Spotlight on cyber: Findings and insights from the cyber pulse survey 2023

Report 776 | November 2023

About this report

This report outlines key findings from the ASIC cyber pulse survey 2023. It summarises important trends, identifies areas for improvement and highlights better practices with practical examples.

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 particular rules or requirements.

Executive summary

A cyber attack can disrupt an organisation's operations and result in significant financial, legal and reputational harm that can quickly spread beyond a single entity. Recent high-profile cyber incidents have highlighted the need for all organisations to have robust cyber capabilities.

The Australian Securities and Investments Commission (ASIC) developed the cyber pulse survey 2023 (survey) to better understand the cyber maturity of regulated organisations in this ongoing heightened threat environment.

The anonymous, voluntary survey was designed to help organisations assess their cyber resilience and allow them to benchmark their cyber maturity against their peers.

The survey measured participants' ability to:

- govern and manage organisation-wide cyber risks
- identify and protect information assets that support critical services, and
- detect, respond to and recover from cyber security incidents.

Ninety-five per cent of survey participants elected to receive an individual report with insights on how they assessed their cyber resilience capability compared to similar organisations in their industry. Individual feedback reports measured a participant's cyber maturity compared to their peers across six functions, with each function given a weighted average maturity score based on the organisation's responses. These scores were reported against the average weighted score for each function across an organisation's selected industry and size.

ASIC has previously conducted cyber self-assessment surveys of firms operating in Australia's financial markets: see Report 555 *Cyber resilience of firms in Australia's financial markets*, Report 651 *Cyber resilience of firms in Australia's financial markets: 2018–19* and Report 716 *Cyber resilience of firms in Australia's financial markets: 2020–21*.

While previous ASIC surveys were restricted to the financial markets sector, the 2023 survey invited participation from public companies, large proprietary companies and entities that hold licences or authorisations from ASIC. Other industry or government surveys of organisational cyber resilience have generally been limited to organisations of a certain size, within a specific industry or sector, or of a particular entity type. The 2023 survey was open to organisations across a broad range of sectors, entity types and sizes.

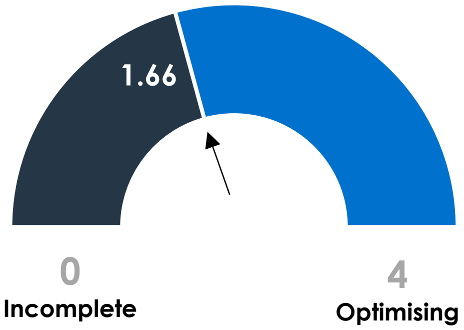
The findings from the survey will help ASIC identify gaps within certain sectors, guide initiatives and work with industry to uplift cyber resilience.

> 'There is a need to go beyond security alone and build up resilience – meaning the ability to respond to and recover from an incident. It's not enough to have plans in place. They must be tested regularly.'
>
> – Chair Joseph Longo

Key findings

The cyber pulse survey 2023 (survey) has exposed gaps in cyber security risk management of critical cyber capabilities. With a weighted average participant cyber maturity score of 1.66 (on a scale of 0 to 4), the results indicate organisations are reactive rather than proactive when it comes to managing their cyber security.

Figure 1: Weighted average cyber maturity score



About the survey

The voluntary survey was completed by 697 participants with representation across different organisation sizes, types, sectors and subsectors. The findings represented in this report need to be considered in light of participating organisations' demographics: see Appendix A for a breakdown of participants by organisation size, type, sector and subsector.

The survey was designed to assess participants' cyber resilience against six functions: governance and risk management, identifying information assets, protecting information assets, detecting cyber security events, responding to cyber security incidents, and recovering from cyber security incidents. The questions within each function were divided into 12 distinct cyber risk categories.

Participants were asked to answer each question based on their assessment of their organisation's cyber capability maturity, ranging from no existing capability (incomplete, 0) through to advanced capability with policies and procedures that evolve over time (optimising, 4). See Appendix B for more information on the methodology.

What the survey responses showed

Medium and large organisations consistently self-reported more mature cyber capabilities than small organisations. Small organisations lagged behind in supply chain risk management, data security, and consequence management.

According to the survey results, 42% of the participants held an Australian financial services (AFS) licence. However, a significant number of respondents did not identify as belonging to any sector.

What organisations consider to be the **top cyber security threat** to the continued operation of the organisation

26% Phishing

17% Ransomware

13% Business email compromise

What organisations are doing well

- Identity and access management
- Governance and risk management
- Information asset management

The top four areas for improvement

1. Supply chain risk management
2. Data security
3. Consequence management
4. Adoption of cyber security standards

The survey responses also showed that:

- **44% do not manage third-party or supply chain risk.**

Organisations should consider the risks introduced by external third parties. These parties could be vendors, suppliers, partners, contractors or service providers with access to an organisation's internal or confidential information.

