Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Cybersecurity incident response planning: Practitioner guidance

First published: January 2022
Last updated: December 2024

Table of contents

Introduction

Context

Australian organisations are continually targeted by malicious actors, with the Australian Signals Directorate (ASD) assessing that malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale and sophistication. As malicious actors become more adept, the likelihood and severity of cyber attacks is also increasing due to the interconnectivity and availability of information technology (IT) platforms, devices and systems exposed to the internet.

Managing responses to cybersecurity incidents is the responsibility of affected organisations. As such, all organisations should have a cybersecurity incident response plan (CIRP) to ensure an effective response and prompt recovery in the event that system controls do not prevent a cybersecurity incident from occurring. This plan should be regularly tested and reviewed.

To be effective, a CIRP should align with organisations' emergency, crisis and business continuity arrangements, as well as jurisdictional and national cyber and emergency arrangements. It should support personnel to fulfil their roles by outlining their responsibilities and all legal and regulatory obligations.

While organisations are responsible for managing cybersecurity incidents affecting their business, Australia's Cyber Incident Management Arrangements outline the inter-jurisdictional coordination arrangements and principles when responding to national cybersecurity incidents.

Purpose

This guidance (which acts as a CIRP template) and the cybersecurity incident response readiness checklist (Appendix B) are intended to be used as a starting point for organisations to develop their own CIRP and readiness checklists. Each organisation's CIRP and checklist will need to be tailored according to their own unique operating environment, priorities, resources and obligations.

In addition to a CIRP, organisations can develop more detailed day-to-day processes and procedures to supplement the CIRP. This could include detailed playbooks to aid in the response to common types of cybersecurity incidents, such as ransomware or data breaches, and standard operating procedures (SOPs) to respond to cybersecurity incidents affecting specific assets.

Using this guidance

This guidance is designed to assist organisations in the development of their own CIRP as part of cybersecurity incident response planning activities. As part of this guidance, a separate CIRP template is available for organisations to fill in with some fields containing example text for demonstrative purposes. Note, the CIRP template is not exhaustive. Each organisation's CIRP should be tailored according to their own unique operating environment, priorities, resources and obligations.

Acknowledgements

This guidance was created using multiple resources. ASD acknowledges the following resources used in its development:

- ASD *Information security manual*

- Australian Prudential Regulation Authority *Prudential Practice Guide CPG 234 Information Security*
- CIRP template developed by the Australian Energy Sector Readiness and Resilience Working Group in 2019, specifically with support from the Australian Energy Market Operator, Tasmanian Department of State Growth, the Victorian Government Department of Premier and Cabinet and ASD
- Queensland Government *Incident Management Guideline*
- Victorian Government *Cyber Incident Management Plan* and *Cyber Incident Response Plan Template*
- Cybersecurity & Infrastructure Security Agency *Federal Government Cybersecurity Incident and Vulnerability Response Playbooks*
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2, *Computer Security Incident Handling Guide*
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27035-1:2023, *Information technology – Information security incident management – Part 1: Principles and process*
- ISO/IEC 27035-2:2023, *Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*
- ISO/IEC 27035-3:2020, *Information technology – Information security incident management – Part 3: Guidelines for ICT incident response operations*.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Authority and review

Include information about the document owner, document reviewer, approver, version control and date of next review or other thresholds to review the CIRP. For example, a CIRP could be reviewed on a time bound basis, such as bi-annually or annually. A CIRP could also be reviewed when implementing changes following a cybersecurity incident, a cybersecurity exercise or organisational shifts. Finally, a CIRP could be reviewed following changes to relevant policies, plans, legislation, regulation or jurisdictional arrangements.

Document control and review

Document Control	
Author	*Person responsible for developing the CIRP.*
Owner	*The risk owner or role responsible for enacting the CIRP.*
Date created	
Last reviewed by	
Last date reviewed	
Endorsed by and date	
Next review due date	

Version control

Version	**Date of Approval**	**Approved By**	**Description of Change**
0.1	*20/06/2022*	*action officer*	*Initial draft*

Purpose and objectives

Include the purpose and objectives of the CIRP.

