ASIC
Australian Securities &
Investments Commission

Cyber resilience of firms in Australia's financial markets: 2020–21

Report 716 | December 2021

About this report

This report provides an update to Report 651 *Cyber resilience of firms in Australia's financial markets: 2018–19* (REP 651). 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. This is important for the financial markets sector, where the trust between an organisation and its clients is essential to its future.

In 2017 and 2019, we reported on the cyber resilience of firms operating in Australia's financial markets: see Report 555 *Cyber resilience of firms in Australia's financial markets* (REP 555) (cycle 1) and Report 651 *Cyber resilience of firms in Australia's financial markets: 2018–19* (REP 651) (cycle 2).

To allow ASIC to evaluate firms' cyber resilience, participants were asked to self-assess their firm's resilience against the National Institute of Standards in Technology (NIST) Cybersecurity Framework.

Participants were made up of a cross-section of organisations in Australia's financial markets, including stockbrokers, investment banks, market licensees, market infrastructure providers and credit ratings agencies.

In 2020 and 2021 (cycle 3), we asked participants to reassess their cyber resilience using the NIST Framework to measure their actual progress against their targets in previous cycles.

Results indicated that, while management of cybersecurity risk was steadily improving overall, there was still opportunity for improvement across the entire sector. The COVID-19 pandemic had a detrimental impact on planned improvements and investment was reprioritised to mitigate other emerging cyber risks.

Note: *This is a voluntary assessment and the number and type of participants has changed over the cycles.*

Key findings

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

The overall cyber resilience of firms operating in Australia's financial markets has remained steady, with a slight improvement of 1.4% overall. However, this falls short of the 14.9% improvement targeted by respondents for the period, and is also lower than the 15% improvement achieved between cycle 1 and cycle 2.

This shortfall can be attributed to:

- overly ambitious targets
- escalation in the threat environment
- reprioritisation due to the pandemic.

The pandemic has caused firms to reassess priorities and divert resources to firm up the resilience of critical business activity to:

- enable secure remote working at scale to ensure continuity of business operations
- focus on supply chain risks to ensure the delivery of products and services to customers.

Overall, cycle 3 saw improvements in the management of digital assets (7.2%), business environment (6.0%), staff awareness and training (4.7%), and protective security controls (4.5%).

90% of firms have strengthened user and privileged access management.

88% of firms are ensuring users are trained and aware of cyber risks—an important line of defence.

86% of firms have mature cyber incident response plans in place.

Small and medium-sized entities (SMEs) are continuing to close the gap on larger firms with an overall improvement of 3.5%.

In contrast, larger firms reported a slight drop in confidence of 2.2%. However, this comes off a strong base and can be attributed to large firms reassessing their response and recovery capabilities in light of:

- increased complexity of their business operating models
- a significant increase in threats to critical products and services reliant on third parties and supply chains.

The greatest gaps between large firms and SMEs are in supply chain risk management, cyber intrusion monitoring and detection, and recovery planning. Concerningly, we see no material improvements in supply chain risk management between cycle 2 and cycle 3, and the majority of firms identified this as an ongoing priority over the next period.

Cycle 3 saw credit rating agencies investing heavily in cyber resilience, triggered by the 2017 Equifax incident. While investment banks continue to set high targets for all NIST Framework categories.

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

22% of firms are developing more robust plans for effective hardware, software and information asset management.

Approach

The NIST Framework allows firms to assess their cyber resilience against five functions—*identify*, *protect*, *detect*, *respond* and *recover*—using a preparedness 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.