Third-party relationships provide threat actors with easy access to an organisation's systems and networks. An organisation can implement robust cyber security measures for its internal networks and IT infrastructure. However, unless these efforts are extended to third parties, it will be exposed to supply chain vulnerabilities.

- **58% have limited or no capability to protect confidential information adequately.**

Ransomware threat actors target confidential information. To limit the impact of cyber breaches, organisations should identify, classify and secure confidential information – and limit what is stored.

To protect confidential information from unauthorised disclosure, alteration or destruction, organisations should classify information based on risk exposure in the event of a breach and implement cyber risk controls proportionate to the classification of the data.

- **33% do not have a cyber incident response plan.**

A well-defined cyber incident response plan ensures that an organisation can quickly and effectively respond if its cyber security measures fail to prevent an incident. Regularly testing and updating the plan is necessary to maintain its effectiveness.

An effective response plan should be consistent with an organisation's protocols for incident, emergency, crisis and business continuity management. It should also identify regulatory reporting obligations and interactions with critical third parties.

- **20% have not adopted a cyber security standard.**

Cyber security standards and frameworks help organisations to improve their cyber security and resilience by taking a comprehensive approach to:

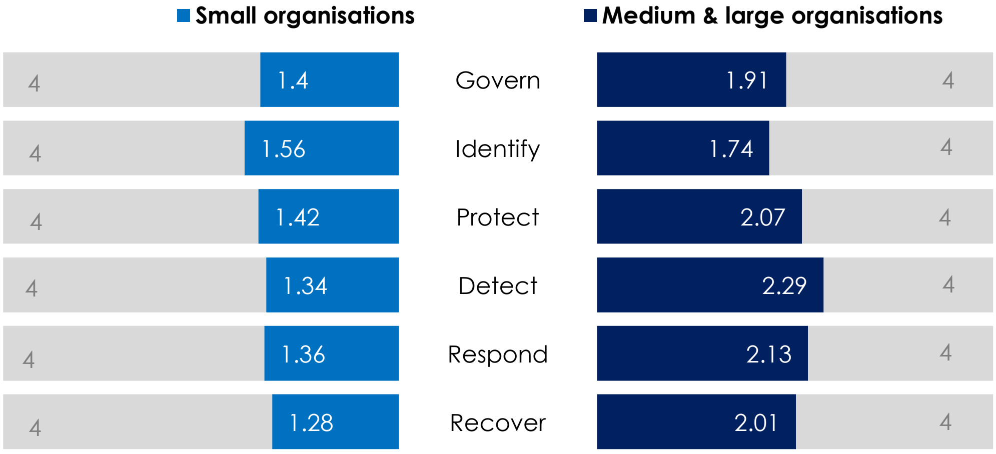
- identifying and managing cyber risk
- protecting confidential information
- mitigating and managing cyber threats, and
- guiding appropriate investment in cyber security.

An organisation should adopt and implement a cyber security standard that is proportionate to the nature, size and complexity of the organisation.

Implementing a cyber security standard begins with a cyber risk assessment and identification of gaps in cyber risk management.

Small organisations

Figure 2: Weighted average cyber maturity score by function for small vs medium and large organisations



Note: See Table 10 for the data shown in this figure (accessible version).

Considering small organisations are regularly required to manage competing priorities with limited financial and human resources, it's unsurprising that they consistently reported a lower level of cyber maturity capability than medium and large organisations. For many small organisations, outsourcing is essential to managing cyber risk. These relationships can become critical to their success. Responses to the survey indicate that:

- **34%** of small organisations do not follow or benchmark against any cyber security standard
- **44%** do not perform risk assessments of third parties and vendors
- **33%** have no or limited capability in using multifactor authentication
- **41%** do not patch applications
- **45%** do not perform vulnerability scans, and
- **30%** do not have backups in place.

Attackers extort organisations by infiltrating systems, installing malicious software, deploying ransomware, rendering systems unavailable and, ultimately, exfiltrating confidential information. Examples include:

- **exploiting unpatched and known vulnerabilities** to remotely access systems
- tricking employees (through **phishing** or other means) into opening a Microsoft Office attachment containing a macro that installs malicious software, allowing an attacker to access systems

- **installing malicious software** to extract usernames and passwords, move between systems and gain access to confidential information.

Essential Eight strategies for preventing cyber security incidents

The Australian Signals Directorate (ASD)'s Australian Cyber Security Centre (ACSC)'s *Essential Eight* can help small organisations enhance their cyber security and mitigate cyber attacks. Strategies may include:

- Creating, implementing and managing a **whitelist of approved applications**.
- Implementing a process to regularly update and **patch systems, software and applications**.
- **Disabling macros in Microsoft Office applications** unless specifically required. Training employees not to enable macros in unsolicited email attachments or documents.
- **User application hardening** by ensuring web browsers are configured securely to block malicious content. Only using necessary browser extensions and keeping them updated.
- Restricting **administrative privileges** to those who need them.
- Setting up automatic updates for **patching operating systems**.
- Using strong, unique passwords and enabling **multifactor authentication**.
- Conducting **daily backups** of critical data and isolating backups from your network.