Purpose

To support a swift and effective response to cybersecurity incidents aligned with the organisation's security and business objectives.

Objectives

- To provide guidance on the steps required to respond to cybersecurity incidents.
- To outline the roles, responsibilities, accountabilities and authorities of personnel and teams required to manage responses to cybersecurity incidents.
- To outline legal and regulatory compliance requirements for cybersecurity incidents.
- To outline internal and external communication processes when responding to cybersecurity incidents.
- To provide guidance on post cybersecurity incident activities to support continuous improvement.

Standards and frameworks

Include the relevant standards and frameworks used to inform the CIRP.

- National standards and frameworks:
  - *Information security manual*
  - *Prudential Practice Guide CPG 234 Information Security*
  - *Australian Energy Sector Cyber Security Framework*
- State/Territory Government standards and frameworks
  - New South Wales Government *Cyber Security Incident Emergency Sub Plan*
  - Queensland Government *Incident Management Guideline*
  - South Australian Government *Cyber Security Incident Management*
  - Tasmanian Government *Incident Management Cyber Security Standard*
  - Victorian Government *Cyber Incident Management Plan*
  - Western Australian Government *Cyber Security Incident Coordination Framework*
- International standards and frameworks:
  - NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide*
  - ISO/IEC 27035-1:2023, *Information technology – Information security incident management – Part 1: Principles and process*
  - ISO/IEC 27035-2:2023, *Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*
  - ISO/IEC 27035-3:2020, *Information technology – Information security incident management – Part 3: Guidelines for ICT incident response operations*.

High level cybersecurity incident response process

Include a summary of the cybersecurity incident response process.

Common cybersecurity incidents and responses

Include commonly used terms and their definitions. A list of commonly used terms and definitions is provided at Appendix A.

Common threat vectors

Include a summary of common threat vectors.

Type	Description
Attrition	An attack that employs brute force methods to compromise, degrade or destroy systems, services or networks (e.g. a Distributed Denial of Service intended to impair or deny access to a service or application; or a brute force attack against an authentication mechanism, such as passwords or digital signatures).
Email	An attack executed via an email message or attachment (e.g. exploit code disguised as an attached document or a link to a malicious website in the body of an email message).
External/Removable Media	An attack executed from removable media or a peripheral device (e.g. malicious code spreading to a system from infected removable media).
Impersonation	An attack involving replacement of something benign with something malicious (e.g. spoofing, person-in-the-middle attacks, rogue wireless access points and SQL injection attacks).
Improper usage	Any event resulting from the violation of an organisation's acceptable usage policies by an authorised user (e.g. a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system).
Loss or theft of equipment	The loss or theft of a computing device or media used by an organisation, such as a laptop, smartphone or authentication token.
Web	An attack executed from a website or web-based application (e.g. a cross-site scripting attack used to steal credentials or redirect to a site that exploits a web browser vulnerability and installs malware).
Other	An attack that does not fit into any of the above categories.

Common cybersecurity incidents

Include a summary of common cybersecurity incident types and the initial response activities.

Type/Description	Response
Data breach: Unauthorised access and disclosure of data.	

Denial of Service and Distributed Denial of Service: Overwhelming a service with traffic, sometimes impacting availability.
Industrial Control System compromise: Unauthorised access to an Industrial Control System.
Malware: A trojan, virus, worm or any other malicious software that can harm systems, services or networks.
Phishing: Deceptive messaging designed to elicit users' sensitive data (such as banking logins or business login credentials) or used to execute malicious code to enable remote access.
Ransomware: A tool used to lock or encrypt victims' files until a ransom is paid.

Roles and responsibilities

Include details of the roles and responsibilities of core personnel and teams responsible for cybersecurity incident response and decision making. At a minimum, include the personnel responsible for receiving the initial notification, the operational level Cybersecurity Incident Response Team (CIRT) and the strategic level Senior Executive Management Team (SEMT).

All personnel listed should be familiar with their responsibilities in the CIRP and have practise their response.