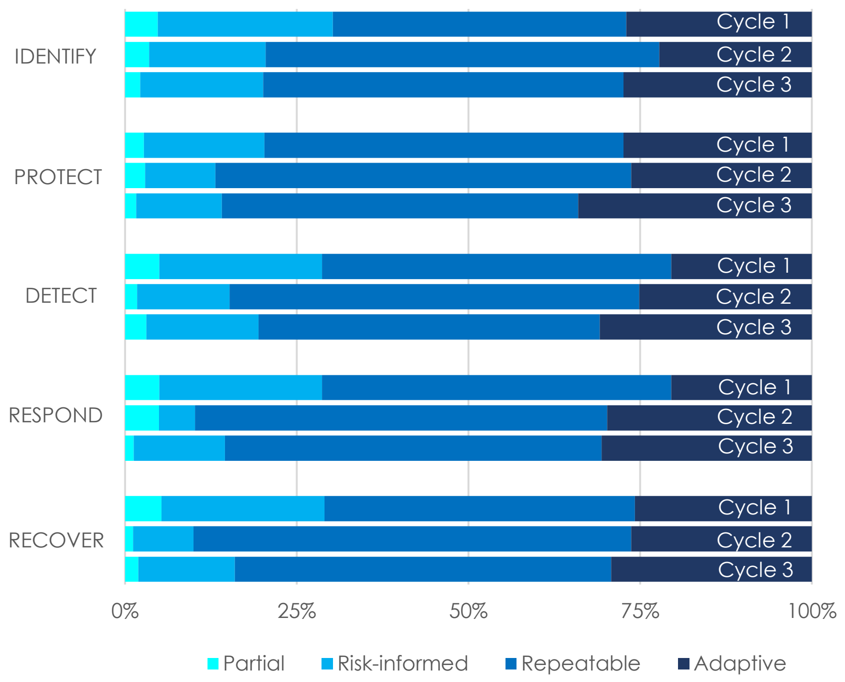
The **RESPOND** function identifies appropriate activities to minimise the impact of cybersecurity events.

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

Firms rate their cyber resilience functions using the partial, risk-informed, repeatable and adaptive scale.

● **Partial**	● **Risk-informed**	● **Repeatable**	● **Adaptive**
Policies and procedures are not formalised. Responses are reactive	Policies and procedures are rarely updated and not followed consistently	Policies and procedures are approved, followed and regularly updated	Policies and procedures evolve in response to changes in cybersecurity threats

Figure 1: Improvement in cyber resilience preparedness between cycles (by function)



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

Cyber resilience of SMEs

Identify

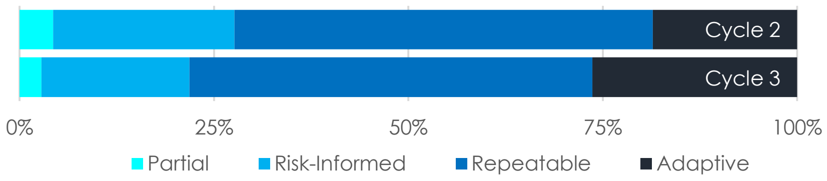
SMEs showed an overall increase of 6.4% across all cyber resilience functions, with the biggest change arising from a 12.4% improvement in understanding the business environment (including critical services and products, suppliers and potential threat actors).

Supply chain risk management showed almost no improvement since cycle 2 with 40.3% of SMEs assessing themselves as 'partial' or 'risk-informed'. However, it had the highest target improvement, at 19.4%.

SMEs assessed themselves as 'repeatable' or better in cybersecurity risk governance (84.2%), risk strategy (80.1%) and risk assessment (82.5%). This is good progress from cycle 2.

Supply chain risk management: 'Suppliers are not contractually obligated to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan'—*Partial*

'No testing is performed with suppliers—due to size & complexity of business there are no plans to perform at present'—*Partial*



Protect

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

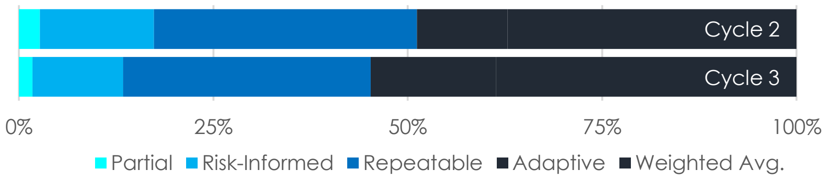
Cycle 3 showed an overall improvement of 4.7% against a target of 14.7%. A less ambitious target of 7.7% is planned for the next cycle.

Awareness and training (10.2%) and information protection processes (7.2%) make up the majority of this improvement. Data security remains the weakest category across SMEs, with 19.7% 'partial' or 'risk-informed'.