In addition to the *Essential Eight* strategies, small organisations could consider:

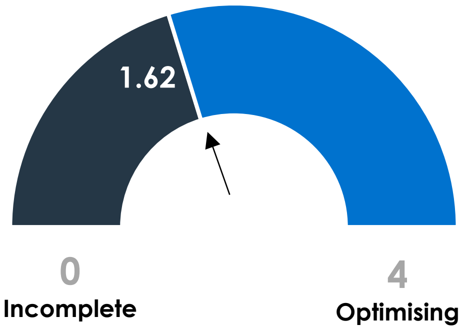
- educating employees about cyber security best practices
- developing a cyber incident response plan and enforcing cyber security policies and procedures
- conducting regular security assessments and vulnerability scans
- assessing the cyber security practices of third-party vendors
- implementing thorough background and reference checks when hiring, and
- implementing robust monitoring and logging solutions to detect and respond to suspicious activities on networks.

For more information and resources to help small organisations enhance their cyber security, visit the Small business section of the ASD's ACSC website.

Governance and risk management

The governance and risk management function assessed participants' ability to govern and manage organisation-wide cyber risks.

Figure 3: Weighted average cyber maturity score for governance and risk management



Participants exhibited strong capabilities in:

- understanding their cyber risk landscape
- managing cyber risk in line with their organisation's risk management framework, and
- monitoring physical vulnerabilities and threats to information assets.

However, there are opportunities for uplift in:

- defining cyber security roles and responsibilities
- complying with regulatory obligations, and
- identifying and prioritising vulnerabilities to information assets.

Red flags: Third-party risk management

A concerning 69% of participants indicated they had minimal or no capabilities in supply chain and third-party risk management. In particular, 58% of participants indicated they do not test cyber security incident responses with critical suppliers. Red flags include:

- the board and leadership lacking visibility of third-party risks
- failing to conduct due diligence and ongoing risk assessments before partnering with a third party
- third parties that are unwilling to provide information about their own cyber security
- third parties that are unable to confirm the protection of confidential information
- allowing third parties access to critical business systems without multifactor authentication
- failing to regularly review third-party access to systems, and
- third parties that do not conduct independent cyber risk assessments of their environment.

Case study 1

Failure to manage third-party risks may expose organisations to cyber attacks through vendors.

Since the disclosure of the Progress MOVEit Software vulnerability on 31 May 2023, the cybercriminal group, Clop, have exploited the vulnerability and used it to target a wide-ranging number of organisations across multiple industries and geographies, including human resource providers, the British Broadcasting Corporation and various overseas government agencies.

Better practices

An effective cyber security strategy – and governance and risk framework – should help identify, manage and mitigate cyber risks within the risk tolerance set by management and the board.

The design, implementation and effectiveness of a framework or standard must be set from the top and monitored by the organisation's leadership. Leaders should be well informed about the organisation's key cyber risks, implications of cyber control failures (including response arrangements) and status of cyber controls.

Organisations should:

- conduct third-party risk assessments and due diligence
- establish clear contractual obligations with third parties – including specific cyber security requirements – and implement continuous monitoring and incident response protocols
- foster a culture of cyber security awareness through employee education and training
- ensure all confidential information shared with third parties is protected
- implement fundamental security measures, including access controls, multifactor authentication and encryption protocols to protect confidential information from unauthorised access – especially if third parties have access to systems containing confidential information
- regularly review data handling processes to help identify and address third-party vulnerabilities, and
- conduct simulated cyber-attack exercises to evaluate the effectiveness of cyber incident response plans with third parties – and refine procedures in response to these exercises.

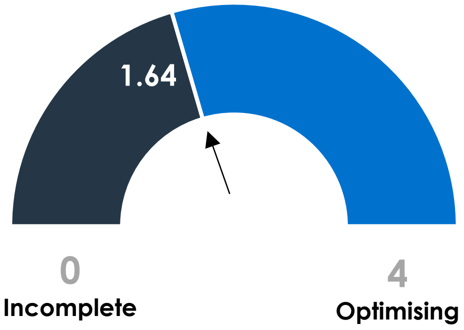
Small organisations should consider:

- engaging a cyber security expert to evaluate the organisation's key cyber risks and implement an appropriate security standard
- strengthening their cyber defences and implementing proportional cyber risk controls while efficiently managing their cyber security investments
- adopting risk management practices that prioritise critical assets, key cyber risks and potential threats, and
- ensuring limited resources are used efficiently to protect against cyber threats that have the potential to impact their operations (e.g. by outsourcing their cyber security functions to specialised providers to allow access to expert knowledge and advanced technologies).

Identify information assets

The identify function measured participants' ability to identify information assets that support critical business services.

Figure 4: Weighted average cyber maturity score for identifying information assets



Participants demonstrated well-developed capabilities in:

- identifying critical business services and their dependencies, and
- identifying and prioritising their information assets.