Points of contact for reporting cybersecurity incidents

Include details about primary and secondary internal points of contact for personnel or stakeholders to report cybersecurity incidents to over a 24/7 period.

Name	Availability	Contact Details	Role/Title	Responsibilities
			on-call point of contact	▪ *Primary point of contact*

Cybersecurity Incident Response Team

Include details of the CIRT personnel responsible for managing responses to cybersecurity incidents. The composition of the CIRT will vary depending on the size of an organisation and available skills and resources.

Include details of any 3rd party vendors that provide or manage systems, services and/or networks. If applicable, include details of external cybersecurity incident response providers and the services they provide.

Name	Availability	Contact Details	Role/Title	Responsibilities
			cybersecurity incident manager	▪ *Response planning* ▪ *CIRT operations*
			deputy cybersecurity incident manager	▪ *Situational analysis* ▪ *Threat intelligence* ▪ *Technical advice*
			security manager	▪ *Investigation (if suspected malicious insider)* ▪ *Law enforcement liaison*
			cybersecurity incident responder	▪ *Technical investigation (collection and processing of network and host data)* ▪ *Containment, remediation and recovery efforts* ▪ *Investigation findings report*

	communications, engagement and media advisor	▪ *Internal communications* ▪ *Media and community liaison*

Other CIRT roles could include system administrators, network engineers, change managers, internal auditors, legal advisors, finance and procurement specialists, and administration and recording keeping personnel.

Surge arrangements

Include process for implementing surge arrangements, the resources involved in those arrangements and thresholds for triggering those surge arrangements. Surge arrangements can include, but are not limited to people, hardware, software and financial resources.

Senior Executive Management Team

Significant cybersecurity incidents may require the formation of the SEMT to provide strategic oversight, direction and support to the CIRT, with a focus on:

- strategic issues identification and management
- stakeholder engagement and communications (including Board and ministerial liaison, if applicable)
- resource and capability demand (including urgent logistics or finance requirements, and human resources considerations during response effort).

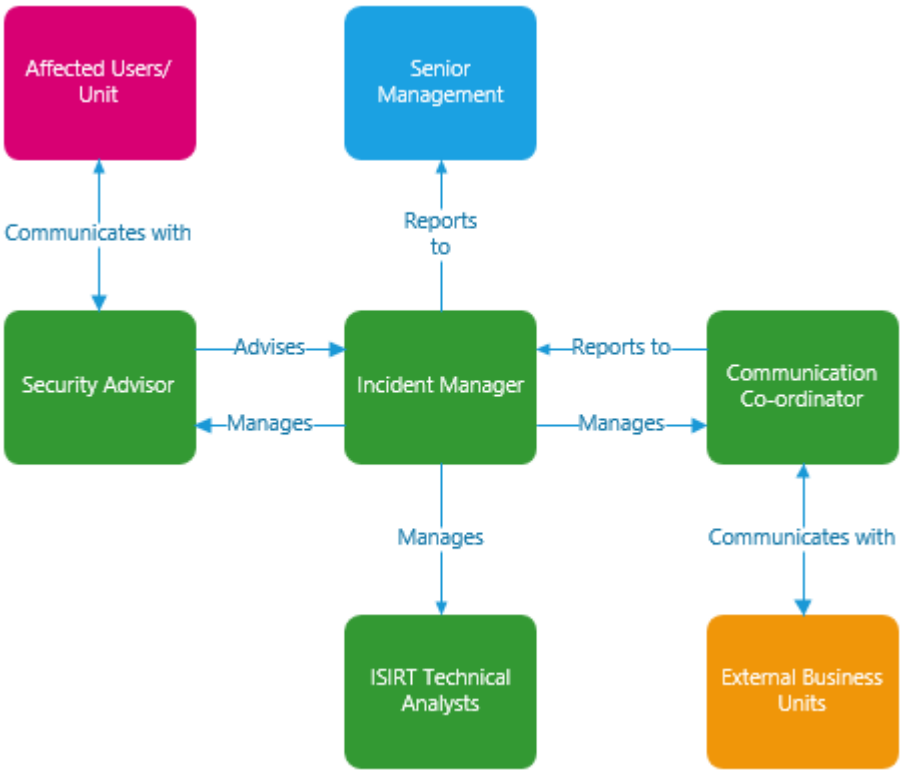
Include details of the SEMT responsible for managing responses to cybersecurity incidents. The composition and roles of the SEMT may vary depending on the cybersecurity incident impact and size and structure of an organisation, as some roles may not be relevant or multiple roles may be held by the same individual.