Protective measures are high on the list of priorities for all firms—SMEs plan to drive a 9.1% improvement on data security, and will continue to develop all other categories in this area equally.

Data security: 'Very basic protections are in place to protect against data leaks, however we recognise the need to enhance measures across the entire enterprise.'—*Risk-informed*

Training and awareness: 'Annual & onboarding awareness outlines the requirement of cyber security within everyone's roles. This is outlined in the corporate strategy.'—*Adaptive*



Detect

An undetected cyber intrusion can remove sensitive information or cause damage to an organisation's internal assets.

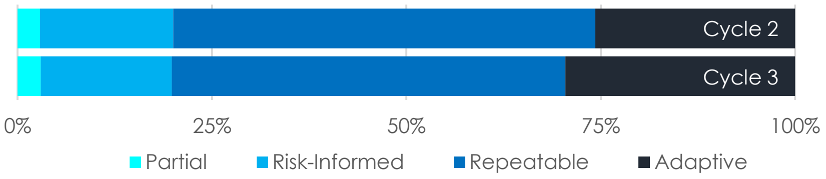
SMEs reported a 25% improvement in detection capabilities in cycle 2, but only a modest 1.5% increase in cycle 3—compared to an improvement target of 16.2% across all categories. This amounted to a small shift from 'repeatable' to 'adaptive' for 4% of SMEs.

Across the three categories within the detect function, almost 21% of SMEs rate themselves as 'partial' or 'risk-informed'. Over 10% of these firms plan to increase their capability to 'repeatable' or better in the next two years.

Detection processes: 'There is no predictive technology for detection. Corrective actions are only performed after an incident has occurred.'—*Partial*

Continuous monitoring: '… network has endpoint protection software that includes anti-malware and behaviour-based threat detection and prevention.'—*Repeatable*

'Traffic flows between major security zones of the network are defined and understood. Traffic logs are sent to the internal SIEM platform for traffic analysis and monitoring.'—*Repeatable*



Respond

An overall improvement of 3.7% was achieved across the respond function, falling short of the 12.9% target. Response planning (9.2%), forensic analysis (3.3%) and mitigation plans (4.1%) had the greatest increase.

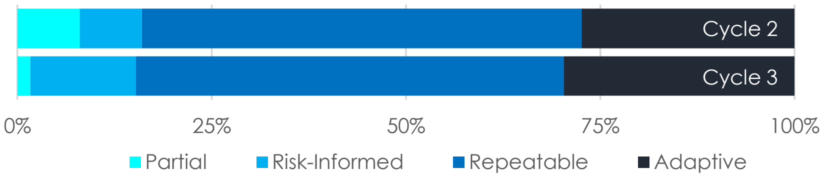
Over 32% of firms identified voluntary information-sharing arrangements as challenging or non-existent. A quarter (25%) of firms identified the ability to establish processes to receive and process cyber threat information as 'partial' or 'risk-informed'.

Response planning demonstrated a positive trend, with over 85% of firms rating their level as 'repeatable' or 'adaptive'.

The targets set by SMEs indicate the categories of greatest priority for the coming years. These are response planning, testing, and driving continuous improvements from lessons learned.

Communications: 'Small organisation. No formal policy in place but response plan activated by Technology Representative and documented as required.'—*Risk-informed*

Response planning: 'Incident responses process exist but is not formally documented—Cyber Incident Response Plan will be implemented in future.'—*Risk-informed*



Recover

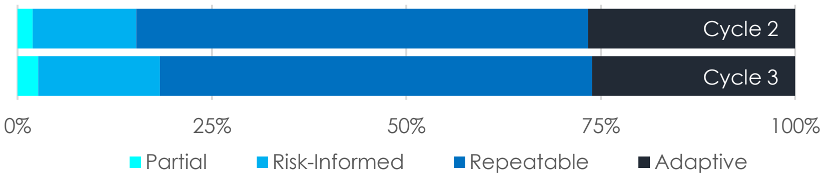
SMEs reported slightly lower confidence in their recovery capabilities. There was an increase in the number of firms identifying their recovery planning as 'partial' or 'risk-informed'—falling short of the 10% improvement targeted in cycle 2.