However, 70% of participants showed minimal to no capabilities in mapping information flows between their information assets. Mapping information flows helps an organisation identify risks from potential weaknesses, redundancies or single points of failure.

Visualising potential risks associated with critical business services allows an organisation to determine the security controls needed to mitigate those risks and protect the system overall.

Failure to map information flows between critical business services may lead to distributed and unprotected confidential information. Critical business systems rely on the distribution, storage and processing of information. Without a clear view of the flow of information an organisation would not be able to determine the appropriate level of protection.

Better practices

Proactive identification of critical business services and dependencies – including information assets – helps organisations to identify and mitigate risks and respond efficiently to potential incidents.

Mapping the flow of information can enable an organisation to:

- identify vulnerabilities by understanding how data moves between systems
- assess the risks associated with data movement and prioritise protection of confidential information
- define access controls and permissions, preventing unauthorised access to critical systems and confidential information

- identify the source and scope of a cyber breach, contain it, and mitigate the damage
- enable early detection of potential threats or attacks by triggering alerts when there is a deviation from established information flow patterns, and
- use information flow maps to help employees understand the importance of data security, their role in protecting information, and how their actions can impact the organisation's cyber security.

Mapping information flows is not a one-time task – it should be an ongoing process. Regularly updating and refining information flow maps can help organisations adapt to changes in technology and the threat environment.

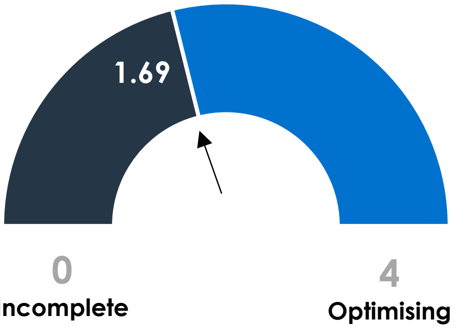
How to: Map information flows between critical business services

- Define and document business services critical to your organisation’s operations.
- Identify dependencies for each critical business service to understand which systems, applications and networks support them.
- Identify, classify and catalogue your organisation’s confidential information. Develop detailed information flow maps illustrating how confidential information moves within your organisation.
- Conduct a comprehensive risk assessment for each information asset and confidential information flow.
- Classify the impact of the loss of confidentiality, integrity and availability.
- Evaluate the likelihood of potential threats and vulnerabilities. Measure the risk of a threat by estimating the likelihood of the threat exploiting a vulnerability and the impact of any harmful consequences.
- Prioritise information assets based on their criticality to the business and the identified risk.
- Implement security measures proportionate to the risk to each critical business service and its confidential information flows.

Protect information assets

The protect function evaluated participants' ability to protect information assets that support critical business services.

Figure 5: Weighted average cyber maturity score for protecting information assets



Identity and access management had the highest average category score across all 12 categories, with participants expressing confidence in managing user and administrative privileges, using multifactor authentication, protecting their network, and providing cyber security awareness training.

However, from a data security perspective, two-thirds of participants indicated they had limited or no capability to protect their confidential information. The results also showed that:

- 29% of participants do not encrypt confidential information
- 31% of participants do not have controls to prevent unauthorised transmission of confidential information, and
- 40% of participants do not manage their data destruction.

Red flags: Confidential information

Red flags relating to limited protection of confidential information include:

- assuming the default settings on software or systems provide sufficient security
- having inconsistent or poorly enforced password policies across the organisation, allowing use of default passwords on systems, and not monitoring weak or compromised passwords
- not implementing mechanisms to limit data leakage
- allowing employees to transmit confidential information externally without restrictions
- turning off security features on communication tools or email systems without a risk assessment
- failing to educate employees about the importance of data security and the risks of unauthorised data transmission
- allowing data to accumulate indefinitely without a data retention and destruction policy, not implementing secure data destruction (e.g. shredding physical documents or securely erasing digital data), and failing to assign responsibility for data destruction, and
- assigning privileges to users or service accounts beyond their requirements.

Case study 2

Failure to protect information assets may lead to data breaches and business disruption.

On 19 July 2019, Capital One suffered an incident leading to breach of personal information about its credit card customers and individuals who had applied for credit card products. Impacted information included customer status data such as credit scores, credit limits, balances, payment history and contact information. This event affected approximately 100 million individuals in the United States and approximately 6 million in Canada.

Better practices

Encryption of confidential information

To ensure encryption of confidential information, consider:

- establishing data encryption policies that mandate encryption of high-risk confidential information in transit and at rest, and ensuring these policies cover all relevant systems and communication channels, and are proportionate to the data classification
- using robust encryption algorithms and industry-recognised encryption standards to protect confidential information, and
- implementing management practices to generate, store and distribute encryption keys securely.