Name	Availability	Contact Details	Role/Title	Responsibilities
			chief executive officer	▪ *SEMT chair*
			chief information officer	▪ *SEMT deputy chair*
			chief information security officer	▪ *SEMT deputy*
			chief operating officer	▪ *Operational functions of the business*
			chief financial officer/procurement manager	▪ *Emergency procurement and expenditure oversight*
			legal council	▪ *Regulatory compliance, cyber insurance*

	media and communications manager	▪ *Public relations and stakeholder engagement*
	people and culture manager	▪ *Personnel welfare management*

Roles and responsibilities

Include a diagram picturing the relationship between the key personnel and teams involved in cybersecurity incident response. For example, the below diagram is taken from the Queensland Government Incident Management Guideline.



Communications

Include the process for managing internal and external communications. Be prepared to:

- support the CIRT and SEMT communications requirements
- respond to potential increases in internal and external enquiries or complaints about the cybersecurity incident or the effects, with common questions including:
    - How will the customer helpdesk manage enquiries and be supported?
    - How will the IT helpdesk (or equivalent) manage enquiries and be supported?
    - What communication channels are available to affected customers (e.g. telephone hotline, information on the website or social media)?
- communicate externally about the cybersecurity incident, including to the public and the media:
    - Who has the primary responsibility for authorising and speaking on behalf of the organisation? How will this person be supported?
    - Who has responsibility for producing and approving information for release to the public and media?
- monitor news media, social media and other forms of media and use it to support communications.

Include details for backup communication channels to communicate with stakeholders and customers.

Internal communications

Include the process and expected timeframes to communicate relevant cybersecurity incident information to personnel (for example, system users, customer service teams, senior executives and the Board).

In internal messaging, consider how to inform personnel about the cybersecurity incident and support business continuity. Consider providing:

- a brief summary of the cybersecurity incident and business impact
- actions currently being undertaken to resolve the cybersecurity incident
- actions personnel can take to assist
- business continuity options for personnel who are affected by the cybersecurity incident
- messaging for external stakeholders
- key points of contact for enquiries
- expected timeframes for further updates.

External communications

Include the process and timeframes to communicate relevant cybersecurity incident information to external stakeholders and customers.

Depending on the impact and severity of the cybersecurity incident, it may be necessary to communicate with:

- stakeholders required to support with cybersecurity incident response activities such as government bodies, third party cybersecurity incident response, law enforcement, insurance providers and/or sector organisations
- the media and customers seeking information about the cybersecurity incident, such as the general public, government bodies, clients, shareholders, suppliers and/or sector organisations.

In external messaging, consider how to inform external stakeholders and customers about the cybersecurity incident based upon their role or interest. Consider:

- information they need to know:
  - systems, services or networks affected
  - steps being taken to resolve the cybersecurity incident
  - who is supporting cybersecurity incident remediation activities
- any options or actions for stakeholders affected by the cybersecurity incident to take
- key points of contact for enquiries
- expected timeframes for further updates.

Consider supporting requests for information from interested sector and government bodies following the cybersecurity incident for the purpose of information sharing and learning from the experience.

Supporting procedures and playbooks

Supporting procedures

Include a list of SOPs developed to support cybersecurity incident response, and their physical and electronic locations. Examples of SOPs are:

- event detection, triage and analysis
- post cybersecurity event/incident detection or notification
- cybersecurity incident detection, investigation and analysis
- cybersecurity incident containment, remediation and recovery
- communications plan (internal and external)
- emergency management plan
- crisis management plan
- business continuity plan
- disaster recovery plan.

