ASIC
Australian Securities & Investments Commission

REPORT 468

# Cyber resilience assessment report: ASX Group and Chi-X Australia Pty Ltd

March 2016

## About this report

This report presents the findings of our cyber resilience assessments of ASX Group and Chi-X Australia Pty Ltd. It also provides some examples of emerging good practices implemented by a wider sample of organisations operating in the Australian financial sector.

**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**

Licensed market and clearing and settlement (CS) facility operators are required to have, amongst other things, sufficient resources to operate properly. This includes the resources to properly support their cyber resilience—which is now regarded as one of the most significant concerns for the financial services industry and the economy at large.

The cyber resilience of our regulated population is a key focus for ASIC. Given the central role that financial market infrastructure providers play in our economy, their cyber resilience is of particular importance, and the reason for this assessment of Australia's major domestic financial market infrastructure providers—ASX Group and Chi-X Australia Pty Ltd (Chi-X).

Overall, our assessment concluded that ASX Group and Chi-X have, up to this point in time, met their statutory obligations to have sufficient resources for the management of cyber resilience.

Because of the dynamic nature of cyber threats, financial market infrastructure providers' cyber resilience frameworks need to continuously evolve. For that reason, a comprehensive and long-term commitment to cyber resilience is essential to help organisations deal with these challenges as and when they arise. Working closely with the RBA on ASX Group's CS facilities, we will continue to engage with financial market infrastructure providers on this issue.

We will also work to assist other organisations in our financial markets to enhance their cyber resilience framework and environment. To support this, we have provided:

- examples of good practices identified across the financial services industry (see Section C); and
- some questions board members and senior management of financial organisations should ask when considering their cyber resilience (see the appendix).

1 The increasing incidence, complexity and reach of malicious cyber activities can undermine businesses and destabilise our markets, eroding investor and consumer trust and confidence in the financial system and the wider economy. The cyber resilience of our regulated population is, therefore, a key focus for ASIC. In 2015, ASIC released Report 429 *Cyber resilience: Health check* (REP 429) to highlight the escalating threat of malicious cyber activities against organisations participating in Australian financial markets, and to increase awareness of cybersecurity across our regulated population.

2 Given the central role financial market infrastructure providers have in our economy, we have selected them for our first formal cyber resilience review. In recognition of the importance of cyber resilience for financial market infrastructure providers, the RBA also used its recent assessment of ASX

Group's CS facilities to indicate its intention to continue engagement (jointly with ASIC) with ASX Group on cyber resilience issues: see RBA, *2014/15 Assessment of ASX clearing and settlement facilities*, September 2015.

## Our new approach to assessments

3 Under s794C(1) and s823C(1) of the *Corporations Act 2001* (Corporations Act) we may assess how well a market or CS facility licensee is complying with any or all of its obligations in the Corporations Act.

4 We were previously required to conduct annual assessments of how well market licensees and CS facility licensees were complying with the wide set of prescribed obligations under s792A(c) and s821A(c), respectively. Following legislative changes, we are no longer required to undertake a review of the entire set of obligations—we can now assess discrete obligations to more effectively target specific high-risk areas. This targeted approach also reduces unnecessary regulatory burden on the financial market infrastructure providers that are being assessed. This report is ASIC's first assessment under the amended legislative framework.

## Purpose of this report

5 The purpose of this report is to:

(a) assess the extent to which ASX Group and Chi-X have met their obligations under s792A(d) and s821A(d) to have sufficient resources to operate properly—in this case, the resources to properly manage their cyber resilience (see Section B);

Note: Section 792A(d) applies to market operators and s821A(d) applies to CS facilities. ASX Group operates both forms of market infrastructure; however, Chi-X only operates a market, therefore, s821A(d) does not apply to Chi-X.

(b) provide examples of good practices we have observed in the wider Australian financial services industry to date, as well as some shared by our regulatory counterparts overseas (see section C); and

(c) raise awareness of good cyber resilience practices within the financial services industry, and encourage organisations to collaborate and share threat intelligence to prevent cyber threats.

### Assessment

6 We have concluded that, up to this point in time, ASX Group and Chi-X have met their obligations to have adequate resources to manage cyber resilience.

7 In carrying out the cyber resilience assessments of ASX Group and Chi-X, we have chosen to apply the US National Institute of Standards and Technology (NIST) Cybersecurity Framework for Critical Infrastructure (PDF 930 KB) (NIST Cybersecurity Framework). As part of our assessment, ASX Group and Chi-X were required to complete a self-evaluation against the framework which was later validated by ASIC through a series of document reviews and detailed discussions. In doing so, we worked closely with the RBA, which reported on the results of the self-assessment in the *2014/15 Assessment of ASX clearing and settlement facilities* in September 2015. We also compared our findings with practices used by a sample of other important financial organisations operating in Australian markets.