Prevention of unauthorised transmission

Organisations can reduce unauthorised transmission of data by:

- considering data leakage solutions that monitor and prevent unauthorised transmission of confidential information, and configure policies to detect and block confidential information transfers
- implementing network segmentation to restrict movement of confidential information (e.g. firewall rules and network access controls to limit data flows and user access to authorised systems)
- enhancing email security with email filtering, content scanning and outbound controls to prevent transmission of confidential information
- implementing secure file transfer protocols and solutions for sharing confidential information within and outside the organisation
- disabling outgoing Secure File Transfer Protocol/File Transfer Protocol (SFTP/FTP) and Secure Copy Protocol (SCP), and other protocols, used by threat actors to exfiltrate data
- preventing unauthorised software execution by whitelisting allowed business applications
- reviewing the network and file shares for clear text or configuration files containing usernames and passwords, and
- educating employees about the risks of unauthorised data transmission and providing guidance on secure data-sharing practices.

Data destruction management

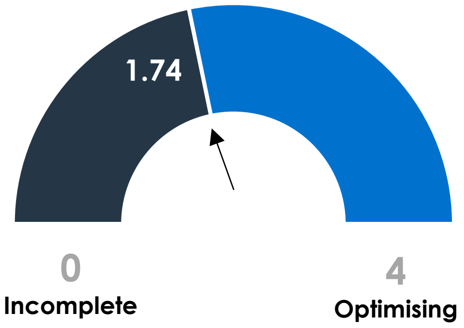
Better practices for effective data destruction management include:

- developing and enforcing a data retention policy that specifies how long data should be retained and when it should be securely destroyed
- using secure data destruction methods appropriate to the data type and media (e.g. shredding physical documents, degaussing magnetic media and securely erasing digital data)
- establishing data destruction procedures for secure disposal of data
- considering reputable third-party data destruction services for physical media, and
- conducting regular audits and inspections of data destruction processes to verify effectiveness.

Detect cyber security events

The detect function assessed participants' ability to detect cyber security incidents and events.

Figure 6: Weighted average cyber maturity score for detecting cyber security events



The detect function had the highest average participant score across all functions. This was driven by well-developed capabilities in monitoring network activity and patching information assets.

Despite the high maturity in this function's capabilities, almost one in three participants admitted to failing to perform vulnerability scans of assets. A substantial proportion also showed limited capabilities in:

- monitoring for unauthorised connections, devices and software
- baselining normal network activity
- performing vulnerability scans, and
- patching information assets.

Red flags: Detecting cyber security incidents and events

Red flags relating to detecting cyber security incidents and events include:

- poor capabilities in monitoring, vulnerability scans and patching information assets, which can enable a threat actor to compromise an organisation and prevent it from determining whether an active attacker is resident within its systems, and
- failing to apply patches or perform vulnerability scans, which can cause an organisation to have minimal or no visibility over potential entry points for an attacker.

Failure to detect a bad actor in your systems may increase the disruption to your business-critical services and cause harm to your customers.

Case study 3

Hackers targeted SolarWinds in September 2019 by deploying malicious code into its Orion IT monitoring and management software, which is used by thousands of organisations and government agencies worldwide. The attackers went undetected for a significant amount of time. They were eventually detected by baselining normal network activity and monitoring for unauthorised connections using extensive monitoring techniques.

Better practices

Monitoring for unauthorised connections, devices and software

Better practices for monitoring for unauthorised connections, devices and software include:

- implementing intrusion detection system tools that continuously monitor network traffic for suspicious or unauthorised connections and send an alert when unusual activities are detected
- implementing endpoint detection and response solutions that monitor and detect unauthorised devices and software, provide real-time visibility into endpoint activities and flag anomalies
- implementing user and entity behaviour analytics solutions that analyse patterns and identify deviations from normal behaviour that could indicate unauthorised access or compromised accounts
- developing a well-defined cyber incident response plan that outlines procedures for responding to unauthorised connections or intrusions, including containment and mitigation strategies, and
- establishing continuous monitoring practices to detect and respond to unauthorised activities promptly, including regular log reviews and alerts from security tools and devices.

Baselining normal network activity

Better practices for baselining normal network activity include:

- implementing network traffic analysis tools to establish a baseline of normal network activity and help identify deviations and anomalies, and
- regularly reviewing and updating the baseline as network and application configurations change to reflect evolving business needs.

Performing vulnerability scans

Better practices for performing effective vulnerability scans include:

- using automated vulnerability scanning tools to regularly scan networks, systems and applications for vulnerabilities

- prioritising vulnerabilities based on assessment of risk severity and potential organisational impact
- establishing a formal vulnerability management process for identifying, assessing, remediating and tracking vulnerabilities
- coordinating vulnerability scans with a patch management process to ensure identified vulnerabilities are patched promptly, and
- maintaining records of vulnerability scans, assessment results and actions to address vulnerabilities for auditing and compliance purposes.

