has been a breach of their personal data. You should consider any obligations that you may have under privacy law. The *Data breach notification guide: A guide to handling personal information security breaches* by the Office of the Australian Information Commissioner (OAIC) can assist you prepare and implement a data breach policy and response plan (that includes notifying affected individuals and the OAIC).
Recover	16. Whether you have suitable recovery plans?	Proactive policies, which are regularly reviewed and updated, can enable you to manage your recovery from a cyber attack. Policies can include: • formal communication plans to manage internal and external communication during and after a recovery process; and • formal review processes to learn lessons from any cyber attacks that do occur (i.e. on how the attack was identified, responded to and recovered from), which can be fed back into the policies, procedures and risk assessment.

Have you considered …		
Regulatory context (one or more may apply to you: see Action D1.		
If you are a director	17. If as a director, you are meeting your legal obligations?	You may not have considered how cyber risks may affect your directors' duties and annual director report disclosure requirements. We encourage you to review your board-level oversight of cyber risks and cyber resilience as part of your systems managing your material business risks, and consider if you need to incorporate greater consideration of cyber risks into your governance and risk management practices.
If you are a corporation	18. Your disclosure of the cyber risks in a prospectus?	Cyber risks may need to be disclosed if they are a significant factor that would form part of information that investors and their professional advisers would reasonably require to make an informed assessment of any offer.
If you are a listed entity	19. Your continuous disclosure obligations?	A cyber attack may need to be disclosed as market-sensitive information.
If you are an AFS licensee	20. How cyber risks affect your general licensing obligations? See Action D2.	Your risk management plans, policies and procedures may need to take cyber risks into account. Inadequacies in your risk management systems may amount to a significant breach of your obligations that you must report to us. Note: Alternative arrangements apply to Australian Prudential Regulation Authority (APRA) regulated entities (see paragraphs 175–176).
	21. Your disclosure of cyber risks in a Product Disclosure Statement (PDS)? See Action D3.	Cyber risks may need to be disclosed as a significant risk associated with holding the product.
If you are a responsible entity	22. If your compliance plan is up to date?	A compliance plan must reflect, among other things, the major compliance risks that investors face. This may include cyber risks.

Have you considered …		
If you are a market participant	23. How you identify and deal with unauthorised transactions on client accounts? See Action B4.	It is useful to pay particular attention to client accounts that appear to be trading unprofitably and take action to verify the origin of such orders, and address complaints of unauthorised transactions from clients. You could also encourage your clients to monitor their accounts and change passwords regularly.
If you are a credit licensee	24. How cyber risks affect your general licensing obligations? See Action D4.	Your risk management plans, policies and procedures may need to take cyber risks into account. Note: Alternative arrangements apply to APRA-regulated entities: see paragraphs 175–176.
If you operate a financial market infrastructure	25. How cyber risks affect your licensing obligations?	Your cyber-risk management should be proportionate to your heightened cyber risks.
If you provide essential services or are a major Australian business	26. Establishing a partnership with our national computer emergency response team, CERT Australia? See Action C3.	CERT Australia is the main point of contact for cybersecurity issues affecting major Australian businesses. It provides major businesses with the best cybersecurity advice and support possible, as soon as possible. You should: • partner with CERT Australia before an incident occurs; and • report all cybersecurity incidents to CERT Australia. All information provided to CERT Australia is held in the strictest confidence.

Feedback

24 We welcome feedback on the issues raised in this report—in particular, your views on:

(a) the cyber risks posed, and the extent of those risks to ASIC's regulated population; and

(b) options for mitigating cyber risks, including the actions identified in this report.

25 Please provide any feedback by 31 June 2015 to:

Rushika Curtis-Hunting
Senior Policy Adviser
Strategy Group
Australian Securities and Investments Commission
email: policy.submissions@asic.gov.au

B Cyber risk landscape

Key points

Over recent years, there has been significant growth in the number and severity of cyber attacks around the world.

The heightened risk of a cyber attack is recognised as a regulatory concern across a range of international organisations. There are various approaches being adopted globally, some legislative driven and some voluntary.

Businesses face a range of cyber risks, both external threats and internal vulnerabilities that continue to evolve over time.

Our regulated population is exposed to evolving trends that are specific to their activities. Our regulated population should be aware of, and prepare for, the risks it may face.

What is a cyber attack?

26 A cyber attack is an attempted or actual incident that either:

(a) uses computer technology or networks to commit or facilitate the commission of traditional crimes, such as fraud and forgery—for example, identity or data theft (computer assisted); or

(b) is directed at computers and computer systems or other information communication technologies—for example, hacking or denial of services (computer integrity).

27 The number, sophistication and complexity of cyber attacks has increased markedly in recent years.[2] This trend is expected to accelerate in the future.[3] PricewaterhouseCooper's Global State of Information Security Survey 2015, which surveyed more than 9,700 security, IT, and business executives, suggests that the total number of cybersecurity incidents detected in 2014 was 42.8 million, an increase of 48% from 2013.[4]

28 More problematic is that an estimated 71% of incidents go undetected.[5]

[2] Murray Inquiry, *Financial System Inquiry interim report*, report, July 2014, p. 4-55.
[3] The compound annual growth rate of cybersecurity incidents is 66%: PricewaterhouseCoopers, *Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015*, report, 30 September 2014.
[4] PricewaterhouseCoopers, *Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015*, report, 30 September 2014, p. 7.
[5] Trustwave Holdings, *2014 Trustwave global security report*, report, May 2014.

Impacts of a cyber attack

29 A cyber attack can affect us all. It can undermine businesses and affect our economy. It may also erode investor and financial consumer trust and confidence in the financial system and wider economy.

30 The estimated annual cost of cyber attacks to the global economy is more than $400 billion.[6] In 2013, cyber attacks affected 5 million Australians at an estimated cost of $1.06 billion.[7] As well as these direct costs, cyber attacks may:

(a) result in significant loss of opportunity costs for an organisation—for example, through stolen intellectual property; or

(b) undermine confidence in an organisation and damage its reputation in the community—for example, through data and privacy breaches as a result of hacking.

31 In response, international regulators and regulatory organisations are focusing on improvements that can be made across government and industry, including the financial system, to build resilience against cyber attacks and to improve industry and government cooperation.

International developments

32 Heightened cyber risk is recognised as a regulatory concern across a range of international organisations. There is an increased focus on industry information-sharing and public-private collaboration to deal with cyber risks.

33 An overview of some international developments is set out in Appendix 4.

34 Cyber risk management is still a largely voluntary exercise for most companies in the United States, Asia and Europe. The UK Government has indicated that it prefers to work directly with industry to raise awareness and share best practice of cyber resilience.

35 However, the regulatory environment is showing signs of toughening. The European Union is moving to require companies in certain sectors to report all cyber attacks to government and take specific risk management measures to protect systems and data.

36 The International Organization of Securities Commissions (IOSCO) is working on a range of projects to bring together a coordinated policy response: see Appendix 4 for more details.

---

[6] Centre for Strategic and International Studies, *Net losses: Estimating the global cost of cybercrime—Economic impact of cybercrime II*, report, June 2014, McAfee, p. 2.
[7] Symantec, *2013 Norton report: Total cost of cybercrime in Australia amounts to AU$1.06 billion*, media release, 16 October 2013.

37 The United States is also ramping up its efforts following President Obama's State of the Union address in January 2015, which declared cybersecurity a government priority. It was followed by a range of proposed reforms including proposals for nationally consistent mandatory reporting of data breaches to consumers: see Appendix 4 for more details.

38 Due to the United States' global reach in business, IT services and financial markets, any US legislation or guidance relating to cyber resilience is likely to significantly influence the practices of global businesses, or those who engage with US businesses, IT services or financial markets. Software that is produced for the US market and used globally will likely be developed to reflect US cyber resilience requirements.

Cyber risks

Threats and vulnerabilities

39 There are a range of cyber risks faced by business—both external threats and internal vulnerabilities.

40 Any business that interacts over electronic networks or the internet, or is reliant on third-party technology vendors and suppliers, carries a risk of exposure.

41 The ongoing evolution of technology means that that the risk environment is constantly changing.

42 Cyber risks are recognised as being increasingly diverse and sometimes unforeseeable—placing a greater emphasis on responding to risks and managing their effects, not just trying to prevent or avoid them.

43 It is not possible for businesses—including those within our regulated population—to protect themselves against every cyber risk. However, it is important that businesses are aware of the risks they may face.

44 Common sources of cyber attack, threats and vulnerabilities that may increase the cyber risk exposure of a business are identified in Appendix 1.

Action

B1 We encourage businesses to identify and monitor their cyber risks.

Sources of threats

45 Cyber criminals include individuals acting alone, but also industrialised, organised groups with vast resources at their disposal. They can be

financially, ideologically or politically motivated to sabotage companies or destabilise financial markets or services.

46 The principal source of cyber attacks to Australia is likely to arise offshore.[8] This could include individuals or temporary networks of people who collaborate across borders.

Trends in cyber risks

47 Cyber risks are dynamic—they can evolve or adapt quickly to changing environments. It is important to appreciate the trends and challenges in the cyber environment that may produce new or different cyber risks.

Action

B2 We encourage businesses to actively monitor trends in cyber risks and adapt to new cyber risks as they arise.

Data breaches

48 Data breaches are a key business risk. Companies can hold large amounts of personal information (including financial information) about individuals, customers, suppliers, or employees.

49 Hacking from external sources is considered the primary cause of data breaches in recent times.[9] High-profile hacking attacks of companies in 2013–14 that resulted in significant data breaches have increased awareness of cyber attacks in the community.[10]

Case Study 1: Target data breach[11]

In 2014, 40 million credit card numbers and the personal information of 70 million individuals were stolen from US retail chain Target through the installation of malware in Target's security and payment system.

The malware was designed to steal every credit card used in Target's 1,797 US stores. At point of sale—when the shopper's purchases had been scanned and they were about to pay for their goods—the malware would step in and capture the shopper's credit card number and store it on the Target server that had been commandeered by the hackers.

Target became aware of the breach in mid-December 2014 after being notified by the US Department of Justice. While Target's IT security

[8] Australian Crime Commission, *Cyber and technology enabled crimes*, crime profile fact sheet, p. 2.
[9] Identity Theft Resource Center, *Surpasses more than 5,000 reported breaches and 675 million records exposed since 2005*, press release, 12 January 2015.
[10] Symantec, *Internet security threat report 2014*, vol 19, April 2014, p. 5.
[11] M Riley, B Elgin, D Lawrence and C Matlack, 'Missed alarms and 40 million stolen credit card numbers: How Target blew it', *Bloomberg Businessweek*, 13 March 2014.

systems detected the breaches in late November and early December, they were not followed up.