Recovery communications, particularly around managing reputational risk, is a concern for the 20% of firms that identified their level as 'partial' or 'risk-informed'.

Maintaining recovery strategies and plans to take account of ever-changing recovery scenarios continues to be a developing area.

Communications: 'Management will engage the Comms team where a cybersecurity incident is deemed to have potential PR impact. This is handled as a natural part of escalation for significant incidents.'—*Partial*

Continuous improvements: 'Response strategies are in place to enable us to respond to an attack, we are currently in the process of building detailed recovery strategies in the event that cyber-attacks are successful and all data is lost—Target to improve overall resilience/recovery against cyber-attack (e.g., ransomware).'—*Risk-informed*



Cyber resilience of large firms

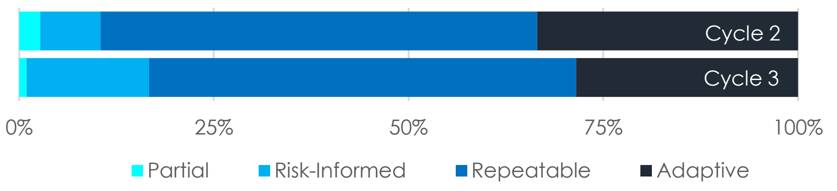
Identify

Firms expressed a drop in confidence of 3.4% for the identify function since cycle 2. This is due to the complexity of large firms, the breadth of services they offer, and the increase in cyber intrusions since cycle 2. However, firms have largely maintained strong cyber resilience.

Firms assessed themselves as 'repeatable' or better in the categories of cybersecurity risk governance (85.3%), risk strategy (88.1%) and risk assessment (85.3%)—a reduction in confidence since cycle 2.

Supply chain risk management continues to be a significant challenge, even for larger firms, with 22.9% rating themselves as 'partial' or 'risk-informed'. Firms are targeting a 16.9% improvement over the next 12 to 24 months.

Asset management: '… Software platforms and applications within the organization are inventoried. Management of inventories is not of uniform quality across technology stacks, with some technologies (such as Unix servers) being managed more robustly than others.'—*Risk-informed*



Protect

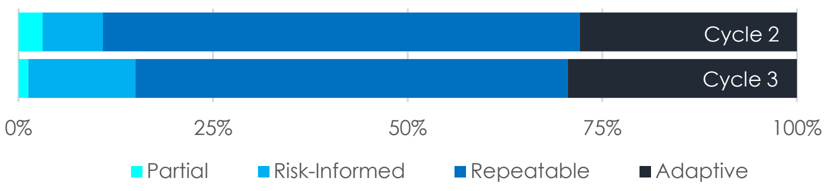
Large firms have long considered employees and suppliers an effective defence against cybersecurity events—and continuous improvements are evident in the responses to these categories.

Data security and protective technologies were priorities this cycle and will continue to be going forward—both with improvement targets of around 10% over the next 12 to 24 months.

Data security is reported to be the weakest area, with 20.6% of firms rating their level as 'partial' or 'risk-informed'. All other categories in this function are at least 85% 'repeatable' or 'adaptive'.

Data security: 'Very basic protections are in place to protect against data leaks, however we recognise the need to enhance measures across the entire enterprise—Continue to enhance measures to protect against data leaks.'—*Risk-informed*

Protective technologies: 'An access management process is in place to govern and manage the restriction of access to the network, services, and data. No access is granted beyond that which is required for a user to fulfill his or her responsibilities. Changes are deployed only by authorized personnel.'—*Adaptive*



Detect

The time taken from a cyber intrusion to its detection and remediation is a critical metric for many firms. Large firms have been maturing this capability over many years, more so than SMEs.

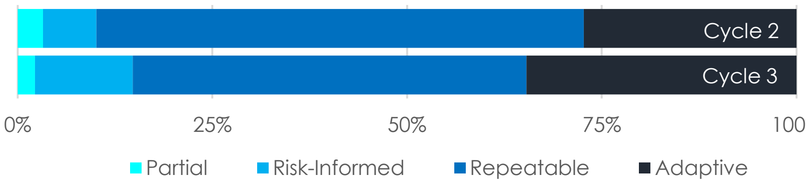
Over 85% of large firms rate their detect function as 'repeatable' or 'adaptive'. However, detection capabilities continue to be a priority because of the rapidly evolving nature of threats.