Patching information assets

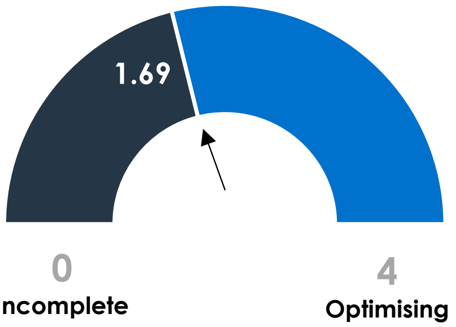
Better practices for ensuring adequate patching of information assets include:

- developing a clear, documented patch management policy that outlines roles, responsibilities and procedures for applying patches
- prioritising and applying timely critical security patches, especially for systems and applications that handle confidential information
- patch testing in a controlled environment to ensure they do not disrupt critical business processes or introduce new issues
- considering automated patch management solutions to streamline the patching process and reduce the risk of human error, and
- continuously monitoring for new patches and updates – and incorporating them into the patch management program as they become available.

Respond to cyber security incidents

The respond function assessed participants' ability to respond to cyber security incidents.

Figure 7: Weighted average cyber maturity score for responding to cyber security incidents



Most participants indicated well-developed capabilities in investigating cyber security incidents, using external threat intelligence sources, and conducting root cause analysis.

While these results are encouraging, almost one in five admitted to not investigating a cyber security incident and 13% did not seek to understand the root cause of an incident. In addition, several participants indicated they are not proactive in their approach to cyber incident response plans with:

- 33% not having a cyber incident response plan, and
- 35% not testing their response plan.

A failure to develop and implement a cyber incident response plan can expose an organisation to potential data breaches, system outages and reputational damage. Without an adequate plan, a reactive approach to cyber security incidents is likely to result in poor communication, inadequate responses, confusion and delays.

It is essential to consistently test cyber incident response plans to ensure their ongoing effectiveness. A response plan that is not tested may not adapt to evolving threats and technologies, rendering it less effective or obsolete over time.

Case study 4

Not having a tested response plan in place will negatively impact an entity's ability to respond to a cyber incident.

In November 2016, attackers emailed Uber's security chief and told him they had stolen a large amount of data, which they would delete in return for a ransom, according to the US Department of Justice. Uber's security chief confirmed that data, which included the records of 57 million Uber users and 600,000 driving licence numbers, had been stolen.

The Uber security chief arranged for the hackers to be paid $100,000 in exchange for them signing non-disclosure agreements to not reveal the hack to anyone. A jury in San Francisco found the Uber security chief guilty of obstruction of justice and concealing a felony.

Better practices

Leadership and sponsorship

Better practices include:

- ensuring there is executive leadership buy-in and sponsorship of the cyber incident response plan because a clear commitment from senior management is essential for its success, and
- including members from IT, legal, compliance, public relations and other relevant business units in incident response teams, and clearly defining their roles and responsibilities.

Incident classification

Better practices include:

- establishing a clear classification system for potential incidents based on severity and impact, and
- defining criteria for each classification level to guide response actions.

Incident detection and reporting

Better practices include:

- developing clear procedures for containing incidents to prevent further damage and eradicate the root cause
- defining isolation measures and strategies for removing threats
- establishing a communication plan that outlines who should be informed during an incident, internally and externally
- ensuring compliance with data breach notification obligations and regulations
- emphasising the importance of thoroughly documenting incident details, actions taken and evidence preservation for forensic purposes
- providing regular training and awareness programs to educate employees about the incident response plan and their roles during an incident, and
- reporting incidents to the ASD's ACSC and seeking technical support from them if required.

Incident response plan testing

Better practices include:

- conducting tabletop exercises or simulated incident scenarios regularly, including involving the incident response team and stakeholders to practise decision making and coordination
- creating different incident scenarios to test the organisation's ability to respond effectively, ranging from common to advanced threats
- gathering feedback from participants after each exercise to identify strengths and weaknesses, and then using this feedback to improve the cyber incident response plan and processes

- after an incident, conducting a thorough post-incident review to analyse what worked well and what needs improvement, with these insights used to further refine the incident response plan, and
- providing ongoing training and skill development for the incident response team to ensure they stay current with evolving threats and technologies.

Third parties

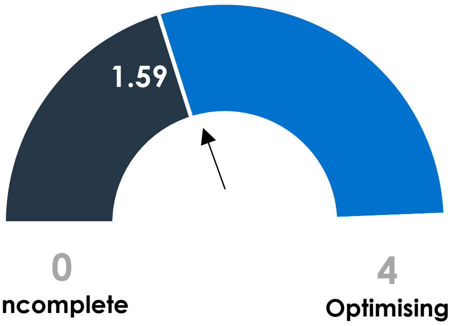
Better practices include:

- considering engagement of a third party to independently assess the effectiveness of the cyber incident response plan, and
- considering critical third-party suppliers in incident response plans and testing exercises.

Recover from cyber security incidents

The recover function assessed participants' ability to recover from cyber security incidents.

Figure 8: Weighted average cyber maturity score for recovery from cyber security incidents



Fifty-two percent of participants indicated strong capabilities in recovery planning, with 59% confirming they incorporate lessons learned in their cyber incident response plans.