50 In 2013, over 552 million identities were compromised through cyber attacks, putting a range of personal information—including credit card details, birth dates, government identification numbers, medical records, financial information, email addresses and passwords—into the criminal realm.[12]

51 Data breaches can raise significant privacy concerns and result in financial loss for individuals and businesses. A company may be open to liability for the breach of privacy and it can affect company value. It may also result in reputational loss for a company.

52 Those operating in the financial system or listed and unlisted companies in the retail sector can hold a range of sensitive data—including financial information—about their customers and clients. They can be a specific target for a cyber attack seeking access to personal data.

Case Study 2: JP Morgan Chase & Co

The names, addresses, phone numbers and email addresses of approximately 76 million households and 7 million small businesses were exposed when computer systems at JP Morgan Chase & Co was hacked in 2014. JP Morgan & Chase became aware of a cyber attack in August 2014.

However, more sensitive data—such as customer account information or social security numbers—was not compromised.

It is understood that hackers were able to get into JP Morgan Chase & Co's network by compromising the computer of an employee with special privileges both at work and at home to access the bank's network to obtain contact data. A key vulnerability was that JP Morgan Chase & Co had failed to ensure all of its servers were installed with a two-layered security system (two-factor authentication) like most major banks.

This matter is the subject of ongoing investigation in the United States.

53 In March 2015, the Australian Government agreed to introduce a mandatory data breach notification scheme to be effective by end of 2015 for individuals affected by a data breach. The Government will consult on draft legislation prior to its introduction. This was in response to a recommendation by the Parliamentary Joint Committee on Intelligence and Security's *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*.[13]

[12] Symantec, *Internet security threat report 2014*, vol 19, April 2014.
[13] Senator the Hon George Brandis QC, Attorney-General, and the Hon Malcolm Turnbull, Minister for Communication, joint press release, *The Australian Government has responded to the inquiry of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, 3 March 2015.

Action

B3 We encourage businesses to let their customers and clients know if their personal data has been compromised.

User developments

54 Australians are rapid adopters of technology, with 7.5 million Australians accessing the internet via their mobile phones in 2013 (an increase of 33% from 2012).[14] This contributes to the swift growth of financial services, such as mobile banking and electronic payments.

55 By way of illustration, more Australians shop online for insurance and financial services than their counterparts in the United States and major European economies.[15]

56 As mobile and digital technologies get more complex and increase in use, the risks associated with them also increase—for example, 38% of mobile users have experienced cybercrime.[16] Cyber attacks specific to mobile technologies include the use of hidden malware inside mobile apps.

57 Social media scams are also increasing.[17] Social media can make users more susceptible to cyber attack due to its accessibility and use on mobile devices. For example, fake offers intended to obtain personal and financial details of the person or other 'phishing' accounted for the largest number of attacks of Facebook users in 2013—81% in 2013, compared to 56% in 2012. [18]

Internet of Things

58 Australians have also become more wired and interconnected through a range of connected consumer devices—also known as the Internet of Things (IOT) devices. This includes baby monitors, smart televisions, security cameras, cars and medical equipment.

59 There has been an increase in cyber attacks on IOT devices.[19] IOT devices can have access to, or provide a link to some of our most sensitive personal data, such as banking and financial information. A recent study of IOT devices found that 70% of the 10 most commonly used devices contained serious vulnerabilities, such as poor software protections.[20]

[14] Australian Communications and Media Authority, *Communications report 2012–13*, report, 2013.
[15] Boston Consulting Group, *2013 Global Consumer Sentiment Survey*, report, 2013.
[16] Symantec, *Internet security threat report 2014*, vol 19, April 2014, p. 7.
[17] Symantec, *Internet security threat report 2014*, vol 19, April 2014, p. 8.
[18] Symantec, *Internet security threat report 2014*, vol 19, April 2014, p. 7.
[19] Symantec, *Internet security threat report 2014*, vol 19, April 2014, p. 7.
[20] HP Fortify on Demand, *Internet of Things research study*, report, July 2014, Hewlett Packard.

Cloud technology

60 Cloud technology or 'shared' computing services allows organisations and individuals to store and access data and programs over the internet, instead of building and maintaining their own infrastructure.

61 Cloud technology can increase efficiency and lower data costs. It is increasingly being used by the financial services sector.[21] However, it also has unique cyber risks, including that:

(a) it may dilute an organisation's control over its data and systems, particularly if the cloud provider is a third party or offshore;

(b) cloud providers generally do not guarantee the security of data stored in their cloud and may limit their contractual exposure; and

(c) the shared storage of information may increase exposure to cyber attack—for example, data from one company can be compromised if another company on the same cloud service is being hacked.

Cyber insurance

62 There has been increasing appetite for, and developments in, targeted cyber insurance liability cover. Existing insurance (e.g. business continuity or professional indemnity cover) may not adequately cover the impact of a cyber attack.

63 Cyber insurance can include a range of covers tailored to relevant cyber risks, such as:

(a) data or privacy breach cover—relating to the management of an incident, notification of the data subject, remediation, court costs and regulatory fines;

(b) media liability cover—for example, third-party damages for a defacement of a website, or intellectual property infringements;

(c) extortion liability cover—typically due to losses as a result of a threat of extortion; and

(d) network security liability cover—third-party damages as a result of a cyber attack on network security, such as a disruption of service attack or a theft of data on third-party systems.

64 Considering cyber insurance may be an appropriate business decision based on a company's risk profile.

[21] For example, shifting to cloud services has reduced the Commonwealth Bank's storage, app testing and development costs by 50%: C Duckett, 'CBA striving for 'pure cloud' amid vendor garbage', *ZDNet*, 14 November 2012, viewed 3 February 2015.

Specific concerns for our regulated population

65 Certain cyber risks can be unique or problematic to our regulated population or sectors of our regulated population. We have identified issues that may raise particular concerns. This is not an exhaustive list, but is intended to provide some context for the cyber risks and the impacts of a cyber attack you may face.

Critical infrastructure and systemic risk

66 The term 'critical infrastructure' refers to assets that are essential for the functioning of society and the economy, and to ensure national security. [22]

67 The financial system is considered part of Australia's critical infrastructure.[23] It plays a vital role in supporting economic growth and meeting the financial needs of Australians. It provides critical economic functions, such as credit and payments services.

68 Cyber attacks are now considered a systemic risk for the financial system.[24]

69 Systemic risk can be broadly defined as 'the risk of disruption to the flow of financial services that is caused by an impairment of all or parts of the financial system and has the potential to have serious negative consequences for the real economy'.[25]

70 In that context, we are concerned about the impact of a cyber attack on our regulated population having a significant effect on investors and financial consumers or market integrity.

71 Some of ASIC's regulated entities may have a role to play in ensuring the continuity of essential (non-substitutable) services to the community—for example, financial market infrastructure or banks providing payments or access to funds. Others should be aware of the impact a cyber attack on them will have on the wider economy—particularly if it may have a significant effect on investors and financial consumers or on market integrity.

[22] The Commonwealth, state and territory governments define critical infrastructure as those physical facilities, supply changes, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would have a significant impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.
[23] Murray Inquiry, *Financial System Inquiry interim report*, report, July 2014, p. xliii.
[24] Murray Inquiry, *Financial System Inquiry interim report*, report, July 2014, p. 4-59.
[25] Financial Stability Board, International Monetary Fund and Bank of International Settlements, *Guidance to assess the systemic importance of financial institutions, markets and instruments: Initial considerations—Background paper*, report to the G20 Finance Ministers and Central Bank Governors, 28 October 2009.

Financial market infrastructure

72 Technology in financial markets is enhancing the capacity, accuracy and speed of order transmissions and executions, and stimulating competition, which has put downward pressure on trading fees.

73 However, the increased digitisation of financial markets, with sensitive data and critical processes being moved to computer-based platforms, increases their susceptibility to cyber attack.

74 Over half (53%) of world security exchanges surveyed by IOSCO in 2013 reported experiencing a cyber attack in the preceding year.[26]

Case Study 3: Warsaw Stock Exchange[27]

In October 2014, hackers breached the Warsaw Stock Exchange and exposed the login credentials of a number of brokers.

Using the stolen credentials, they managed to enter into the private email inbox of the stock exchange and steal customer data from them (including intimate pictures).

Hackers represented themselves as cyber terrorists. The attack lasted 10 days as the Warsaw Stock Exchange struggled to get the attackers out of the system.

Systemic risk

75 In the IOSCO survey, a significant majority of world security exchanges identified a cyber attack as a potential systemic risk.[28]

76 Systemic risk in the securities market could result in widespread mistrust and retreat from markets—affecting market integrity, including the fair, efficient and orderly operation of markets.

77 More generally, cyber threats have emerged as a growing systemic risk to all types of financial market infrastructures—their biggest cyber vulnerability is managing their complexities and interdependencies.[29]

Disruptive cyber attacks

78 IOSCO also identified that the most common types of attacks against security exchanges were disruptive in nature and did not involve significant direct financial loss—such as denial of service or other attacks arising out of

[26] R Tendulkar and G Naacke, *Cyber-crime, securities markets and systemic risk* (SWP1/2013), joint staff working paper, IOSCO Research Department and World Federation of Exchanges, 16 July 2013.
[27] C Bennett, 'Hackers breach the Warsaw Stock Exchange', *The Hill*, 24 October 2014.
[28] R Tendulkar and G Naacke, *Cyber-crime, securities markets and systemic risk* (SWP1/2013), joint staff working paper, IOSCO Research Department and World Federation of Exchanges, 16 July 2013.
[29] Committee on Payments and Market Infrastructure, *Cyber resilience in financial market infrastructures*, report, Bank for International Settlements, November 2014, p. 4.

malware.[30] The attacks targeted core infrastructures and providers of essential services.

79 This suggests that the primary motive of cyber attacks in financial markets is destabilisation and not financial gain. This is distinct from the more traditional crimes against the financial sector, such as fraud and theft.

Financial services

Market participants

80 The increased reliance on online accounts by investors and electronic trading can contribute to increased cyber risks for market participants.

Unauthorised trading

81 Market participants may face various risks, including the risk of their client accounts being hacked or manipulated.

82 ASIC has discovered identity fraud on client accounts through alerts generated by ASIC's Market Analysis Intelligence (MAI) surveillance system in response to price and volume anomalies. We notified and worked with relevant market participants to ensure appropriate action was taken.

Case Study 4: Identify fraud in client accounts

Instances of identity fraud in financial markets that ASIC has discovered include:

- clients being impersonated by mimicking the client's email address or establishing an email address which is markedly similar to that of an existing client. After establishing email contact with a broker, the criminal issues instructions to liquidate the client's positions and distribute the proceeds to alternative bank accounts (including third party accounts); and
- clients overseas having their mail intercepted and personal details stolen, such as the client's full name, address, date of birth and share trade account information. The criminal supplies relevant information to Australian brokers, including certified copies of passports and drivers' licences, to effect share sales. The legitimate clients' securities have then been sold without their approval or knowledge.