Anomalous events detection is considered the strongest category by many firms. Cyber intrusion detection processes are continuing to evolve, with 15.9% of large firms rating their level as 'partial' or 'risk-informed'.

Large firms have set targeted improvements equally across all three detect categories, at around 9% each—half of the target (18%) set in cycle 2.

Detection processes: 'Detection processes are continuously improved by our MDR service provider, and internal Information security team. Lessons learned from previous detections are used to update procedures/configurations.'—*Repeatable*

Anomalies and events detection: 'Events generated from the SIEM are based not only on raw thresholds being exceeded, but based on a combination of events or single events that may be an indicator of a successful or incoming attack against [*Firm*] systems.'—*Repeatable*



Respond

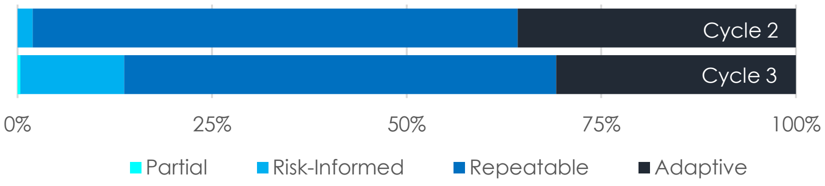
Firms reported lower confidence in all five respond function categories. This represents an average decline in confidence of 6% from cycle 2, compared to the 10.6% improvement originally targeted.

Around 15% of firms rated their response planning as 'partial' or 'risk-informed', compared to 0% in cycle 2. Forensic analysis saw a similar trend, with 18.2% of firms rating it as 'partial' or 'risk-informed', compared to 1.1% in cycle 2.

Large firms are still well positioned in their response capabilities. Many are 'repeatable' or better in response planning (85.3%) (including testing and improvements), and management of information sharing arrangements, coordination and forensic analysis (81.8%).

Response planning: 'Plans are supported by Cyber Playbooks covering specific scenarios known by the industry or where it has been deemed useful to pre-plan the incident response steps. The Playbooks are reviewed annually.'—*Repeatable*

Analysis of events: '… resources from across the organization who may assist in the investigation and remediation of the issue. In addition, a post-mortem analysis may be conducted during which ancillary risks are identified, prioritized, and assigned to appropriate departments.'—*Adaptive*



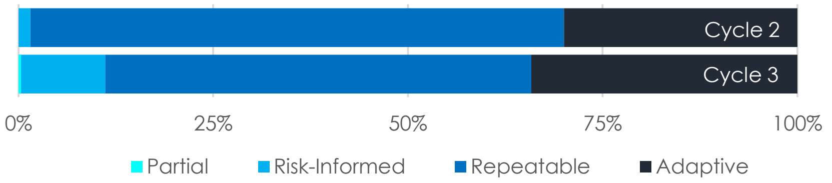
Recover

Firms reported slightly lower confidence in their ability to recover to full operational status following a cyber incident than in cycle 2. Indeed, the share of firms identifying as 'partial' or 'risk-informed' across all categories of the recovery function increased to 10%. This includes planning, continuous improvements and response communications.

Firms have been challenged in maintaining recovery protocols against the numerous emerging threat sources and types (e.g. ransomware has become prominent) since cycle 2.

Firms have identified maintaining recovery strategies, incorporating lessons learned to account for new and emerging risk scenarios, and maintaining the associated communications plans as the most challenging categories.