> Note: The NIST Cybersecurity Framework is one of a number of frameworks that can be used to assess an organisation's cyber resilience. It was used for this assessment because it takes a risk-based approach that is relevant to ASIC's regulated population. ASIC recognises, however, that some organisations may consider other available frameworks to be better suited to their particular circumstances.

8 Because of the dynamic nature of cyber threats, financial market infrastructure providers' cyber resilience frameworks need to continuously evolve. A comprehensive and long-term commitment to cyber resilience is essential to help all organisations deal with these challenges as and when they arise. With this in mind, we intend to use the information collected from this assessment to work closely with ASX Group and Chi-X to monitor future developments in this area—particularly the ongoing evolution of international and domestic regulatory settings and expectations.

### ASX Group's CS facilities

9 In respect of ASX's CS facilities, this work will be conducted in cooperation with the RBA, which is consistent with the position set out in the *2014/15 Assessment of ASX clearing and settlement facilities*.

10 Of particular importance to ASX Group's CS Facilities, is the Committee on Payments and Market Infrastructure (CPMI) and the International Organization of Securities Commissions (IOSCO) *Principles for financial market infrastructures* (PDF 1.6 MB) (CPMI–IOSCO Principles). The CPMI–IOSCO Principles are international standards for the design and operation of systemically important CS facilities, trade repositories and payment systems. The CPMI–IOSCO Principles have been implemented in Australia and are jointly applied as regulatory standards by ASIC and the RBA: see Regulatory Guide 211 *Clearing and settlement facilities: Australian and overseas operators* (RG 211) and the RBA's Financial Stability Standards (FSS) for CS facilities.

11 In November 2015, CPMI–IOSCO published draft cyber resilience guidance for consultation in *Consultative paper: Guidance on cyber resilience for financial market infrastructures* (the proposed Cyber Guidance). The proposed Cyber Guidance is intended to interpret how relevant requirements

in the CPMI–IOSCO Principles apply to cyber resilience (i.e. it does not propose new requirements). Once finalised, the Cyber Guidance will be the basis for our future engagement on cyber resilience with ASX Group's CS facilities and will also provide helpful guidance for the markets operated by ASX Group and Chi-X—and across the broader financial system.

12 The proposed Cyber Guidance covers a number of key concepts that are consistent with the various lines of inquiry undertaken by ASIC as part of this assessment of ASX Group and Chi-X.

## Good practice guidance

13 In Section C we provide examples of good practices we observed across a wider sample of organisations in the Australian financial services industry, as well as some shared by our regulatory counterparts overseas. The purpose of this is to supplement the proposed Cyber Guidance and raise awareness of cybersecurity to help organisations identify ways to increase their cyber resilience. We also encourage organisations to collaborate with each other and share good practices to increase cyber resilience across the entire financial system.

14 We expect all organisations within our regulated population to consider the good practice guidance presented in this report as they develop or enhance their cyber resilience frameworks.

# B Summary of assessments

**Key points**

In this section we:

- discuss the increasing importance of cyber resilience for all organisations in Australia's financial sector (see paragraphs 15–21);
- present our findings from the assessments of ASX Group and Chi-X, together with data from industry self-assessments undertaken by a wider sample of Australian financial organisations (see paragraphs 22–35); and
- discuss in further detail the proposed Cyber Guidance for financial market infrastructure providers (see paragraphs 36–42).

## Background to the self-assessments

15 The financial sector is undergoing an unprecedented rate of technological innovation with the commoditisation of internet-based offerings and increasing customer demand for personalised, distributed services. Organisations of all sizes are innovating to access new markets and create greater value for stakeholders and customers.

16 We support and actively assist organisations to realise the potential these new opportunities can provide. One by-product of technological innovation is that organisations are now exposed to:

(a) an increased risk of cyber crime (both internal and external to an organisation); and

(b) the potential for weaknesses to be exploited in globally connected networks of information and communication systems.

17 Organisations need to adopt and implement highly responsive processes to operate effectively in this changing environment. Because of the dynamic nature of cyber threats, a comprehensive and long-term commitment to cyber resilience is essential to help organisations to deal with these challenges as and when they arise.

