ASIC
Australian Securities &
Investments Commission

Cyber resilience of firms in Australia’s financial markets: 2018–19

Report 651 | December 2019

About this report

This report provides an update to Report 555 *Cyber resilience of firms in Australia’s financial markets*. It identifies key trends from self-assessment surveys completed by financial markets firms, and highlights existing good practices and areas for improvement.

Contents

About ASIC regulatory documents

In administering legislation ASIC issues the following types of regulatory documents: consultation papers, regulatory guides, information sheets and reports.

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 rules or requirements.

Overview

Cyber resilience is vital to all organisations operating in the digital economy, and nowhere is this more important than the financial markets sector, where the trust between an organisation and its clients is essential to its future.

In 2017, we reported on the cyber resilience of firms operating in Australia's financial markets (cycle 1): see Report 555 *Cyber resilience of firms in Australia's financial markets*.

To determine their cyber resilience maturity, participants provided answers to the National Institute of Standards in Technology (NIST) Cybersecurity Framework. The results indicated that, while awareness and management of cybersecurity risk was improving, there was still opportunity for improvement across the entire sector.

In 2017 and 2018, we asked participants to reassess their cyber resilience against the updated NIST Framework to determine how their progress was tracking (cycle 2).

To develop a better understanding of how an organisation's size and complexity influenced its cyber resilience we supplemented the responses with financial data from firms' annual accounts and, where relevant, trade data from our surveillance database.

Key findings

Cyber resilience is an organisation's capacity to prepare for, respond to and recover from cybersecurity events

The cyber resilience of firms operating in Australia's markets has improved since Report 555, with an average increase of 15% across all cyber resilience functions between cycle 1 and 2. Organisations are alert to cybersecurity threats to their business and have focused their resources and efforts on improving their cybersecurity governance, risk management, and response and recovery capabilities.

80% have formal processes for information risk management and governance (16% improvement).

80% consider their response and recovery practices to be well managed (20% improvement).

While the cyber resilience of firms has improved, firms have found it challenging to meet the targets they set in cycle 1. This can be attributed to:

- overly ambitious targets
- continually changing threat environment
- limited organisational capability
- limited access to specialised skills and resources.

Interestingly, firms that set more ambitious targets in the first cycle demonstrated the most improvement.

Investment, education, acquisition and retention of skilled resources, and strong leadership from senior management are critical to a firm's ability to maintain strong cyber resilience.

Emerging trends

Although improvements in cyber resilience have largely been driven by small and medium-sized entities (SMEs), large and technologically sophisticated firms continue to demonstrate greater confidence in their cyber resilience.

40% of SMEs indicated weak supply chain risk management practices.

Concerningly, the trend towards outsourcing of non-core functions to third-party providers has created difficulties in the management of cybersecurity risks in the supply chain.

ASIC will ...

Raise awareness of cybersecurity risk by providing good practice guidance and key questions

Measure and assess the level of cyber resilience in financial markets

Engage and collaborate with regulated firms

Conduct one-on-one conversations with firms

Review progress made by firms against their targets

Approach

The NIST Framework allows firms to assess their cyber resilience against five functions – *identify*, *protect*, *detect*, *respond* and *recover* – using a maturity scale of where they are now (current) and where they intend to be in 12–18 months' time (target).

The **IDENTIFY** function assists in developing an organisational understanding of how to manage cybersecurity risk to systems, people, assets, data and capabilities.