Supporting playbooks

Playbooks are documents that are intended to contain easy to follow instructions to assist in ensuring all appropriate steps are taken when responding to specific types of cybersecurity incidents. Include a list of playbooks and their physical and electronic locations. Example cybersecurity incidents that may have a playbook are:

- Cybersecurity Incident Response Playbook: Phishing
- Cybersecurity Incident Response Playbook: Data Breach/Theft
- Cybersecurity Incident Response Playbook: Malware
- Cybersecurity Incident Response Playbook: Ransomware
- Cybersecurity Incident Response Playbook: Denial of Service.

Sector, jurisdictional and national cybersecurity incident response arrangements

Include information about the relevant sector, state and/or territory and national arrangements for cybersecurity incident related activities, including, but not limited to, notification, reporting and/or seeking additional support.

The CIRP could include a process chart of when to report cybersecurity incidents to relevant government bodies and/or seek assistance.

Sector arrangements

Include information about the relevant sector arrangements and the process for implementing these arrangements.

Jurisdictional arrangements

Each state/territory jurisdiction has its own cybersecurity incident response arrangements. Organisations should contact the relevant government body in their jurisdiction to understand the arrangements that apply.

Include information about the process for reporting to and/or seeking assistance from state/territory law enforcement.

National arrangements

Include information about the process for reporting to and/or seeking assistance from Federal Government bodies. For example, Australia's Cyber Incident Management Arrangements outline the inter-jurisdictional coordination arrangements and principles when responding to national cybersecurity incidents.

Examples of potential national cybersecurity incidents include:

- an organisation with links across multiple jurisdictions being compromised through a cybersecurity incident
- malicious cyber activity affecting critical national infrastructure where the consequences have the potential to cause sustained disruption of essential services or threaten national security
- malicious cyber activity where the cause and potential extent of its geographic impact is uncertain
- a large-scale breach of sensitive data affecting persons or organisations in multiple jurisdictions.

ASD leads the Australian Government's response to cybersecurity incidents. For information on how to report cybersecurity incidents to ASD, and to seek advice and assistance, visit ASD's reporting website.

ASD takes the protection of information seriously. Under the limited use obligation, information voluntarily provided to ASD about cybersecurity incidents, potential cybersecurity incidents or vulnerabilities impacting organisations cannot be used for regulatory purposes.

Appendix C lists some of the common triage questions ASD will use to assess the severity of a reported cybersecurity incident.

Cybersecurity incident notification and reporting

Include internal and external processes for cybersecurity incident notification and reporting. Consider sector, state/territory and national cybersecurity incident notification and reporting obligations.

Include details about who is responsible for cybersecurity incident notification and reporting to external entities.

Type	Organisation to Notify	Reporting Contact Details	Key Reporting Requirements	Reporting Personnel
Ransomware	*ASD*	*https://www.cyber.gov.au/about-us/about-asd-acsc/contact-us*	*https://www.cyber.gov.au/report-and-recover/report*	*chief information security officer*
Data breach	*Office of the Australian Information Commissioner (OAIC)*	*https://www.oaic.gov.au/contact-us*	*https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach*	*chief information security officer*

Legal and regulatory requirements

Include details about any legal and regulatory obligations, such as contractual and legislative reporting requirements. Work with any compliance and legal personnel to ensure the CIRP covers all relevant requirements, noting that different cybersecurity incidents may require different or multiple legal and regulatory responses.

The CIRP could include a process chart of when to report cybersecurity incidents to relevant government bodies, regulators and other external parties.

Insurance

Include relevant details about any insurance policies for cybersecurity incidents.

Detection, investigation, analysis and activation

Include the decision making framework for activating the CIRP.

Detecting cybersecurity incidents

Cybersecurity incidents could be detected in several ways, including, but not limited to:

- self-detected (e.g. via Intrusion Detection and Prevention Systems)
- notifications received from service providers or vendors
- notifications received from trusted third parties, such as ASD.