83 Client accounts that appear to be trading unprofitably or complaints of unusual trading from clients may be a sign of unauthorised account trading.

84 We encourage market participants to continue their positive engagement with ASIC in acting swiftly to identify and address cyber attacks.

[30] R Tendulkar and G Naacke, *Cyber-crime, securities markets and systemic risk* (SWP1/2013), joint staff working paper, IOSCO Research Department and World Federation of Exchanges, 16 July 2013.

Action

B4 Market participants are encouraged to:

(a) pay particular attention to client accounts that appear to be trading unprofitably and take action to verify the origin of such orders;

(b) address complaints of unauthorised transactions from clients;

(c) encourage their clients to monitor their accounts and change passwords regularly; and

(d) continue to engage with ASIC on cyber risks and cyber attacks.

Market manipulation

85 ASIC is also aware of cyber attacks being used to manipulate share prices—for example, through account hacking to obtain financial gain.

Case Study 5: Eastern European stock manipulation

ASIC has detected instances where an account holder based overseas purchase shares on an Australian market through a market participant. Suspected related parties gain unauthorised access to other client accounts (hacking) and use them to sell their holdings for cash. The cash is then invested into the particular shares purchased by the account holder, to increase the price of the relevant stocks. The account holder based overseas then sells their shares at the higher price, generating a profit.

The shares involved are usually 'penny stocks' and are not traded frequently under normal market conditions. The price and trading volume of these shares often increase significantly on the days when account hacking activities occurred.

Cyber risks of dark pool and high-frequency trading

86 Advances in technology have changed the way orders are generated and executed by users of the market, with most orders now generated and executed by computer programs running decision and execution algorithms.

87 These advances have also made it easier to trade away from exchange markets; there has been an increased use by market participants of dark trading venues known as 'crossing systems' and 'dark pools'.[31]

88 A cyber attack on crossing systems or automated trading may take advantage of trading complexity and capacity, increasing the risk of disorderly markets (through the malfunction of algorithmic programs) and the risk of market misconduct (such as unsolicited information leakage and possible market manipulation of dark pools).

[31] A 'dark pool' is a system that enables assets such as shares to be traded away from public exchanges by 'matching' client orders. The matching of client orders can be described as a 'crossing system'.

Banking and payment systems

89 The use of electronic payment methods and the range of payment channels have grown significantly. Innovations are making electronic payments faster and more convenient, but are also elevating the risk of cyber attacks on financial institutions.

Banking transactions

90 Cyber attacks on banking services can have broad ramifications—including having systemic risk implications.

91 Cyber criminals may target weaknesses in the system to access funds—for example, targeting pre-paid debit cards because such cards are not linked to specific accounts, minimising early detection.[32]

92 The increased use of mobile banking is also a significant vulnerability. Symantec's *Internet security threat report 2014* identified a 58% increase in mobile malware compared with a year earlier, and a 32% increase in the number of reported vulnerabilities in mobile operating systems during the same time frame.[33]

Case Study 6: Operation High Roller[34]

In 2012, an orchestrated cyber attack fraudulently took between $78 million to $2.5 billion from bank accounts in Europe, the United States and Latin America.

It targeted high-value commercial accounts or high net-worth individuals in a range of financial institutions—from small credit unions and regional banks to large global banks.

The attackers used heavily automated intervention strategies through remote servers to overcome 'multi-factor' authentication processes financial institutions commonly use to verify banking transactions (i.e. a security challenge question, a one-time digital token such as a password sent by text message, or account log-in details).

The malware automatically found a victim's highest value account and transferred money to an account controlled by a 'mule' in another country.

Settlement risk

93 A cyber attack on a payments system may crystallise in settlement risk—that is, the inability of one financial institution to make payments to another financial institution on an agreed timetable. Financial institutions that do not receive payments may need those funds to make payments to other parties—

[32] E Flitter and T Agrawal, *Prepaid debit cards: a weak link in bank security*, Reuters, 11 May 2013.
[33] Longitude Research, *Cyberrisk in banking*, report, September 2014, p. 9.
[34] D Marcus and R Sherstobitoff, *Dissecting Operation High Roller*, white paper, McAfee and Guardian Analytics, 2012.

for example, their customers. Such failures, if sufficiently large, can cause liquidity shortages and significantly disrupt the financial system.

Point-of-sale risks

94 Financial institutions that are payments system providers may be susceptible to increased cyber risks due to point-of-sale vulnerabilities.

95 The 2014 Target cyber attack (see Case Study 1) and Neiman Marcus cyber attack (involving the theft of thousands of credit card details) show that merchants are vulnerable to cyber attack—often at point-of-sale.

96 Retailers can be targeted by malware that exploit point-of-sale software and network vulnerabilities to obtain access to the personal and financial information of consumers. Smaller retail organisations may have less sophisticated or secure systems, making them easier targets for attackers aiming to access financial information and payment system networks.

97 This can increase the vulnerability of a payments system provider (i.e. a bank or other financial institution) to cyber attacks.

98 A financial institution may also be liable for the losses of their customers. Significant liability may raise prudential concerns for the financial institution.

Contactless payments

99 There is increased use of contactless payments—for example, through 'card present' transactions where a customer places a chip-enabled card or app-enabled mobile phone against a merchant's terminal.

100 This is vulnerable to exploitation—for example, through data interception where the card or phone is in close proximity or communicating with a compromised or custom-built device intended to intercept and extract personal and financial information.

Other financial services (including credit)

101 A cyber attack on a smaller financial service provider, registered managed investment scheme or credit service provider may not have an immediate significant impact on financial consumers, investors or the integrity of the market. However, due to the interconnectedness of the financial system and technology, the vulnerabilities of smaller entities may also increase the vulnerabilities of others.

Case Study 7: Vendor risks in the United States

In a 2014 examination of a selection of registered investment advisers, the US Securities Exchange Commission (SEC) identified that few advisers

(24%) incorporated requirements relating to cybersecurity risk into their contracts with vendors and business partners. This may pose third-party vulnerabilities to advisers.

Corporations and listed entities

Board involvement

102 We consider board participation important to promoting a strong culture of cyber resilience.

103 The PricewaterhouseCoopers Global State of Information Security Survey 2015 found that, of the financial service companies surveyed, only:

(a) 50% of boards participated in the overall security strategy;

(b) 44% of boards were involved in the security budget;

(c) 37% of boards participated in security policies; and

(d) 33% of boards were involved in the review of security and privacy risks.

Market-sensitive information

104 A cyber attack on a listed entity may amount to market-sensitive information. The release of news of a cyber attack can have significant implications for the market value of a particular company, and for the operation and integrity of the market.

105 Research by Freshfield Brukhaus and Deringer[35] found that global listed companies hit by a cyber attack between January 2011 and April 2013 saw a combined loss in market value of $53 billion on the first day's trading following the revelation of an incident. Those affected took an average of 24 days to recover pre-crisis valuations. 'Hactivism' is considered to have the longest effect on share prices.

Loss of intellectual property

106 A company may also experience corporate espionage through a cyber attack that results in the loss of future opportunity and financial gain.

Financial consumers and investors

107 Financial consumers and investors face a range of cyber risks.

[35] Freshfields Bruckhaus Deringer, 'Cyber attacks wipe $53bn off listed company values but investors remain largely unfazed by cyber risk', article, 31 October 2013.

108 Technological change has played a role in increasing fraud and misconduct against financial consumers and investors: criminals adapt traditional misconduct (such as investment fraud and theft) to the online environment.[36]

109 Financial consumers and investors are typically targeted directly by cyber criminals to obtain personal information for economic benefits. They may also be affected indirectly by cyber attacks on organisations that they deal with or who hold their personal information. The impacts of a cyber attack may include:

(a) privacy breaches through identity theft or compromise of personal information, including financial details. This information can be fraudulently used to open bank accounts and obtain credit cards, start an illegal business, or apply for a false passport;

(b) financial loss—for example, though online fraud; or

(c) being denied essential services, such as access to funds, as a result of a cyber attack on a financial service provider.

110 ASIC has provided information to financial consumers and investors on our MoneySmart website, to assist them to better understand and limit their exposure to cyber risks: www.moneysmart.gov.au/scams/avoiding-scams/protecting-yourself-from-online-scams.

[36] See also our discussion of data breaches at paragraphs 48–53, user developments at paragraphs 54–57, IOT devices at paragraphs 58–59, cloud technology at paragraphs 60–61, unauthorised trading at paragraphs 81–84, and banking and payment systems at paragraphs 89–93.

C Improving your cyber resilience

Key points

Businesses, particularly regulated entities, should look to assess and, if necessary, improve their cyber resilience.

We encourage businesses—particularly where their exposure to a cyber attack may have a significant impact on financial consumers, investors or on market integrity—to consider using the NIST Cybersecurity Framework to assess and mitigate their cyber risks or to stocktake their cyber risk management practices.

We expect our regulated population to engage with Government initiatives to improve information sharing to address cyber risks, including notifying relevant authorities of a cyber attack. We encourage collaboration with industry and the Government to ensure responses to cyber attacks can be coordinated and information on risks shared.

111 We recognise that our regulated population is at the frontline of cyber risk management. Many have proactive and sophisticated risk management practices to address cyber risks.

112 It is not possible to protect against all cyber risks. As cyber attacks continue to increase in complexity and sophistication, invariably you may be subject to an attack. However, you can seek to improve your overall cyber resilience so you can survive and recover from an attack as quickly as possible.

113 We encourage every business to take responsibility for improving their cyber resilience. Businesses are connected in various ways—in the online world, through the financial system or through business dealings. Cyber resilience improvements in one organisation have flow-on effects—it is a small step in improving the whole system.

114 Effective cyber resilience requires initiative and a commitment of resources to assess and develop appropriate strategies, including planning responses to a cyber attack. You should seize the opportunity to assess your threats and vulnerabilities now, and understand where and how your most valuable information is held. Through that assessment, you can prioritise resources to mitigate the risk of being affected disproportionately by a cyber attack.

NIST Cybersecurity Framework

115 There are a range of standards and methodologies that can be used to assist you improve your cyber risk management. However, we consider that the

NIST Cybersecurity Framework has particular relevance for our regulated population—specifically financial service providers that operate in a global environment, given the reach and dominance of US markets and the businesses operating within them.[37]

116 The NIST Cybersecurity Framework is being adopted by critical infrastructure providers in the United States, including those operating in financial services and markets. It is expected to become an effective global benchmark for financial markets.