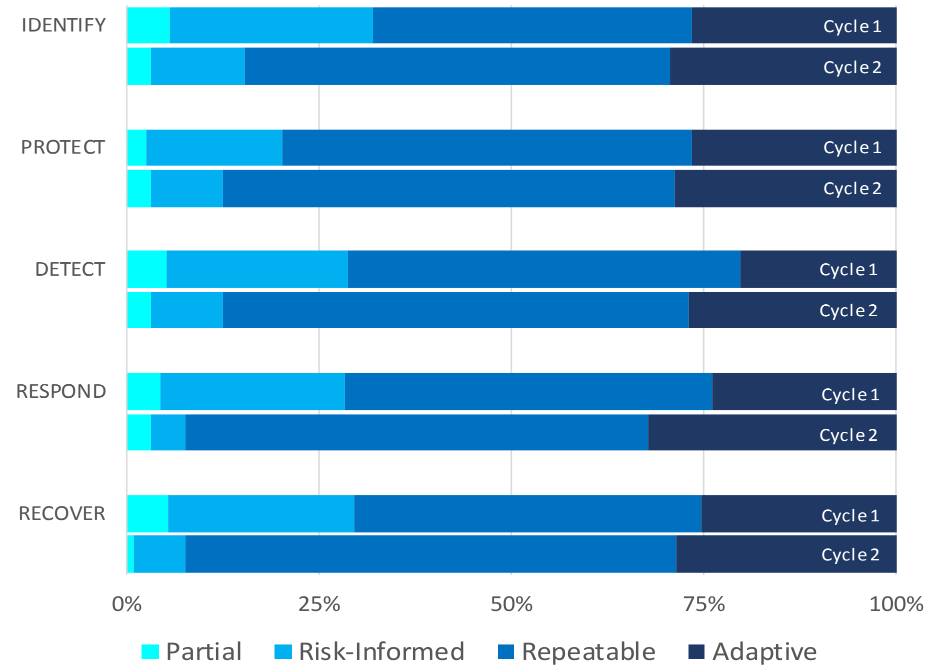
The **PROTECT** function supports the ability to limit or contain the impact of potential cybersecurity events and outlines safeguards for delivery of critical services.

The **DETECT** function defines appropriate activities to identify cybersecurity events in a timely manner.

The **RESPOND** function identifies appropriate activities to minimise the impact of cybersecurity events.

The **RECOVER** function identifies appropriate activities to maintain cyber resilience and restore services affected by cybersecurity events.

Figure 1: Improvement in current cyber resilience maturity between cycle 1 and cycle 2 (by function)



Note: See Table 1 for the data shown in this figure (accessible version).

● **Partial**
Policies and procedures are not formalised. Responses are reactive

● **Risk-informed**
Policies and procedures are rarely updated and not followed consistently

● **Repeatable**
Policies and procedures are approved, followed and regularly updated

● **Adaptive**
Policies and procedures evolve in response to changes in cybersecurity threats

Cyber resilience of SMEs

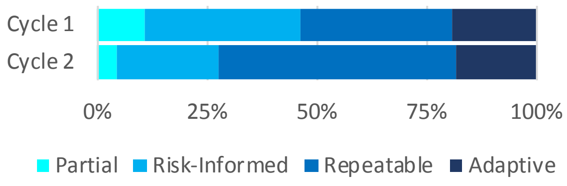
Identify

Effective information risk management requires an organisation-wide approach to governance. SMEs have made good progress since cycle 1, but further improvement is required to ensure appropriate risk management practices are implemented.

Eighty percent of SMEs assess themselves as 'repeatable' or better in cybersecurity risk governance – a 27% improvement on cycle 1. However, there is still opportunity for improvements in risk management, which showed the least progress.

Supply chain risk management is a significant challenge, with 42.9% of SMEs 'partial' or 'risk-informed'. All indicated this would be an area of focus over the next 18–24 months – however, improvement is expected to be gradual.

Supply chain risk management: 'Third-party vendor risk management program addresses cybersecurity threats introduced by material third-parties and suppliers. External parties are required to implement appropriate measures to meet the objectives of the information security program.' – *Repeatable*



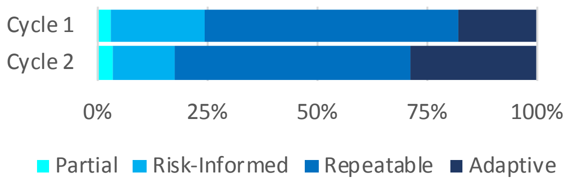
Protect

The protect function involves preventative measures aimed at minimising opportunities for cybersecurity events to occur. Examples include user access management, training and awareness programs and data protection policies and procedures.

The two areas that showed the most improvement (16% improvement on cycle 1) include awareness and training programs (77% 'repeatable' or 'adaptive') and user access management (91% 'repeatable' or 'adaptive'). However, given the importance of employees as a line of defence against cybersecurity events, there is still room for improvement in user awareness and training.