### Our approach to assessments

18 This is ASIC's first formal assessment of cyber resilience following the release of REP 429. In addition to this formal assessment, we also engaged with a large number of other Australian financial organisations to support them in self-assessing their cyber resilience. For this engagement, and our more detailed assessment of ASX Group and Chi-X, we chose to use the NIST Cybersecurity Framework.

19 The NIST Cybersecurity Framework is one tool that can be used to evaluate cyber resilience. It was selected because of its wide use by critical infrastructure providers and other organisations in a number of overseas jurisdictions: see Appendix 3 of REP 429 for a summary of the NIST Cybersecurity Framework.

20 As part of our wider work in this area, we will continue to collaborate with various Australian Government agencies (including the Department of the Prime Minister and Cabinet and the RBA) and a range of international market regulators, including in the United States, European Union and Asia.

> Note: We work closely with the RBA on all matters relevant to Australian CS facilities. The RBA has oversight of the FSS, which applies to all Australian licensed CS Facilities, and ASIC has responsibility for the other provisions of Ch 7.3 of the Corporations Act: see *2014/15 Assessment of ASX clearing and settlement facilities*.

21 This collaboration is designed to help monitor approaches adopted by international and domestic regulators, and guidance being developed by international standard-setting bodies such as CPMI and IOSCO. The goal is to ensure the ongoing development of an approach that best serves ASIC's stakeholders and the broader Australian financial sector.

## Our findings

22 We have concluded that, up to this point in time, ASX Group and Chi-X have met their obligations to have sufficient resources for the management of cyber resilience. In reaching this conclusion, we have used data and information provided to us by ASX Group and Chi-X, including the results from their self-assessments against the NIST Cybersecurity Framework.

23 In the course of our assessment, we also requested and reviewed supporting documentation, and conducted further detailed inquiries through discussions with ASX Group and Chi-X to clarify responses and seek further information. The more detailed findings of this assessment have been shared with both ASX Group and Chi-X.

24 In presenting the findings in this report, we were conscious about maintaining the confidentiality of data from ASX Group and Chi-X. For that reason, data from these organisations has been anonymously incorporated with data received by ASIC from a wider sample of Australian financial organisations, which were subject to a separate NIST Cybersecurity Framework self-assessment process.

25 Although we have not independently validated all of the data received from this wider sample of organisations, it did enable us to compare the approaches undertaken by ASX Group and Chi-X, and assist in identifying

other emerging good practices across a wider set of significant participants in the Australian financial sector.

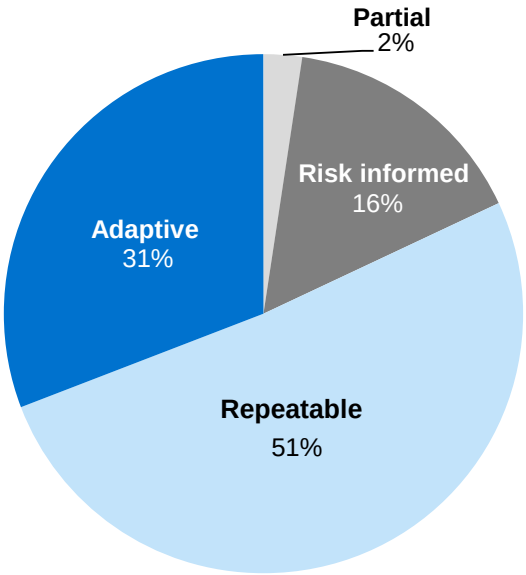
## Self-assessment results against the NIST Cybersecurity Framework

26 The findings presented in this section of the report reflect those of the different organisations that have worked with ASIC in responding to the NIST self-assessment process—being ASX Group, Chi-X and the wider range of financial organisations that undertook the NIST Cybersecurity Framework self-assessment.

27 Figure 1 shows the level of sophistication and rigor ('tier ratings') of an organisation's cybersecurity practices. The tiers range from least to most progressed (i.e. partial, risk informed, repeatable and adaptive).

> Note: *Adaptive* means processes are operated and adjusted in 'real time' as and when events occur; *repeatable* means organisation-wide cybersecurity processes are in place and are operated and updated on a regular basis; *risk informed* means a cyber risk management policy has been approved by senior management (although not on an organisation-wide basis); *partial* means cyber risk management profiles are not formalised, and are managed on an ad hoc basis.

**Figure 1: Summary of the NIST Cybersecurity Framework tier ratings across all self-assessments**




28 We observed that 82% of cybersecurity practices were self-assessed as *adaptive* (30.9%) or *repeatable* (51.1%). Of the remaining 18%, *risk informed* represented 15.6% of cybersecurity practices, and only 2.4% were self-assessed as *partial*. These results are a positive reflection of the overall cyber resilience health of the organisations.