117 For example, the US Securities Industry and Financial Markets Association (SIFMA) is strongly encouraging its members to use the NIST Cybersecurity Framework.[38] This is supported by the Global Financial Markets Association (GFMA) of which SIFMA is a regional member.[39] The use of the NIST Cybersecurity Framework is also supported by the American Bankers Association[40] and the American Insurance Association.[41]

118 The NIST Cybersecurity Framework enables you to apply or complement existing methodologies and standards. It does not introduce new standards or concepts but integrates existing industry-leading standards on global security and IT governance—that is, those that have widespread adoption and demonstrable successes. It is flexible enough to map onto other standards.

Case Study 8: US Department of Energy

The US Energy Regulator has issued guidance on implementing the NIST Cybersecurity Framework[42] by mapping to its existing Cybersecurity Capability Maturity Model (C2M2)—enabling its regulated organisations to continue using current methods while using the NIST Cybersecurity Framework to communicate its cyber risk posture.

119 The NIST Cybersecurity Framework provides a common language and benchmarks for cyber resilience across your organisation (from boardroom to IT analyst), and when dealing with stakeholders and third parties, or when operating across borders.

120 It also allows you to set your approach to cyber resilience based on your risk appetite. As it is risk-based and scalable, it is flexible enough to apply all businesses and not just those that support critical infrastructures.

[37] See Appendix 3 for more information on the NIST Cybersecurity Framework.
[38] SIFMA, *SIFMA statement on the NIST Cybersecurity Framework*, statement, 12 February 2014.
[39] GFMA, *GFMA submits comments to IOSCO and CPMI on global cybersecurity harmonization*, correspondence, 24 February 2015.
[40] American Bankers Association, *ABA statement on NIST's Cybersecurity Framework*, statement, 12 February 2014.
[41] American Insurance Association, *AIA statement on Cybersecurity Framework*, news release, 12 February 2014.
[42] Office of Electricity Delivery and Energy Reliability, *Energy sector Cybersecurity Framework implementation guidance*, guidance, US Department of Energy, 5 January 2015.

Action

C1 We encourage businesses—particularly where their exposure to a cyber attack may have a significant impact on financial consumers, investors or market integrity—to consider using the NIST Cybersecurity Framework to assess and mitigate their cyber risks or to stocktake their cyber risk management practices. The NIST Cybersecurity Framework can help you develop your cyber resilience in a proportionate way.

121 Figure 1 outlines the 'core' functions defined within the NIST Cybersecurity Framework, namely 'identify', 'protect', 'detect', 'respond' and 'recover'.

122 The core functions can provide a strategic view of your cybersecurity risk management lifecycle—for example, how to:

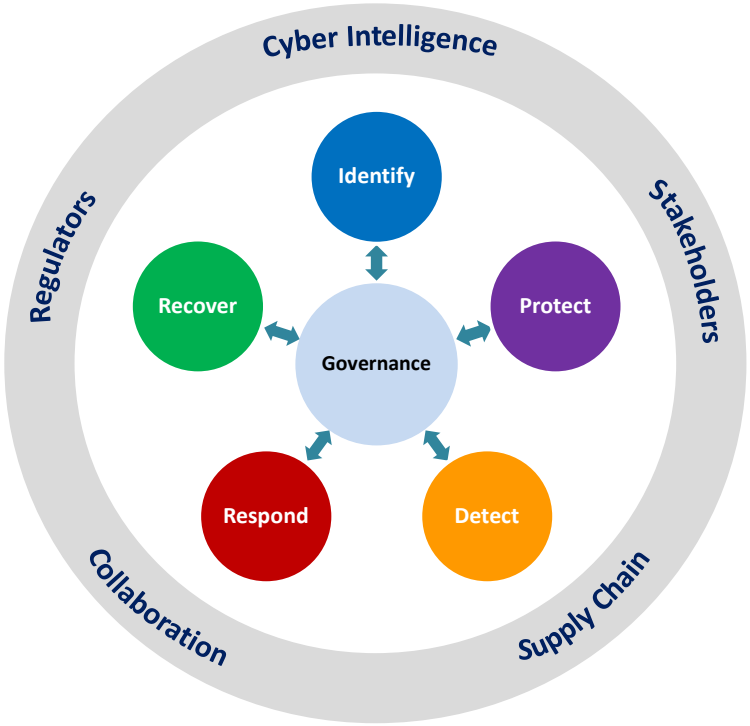
(a) *identify* your most critical intellectual property and assets;

(b) develop and implement procedures to *protect* them;

(c) put in place technology, procedures and resources to *detect* a cybersecurity breach; and

(d) put in place procedures to both *respond* to and *recover* from a breach, if and when one occurs.

Figure 1: Core functions and factors involved in a cyber-resilience framework



123 It also highlights the importance of key external interactions that assist a cyber resilience strategy. They include:

(a) collaboration with others in industry and the Government to improve intelligence on and capacity to mitigate cyber risks; and

(b) effective management of stakeholders (including customers) and businesses that are important to securing the resilience of your distribution and supply chain.

124 Governance is required to bring the core functions together across the entire organisation—from board level to operational level.

125 We encourage you to use the NIST Cybersecurity Framework as a risk-based methodology that can be applied proportionately to your business.

Cyber resilience initiatives in Australia

126 Australia is in the process of reviewing and updating our cyber resilience initiatives—focusing on improved collaboration between industry and public–private information sharing.

National plan to combat cybercrime

127 In 2013, the Australian Government released the *National plan to combat cybercrime* (National Plan). The National Plan represents commitments from the Commonwealth, state and territory governments of Australia to work together to address the threat of cybercrime.

128 As part of the National Plan, the governments have identified six priority areas for action shaped around the critical contributions governments can make in strengthening our national response to cybercrime:

(a) educating the community to protect itself;

(b) partnering with industry to tackle the shared problem of cybercrime;

(c) fostering an intelligence-led approach and information sharing;

(d) improving the capacity and capability of government agencies particularly law enforcement, to address crime;

(e) improving international engagement on cybercrime and contributing to global efforts to combat cybercrime; and

(f) ensuring an effective criminal justice framework.

ACORN

129 In November 2014, the Government launched ACORN, a national online system that allows the public to securely report instances of cybercrime.

130 ACORN is a key initiative under the National Plan. ACORN has been designed to make it easier to report cybercrime and help develop a better understanding of the cybercrime affecting Australians.

Action

C2 We encourage small-to-medium-sized businesses to report instances of cybercrime to ACORN.

ACSC

131 ACSC opened in November 2014. It brings the Australian Government's cybersecurity law enforcement, defence, and security capabilities into a single location to ensure improved collaboration between these agencies. The ACSC:

(a) leads the Australian Government's operational response to cybersecurity incidents;

(b) coordinates national cybersecurity operations and capability;

(c) analyses and investigates cyber threats;

(d) encourages reporting of cybersecurity incidents;

(e) reports on the nature and extent of cyber threats; and

(f) raises awareness of cybersecurity.

132 To achieve this, the ACSC co-locates:

(a) the ASD's cybersecurity mission;

(b) the national computer emergency response team, CERT Australia;

(c) representatives of the Australian Federal Police, who investigate and respond to cybercrime of national significance;

(d) the Australian Crime Commission, which discovers, understands and prioritises cyber threat intelligence to enhance response options;

(e) cyber investigations and telecommunication security specialists from the Australian Security Intelligence Organisation; and

(f) cyber analysts from Defence Intelligence Organisation and Defence Science and Technology Organisation.

Action

C3 We encourage large businesses to report cybersecurity incidents to CERT Australia within the ACSC.

CERT Australia

133 CERT Australia is the national computer emergency response team. It is the point of contact in Government for cyber security issues affecting major Australian businesses.

134 These businesses and industries underpin essential service delivery across Australia, including banking and finance, communications, energy, resources, transport and water.

135 CERT Australia provides advice and support on cyber risks to the owners and operators of Australia's critical infrastructure and systems of national interest, including through a hotline, email support, technical guidance on mitigating cyber threats, incident response support and coordination.

Action

C4 Major Australian businesses, particularly major financial institutions and market infrastructure providers, are encouraged to:

(a) partner with CERT Australia before an incident occurs; and

(b) report all cybersecurity incidents to CERT Australia.

All information provided to CERT Australia is held in the strictest confidence.

Cyber Security Strategy

136 In 2009, Australia adopted a Cyber Security Strategy that outlines a whole-of-government cybersecurity policy.

137 The Cyber Security Strategy's explicit aim is to maintain a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy.

138 Given the rapidly changing nature of the cyber threat environment, in November 2014, the Government announced a review Australia's cybersecurity policies and strategy being led by the Department of the Prime Minister and Cabinet, with advice from a panel of industry experts.

139 The updated Cyber Security Strategy is intended to ensure appropriate, practical mechanisms are in place for effective and timely public–private sector information sharing, particularly real-time threat intelligence.

Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN)

140 TISN provides an environment where business and government can share vital information on security issues relevant to the resilience of Australia's critical infrastructure and the continuity of essential services in the face of all hazards.

The TISN agenda is industry led. Included among the seven TISN sector groups is a Banking and Finance Sector Group. This group comprises representatives from Australia's major banks, financial and insurance institutions, as well as financial regulatory agencies such as ASIC. It shares

information a generic threats and vulnerabilities in the banking and finance sector—including cyber risks.

CREST Australia

141 CREST Australia is a non-profit company that provides accreditation and training to approved companies and certified staff as information security testing providers. It promotes the provision of high-quality, best practice information security services.

142 CREST Australia was established through initial funding by the Australian Government, which remains involved in its work.

Action

C5 You may want to use a CREST Australia approved member organisation to help you test your existing IT systems, processes and procedures to ensure that they respond well to cyber risks.

ASD mitigation strategies

143 The ASD has developed a list of *Strategies to mitigate targeted cyber intrusions* informed by its experience in operational cybersecurity, including responding to serious cyber intrusions and performing vulnerability assessments and testing for Australian government agencies.[43]

144 The mitigation strategies are ranked in order of overall effectiveness. Rankings are based on ASD's analysis of reported security incidents and vulnerabilities detected by ASD in testing the security of Australian government networks.

145 The ASD consider that at least 85% of the targeted cyber intrusions they responds to could be prevented by following their four highest-ranked mitigation strategies.

Action

C6 We encourage our regulated population to mitigate their cyber risks by, at minimum, implementing the ASD's four highest-ranked mitigation strategies.

[43] ASD, *Strategies to mitigate targeted cyber intrusions*, strategy, February 2014.

D What are your regulatory requirements?

Key points

Given the increased threat of cyber attacks, we expect our regulated population, particular licensees, to address cyber risks as part of its legal and compliance obligations—including risk management and disclosure requirements.

Your approach to cyber resilience should be proportionate to the risks you face, and the nature, scale and complexity of your business.

Cyber resilience is an area of ongoing focus for ASIC. It will be considered in our surveillance programs, where appropriate, across our regulated population in the future.

Regulatory requirements

146 If you are a regulated entity, some of the legal and compliance requirements you must take into account when considering your cyber resilience are highlighted in Appendix 2.