Protective processes: 'Audit logs are onerous and are examined reactively, removable media is not restricted. Least functionality-first is best-practice. Firewalls are in-place at internet access points.' – *Risk-informed*

Training and awareness: 'Users are required to undergo security training at onboarding and annually thereafter. Exams are used to measure employee competence. Email messages and office signage are in place to reinforce key security methods.' – *Adaptive*



Detect

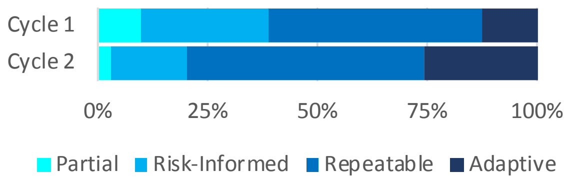
Monitoring and time to detection of a cybersecurity event is critical to the success of a response and recovery strategy. If a cybersecurity intrusion is not detected early, it may operate undetected and exfiltrate sensitive information or cause damage to the organisation's internal assets.

SMEs have driven significant improvement in detection capabilities – continuous monitoring, in particular, experienced a 25% improvement.

Anomaly and events detection and formal detection procedures have also improved by 16% but are still lagging behind, with 23% of firms reporting a 'partial' or 'risk-informed' rating.

Continuous monitoring: 'Virus scanning mandatory across all devices, VPN's are locked down to company-assets only, logins are audited but not analysed regularly for anomalies.' – *Risk-informed*

Anomalies and events detection: 'We recently had any issue where a staff email account was accessed. This led us to look at how we can better monitor unusual behaviour on our network. As a result, two factor authentication was added to email accounts and automated notifications are sent to IT admins if new rules etc. are created.' – *Risk-informed*



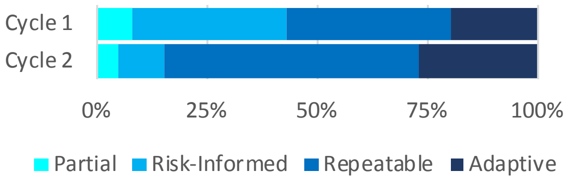
Respond and recover

A major proportion of the improvements reported by SMEs can be attributed to the response and recover functions. Improvements range from 25% to 31.5% for recovery practices, which were identified as a specific area of concern in cycle 1.

Over 80% of SMEs now report their cybersecurity maturity as 'repeatable' or 'adaptive', a big improvement on cycle 1. However, their work here is not done. While firms are targeting progressive improvements in the respond and recover functions, they anticipate that some practices will still be 'risk-informed'.

Communications: 'Formal Response plans are not documented; however experienced qualified personnel are employed and are equipped to respond fluidly - Ad-hoc is appropriate due to the size of the organisation adequate personnel are employed to quickly respond to any event. Formal guidelines can be in place.' – *Partial*

Analysis of events: 'Whilst BCP has been documented, active monitoring and testing of the effectiveness of the solution is yet to be established. Therefore, response and recovery activities may not be accurate. A framework to test and monitor the effectiveness of BCP arrangements needs to be implemented.' – *Risk-informed*



Cyber resilience of large firms

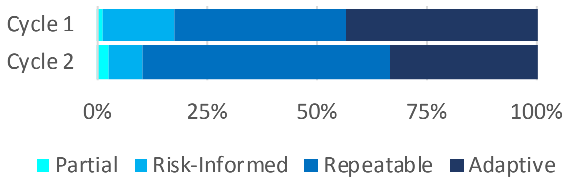
Identify

Cybersecurity governance, risk strategies and management have continued their upward trend since cycle 1 – up 5% to 90% 'repeatable' or 'adaptive'.

Due to the complexity of large firms and the breadth of services they offer, asset management (20% 'partial' or 'risk-informed') and supply chain risk management (22% 'partial' or 'risk-informed') have been identified as areas of improvement.