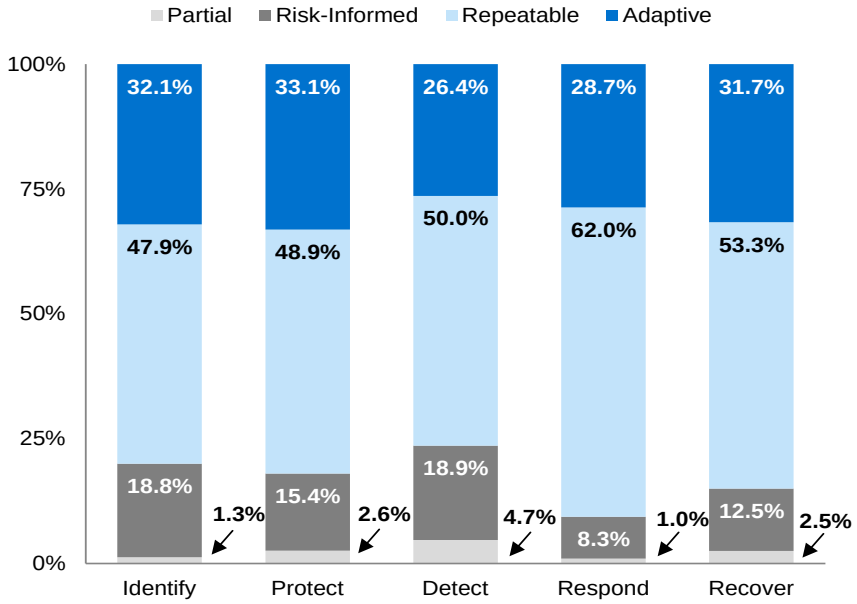
29 We also reviewed the breakdown of the tier ratings in Figure 1 across the five 'core functions' of the lifecycle of an organisation's management of

cyber risk. These core functions are 'identify', 'protect', 'detect', 'respond' and 'recover'.

30 We found that ratings of core functions are generally consistent. That is, organisations believe they perform consistently (whatever that level may be) when 'identifying', 'protecting', 'detecting', and 'recovering' in response to a cyber incident. The exception is 'responding' where responses showed rates at over 90% for *repeatable* and *adaptive* behaviours.

31 More specifically, we assessed both the ASX Group and Chi-X cyber resilience practices to be at the upper levels of the tier ratings (i.e. repeatable or adaptive) across the assessment criteria at the core function level.

**Figure 2: Breakdown by NIST Cybersecurity Framework core functions**




32 In reviewing the responses to the NIST Cybersecurity Framework, we found the following practices rated as 'adaptive' across the organisations:

(a) established information security policies are periodically reviewed and updated;

(b) cybersecurity roles are defined, communicated and understood at the senior management level;

(c) legal and compliance obligations are understood and managed;

(d) response and recovery plans are managed, communicated and tested on a periodic basis; and

(e) cyber events are communicated within the organisation to ensure ongoing awareness of threats.

33 Common challenges across the organisations included:

(a) establishment of a baseline for data flows across organisational networks that could, in turn, enable the detection of any anomalous flow of information; and

(b) management of software across mobile devices to prevent installation of malicious code.

34 We found that although a variety of operational cyber resilience practices are used by organisations, the results are an indication that these organisations rate cyber resilience as high on their risk radar—and are, generally, well progressed in managing and further developing their cyber resilience. Furthermore, all organisations gave a strong indication of continued focus on cyber risks and a desire to move toward, or maintain, a cyber resilience tier rating of *adaptive* across all categories in the short to medium term: see Section C for a more detailed discussion of these good practices.

35 Although the overall results of the NIST Cybersecurity Framework self-assessments can be interpreted as indicating a high level of cyber resilience within organisations, the weakest link is often the real measure of cyber resilience—for both the organisation concerned and the industry more broadly. Organisations should ensure good practices are in place for assessing cyber risk and driving continuous improvement.

## Proposed guidance for financial market infrastructure providers

36 We will continue to monitor developments in the forthcoming guidance on cyber resilience to the CPMI–IOSCO Principles, and in international and domestic regulatory settings and expectations. As we have done to date, we will continue this work in close collaboration with the RBA.

37 The intention of the proposed Cyber Guidance is to interpret how relevant requirements in the CPMI–IOSCO Principles apply to cyber resilience; it does not propose to create a new set of requirements. The proposed Cyber Guidance is also intended to add momentum to, and instil international consistency in, the industry's ongoing efforts to enhance the ability of systemically important CS facilities, trade repositories and payment systems to:

(a) pre-empt malicious cyber activities;

(b) respond rapidly and effectively to cyber activities; and

(c) achieve faster and safer target recovery objectives if they succeed.