147 This is not an exhaustive list, but sets out when obligations to identify and manage cyber risks may arise within the licensing and other regulatory regimes we administer.

148 Depending on the severity, a failure to meet some of these obligations could result in fines, penalties, enforceable undertakings, licensing conditions, or a licence suspension or cancellation. If you are a director or an officer of a company, it may result in being disqualified from your role.

Action

D1 We expect our regulated population, particularly licensees, to address cyber risks as part of their legal and compliance obligations—including risk management and disclosure requirements.

Proportionate approach

149 You are expected to take a proportionate approach to cyber resilience according to:

(a) your legal and compliance requirements;

(b) the risks you face—with a particular emphasis on the risks posed by a cyber attack on critical infrastructure providers and those that could be exposed to an attack that may have a significant impact on financial consumers and investors or market integrity; and

(c) the nature, scale and complexity of your business.

Financial market infrastructure

150 We expect licensees who operate financial market infrastructure to have a level of risk management systems that is proportionate to their heightened cyber risks.

Market licensee

151 If you are a market licensee you must have adequate arrangements for operating the market and sufficient resources to operate the market properly.

152 Among other things, you are expected to have adequate physical and electronic security arrangements to prevent the misuse or unauthorised access to systems, and ensure the integrity of the data and information in the systems.

CS facility licensee

153 If you are a CS facility licensee, you must, among other things, meet the financial stability standards set by the Reserve Bank of Australia (RBA) and, to the extent that it is reasonably practicable to do so, do all things necessary to ensure that the facility's services are provided in a fair and effective way.

154 Among other things, you should have a sound risk management framework for comprehensively managing legal, credit, liquidity, operational and other risks. This may include cyber risks.

155 We work closely with the RBA to assess your compliance with your obligations under the *Corporations Act 2001* (Corporations Act); the RBA focuses on the obligations relating to financial stability standards and systemic risk reduction, and we focus on ensuring that the facility's services are provided in a fair and effective manner.

ADTR licensee

156 If you are an ADTR licensee, among other things, you have specific obligations that require your policy and procedures to at least address and minimise all foreseeable risks arising from:

(a) unauthorised cyber intrusions;

(b) viruses, malware and data corruption;

(c) the deliberate or negligent misuse of data or access privileges by staff, contractors, users and regulators, including those associated with staff or contractor departures; and

(d) internet denial of service.

Financial services

AFS licensee

157 If you are an AFS licensee you are required to have in place adequate risk management systems and resources.

Note: Alternative arrangements apply to APRA regulated entities (see paragraphs 175–176).

158 As part of your requirements, you are expected to explicitly identify the risks you face and have measures in place to mitigate or avoid those risks. We consider that cyber risks are a key risk you may face.

159 We expect your risk management systems will:

(a) be based on a structured and systematic process that takes into account your obligations under the Corporations Act;

(b) identify and evaluate risks faced by your business, focusing on risks that adversely affect consumers or market integrity (this includes risks of non-compliance with the financial services laws);

(c) establish and maintain controls designed to manage or mitigate those risks; and

(d) fully implement and monitor those controls to ensure they are effective.

160 You are also expected to regularly review the adequacy of your technological resources. This may include IT system security, disaster recovery systems and business resumption capacity.

Action

D2 We encourage AFS licensees to review the adequacy of their risk management systems and resources to address cyber risks.

Disclosure

161 You are required to disclose in a PDS (excluding shorter PDSs) to an investor or financial consumer, any significant risks associated with holding the product, information about any other significant characteristics or features of the product, or any other information that might reasonably be expected to have a material influence on the decision on a reasonable person, as a retail client, about whether to acquire the product.

162 You should consider if and how cyber risks should be disclosed as a significant risk associated with holding the product.

Action

D3 We encourage AFS licensees to consider if cyber risks should be disclosed in a PDS.

Breach reporting

163 A cyber attack may highlight if you have adequate risk management systems in place.

164 Inadequacies in your risk management systems may amount to a significant breach of your obligations that you must report to us.

Market participant

165 If you are a market participant, you are also expected to have specific protections for electronic trading—including security arrangements for your automated order processing (AOP) system to monitor and prevent unauthorised access, and to ensure that the system does not interfere with the efficiency and integrity of the market or the proper functioning of the trading platform.

166 You may be required to immediately comply with any direction from ASIC to cease, suspend, limit or prohibit automated order processing.

Suspicious activity reporting obligations

167 You are required to notify ASIC of suspicious trading activity if you have reasonable grounds to suspect a person has placed an order or entered a transaction based on insider information, or to manipulate the price of the relevant securities (market manipulation).

Crossing system (dark pool) operators

168 If you are a crossing system operator, you must consider a range of factors relevant to your cybersecurity that may require higher levels of monitoring.

169 For example, you are expected to monitor your system so that users are not using order types or ‘gaming’ the matching algorithm for manipulative or abusive conduct, such as through cyber attacks.

Managed investment scheme

170 If you are the responsible entity of a registered scheme, you must also apply a compliance plan to ensure compliance with the law and the scheme’s constitution.

171 A compliance plan should reflect, among other things, the major compliance risks that investors face. This may include cyber risks.

Credit licensee

172 If you are a credit licensee you are required to have in place adequate risk-management systems and resources.

Note: Alternative arrangements apply to APRA regulated entities (see paragraphs 175–176).

173 We expect credit licensees to identify and evaluate the risks they face, focusing on risks that adversely affect financial consumers or market integrity. We consider that cyber risks are a key risk that you may face.

174 You must ensure that the controls you design to manage or mitigate those risks are fully implemented and monitored to ensure they are effective.

Action

D4 We encourage credit licensees to review the adequacy of their risk-management systems and resources to address cyber risks.

Dual-regulated entities

175 If you are a body regulated by APRA,[44] risk management and resource requirements are set and enforced by APRA, not ASIC.

Note: From 1 July 2015, this excludes superannuation dual-regulated entities that are both a responsible entity of a registered managed investment scheme and a registrable superannuation entity licensee. They will be regulated by both APRA and ASIC for their risk management and resource requirements.

176 However, we will consider how you address cyber risks in compliance with your other general AFS licensing obligations—including the requirements to comply with financial services laws and to act efficiently, honestly and fairly.

ePayments Code

177 The ePayments Code regulates consumer electronic payments, including automatic teller machines (ATMs), electronic funds transfer at point-of-sale (EFTPOS) and credit card transactions, online payments, internet and mobile banking, and BPAY.

178 If you are a subscriber to the ePayments Code, you must generally compensate a consumer for loss if an unauthorised transaction is made on a consumer account, unless the consumer contributed to the loss.

179 You must also report to ASIC information about unauthorised transactions annually, including complaints about unauthorised transactions.

[44] *Australian Prudential Regulation Authority Act 1998*, s3(2).

Corporations and listed entities

Corporate disclosure requirements

180 If you are corporation[45] or listed entity, cyber risks may also affect your disclosure requirements to investors.

Prospectuses

181 If you are required to provide a prospectus, you should consider if your cyber risks form part of information that investors and their professional advisers would reasonably require to make an informed assessment of any offer, and should be disclosed in a prospectus.

Periodic disclosure

182 You may need to disclose your cyber risks in your annual directors' report if it is a significant factor that may affect future financial or operational performance.

183 If you are a listed entity, you must disclose in your annual directors' report the material business risks that could adversely affect the achievement of the financial performance or financial outcome described. Cyber risks and resilience may need to be taken into account in an assessment of these material business risks.

Continuous disclosure

184 If you are a listed entity, you must immediately disclose market-sensitive information to the market operator once you become aware of the information.

185 You need to consider how and when a cyber attack may need to be disclosed as market-sensitive information.

Corporate governance

186 Effective corporate governance should involve active engagement by directors and the board in managing any applicable cyber risks.

187 If you are a director of a company, you may need to take cyber risks into account when undertaking your duties.

[45] Our focus is on public companies but, where relevant, can apply to all corporations.

Corporate Governance Principles

188 The ASX Corporate Governance Council's *Corporate governance principles and recommendations* (Corporate Governance Principles)[46] sets out the corporate governance expectations of listed entities.

189 If you are a board of a listed entity, among other things, the Corporate Governance Principles recommend that you should establish a sound risk management framework and periodically review the effectiveness of that framework.[47]

190 The Corporate Governance Principles recommend that you should have a committee or committees to oversee risk to review and make recommendations to you about the:

(a) adequacy of the entity's processes for managing risk;

(b) any incident involving fraud or other break down of the entity's internal controls; and

(c) the entity's insurance program, given the entity's business and the insurable risks associated with its business.

191 You are also expected to review the entity's risk management framework at least annually to satisfy yourself that it is sound.

192 You must also disclose information about the extent to which you meet the Corporate Governance Principles in your annual report or on your website.

Privacy obligations

193 If you are regulated by the *Privacy Act 2009* (Privacy Act), you must take reasonable steps to protect personal information you hold from misuse, interference and loss, and from unauthorised access, use, modification or disclosure.

194 Appropriate steps should be taken to ensure third parties meet your Privacy Act obligations.

195 Credit providers who engage in credit reporting have additional Privacy Act obligations that apply to information provided and used in a credit report.

196 We expect AFS licensees and credit licensees to take their Privacy Act obligations into account when complying with financial services laws and credit legislation.

---

[46] ASX Corporate Governance Council, *Corporate governance principles and recommendations*, 3rd edition, ASX, 2014\.
[47] Corporate Governance Principles, Principle 7: Recognise and manage risk.

ASIC surveillance

197 Our role is to ensure that our regulated population is aware of their cyber risks and to encourage risk-based and proportionate cyber-resilience management practices within current legal and compliance obligations.

198 We adopt a risk-based approach to surveillance of our regulated population. We work to detect, understand and respond to risks that threaten fair, orderly and transparent markets, and investor and financial consumer trust and confidence.

199 We consider that cyber resilience is a high-risk area for our regulated population and will be considered in our surveillance programs, where appropriate, across our regulated population in the future.

Appendix 1: Cyber risks—Sources, threats and vulnerabilities

Table 2: Sources of cyber risks

Example	Explanation
Employees and other insiders	They are considered the most likely source of an attack and may be motivated for ideological or personal reasons, or for financial gain.
Lone individuals	They generally commit fraud or small scale breaches. However, they may have the potential to create significant disruption as an individual hacker.
Corporate espionage	This includes espionage by competitors, suppliers and trusted third-party service providers.
Hactivists	They are motivated by political, ideological reasons and use technology to facilitate criminal conduct in a coordinated and systematic way.
Organised crime	They are generally motivated by financial benefits and use technology to facilitate criminal conduct in a coordinated and systematic way.
State sponsored activity	Attacks from this source are often highly resourced. They may focus on espionage, whether for commercial, political or ideological motives.