Recovery planning: 'The firm has a mature and comprehensive global Business Continuity Planning/ Disaster Recovery/ Incident Response program as it relates to infrastructure / application failures and data recovery. Based on the documented recovery plan multiple response teams are engaged as necessary based on the incident during and after the security incident. Playbooks remain current and are revised regularly.'—*Adaptive*



Supply chain risks

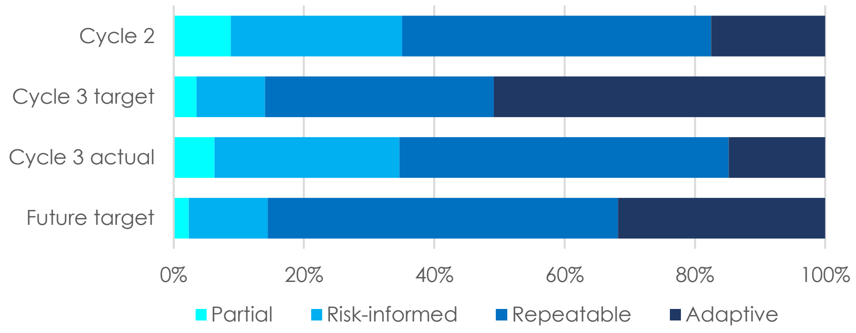
Thirty-five percent of firms report that more visibility is needed of supply chain and third-party risks

Some business leaders recognise outsourcing as essential to remaining competitive. Over time, these relationships become critical to a firm's success, increasing its risk exposure.

Firms reported supply chain risks as the area with the highest improvement target in cycle 2 (26.7%). However, our findings indicate no material improvements in cycle 3—and this remains a high priority over the next period.

Large firms continue to improve practices, while SMEs lag—40% of SME firms rate their supply chain risk management as 'partial' or 'risk-informed'.

Figure 2: Targeted and actual ratings of supply chain risk management

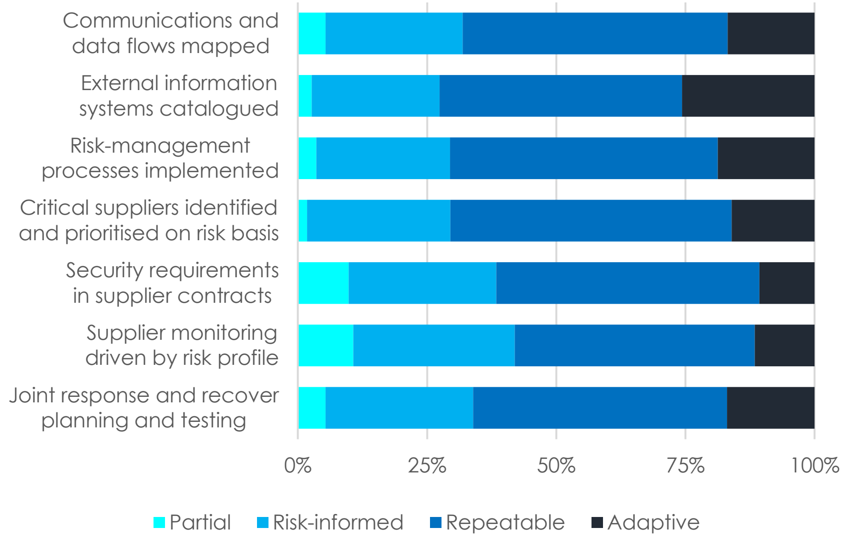


Note: See Table 2 for the data shown in this figure (accessible version).

Firms are improving their supplier management processes and prioritising suppliers based on risk. However, areas of challenge include:

- identifying details of information flows (31.8% of firms rated themselves as 'risk-informed' or 'partial')
- incorporating security requirements into supplier contracts (38.4% of firms rated themselves as 'risk-informed' or 'partial')
- adequate supplier monitoring to maintain visibility of risks (42% of firms rated themselves as 'risk-informed' or 'partial') (see Figure 3).

Figure 3: Ratings for key areas of supplier management processes



Note: See Table 3 for the data shown in this figure (accessible version).

Good practices

Some of the good practices identified in this cycle include:

- assessing suppliers and monitoring them for risks
- mapping critical information and data flows
- incorporating security requirements into supplier contracts.

Supplier assessment and risk monitoring

Good practice: Critical suppliers are treated similarly to internal threats, attracting equal levels of scrutiny. These suppliers are incorporated into risk governance frameworks and standards—and are monitored based on their risk profile and ability to affect the firm's service delivery.