38 The proposed Cyber Guidance sets out the preparations and measures that these organisations should use to enhance their cyber resilience capabilities. The aim is to limit the escalating risks that cyber threats pose to individual financial market infrastructure providers and financial stability. It also

provides regulators with a set of internationally agreed guidelines to support consistent and effective oversight and supervision of financial market infrastructure providers in the area of cyber risk.

39 The key concepts of the proposed Cyber Guidance include that:

(a) the attention of the board and senior management is critical to a successful cyber resilience strategy;

(b) the ability to resume operations quickly and safely after malicious cyber activities is paramount;

(c) providers should make use of good-quality threat intelligence and rigorous testing;

(d) cyber resilience requires a process of continuous improvement; and

(e) cyber resilience cannot be achieved by a financial market provider alone, it is a collective effort of the whole 'ecosystem'.

40 The proposed Cyber Guidance reflects the urgency of addressing the increasing risks that cyber threats pose to financial stability. It also highlights the need for a coordinated approach. In our highly interconnected financial sector, cyber resilience cannot be achieved by individual organisations alone—the broader 'ecosystem' needs to work in unison.

Note: It is anticipated that the Cyber Guidance will be finalised in the second half of 2016.

41 A number of the key concepts in the proposed Cyber Guidance were considered by ASIC as part of our assessment of ASX Group and Chi-X. The final Cyber Guidance will apply directly to the operation of ASX Group's CS facilities, and will also informally provide a set of considerations for the markets operated by ASX Group and Chi-X. We may choose to review market operators in light of these considerations and the ASIC market integrity rules.

42 ASIC anticipates working closely with ASX Group, Chi-X and other regulators (including the RBA in respect of CS facilities) to ensure the effective application of the proposed Cyber Guidance in the period following its finalisation.

# C Cyber resilience good practices

**Key points**

This section sets out examples of some of the emerging good practices we identified as part of our assessment of ASX Group and Chi-X, and through our wider engagement with a number of other financial organisations. These practices have been identified through both the self-assessment process conducted under the NIST Cybersecurity Framework, as well as more detailed follow-up discussions.

We consider the benefit of identifying these good practices goes beyond the organisations that we have formally engaged with to date. We encourage all organisations to discuss, share and consider the application of these practices in the pursuit of a collective and robust defence against cyber threats in Australia's financial markets.

43 The following examples of emerging good practices were rated as 'adaptive' by organisations in the self-assessments conducted against the NIST Cybersecurity Framework. These practices enable organisations to operate highly adaptive and responsive cyber resilience processes—and could be applied by other organisations to improve their cyber resilience preparedness.

## Cybersecurity strategy and governance

44 The good practices we observed in relation to cybersecurity strategy and governance were characterised by board 'ownership', and responsive and agile governance models.

**Good practice 1: Board engagement**

*Periodic review*

The board takes ownership of cyber strategy and ensures it is reviewed on a periodic basis to assess progress against success measures outlined in the strategy. Measures include time to detection, speed of response and recovery process.

*Cyber resilience as a management tool*

The management of cyber resilience is viewed by the board as a critical management tool for understanding risk status and making important investment decisions on cyber risk. It is seen as a tool for 'enabling' (not limiting) the organisation—by anticipating scenarios and building protection against them to take advantage of market opportunities.

*Cyber resilience fluency*

Board members are becoming increasingly educated in the language of cyber resilience and the potential threats to organisations, and are more

readily able to ask risk and audit committees the relevant questions. This reflects an active understanding of the cyber threat landscape and the planning and testing of response scenarios: see the appendix for a set of questions for board members to consider when evaluating cyber resilience within their organisations.

*Assurance processes*

Assurance processes are focused on end-to-end business processes. This is undertaken with a view to confirming that critical business operations, technology applications and infrastructure—and the supporting data—are tested as a whole rather than independently of business processes and technology functions. Ensuring that critical business processes can be re-activated if and when an incident occurs.

**Good practice 2: Governance**

*Responsive governance*

Organisations are tailoring traditional governance processes, to ensure 'responsive governance'. In a rapidly changing cyber risk environment, the policies and procedures of today are not necessarily valid for long periods of time, and may not remain valid between typical annual review cycles.

This approach considers how adjustments can be driven by events and incidents, rather than by keeping to a fixed review period which might ignore the need for change that arises in between set periodic review points.