Risk management: '… risk tolerance is determined based on the materiality of the potential impact (financial, reputational or other) to the organisation and its stakeholders … if the risk were to materialise resulting in the loss of critical services.' – *Adaptive*

Supply chain risk management: 'Project underway in APAC to identify contracts / suppliers that hold data and update those contracts with new Terms and Conditions arising from the new Notifiable Data Breach Legislation - Suppliers under contract are provided the External Information Security Standard.' – *Partial*



Protect

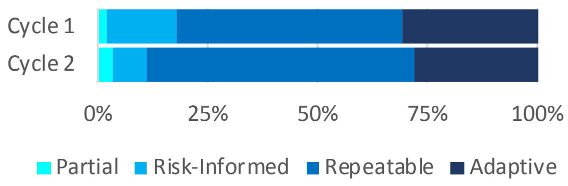
Large firms have long considered employees and suppliers to be an effective defence against cybersecurity events. This has been maintained with continued investment in staff awareness and training, resulting in an improvement of 10% since cycle 1.

User access management is also tightly managed with 91% of firms indicating a 'repeatable' or 'adaptive' rating.

Within the next 18–24 months, 13% of the firms rated as 'risk-informed' for data security and preventative technologies are targeting a rating of 'repeatable' or higher. This conservative improvement is indicative of the time and effort required to implement such capabilities across an organisation.

Data security: 'The Firm has become aware of physical hardware risks and is the nascent stages of finding a way forward.' – *Partial*

Training and awareness: 'All employees and in-scope third-party stakeholders are required to take annual cyber security training. This training is aligned to several various policy domains that define cyber security responsibilities based on that role.' – *Adaptive*



Detect

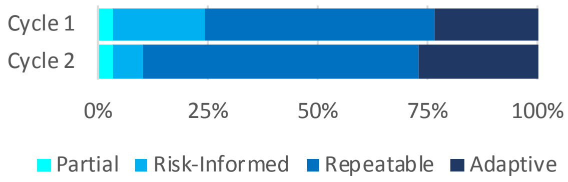
Many large firms consider the time taken from a cybersecurity intrusion to its detection and removal is an important reporting tool and measure of its detection capabilities.

While all NIST functions are of equal importance, detection capabilities are more advanced in organisations that demonstrate more cybersecurity maturity, which enables them to be more proactive in monitoring threats.

Large firms are extending the limits of their monitoring and detection capabilities – with 60% 'repeatable' and 20–25% 'adaptive'. Many have invested in security operation centres that have skilled teams proactively monitoring threats against their organisations.

Continuous monitoring: 'The SIEM system takes security events, correlates them and alerts Cybersecurity Operations analysts of the event.' – *Risk-informed*

Anomalies and events detection: 'The centralised security incident and event monitoring system has established baselines for network traffic, and anomalies trigger alerts to the Cybersecurity Co-ordination Centre. The depth and coverage of this monitoring and response capability is continually growing, being driven by Security Program funding.' – *Adaptive*



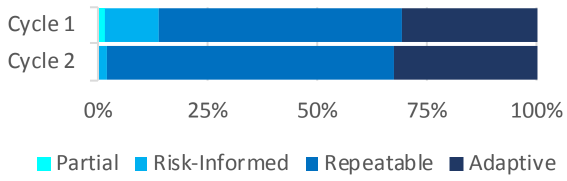
Respond and recover

Firms are reporting to be in a much more mature state with their response and recovery planning, testing and ongoing improvements than 24 months ago. They have made significant strides towards eliminating 'partial' and 'risk-informed' practices within this functional area. We see considerable improvements to response planning (19.4%), and mitigation action planning and improvements (16.1%) to ensure events, when they occur, are contained, do not propagate and are neutralised as quickly as possible.

Plans over the coming period indicate that all response and recovery practices will be 'repeatable' or 'adaptive'.

Response planning: 'Response plans are in place to inform personnel of their roles and responsibilities in the event of a cyber incident ... For any cyber incident which involves a data breach, [Entity] has a data response plan which is available internally. This includes details of appropriate escalation of incidents, information which needs to be provided as part of the escalation, and retention/analysis requirements.' – *Repeatable*

Improvements: 'Upon detection of an incident in the Cyber Security Operation centre the incident is contained by removing the affected system from the network.' – *Adaptive*

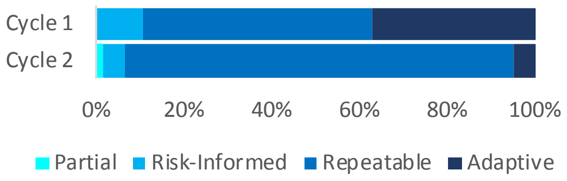


Credit rating agencies

The responses provided by credit rating agencies (CRAs) in cycle 1 identified disparities between the cyber resilience of CRAs and organisations of similar size and resources – CRAs had reported highly confident cyber resilience profiles.