Table 3: Examples of threats

Example	Explanation
Data breaches	Theft or compromise of personal information, particularly of staff or customers, to use or sell in the black market
Denial of service	Attempts to make a computer device, system or network resource (such as bank or payment system) unavailable to its intended users through, among other things, overloading it with computer traffic, 'malware' or a virus
Hacking	Technically manipulating the behaviour of computer devices, network connections or connected systems for their own end (e.g. cracking passwords to access a computer).
Identity and data theft	Information can be harvested through a range of methods, including phishing (getting access to personal details or money by pretending to be a trusted source), card skimming (information is copied from the magnetic strip of a debit or credit card), or through social media.
Industrial espionage	Theft of secrets and intellectual property of a business.
Malware	The use of malicious software to infect a person or organisation's computer, computer system or network—for example, through the use of 'trojans', viral attacks spread via email, spyware, spam and adware—enabling the perpetrator to monitor online activity or cause damage to the computer, system or network.

Example	Explanation
Money laundering	Transferring money (e.g. the proceeds of crime) through online payment systems or e-cash facilities to make it legitimate. Financial consumers or entities may be unaware that their accounts or networks are being used
Network interruption	This involves the disruption or damage to information networks, including through physical attacks of IT infrastructure.
Online fraud	Attempts to access personal details or financial information through phishing and email scams (e.g. money transfer requests).
Pharming or 'drive-by' attacks	Web attacks where a user visits a malicious webpage and is infected without conventionally downloading a file, or re-directing users from legitimate websites to fraudulent ones.
'Ransomware'	Attackers threaten the encryption of files or removal of data and files unless money is paid.
Unauthorised access	The unauthorised access of a computer device, computer system or network to obtain information (e.g. through cracking passwords)
User tracking	Spying on a person or entity (e.g. tracking calls, emails, pictures and messages, particularly through mobile technologies).

Table 4: Examples of vulnerabilities

Example	Explanation
Corporate vulnerabilities	
Effectiveness not monitored	Existing systems and procedures are not tested, reviewed and adapted, or are too inflexible, making them more susceptible to cyber attacks.
Lack of board involvement	Senior management is not sufficiently involved in cyber resilience—key changes or legal and compliance requirements may be overlooked.
Limited resources	Insufficient resources, with costs and impact of a cyber attack underestimated, creating gaps and weaknesses in security.[48]
People vulnerabilities	
Employee or other 'insider' actions	Lack of employee awareness, poor compliance with or inadequate security protocols for employers and other insiders.
Lack of cyber-security skills	The need to build skills in non-technical disciplines so cyber resilience is integrated in the core business, or lack of available trained staff.
'Social Engineering'	The psychological manipulation of people into performing actions or divulging confidential information on or about an information system.

[48] Global information security budgets in 2014 decreased 4% compared to 2013: PricewaterhouseCoopers, *Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015*, report, 30 September 2014, p. 19.

Example	Explanation
Third-party providers	Poor cyber resilience of third-party providers such as business partners, service providers, contractors and suppliers, or weaknesses that can arise from sharing networks and data—including offshoring and outsourcing.
System vulnerabilities	
Application or technological weaknesses	Failure or delays to update software or information controls (e.g. continued use of the Microsoft XP operating system, which no longer offers IT security support and updates).
Operational systems	Lack of resilience of physical infrastructure that supports the information system, such as power generators and servers.
Use of virtual platforms (i.e. cloud) and portable devices	Increases the risk of access to confidential information if appropriate protections are not in place.
Weak access protections	Poor access protections may make it easy for employees or hackers to get inappropriate access to confidential information.
'Zero-day' vulnerability	Exploitation of a previously unknown vulnerability in a computer application or operating system, with no time to address and patch the problem.

Appendix 2: Relevant legal and compliance requirements

Regulated entity	Relevant requirements	General summary
Corporation	Corporations Act: • s180 (directors duties); and • s140 (effect of constitution and replaceable rules).	A director or officer of a corporation must: • act with reasonable care and diligence; and • act consistently with the powers and functions set out in the company's constitution or rules.
Corporation and/or registered managed investment scheme	Corporations Act: • s292 (directors' reports); and • s299 (annual director's report, general information).	Information in an annual directors' report must give details of any matter or circumstance that has arisen since the end of the year that has significantly affected or may significantly affect: • the entity's operation in future financial years; • the results of those operations in future financial years; or • the entity's state of affairs in future financial years.
Corporation making an offer of securities	Corporations Act: • s710 (content of a prospectus); and • s715 (content of offer information statement).	Information in a: • a *prospectus* must contain all the information investors and their professional advisers would reasonably require to make an informed assessment of, among other things, matters relating to the financial position and performance, profits and losses and prospects of the body; and • an *offer information statement* must state the nature of the risks involved in investing in the securities.
Listed entity	Corporations Act: • s674, 677 (continuous disclosure obligations).[49] ASX Listing Rules: • Rules 3.1, 3.1A.	A listed disclosing entity must immediately disclose market-sensitive information (information a reasonable person would expect to have a material effect on the price or value of the securities) to the market operator once they become aware of the information.

[49] Unlisted disclosing entities also have continuous disclosure obligations: Corporations Act, s675.

Regulated entity	Relevant requirements	General summary
Listed entity (cont.)	Corporations Act: • s292 (directors' reports); • s299 (annual directors' report, general information); and • s299A (listed entities operating and financial review).	The operating and financial review in the directors' report of a listed entity must contain information that shareholders would reasonably require to make an informed assessment of the entity's: • operations; • financial position; and • business strategies and prospects for future financial years.
	Regulatory Guide 247 *Effective disclosure in an operating and financial review* (RG 247)	This should include disclosure of the material business risks that could adversely affect the achievement of the financial performance or financial outcome described.
	Corporate Governance Principles: • Principle 5 (Make timely and balanced disclosure); and • Principle 7 (Recognise and manage risk). ASX Listing Rules: • Rules 4.7 and 4.10.3.	A listed entity should: • make timely and balanced disclosure of all matters concerning it that a reasonable person would expect to have a material effect on the price or value of its securities; and • establish a sound risk management framework and periodically review the effectiveness of that framework. A statement must be included in the annual report or on its website disclosing the extent in which the Corporate Governance Principles have been met. If the statement is not included in the annual report, it must be provided to the ASX as a separate document at the same time as its annual report.

Regulated entity	Relevant requirements	General summary
Market licensee	Corporations Act: • s792A (general obligations) Regulatory Guide 172 *Australian market licences: Australian operators* (RG 172), including the addendum published in November 2012.	A market licensee must: • do all things necessary to ensure that the market is a fair, orderly and transparent market; • have adequate arrangements for operating the market; and • have sufficient resources (including financial, technological and human resources) to operate the market properly. A market licensee is expected to have: • adequate business continuity, backup and disaster recovery plans for their systems; • arrangements to ensure that critical business functions will be available and minimise the impact of a disruption or outage of services on stakeholders; • capacity management and stress testing; • adequate physical and electronic security arrangements to prevent misuse or unauthorised access to systems, and ensure the integrity of the data and information in the systems; • procedures in place to restrict access to servers and systems to internal or external personnel with appropriate security clearance; and • procedures for undertaking periodic monitoring and review.

Regulated entity	Relevant requirements	General summary
ADTR licensee	ASIC Derivative Trade Repository Rules 2013: • Rules 2.4.4, 2.4.6, 2.4.8 Regulatory Guide 249 *Derivative trade repositories* (RG 249)	An ADTR licensee must have comprehensive governance and management strategy and arrangements that, among other things: • identify, measure, monitor and effectively manage risks to the secure or efficient or effective operation of the derivative trade repository, including legal, operational and business risks; • maintain the integrity, security and confidentiality of derivative trade data at all times and prevent unauthorised use or disclosure of, or access to the data; and • establish and maintain sufficient and appropriate human, technological and financial resources to ensure that the derivative trade repository operates at all times securely, efficiently and effectively. Policies and procedures should at least address and minimise all foreseeable risks arising from: • unauthorised cyber intrusions; • viruses, malware and data corruption; • the deliberate or negligent misuse of data or access privileges by staff, contractors, users and regulators, including those associated with staff or contractor departures; and • denial of service attacks.
CS facility licensee	Corporations Act: • s821A. Regulatory Guide 211 *Clearing and settlement facilities: Australian and overseas operators* (RG 211)	A CS facility licensee must: • meet their financial stability standards; • do all things necessary to reduce systemic risk; • to the extent reasonably practicable, do all things necessary to ensure that the facilities services are provided in a fair and effective way; and • have sufficient financial, technological, and human resources.

Regulated entity	Relevant requirements	General summary
CS facility licensee (cont.)	Corporations Act: • s827D: financial stability standards determined by the RBA. RBA *Financial Stability Standards for Central Counterparties*: • CCP 2 (governance); • CCP 3 (risk management); • CCP 8 (settlement finality); • CCP 16 (operational risk); and • CCP 20 (disclosure). RBA *Financial Stability Standards for Securities Settlement Facilities*: • SSF 2 (governance); • SSF 3 (risk management); • SSF 7 (settlement finality); • SSF 9 (depository functions); • SSF 12 (general business risk); • SSF 14 (operational risk); and • SSF 18 (disclosure).	A CS facility licensee must have a sound risk management framework for comprehensively managing legal, credit, liquidity, operational and other risks, including: • risk management policies, procedures and systems that enable it to identify, measure, monitor and manage the range of risks that arise in or are borne by the central counterparty; • regularly review the material risks it bears from and poses to other entities as a result of interdependencies, and develop appropriate risk management tools to address these risks; and • identify scenarios that may potentially prevent it from being able to provide its critical operations and services as a going concern, assess the effectiveness of a full range of options for recovery or orderly wind down, and prepare appropriate plans based on the results of that assessment. Among other things, a CS facility should also have: • a clear, documented risk management framework that includes their risk tolerance policy established by the board, that assigns responsibilities and accountability for risk decisions, and addresses decision making in crises and emergencies; and • robust operational risk management framework with appropriate systems, policies, procedures and controls to identify, monitor and manage operational risks, including comprehensive physical and information security policies.