*Alignment with the organisations overall governance framework*

Cybersecurity governance is clearly and visibly aligned to other organisation-wide governance processes and procedures. This means that documented strategies, principles, policies, rules and procedures are in line with the overall governance framework.

## Cyber risk management and threat assessment

45 Good practice in the area of cyber risk management and threat assessment is led by intelligence gathering through the use of third-party experts, and driven by routine threat assessments, including of relevant third parties.

**Good practice 3: Cyber risk management**

Cyber risk management is increasingly becoming intelligence-led and moving to near real-time processes. This is occurring through automation and use of risk management tools that can integrate many sources of risk—including those from collaboration and information-sharing sources such as peers in the industry, police and government agencies.

*'Fusion' centres*

Some organisations have taken the step of establishing specialist functional groups within their organisations to monitor and address risks in real time, often known as 'fusion' centres.

### Third-party risk management

46 As outsourcing and cloud-based services become more prevalent, the reliance on third-party service providers and partners has become essential to the provision of products and services for many organisations.

**Good practice 4: Third-party risk management**

Organisations have developed risk-based assessment methods and tools to ensure that third-party suppliers and partners are regularly assessed to guarantee compliance with required security standards. Some organisations are also using external service providers to carry out periodic assessments of partners and vendors.

## Collaboration and information sharing

47 Collaboration is often characterised by confidential information-sharing arrangements with other financial institutions, security agencies and law enforcement. Information sharing is fundamental for organisations that are intelligence-led and aids in understanding attackers and potential threats, including terrorist organisations, political activists, organised crime and nation-state-sponsored attackers. This process also helps organisations to understand attackers' motives—whether it be information, funds or general disruption.

**Good practice 5: Collaboration and information sharing**

To gather intelligence, organisations are often engaging specialist third-party organisations to undertake security monitoring and assessments. By employing the services of specialist individuals and companies operating in foreign jurisdictions, organisations are able to gather threat intelligence.

Organisations also have confidential information-sharing arrangements in place with other financial institutions, security agencies and law enforcement.

## Asset management

48 Effective management of organisational assets is characterised by centralised management systems for critical internal and external assets (e.g. software and data), and configuration management that ensures visibility of critical assets.

**Good practice 6: Asset management**

*Centralised asset management system*

Asset inventories for hardware, software and data, both internal and external to organisations, are managed through a centralised asset management system.

*Configuration management*

Configuration management is important for ensuring there is visibility of critical assets across the organisation, and for managing software versions and security patches.

## Cyber awareness and training

49 There is clear recognition that effective cyber resilience requires a strong 'cultural' focus driven by the board and reflected in organisation-wide programs for staff awareness, education and random testing, including of third parties.

**Good practice 7: Cyber awareness and training**

*Training*

Development of organisation-wide programs and strategies to ensure staff awareness and education—including for contractors and partners—which is effectively managed and monitored against success criteria.

*Continuous development*

Strategies based on a program of continuous development of knowledge and awareness—so that, through active vigilance, staff become an effective defence against malicious cyber activities by preventing incidents arising from attempted phishing attacks and other forms of social engineering.

*Random staff testing*

Random testing of staff enables the organisation to measure the effectiveness of cyber-awareness programs (e.g. a test email containing malware is sent to a staff member or group to test their response) and to take appropriate measures based on the response (i.e. staff may be required to undertake further training if they do not manage the situation in accordance with their training).

## Proactive measures and controls

50 Proactive measures and controls for cyber risks are characterised by implementation of the Australian Signals Directorate's (ASD) *Strategies to mitigate targeted cyber intrusions (or equivalent)*, as well as a range of additional controls (e.g. encryption for 'data in transit' based on a risk assessment of the asset in question).

**Good practice 8: Proactive measures and controls**

Organisations have already implemented, or have made it a priority to implement the ASD's 'top four' *Strategies to mitigate targeted cyber intrusions*. These are:

- application whitelisting;
- application patching;
- operating system patching; and
- restricting administrative privileges.

Additionally, the more progressive organisations have also sought to apply:

- security as integral to the systems development lifecycle, sometimes known as the Security Development Lifecycle (SDL);

- encryption for stored data and 'data in transit' based on a risk assessment of the assets in question;
- filtering and monitoring of outbound email messages to ensure that data is not transmitted outside of the organisation's network in error or through intent; and
- highly restricted access to use of USB ports on computer equipment to minimise risks of data leakage or introductions of unauthorised software or files.