However, one in three participants indicated they do not have strategies for dealing with the repercussions of a cyber security incident, signalling opportunities for significant improvement in consequence management. Exfiltration of confidential information and disruption of critical business systems using ransomware are the primary currency of extortion for financially motivated threat actors.

Case study 5

Not having the ability to recover from a major incident will negatively impact an organisation's ability to restore operations after a cyber incident.

Travelex, a foreign exchange firm, collapsed into administration seven months after it was crippled by ransomware. The firm suffered more than a month of disruption after it discovered it had been attacked on 31 December 2019. It was later reported that the REvil ransomware gang encrypted more than 5GB of sensitive data and demanded $6 million for its return.

Better practices

Better practices include:

- transparent communication with all stakeholders, including updates on recovery progress
- offering support and resources to affected individuals, customers and partners to help them recover from the incident and rebuild their trust
- implementing a reputation management plan to show the organisation's commitment to security
- working with government to reduce the impact of the incident by consulting with regulators and complying with inquiries, and
- incorporating lessons learned into cyber security frameworks and incident response plans.

How to report a cyber security incident

- Report cybercrime, incidents or vulnerabilities to the ASD’s ACSC.
- When personal information has been breached, notify the Office of the Australian Information Commissioner (OAIC).
- Notify ASIC and/or the Australian Prudential Regulation Authority (APRA) in the event of a cyber security incident.
- Alert individuals as soon as possible after a potential breach of their personal information.

Appendix A: Participants by organisation size, type, sector and subsector

Table 1: Average maturity across functions

Function	Small average	Medium/large average	Weighted function average
Governance	1.54	1.96	1.62
Identify	1.52	1.58	1.64
Protect	1.41	1.97	1.69
Detect	1.31	2.11	1.74
Respond	1.34	1.94	1.69
Recover	1.24	1.90	1.59

Table 2: Weighted maturity distribution by function

Function	Tier 0	Tier 1	Tier 2	Tier 3	Tier 4
Governance	17%	26%	21%	15%	20%
Identify	13%	43%	18%	13%	12%
Protect	20%	26%	25%	13%	16%
Detect	22%	23%	19%	14%	21%
Respond	21%	27%	18%	17%	17%
Recover	20%	32%	20%	12%	16%

Table 3: Weighted maturity distribution by category

Category	Tier 0	Tier 1	Tier 2	Tier 3	Tier 4
Governance	14%	25%	22%	17%	23%
Vulnerabilities and threats	15%	30%	24%	12%	19%
Supply chain risk	42%	27%	11%	12%	8%
Information asset management	13%	43%	18%	13%	12%
Identity and access management	9%	20%	32%	17%	22%
Cyber security awareness training	24%	21%	30%	9%	16%
Data security	33%	31%	20%	8%	8%
Protection of information assets	19%	29%	21%	15%	17%
Continuous monitoring	22%	23%	19%	14%	21%
Incident management	21%	27%	18%	17%	17%
Recovery planning	16%	32%	20%	14%	19%
Consequence management	27%	33%	21%	9%	10%

Table 4: Number of questions by organisation size

Function	Category	Small organisations	Medium/large organisations
Governance	Governance	4	12
	Vulnerabilities and threats	2	4
	Supply chain risk management	1	2
Identify	Information asset management	1	3
Protect	Identity and access management	3	5
	Cyber security awareness training	1	1
	Data security	3	3
	Protection of information assets	2	5
Detect	Continuous monitoring	3	6
Respond	Incident management	3	6
Recover	Recovery planning	1	2
	Consequence management	1	1
Total questions		25	50

Table 5: Subsectors presented with 50 questions, irrespective of size

Sector	Subsector
Deposit-taking, payments and credit sector	Credit providers
	Deposit product providers
	Payment product providers
Investment management	Responsible entities
	Custodians
Superannuation sector	Superannuation trustees
Market infrastructure sector	Domestic market operators
	Overseas market operators
	Clearing and settlement facility operators
	Other market participants, including derivative trade repository operators
	Credit rating agencies

Sector	Subsector
Market intermediaries' sector	Securities exchange participants
	Futures exchange participants
	Securities dealers
	Retail OTC derivative issuers
Insurance sector	Insurance product providers
	Insurance product distributors

Table 6: Organisation sizes

Organisation size	Number of persons employed
Small	1 to 25
Medium	26 to 199
Large	200 or more

Table 7: Number of participants by sector

Sector	Number of participants
Auditors and liquidators	18
No sector selected	360
Financial advice	120
Superannuation	12
Investment management	64
Market intermediaries	23
Deposit-taking, payments and credit	42
Insurance	29
Anonymised	19
Markets infrastructure	10

Appendix B: Methodology

The survey was designed to assess participants' cyber resilience against six functions: see Table 8. These functions were based on the five functions defined in the National Institute of Standards and Technology (NIST) Framework – with the addition of a separate function for governance and risk management. The questions within each function were divided into 12 distinct cyber risk categories.