Cybersecurity incident classification

Include the framework and decision making process for classifying a cybersecurity incident. This can assist with prioritising resources. Classification factors could include:

- effects of the cybersecurity incident (confidentiality, integrity and availability of systems and their resources)
- stakeholders affected (internal and external)
- cybersecurity incident type
- impact on the business and community.

Classification	Description
Critical	▪ *Over 80% of personnel (or several critical staff/teams) unable to work.* ▪ *Critical systems offline.* ▪ *High risk to/definite breach of sensitive client or personal data.* ▪ *Financial impact greater than $100,000.* ▪ *Severe reputational damage – likely to impact business long term.*
High	▪ *50% of personnel unable to work.* ▪ *Non-critical systems affected.* ▪ *Risk of breach of personal or sensitive data.* ▪ *Financial impact greater than $50,000.* ▪ *Potential serious reputational damage.*
Medium	▪ *20% of personnel unable to work.* ▪ *Small number of non-critical systems affected.* ▪ *Possible breach of small amounts of non-sensitive data.* ▪ *Financial impact greater than $25,000.* ▪ *Low risk to reputation.*

Low	▪ *<10% of non-critical personnel affected temporarily (short term).* ▪ *Minimal, if any, impact.* ▪ *One or two non-sensitive/non-critical machines affected.* ▪ *No breach of data.* ▪ *Negligible risk to reputation.*

For information about the ASD cybersecurity incident categorisation matrix see Appendix K.

Cybersecurity Incident Response Team activation

Include the decision making framework for activating the CIRT. This could align with the cybersecurity incident classification framework. Note, some smaller cybersecurity incidents may be manageable without activation of the CIRT.

Logistics and communications

Include core logistical and communications protocols and mechanisms used to support cybersecurity incident response. For example:

- operations room/security operations centre (SOC) location and setup
- equipment required for offsite cybersecurity incident response
- communications technologies such as phone/teleconference/online dial-in details and out-of-band communications (e.g. Slack or other similar applications).

Investigation questions

To guide cybersecurity incident response efforts, and understanding of the scope and impact of the cybersecurity incident, develop a list of investigation questions. Note, not all questions may be answerable with the data available and questions may change as investigations progress.

Possible investigation questions include:

- What was the initial intrusion vector?
- What post-exploitation activity occurred? Have accounts been compromised? What level of privilege was involved?
- Does the malicious actor have persistence on systems, services or networks?
- Is lateral movement suspected or known? Where has the malicious actor laterally moved to and how?
- How is the malicious actor maintaining command and control?
- Has data been accessed or exfiltrated and, if so, what kind of data?

Escalation and de-escalation

Include the escalation and de-escalation triggers and/or thresholds and decision making authorities.

Classification	Action	Triggers/Thresholds for Escalation and De-escalation	Minimum Level of Authority
Critical	De-escalation to High		
High	Escalation to Critical		
	De-escalation to Medium		
Medium	Escalation to High		
	De-escalation to Low		
Low	Escalation to Medium		

Containment, evidence collection and remediation

Containment

Containment actions are implemented in order to minimise damage, prevent the cybersecurity incident from spreading or escalating, and prevent malicious actors from destroying evidence.

When planning containment actions, consider:

- any additional impacts there could be to systems, services or networks
- time and resources required to contain the cybersecurity incident
- effectiveness of the containment solution (e.g. partial vs full containment)
- duration that the containment solution will remain in place (e.g. temporary vs permanent solution).

Documentation

Include processes and procedures for documenting the cybersecurity incident, including responsible personnel and timeframes. Refer to Appendix D for a situation report template and Appendix E for a cybersecurity incident log template.

Situation reports may contain the following information:

- cybersecurity incident date and time
- status of the cybersecurity incident
- cybersecurity incident type and classification
- cybersecurity incident scope and impact
- cybersecurity incident severity
- external assistance required
- actions taken to resolve the cybersecurity incident
- contact details for key CIRT personnel
- date and time of the next update.