## Detection systems and processes

51 There has been a lot of development in the approaches taken by 'good-practice' organisations in the area of cyber detection systems and processes. Good practices are characterised by the use of organisation-wide continuous monitoring systems and the use of data analytics to integrate sources of threats in real time.

**Good practice 9: Detection systems and processes**

*Continuous monitoring systems*

Continuous monitoring systems, often organisation-wide, are implemented to monitor events on an organisation's network and systems using Security Information and Event Management (SIEM) technologies. SIEM technologies enable the detection and alert of anomalous user behaviours such as access to applications or files, as well as abnormal movement of information across the networks measured against a baseline reference of 'normal' activity.

*Data analytics*

Use of data analytics to enable organisations to integrate sources of threats and associated risks into a single view of the threat landscape in real time. Threats detected by the organisation, in addition to information collected through collaboration and information-sharing channels, are analysed to move response capability towards predicting malicious cyber activities.

*'Red teaming'*

Employing technical specialists to work on breaking into an organisation's networks.

## Response and recovery planning

52 Response planning for cyber risks is different from standard business continuity planning because the scenarios are not as predictable, in part due to:

(a) the range of threat sources (e.g. insider threats, which contribute to over 30% of identified incidents); and

Note: See PricewaterhouseCoopers, *Turnaround and transformation in cybersecurity: Financial services* (PDF 215 KB), 2 October 2015.

(b) the speed at which the sophistication levels of attacks are changing.

53 Good practices we observed included routine and detailed scenario planning, war gaming, proactive reporting to the board and well-developed communication plans.

**Good practice 10: Response planning**

Organisations are adopting some of the following practices:

- *Scenario planning*: To predict the types of incidents that may occur based on their specific risk profile, and implementing and exercising response processes.
- *War gaming:* Some organisations are using war gaming techniques to better understand and plan their defence against malicious cyber activities.
- *Proactive reporting to the board*: Reporting of changing threats and the counter measures that are in place.

**Good practice 11: Recovery planning**

In the event of a data breach, organisations have actively determined when and how to notify customers—and there is a well-defined communication plan in place for managing stakeholders and public relations.

# Appendix: Key questions for an organisation's board of directors

54 Recognising and managing risk is a crucial part of the role of an organisation's board of directors and senior management. To enable boards to do this, organisations must have an appropriate framework to identify and manage risk on an ongoing basis. Given the magnitude and prominence of cyber risk for most organisations, informed oversight of risk involves the board being satisfied that cyber risks are adequately addressed by the risk management framework of the organisation. Important controls include ensuring the organisation has appropriate safeguards in place against malicious cyber activities, and that recovery capabilities are adequate.

55 Paragraphs 56–67 contain details of key questions for board members to consider when reviewing their risk management frameworks.

## Risk management framework

### Question 1: Are cyber risks an integral part of the organisation's risk management framework?

56 The board should ensure that cyber risk is an element of the broader risk framework and that exposures are recognised, assessed for impacts based on clearly defined metrics such as response time, cost and legal or compliance implications, and planned for to attract investment commensurate to a risk-based assessment.

### Question 2: How often is the cyber resilience program reviewed at the board level?

57 Given the rate of change in the cyber risk landscape, and the speed at which a business can be severely compromised (potentially within hours or days); the board should consider whether periodic reviews (that are more frequent than for other risks forming part of the risk management framework) should be adopted.

## Identifying cyber risk

### Question 3: What risk is posed by cyber threats to the organisation's business?

58 Different businesses will be exposed to different cyber risks and different potential consequences. It is important for the board to reflect on risks

relevant to the particular business of the organisation. Without understanding the nature of the risk and its consequences it is difficult for a board to set a suitable risk tolerance for the risk and to ensure that cyber risks are adequately dealt with by the organisation's risk management framework.

### Question 4: Does the board need further expertise to understand the risk?

59 Although a board may not require general technology expertise, for many organisations it may be advisable to have one or more directors that have a strategic understanding of technology and its associated risks, or that have a background in cybersecurity.

60 In some circumstances, the board should consider the use of external cyber experts to review and challenge the information presented by senior management.

## Monitoring cyber risk

### Question 5: How can cyber risk be monitored and what escalation triggers should be adopted?

61 Trying to identify a cyber risk may pose particular challenges. Organisations at the forefront of good practice are using intelligence-driven solutions to deal with this challenge.

62 For some organisations malicious cyber activities may be devastating to the organisation's business operations, it is therefore important to consider what might lead to the provision of more detailed information on the risk to senior management and the board.