Table 8: Survey functions and categories

Function	Category
Governance and risk management	Governance Vulnerabilities and threats Supply chain risk management
Identify	Information asset management
Protect	Identity and access management Cyber security awareness training Data security Protection of information assets
Detect	Continuous monitoring
Respond	Incident management
Recover	Recovery planning Consequence management

Participants were asked to answer each question based on their assessment of their organisation's cyber capability maturity. There were five capability maturity tiers to select from, ranging from no existing capability (incomplete, 0) through to advanced capability with policies and procedures that evolve over time (optimising, 4): see Table 9.

Table 9: Cyber capability maturity tiers

Maturity tier	Description
○ 0 **Incomplete**	There is an absence of capability. There are no policies and procedures
◔ 1 **Initial**	Capabilities are reactive. Policies and procedures are not formalised
◑ 2 **Risk informed**	Capabilities exist but policies and procedures are rarely updated and not followed consistently
◕ 3 **Managing risk**	Capabilities exist and are well managed. Policies and procedures are approved, followed and regularly updated
● 4 **Optimising**	Advanced capabilities are in place. Policies and procedures evolve in response to changes in cyber security threats

The survey was open to all ASIC-regulated organisations registered on the ASIC Regulatory Portal. ASIC directly emailed approximately 30,000 regulated entities, inviting them to participate in the survey. Participants were asked demographic questions about their organisation, including:

- size of the organisation
- type of organisation
- sector and subsector of the organisation, and
- type of ASIC licence held by the organisation.

The multiple-choice survey contained either 25 or 50 questions depending on organisation size and subsector selected. Large organisations may have required input from various members of the organisation, including chief risk officers, chief information security officers, executive officers, board members and/or the IT support function. Small organisations may have been able to complete the survey with input from their IT support function.

Appendix C: Accessible version of Figure 2

Table 10: Weighted average cyber maturity score by function on a scale of 0 to 4

Function	Small organisations	Medium & large organisations
Govern	1.40	1.91
Identify	1.56	1.74
Protect	1.42	2.07
Detect	1.34	2.29
Respond	1.36	2.13
Recover	1.28	2.01

Note: This is the data shown in Figure 2.

Key terms and related information

Key terms

administrative privileges	User access ability to modify information asset above the level of basic access
business email compromise	A type of cybercrime where the scammer uses email to trick someone into sending money or divulging confidential information
capability	The collective human and technological skills, abilities and expertise of the organisation
confidential information	Any information that is confidential in nature, including information that has commercial value and personal information
control	A method or means to manage risk
critical business services	Any activity, function, process, operation or service, the loss of which, for even a short period, would materially affect the continued operation of the organisation, or its consumers or investors, market integrity or the broader Australian financial system
cyber attack	A deliberate or malicious attempt to gain unauthorised access to an information asset connected to a network
cyber incident response plan	A set of instructions on how to respond to a cyber security incident
cyber resilience	An organisation's ability to prepare for, respond to and recover from cyber security incidents
cyber risk	The likelihood and impact of a threat exploiting a vulnerability and adversely impacting an information asset or the organisation
cyber security event	An occurrence of an activity in an information asset
cyber security incident	An unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising critical business services
cyber security strategy	A plan of action to manage an organisation's cyber risk and maintain its cyber resilience, whether standalone or integrated into other strategies
framework	A system of organisational policies, procedures, practices and controls, whether standalone or integrated into other frameworks
information asset	Information and IT (including software, hardware, firmware, systems and data (both hard and soft copy)), whether managed by the organisation or a third party (e.g. vendor or supplier)
malicious or threat actor	An individual or individuals who are partially or wholly responsible for an incident that impacts, or has the potential to impact, an organisation's security

malware	Software that has a malicious intent
multifactor authentication	An authentication method that requires the user to provide two or more verification factors
network	Connected computer infrastructure such as computers, digital devices and other information assets
patching	The act of applying a change to installed software that corrects security or functionality problems or adds new capabilities to information assets
penetration testing	A simulated set of cyber attacks against information assets to determine the exploitability of vulnerabilities
personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable
phishing	A type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing confidential information
ransomware	A type of malware that threatens to publish the victim's confidential information or permanently block access to it unless a ransom is paid
recognised standard	A standard, guideline, document or practice that is generally accepted by the industry in which the organisation operates
small organisations	An organisation that is classified as small in accordance with Table 6
social engineering	A manipulation technique that exploits human error to gain access to confidential information
supply chain	A network of people, organisations, information assets and resources involved in delivering goods or services
threat	Any activity that has the potential to exploit a vulnerability
vulnerability	A weakness in information asset security, design, implementation or operation that can be exploited

Related information

ASIC documents

Report 716 *Cyber resilience of firms in Australia's financial markets: 2020–21*

Report 651 *Cyber resilience of firms in Australia's financial markets: 2018–19*

Report 555 *Cyber resilience of firms in Australia's financial markets*

Report 429 *Cyber resilience: Health check*