Regulated entity	Relevant requirements	General summary
AFS licensee	Corporations Act: • s912A (general licensing obligations), specifically: – s912A(1)(d); – s912A(1)(f); and – s912A(1)(h); an • s912D (breach reporting). Regulatory Guide 104 *Licensing: Meeting the general obligations* (RG 104) Regulatory Guide 78 *Breach reporting by AFS licensees* (RG 78)	An AFS licensee must: • do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly; • comply with financial services laws; • have adequate resources, including financial, human, and technological resources (different obligations apply if you are an APRA-regulated entity); • have adequate risk management systems (different obligations apply if you are an APRA-regulated entity); and • ensure representatives are adequately trained and competent. As part of the obligation to have adequate risk-management systems, an AFS licensee is expected to identify and evaluate the risks they face (e.g. cyber risks), focusing on risks that adversely affect financial consumers or market integrity. An AFS licensee is expected to regularly review the adequacy of their technological resources, including IT system security, disaster recovery systems and business resumption capacity. An AFS licensee also remains responsible for complying with their obligations where functions are outsourced. An AFS licensee is required to report to ASIC a significant breach or a likely significant breach of specified obligations—including the obligation to have adequate risk management systems.
AFS licensee that is issuing a financial product	Corporations Act: • s1013A (obligation to prepare a PDS); and • s1013D, 1013E. Regulatory Guide 168 *Disclosure: Product Disclosure Statements (including other disclosure documents)* (RG 168)	A PDS must contain information about: • any significant risks associated with holding the product; • information about any other significant characteristics or features of that product; and • any other information that might reasonably be expected to have a material influence on the decision of a reasonable person, as a retail client, whether to acquire the product. Note: Different requirements apply for shorter PDSs or a short-form PDS.

Regulated entity	Relevant requirements	General summary
AFS licensee that is a market participant	Regulatory Guide 241 *Electronic trading* (RG 241): • Section B (trading management arrangements regarding capacity, business continuity and logging of information, monitoring and review); and • Section C (access by authorised persons). Regulatory Guide 223 *Guidance on ASIC market integrity rules for competition in exchange markets* (223) • Section J (crossing systems). Regulatory Guide 238 *Suspicious activity reporting* (RG 238)	A market participant is expected to have: • adequate business continuity, backup and disaster recovery plans for their systems; • capacity management and stress testing; • security arrangements for its AOP system to monitor and prevent unauthorised access, and to ensure that the system does not interfere with the efficiency and integrity of the market or the proper functioning of the trading platform; • if it accepts orders, adequate physical and electronic security arrangements and seek to adopt and enforce written procedures to ensure reliability and uphold the confidentiality of orders and client account information; • monitoring and control arrangements, arrangements for managing the particular financial and trading risks that are relevant to the business it conducts through automated order processing, and resources for managing change; and • records of the security arrangements for access by an authorised person to the market participant's systems. A market participant should consider assessing its security arrangements against security standards such as AS/NZS 4444 *Information security management* and ISO/IEC 17799 *Information technology—Security techniques—Code of practice for information security management* A market participant must notify ASIC of suspicious trading activity. Crossing system operators must consider a range of factors that may require higher levels of monitoring, including monitoring their system so that users are not using order types or 'gaming' the matching algorithm for manipulative or abusive conduct.
AFS licensee that is the responsible entity of a registered managed investment scheme	Corporations Act: • s601HA (compliance plans). Regulatory Guide 132 *Managed investment schemes: Compliance plans* (RG 132)	A registered scheme must have a compliance plan that the responsible entity is to apply in operating the scheme to ensure compliance with the law and the scheme's constitution. A compliance plan should reflect, among other things: • the major compliance risks that investors face; and • the abuses potentially associated with conducting schemes.

Regulated entity	Relevant requirements	General summary
Credit licensee	*National Consumer Credit Protection Act 2009*: • s47 (general licensing obligations), specifically s47(1)(g)–47(1)(l) Regulatory Guide 205 *Credit licensing*: *General conduct obligations* (RG 205)	A credit licensee must: • do all things necessary to ensure that credit activities by the licence are engaged in efficiently, honestly and fairly; • comply with the credit legislation; • ensure representatives are adequately trained and competent; • have adequate resources, including financial, human and technological resources (different obligations apply if you are an APRA-regulated entity); and • have adequate risk management systems (different obligations apply if you are an APRA-regulated entity). As part of the obligation to have adequate risk-management systems, a licensee is expected to: • identify and evaluate the risks they face (for example, cyber risks) focusing on risks that adversely affect financial consumers or market integrity; • establish and maintain controls designed to manage or mitigate those risks; and • fully implement and monitor those controls to ensure they are effective. A credit licensee also remains responsible for complying with their obligations when functions are outsourced.
ePayments Code subscribers	ePayments Code: • Chapter C. Information Sheet 195 *ePayments Code—Reporting data on unauthorised transactions* (INFO 195)	Generally, ePayments Code subscribers must compensate a consumer for loss on a consumer account if an unauthorised transaction is made on the account, unless the consumer contributed to the loss. ePayments Code subscribers must report to ASIC information about unauthorised transactions annually, including complaints about unauthorised transactions.

Regulated entity	Relevant requirements	General summary
Entity regulated by the Privacy Act	Privacy Act: • Sch 1, Australian Privacy Principles; and • s18G(b) (for credit reporting agencies and credit providers in relation to credit information files and credit reports).	An entity that is regulated by the Privacy Act must take reasonable steps to protect personal information they hold from misuse, interference and loss; and from unauthorised access, use, modification or disclosure. Among other things, appropriate steps should be taken to ensure third parties meet an entity's Privacy Act obligations. See generally, OAIC's *Guide to Information security: 'Reasonable steps' to protect personal information* (April 2013) and *Data breach notification guide: A guide to handling personal information security breaches* (August 2014).
Australian Transaction Reports and Analysis Centre (AUSTRAC) reporting entity	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006*: • s41. *Financial Transaction Reports Act 1988*: • s16.	An AUSTRAC reporting entity must make suspicious matter reports AUSTRAC if they provide a designated service and have a suspicion on reasonable grounds: • that a person (or their agent) is not the person they claim to be; • that information may be relevant to investigate or prosecute a person for an evasion (or attempted evasion) of tax law, or an offence against a Commonwealth, state or territory law; or • of assisting in enforcing the *Proceeds of Crime Act 2002* (or regulations under that Act) or a state or territory law that corresponds to that Act or its regulations.

Appendix 3: NIST Cybersecurity Framework

200 In February 2014, NIST released the NIST Cybersecurity Framework.[50]

201 The NIST Cybersecurity Framework is a voluntary, technology-neutral cyber risk management tool for organisations. It uses a common language to address and manage cyber risk in a cost-effective way based on business requirements, risk tolerances, and resources.

202 It enables organisations—regardless of size, degree of cyber risk, or cybersecurity sophistication—to apply the principles and best practices of risk management. It also provides a consistent and iterative approach to assessing, evaluating, managing and communicating an organisation's relative level of cyber resilience.

203 It is in early adoption phase and is gaining momentum, given it is intended to align to existing standards such as ISO/IEC 27001 and ISO/IEC 27002, ISACA's COBIT 5, and the Payment Card Industry Data Security Standard. It is also flexible enough to map onto other standards.

204 As it references global standards for cybersecurity, it can serve as a model for international cooperation to strengthen the cybersecurity of organisations.

What is the NIST Cybersecurity Framework?

205 The NIST Cybersecurity Framework contains three primary components: Framework Core, Implementation Tiers, and Framework Profiles.

Framework Core

206 The Framework Core is a set of activities to achieve specific cybersecurity outcomes, established through five concurrent and continuous functions—'identify', 'protect', 'detect', 'respond' and 'recover': see Section C for more information.

207 The activities identify reference examples of guidance in standards, guidelines, and practices that illustrate methods to achieve the outcome.

Implementation Tiers

208 'Tiers' describe the increasing degree of sophistication and rigor an organisation employs or would like to employ in applying its cybersecurity practices, and provide a context for applying the Framework Core. They are

[50] NIST, *Framework for improving critical infrastructure cybersecurity*, v. 1.0, 12 February 2014.

not intended to represent maturity levels, but are to be applied where it would reduce cyber risks and be cost-effective.

209 It consists of four levels that describe an organisation's approach to cyber risk management that range from 'informal, reactive responses' to 'approaches that are agile and risk-informed.'

210 Each Implementation Tier can be described as follows:

(a) *Tier 1 (Partial)*: The organisation's cyber risk is managed on an ad hoc or reactive basis. There is a limited awareness of cyber risk across the organisation and an organisation-wide approach to managing cyber risk has not been established.

(b) *Tier 2 (Risk Informed)*: Risk management practices are approved by management and there is awareness of cyber risk at an organisation level—but an organisation-wide approach has not been established. Risk-informed, management-approved processes and procedures are implemented and adequately resourced. The organisation is aware of its role in the broader eco-system but has not formalised its capabilities to interact and share information externally.

(c) *Tier 3 (Repeatable)*: Risk management practices are formally approved and expressed as policy. They are regularly updated based on the application of risk management processes to respond to changes in business requirements and the cyber threat and technology landscape. There is an organisational-wide approach to managing cyber risk. The organisation receives relevant information from its business partners, which allows for collaboration and risk-based management decisions.

(d) *Tier 4 (Adaptive)*: Risk management and cybersecurity practices are adapted 'in real time' based upon lessons learned and predicative indicators derived from previous and current cybersecurity activities. The organisation can rapidly respond to sophisticated threats through a process of continuous improvement incorporating advanced cybersecurity technologies, real-time collaboration with partners, and continuous monitoring of activities on their systems.

Framework Profile

The Framework Profile is a tool that enables organisations to clearly articulate the goals of their cybersecurity program by identifying their current state and desired state of cybersecurity outcomes.

Appendix 4: International developments

211 The heightened risk of a cyber attack is recognised as a regulatory concern across a range of international organisations and regulatory bodies. There are high-level approaches being adopted globally, some legislative driven and some voluntary

212 There is recognition of the value of a coordinated global approach and common principles in addressing cyber risks. There is also increased focus internationally on collaboration between public and private sectors to combat cyber attacks and improve cyber resilience.

United States

213 The United States is at the forefront of work on cybersecurity. President Obama's Executive Orders set out two key foundational elements in building their cybersecurity strategy, by:

(a) developing a common framework for cybersecurity in 2014[51]—which resulted in the development of the NIST Cybersecurity Framework; and

(b) promoting private sector cybersecurity information sharing, including the development of information-sharing and analysis organisations to enable cyber information sharing standards to facilitate the secure sharing of information between the private sector and government. [52]

214 In President Obama's State of the Union address in January 2015, he declared cybersecurity a government priority, and sought support for legislation to help reduce the impact of future cyber attacks. The legislative proposals include a call for:

(a) nationally consistent mandatory breach reporting—so companies would be required to notify consumers within 30 days of discovering a data breach; and

(b) cybersecurity information sharing between the private sector and government—to better protect information systems and more effectively respond to cyber attacks.[53]

[51] Office of the Press Secretary, *Executive Order on improving critical infrastructure cybersecurity*, press release, The White House, 12 February 2013.
[52] Office of the Press Secretary, *Executive Order—Promoting private sector cybersecurity information sharing*, Executive Order, The White House, 13 February 2015.
[53] Office of the Press Secretary, *Securing cyberspace—President Obama announce new cybersecurity legislative proposal and other cybersecurity efforts*, press release, The White House, 13 January 2015.