To better understand their responses we took a closer look at a sample of licensed CRAs. We conducted one-on-one conversations with firms, and reviewed their progress against their cycle 1 targets. Where necessary, discussions with CRAs are ongoing.

Our findings indicate that, although there has been improvement between cycle 1 and cycle 2, there has also been a recalibration across all CRAs – with over 30% downgrading their 'adaptive' ratings from cycle 1 to 'repeatable'.



Cybersecurity strategy and governance

Good practice: Boards take ownership of their organisation's cybersecurity strategy and actively engage in communication, execution and monitoring of its success.

What we found:

- There is inconsistent board-level ownership of cybersecurity matters – some boards are driving their organisation's cybersecurity strategy, while others are led by management or IT.
- Several CRAs did not have a single, coordinated cybersecurity strategy in place – instead they had a collection of documents that described the strategy, framework and policies. This can make the strategy difficult to navigate and update.

Board reporting

Good practice: Boards are aware of the organisation's key assets, the risks associated with compromise of these assets and how they are protected.

What we found: Boards are not always given the information needed to properly understand their organisation's cyber resilience or to aid decision making. There are also large variances in the type of information reported to boards – from detailed updates on technical projects through to targeted updates assessing the latest threats and recommending actions for the board.

Cybersecurity event response playbooks

Good practice: Threat scenarios in playbooks are current, reflective of the latest threats to the organisation and tested on a periodic basis.

What we found: While all CRAs perform table top exercises with varying degrees of regularity, there are significant disparities in the quality of event response playbooks.

Third-party risk management

Good practice: Organisations understand the risks posed by third parties and implement policies and procedures to assure priority assets are safeguarded.

What we found: Overall, robust procedures are in place. Third parties are prioritised by the risk they pose to the business, and this is reflected in the frequency they are assessed. However, one CRA indicated there was no formal approach to third-party risk assessment.

External independent assessments

Good practice: An external independent expert is engaged to carry out regular assessments of the organisation's cyber resilience.

What we found: There is inconsistent appointment among CRAs of independent external experts engaged to carry out regular cyber resilience assessments.

Appendix: Accessible version of Figure 1

This appendix is for people with visual or other impairments. It provides the underlying data for Figure 1.

Table 1: Improvement in current cyber resilience maturity between cycle 1 and cycle 2 (by function)

Maturity	Identify		Protect		Detect		Respond		Recover	
Partial	Cycle 1	5.5%	Cycle 1	2.4%	Cycle 1	5.1%	Cycle 1	4.4%	Cycle 1	5.4%
	Cycle 2	3.1%	Cycle 2	3.2%	Cycle 2	3.2%	Cycle 2	3.2%	Cycle 2	0.9%
Risk-informed	Cycle 1	26.6%	Cycle 1	17.8%	Cycle 1	23.7%	Cycle 1	23.9%	Cycle 1	24.2%
	Cycle 2	12.1%	Cycle 2	9.2%	Cycle 2	9.3%	Cycle 2	4.3%	Cycle 2	6.6%
Repeatable	Cycle 1	41.3%	Cycle 1	53.3%	Cycle 1	50.9%	Cycle 1	47.7%	Cycle 1	45.0%
	Cycle 2	55.4%	Cycle 2	58.8%	Cycle 2	60.6%	Cycle 2	60.2%	Cycle 2	63.7%
Adaptive	Cycle 1	26.7%	Cycle 1	26.5%	Cycle 1	20.4%	Cycle 1	23.9%	Cycle 1	25.4%
	Cycle 2	29.4%	Cycle 2	28.8%	Cycle 2	26.9%	Cycle 2	32.3%	Cycle 2	28.7%

Note: This is the data contained in Figure 1.