## Controls

### Question 6: What is the people strategy around cybersecurity?

63 Despite significant advances in cybersecurity technology; products, lack of staff awareness of safe cyber practices, social engineering and negligent behaviours remain a major source of cyber issues.

64 The boards should satisfy itself that there is sufficient investment in staff awareness training given its prominence as a source of risk—and because a collective effort against cyber threats will better serve an organisation.

### Question 7: What is in place to protect critical information assets?

65 The board should be satisfied that critical information assets of the organisation are appropriately secure. There should be transparency surrounding the location of all critical assets (including third-party partners and service providers), how they are protected and how protection is being assured.

## Response

### Question 8: What needs to occur in the event of a breach?

66 The boards should ask itself:

(a) If and when a problem arises, what processes are in place for communicating effectively, internally and externally, and managing the situation?

(b) Has there been a sufficient level of scenario planning and testing to ensure that response plans are valid and up-to-date, including with third-party suppliers and dependents?

67 The board may need to ensure that security and customer trust are central considerations as companies strive to deliver innovative products and services through technology.

# Key terms

| Term | Meaning in this document |
|---|---|
| ASD | Australian Signals Directorate |
| ASX | ASX Limited or the exchange market operated by ASX Limited |
| ASX 24 | The exchange market operated by Australian Securities Exchange |
| ASX Clear | ASX Clear Pty Limited (formerly known as Australian Clearing House Pty Limited) |
| ASX Clear (Futures) | ASX Clear (Futures) Pty Limited (formerly known as SFE Clearing Corporation Pty Limited) |
| ASX Compliance | ASX Compliance Pty Limited (formerly known as ASX Markets Supervision Pty Limited) |
| ASX Group | ASX, Australian Securities Exchange, ASX Clear, ASX Clear (Futures) and ASX Settlement |
| ASX Settlement | ASX Settlement Pty Limited (formerly known as ASX Settlement and Transfer Corporation Pty Limited) |
| Australian market licence | Australian market licence under s795B of the Corporations Act that authorises a person to operate a financial market |
| Chi-X | Chi-X Australia Pty Ltd or the exchange market operated by Chi-X |
| clearing and settlement facility licence | An Australian clearing and settlement facility licence under s824B that authorises a person to operate a clearing and settlement facility in Australia |
| clearing and settlement facility licensee | A person who holds a clearing and settlement facility licence |
| Corporations Act | *Corporations Act 2001*, including regulations made for the purpose of that Act |
| CPMI | Committee on Payments and Market Infrastructure |
| CPMI–IOSCO Principles | CPMI–IOSCO *Principles for financial market infrastructures* |
| critical infrastructure | Assets that are essential for the functioning of society and the economy, and to ensure national security |
| CS facility | Clearing and settlement facility |
| CS facility licensee | Clearing and settlement facility licensee |

| Term | Meaning in this document |
|---|---|
| cyber event | An observable occurrence in an information system or network |
| Cyber Guidance | CPMI–IOSCO *Consultative paper: Guidance on cyber resilience for financial market infrastructures* |
| cyber incident | An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences |
| cyber resilience | An organisation's ability to prepare and respond to malicious cyber activity and to continue operation during, or quickly adapt and recover from, the malicious cyber activity |
| cyber risk | A cyber threat or cyber vulnerability |
| cybersecurity | Security measures taken to improve cyber resilience |
| cyber threat | A possible malicious cyber activity, 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 |
| FSS | RBA Financial Stability Standards for CS facilities |
| financial market infrastructure provider | Includes an Australian market licensee, a CS facility licensee or an Australian derivative trade repository (ADTR) licensee |
| IOSCO | International Organization of Securities Commissions |
| malicious cyber activity | An attempted or actual incident that either:<br>• 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<br>• is directed at computers and computer systems or other information communication technologies—for example, hacking or denial of services (computer integrity) |
| market licensee | Holder of an Australian market licence |
| NIST | National Institute for Standards and Technology |
| NIST Cybersecurity Framework | NIST Cybersecurity Framework for Critical Infrastructure |
| RBA | Reserve Bank of Australia |

# Related information

## Headnotes

ASX Group, Chi-X, CPMI–IOSCO Principles, CS facility, cyber resilience, cyber risk, cybersecurity, cyber threat, financial market infrastructure, malicious cyber activity, NIST Cybersecurity Framework

## Consultation papers and reports

REP 429 *Cyber resilience: Health check*

## Regulatory guides

RG 211 *Clearing and settlement facilities: Australian and overseas operators*

## Media and other releases

15-060MR *ASIC issues major cyber resilience report*

16-064MR *ASIC reports on cyber resilience and identifies examples of good practices*