SEC and FINRA

215 The SEC has been focused on improving the cybersecurity of its regulated population for some time.

216 In 2011, the SEC issued guidance on existing disclosure obligations related to cybersecurity risks and incidents to assist public companies frame disclosure of cybersecurity issues. That guidance makes clear it that material information regarding cybersecurity risks and cybersecurity incidents must be disclosed.[54]

217 In 2013, the Commodities Futures Trading Commission and the SEC adopted regulations that require certain regulated financial institutions and creditors to adopt and implement identity theft programs. The regulations build on existing SEC rules for protecting customer data.[55]

218 In 2014, the SEC conducted a cybersecurity examination of 57 registered broker–dealers and 49 registered investment advisers, to better understand how broker-dealers and advisers address the legal, regulatory and compliance issues associated with cybersecurity. The examination revealed significantly varying levels of 'cyber preparedness' within the organisations that were reviewed.[56]

219 These findings have filtered through into the 2015 agenda, where the SEC has declared it will continue its focus on cybersecurity as a market-wide risk.[57] The SEC is working on regulatory guidance on cybersecurity stemming from the 2014 cybersecurity examination.[58]

220 The SEC's concern is shared with the Financial Industry Regulatory Authority (FINRA), the regulatory organisation for broker–dealers.

221 FINRA conducted a targeted examination of a cross-section of registered broker–dealer firms to identify the primary cybersecurity concerns currently affecting the broker–dealer industry. The resulting FINRA report, released in February 2015, focused on presenting a summary of the main cybersecurity issues faced by broker–dealers, as well as principles and effective practices for mitigating the risks or adverse effects of each.[59]

[54] Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2 *Cybersecurity*, guidance, 13 October 2011, SEC.
[55] Commodities Futures Trading Commission and the SEC, *Identity theft red flag rules* (Release no. 34-69359), joint final rules and guidelines, 10 April 2013.
[56] Office of Compliance Inspections and Examinations, 'Cybersecurity examination sweep summary', *National Exam Program Risk Alert*, vol IV, issue 4, SEC, 3 February 2015.
[57] Office of Compliance Inspections and Examinations, *Examination priorities for 2015*, SEC, 13 January 2015.
[58] J Wallace, 'IA brief: Six steps to address US SEC cybersecurity focus', *Reuters*, 11 February 2015.
[59] FINRA, *Report on cybersecurity practices*, report, February 2015.

United Kingdom

222 The UK Government published its Cyber Security Strategy in 2011, which seeks to make the United Kingdom the safest place to do business by the end of 2015. Key features of the strategy include:

(a) investment in developing cybersecurity awareness, skills, knowledge and capabilities to effectively support industry and provide cyber risk management guidance businesses of all sizes; and

(b) partnership with industry to target assessing, measuring and countering the cyber threat.

223 As part of its investment into cybersecurity awareness, the United Kingdom has:

(a) developed cybersecurity advice to businesses such as the *10 steps to cyber security* booklet for larger businesses and tailored guidance for small businesses, as well as further guidance and training for those sectors or roles particularly at risk;

(b) developed a Cyber Essentials scheme to give organisations a clear baseline to aim for to protect themselves against the most common cyber threats and to advertise that they meet this standard; and

(c) reached agreement with industry on a series of guiding principles for internet service providers, setting out a best practice approach to help inform, educate and protect customers from cyber threats.

224 The United Kingdom has also established three significant programs to target improvements in businesses' ability to assess, measure and counter cyber threats:

(a) *Health check for listed companies*: This is a voluntary program to encourage FTSE 350 companies undertake a health check (either a self-assessment or through a government certified assessor), that assesses the level of preparedness of these companies against cyber attacks. The health check continually adapts its strategies based on the assessment results, and on ongoing information sourced from security agencies about the most common cybersecurity threats.

(b) *Cybersecurity Information Sharing Partnership*: This partnership was established to allow the government and industry to exchange information on cyber threats in a trusted environment, enabling security agencies to analyse threats and proactively develop responses to emerging threats; and

(c) *Operation Waking Shark II*: This operation is an annual program of coordinated simulated cyber attacks against financial market entities, undertaken to evaluate the cyber resilience of participants. This has been extended to include US companies following an agreement

between the United Kingdom and the United States to formalise their collaboration efforts in 2015.

Asia–Pacific

Singapore

225 Singapore is establishing a dedicated Cyber Security Agency (CSA) for national cybersecurity to be set up on 1 April 2015. The CSA will come under the Prime Minister's Office and will provide dedicated and centralised oversight of national cybersecurity functions.

226 The CSA will consolidate and build upon the government's cybersecurity capabilities. These include strategy and policy development, cybersecurity operations, industry development and outreach. CSA will also work closely with the private sector to develop Singapore's cybersecurity eco-system.

Indonesia

227 In Indonesia, the government is planning to establish a National Cyber Agency (NCA) to lead a campaign against cyber attacks, including those threatening financial institutions and basic infrastructure, such as cellular services and electricity.

228 The NCA is intended to provide oversight and integration of cyber intelligence at a national level. It will expect organisations—for example, all banks—to have an established cybersecurity program.

Global developments

229 Cyber risks in financial markets and services are increasingly considered a global problem that requires global action. A range of international regulatory bodies in financial markets and services are starting to pay close attention to the issue—and are encouraging cross-border collaboration and involvement.

230 For example, the Financial Stability Board have flagged they will be adjusting their focus to consider new and constantly evolving risks and vulnerabilities in the global financial system. They recognise that to manage the system dynamically and effectively it will require demonstrated

willingness to adjust in the face of new information and new challenges, for example, strengthening cyber resilience.[60]

IOSCO

231 IOSCO is working with the Committee for Payment and Market Infrastructure to consider the implications of cyber attacks against financial market infrastructures, including financial stability implications that go beyond an individual financial market infrastructure. They are considering the issue of any guidance as necessary and appropriate for both authorities and financial market infrastructures, to help them enhance cyber resilience.

232 IOSCO is also working on a range of projects to bring together a coordinated policy response. Through its policy committees, it is considering whether there is any guidance that may be needed in areas such as how cyber risks are managed and disclosure about the management of those risks, and on improving cooperation and information sharing in responding to cyber attacks.

[60] Chairman of the Financial Stability Board, *Financial reforms: Completing the job and looking ahead*, letter to the G20 leaders, Financial Stability Board, 7 November 2014.

Key terms

Term	Meaning in this document
ACORN	Australian Cybercrime Online Reporting Network
ACSC	Australian Cyber Security Centre
ADTR licence	Australian derivative trade repository licence
AFS licence	An Australian financial services licence under s913B of the Corporations Act that authorises a person who carries out a financial services business to provide financial services Note: This is a definition contained in s761A of the Corporations Act.
AOP system	Automated order processing system
APRA	Australian Prudential Regulation Authority
ASD	Australian Signals Directorate
Australian derivative trade repository licence	Australian derivative trade repository licence under s905C of the Corporations Act that authorises a person to operate a trade repository
Australian market licence	Australian market licence under s795B of the Corporations Act that authorises a person to operate a financial market
automated order processing	The process by which orders are registered in a market participant's system, which connects it to a market. Client or principal orders are submitted to an order book without being manually keyed in by an individual (referred to in the rules as a designated trading representative). It is through automated order processing systems that algorithmic programs access our markets
CERT Australia	The national computer emergency response team
COBIT 5	Control Objectives for Information and Related Technology, issued by ISACA
Corporate Governance Principles	ASX Corporate Governance Council, *Corporate governance principles and recommendations*, 3rd edition, ASX, 2014
Corporations Act	*Corporations Act 2001*, including regulations made for the purpose of that Act
credit licence	An Australian credit licence under s35 of the National Credit Act that authorises a licensee to engage in particular credit activities
CREST Australia	Council of Registered Ethical Security Testers Australia

Term	Meaning in this document
critical infrastructure	Assets that are essential for the functioning of society and the economy, and to ensure national security
crossing system	An automated service provided by a market participant to its clients that matches or executes client orders with orders of the market participant (i.e. against the participant's own account) or with other users with orders in the system. These orders are not matched on a pre-trade transparent order book
CS facility	A clearing and settlement facility as defined by s768A of the Corporations Act
CS facility licence	An Australian CS facility licence under s824B of the Corporations Act that authorises a person to operate a CS facility in Australia
cyber attack	An attempted or actual incident that either: • uses computer technology or networks to commit or facilitate the commission of traditional crimes, such as fraud and forgery—for example, identity or data theft (computer assisted); or • is directed at computers and computer systems or other information communication technologies—for example, hacking or denial of services (computer integrity).
cyber insurance	A range of insurance cover tailored to relevant cyber risks
cyber resilience	An organisation's ability to prepare and respond to a cyber attack and to continue operation during, or quickly adapt and recover from, a cyber attack
cyber risk	A cyber threat or cyber vulnerability
cybersecurity	Security measures taken to improve cyber resilience
cyber threat	A possible cyber attack, with the potential to adversely impact organisational operation and assets, individuals, other organisations, or a nation
cyber vulnerability	An inherent weakness in an information system, security procedures, internal controls or implementation that could be exploited by a cyber-threat source
dark pools	Electronically accessible pools of liquidity that are not pre-trade transparent, including crossing systems and dark venues operated by exchange market operators
FINRA	Financial Industry Regulatory Authority (US)
financial market infrastructure	Includes market licensees, CS facility licensees and ADTR licensees
GFMA	Global Financial Markets Association

Term	Meaning in this document
IOSCO	International Organization of Securities Commissions
IOT device	A device that connects to the Internet of Things
ISACA	Information Systems Audit and Control Association
ISO/IEC 27001	ISO/IEC 27001 *Information technology—Security techniques—Information security management systems—Requirements*
ISO/IEC 27002	ISO/IEC 27002 *Information technology—Security techniques—Code of practice for information security management*
market licensee	Holder of an Australian market licence
market participant	A participant of a licensed market
market-sensitive information	Information that a reasonable person would expect to have a material effect on the price or value of an entity's securities that has not previously been announced to the relevant securities exchange or is otherwise not generally available
National Credit Act	*National Consumer Credit Protection Act 2009*
National Plan	Australian Government, *National plan to combat cybercrime*, 2013
NIST	National Institute for Standards and Technology
NIST Cybersecurity Framework	NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity
OAIC	Office of the Australian Information Commissioner
PDS	Product Disclosure Statement
Privacy Act	*Privacy Act 2009*
Product Disclosure Statement	A document that must be given to a retail client in relation to the offer or issue of a financial product in accordance with Div 2 of Pt 7.9 of the Corporations Act Note: See s761A for the exact definition.
RBA	Reserve Bank of Australia
SEC	Securities Exchange Commission (US)
SIFMA	Securities Industry and Financial Markets Association (US)
TISN	Trusted Information Sharing Network for Critical Infrastructure Resilience