What we found: Some firms reported they had no formal monitoring processes for suppliers, but recognised the need to develop structured processes to manage this risk. Some declared confidence in their suppliers to manage cyber risks, or relied on attestations from some of their larger suppliers.

Many firms have initiated third-party supplier management programs that are in their infancy, and are investing in building up their capability in this area over the next period.

The more mature firms report that all critical service providers are subject to an independent annual audit.

Mapping critical information and data flows

Good practice: Information and data flows for internally and externally managed systems are documented using tools that enable easy maintenance and regular risk reviews. These reviews inform the overall risk profile of suppliers.

What we found: Firms are clearly aware of the need for visibility and effective risk management in this area. They reported initiatives that are underway and further progress planned over the next period.

Security requirements incorporated into supplier contracts

Good practice: A minimum set of security requirements incorporated into supplier contracts, including periodic assessments performed by the firm or external assessors.

What we found: A few firms reported that suppliers were not required to implement any security controls. Some reported that cybersecurity requirements are not specifically incorporated into supplier arrangements, but were assessed periodically. Many reported that some, but not all, contracts incorporated security requirements; these firms had plans in place to increase their coverage as contracts come up for renewal.

The more mature firms have a minimum set of security requirements stipulated within contracts with all critical suppliers.

Appendix: Accessible version of figures

This appendix is for people with visual or other impairments. It provides the underlying data for figures in this report.

Table 1: Improvement in cyber resilience preparedness between cycles (by function)

Function and cycle		Partial	Risk-informed	Repeatable	Adaptive	Total
Identify	Cycle 1	4.7%	25.5%	42.7%	27.0%	100.0%
	Cycle 2	3.5%	17.0%	57.3%	22.2%	100.0%
	Cycle 3	2.2%	17.9%	52.5%	27.4%	100.0%
Protect	Cycle 1	2.7%	17.5%	52.3%	27.4%	100.0%
	Cycle 2	2.9%	10.2%	60.5%	26.3%	100.0%
	Cycle 3	1.6%	12.5%	51.9%	34.0%	100.0%
Detect	Cycle 1	5.0%	23.7%	50.9%	20.5%	100.0%
	Cycle 2	1.8%	13.5%	59.7%	25.2%	100.0%
	Cycle 3	3.1%	16.3%	49.7%	30.9%	100.0%
Respond	Cycle 1	5.0%	23.7%	50.9%	20.5%	100.0%
	Cycle 2	4.9%	5.3%	60.0%	29.8%	100.0%
	Cycle 3	1.2%	13.3%	54.8%	30.6%	100.0%
Recover	Cycle 1	5.3%	23.7%	45.2%	25.8%	100.0%
	Cycle 2	1.2%	8.8%	63.7%	26.3%	100.0%
	Cycle 3	1.9%	14.1%	54.8%	29.2%	100.0%

Note: This is the data contained in Figure 1.

Table 2: Targeted and actual ratings of supply chain risk management

Cycle	Partial	Risk-informed	Repeatable	Adaptive	Total
Cycle 2	8.8%	26.3%	47.4%	17.5%	100.0%
Cycle 3 target	3.5%	10.5%	35.1%	50.9%	100.0%
Cycle 3 actual	6.3%	28.4%	50.5%	14.8%	100.0%
Future target	2.3%	12.1%	53.8%	31.8%	100.0%

Note: This is the data contained in Figure 2.

Table 3: Ratings for key areas of supplier management processes

Key area	Partial	Risk-informed	Repeatable	Adaptive	Total
Communications and data flows mapped	5.3%	26.6%	51.3%	16.8%	100.0%
External information systems catalogued	2.7%	24.8%	46.9%	25.7%	100.0%
Risk-management processes implemented	3.6%	25.9%	51.8%	18.8%	100.0%
Critical suppliers identified and prioritised on risk basis	1.8%	27.7%	54.5%	16.1%	100.0%
Security requirements in supplier contracts	9.8%	28.6%	50.9%	10.7%	100.0%
Supplier monitoring driven by risk profile	10.7%	31.3%	46.4%	11.6%	100.0%
Joint response and recover planning and testing	5.4%	28.6%	49.1%	17.0%	100.0%

Note: This is the data contained in Figure 3.