Evidence collection and preservation

Include processes and procedures for collecting, preserving, handling and storing evidence, including responsible personnel and timeframes. As this can be complex, if necessary, seek advice from digital forensic professionals, legal advisors or law enforcement.

When gathering evidence, maintain a detailed log that clearly documents how all evidence has been collected. This should include who collected or handled the evidence, the time and date (including time zone) evidence was collected and handled, and the details of each item collected (including the physical location, serial number, model number, hostname, media access control [MAC] address, Internet Protocol [IP] address and hash values). See Appendix F for a template.

Examples of commonly collected evidence include:

- hard drive/host images
- network packet captures and flows
- IP addresses
- log files
- network diagrams
- configuration files
- databases
- investigation notes
- screenshots
- social media posts
- close-circuit television, video and audio recordings.

Remediation action plan

Include processes and procedures for developing and implementing a remediation action plan to resolve the cybersecurity incident following successful containment and evidence collection. See Appendix G for a template.

When developing the remediation action plan, consider:

- What actions are required to resolve the cybersecurity incident?
- What resources are required to resolve the cybersecurity incident (if not already included in the CIRT)?
    - Are there additional external resources required?
- Who is responsible for remediation actions?
- What systems, services or networks should be prioritised?
- What systems, services or networks will be affected during the remediation process?
    - How will these systems, services or networks be affected?
- What is the expected resolution time?

Recovery

Include processes and procedures for developing, authorising and executing an agreed recovery plan.

The recovery plan should detail the approach to recovering IT and/or operational technology (OT) systems, services and networks once containment and remediation is complete.

When developing the recovery plan, consider:

- How will systems, services and networks be restored to normal operation and in what timeframe?
- How will systems, services and networks be monitored to ensure they are no longer compromised and are functioning as expected?
- How will identified vulnerabilities be managed to prevent similar cybersecurity incidents from occurring in the future?

Stand down

Include decision making processes and procedures for standing down the CIRT and SEMT.

Include the processes and procedures for completing a cybersecurity incident report, including responsible personnel and timeframes. Consider creating a cybersecurity incident report template as an appendix to the CIRP.

Learn and improve

Include an approach to capture lessons learn from the cybersecurity incident.

Post cybersecurity incident review

A post cybersecurity incident review is a detailed review conducted after an organisation has experienced a cybersecurity incident. It can include a hot debrief which is held immediately after an organisation has recovered its systems, services or networks from a cybersecurity incident and/or a formal debrief held after the cybersecurity incident report has been completed, such as within two weeks.

Key questions to consider during a post cybersecurity incident review include:

- What were the root causes of the cybersecurity incident?
- Could the cybersecurity incident have been prevented? How?
- What worked well in the response to the cybersecurity incident?
- How could our response be improved for future cybersecurity incidents?

Refer to Appendix H for more detailed questions to consider in post cybersecurity incident reviews.

Recommendations that arise from the review can be documented in a corresponding action register. Refer to Appendix I for an action register template.

PPOSTTE model

The PPOSTTE model can assist in reflecting on key elements of the cybersecurity incident response:

- **People:** Roles, responsibilities, accountabilities, skills.
- **Process:** Plans, policies, procedures, protocols, processes, templates, arrangements.
- **Organisation:** Structures, culture, jurisdictional arrangements.
- **Support:** Infrastructure, facilities, maintenance.
- **Technology:** Equipment, systems, standards, security, inter-operability.
- **Training:** Qualifications/skill levels, identification of required courses.
- **Exercise management:** Exercise development, structure, management, conduct.

Update and test the cybersecurity incident response plan

The post cybersecurity incident review may result in changes to the CIRP, playbooks and templates. Changes should be communicated to the relevant personnel.

Significant changes may require the CIRP, playbooks and templates to be tested. Regular testing is important to ensure these documents remain current and are familiar to relevant personnel. Testing methods could include tabletop exercises or functional exercises.

Training

Include training activities, and associated support, required for personnel to effectively undertake their roles when responding to a cybersecurity incident.

The post cybersecurity incident review may identify additional specialised training for personnel involved in cybersecurity incident response or general cybersecurity awareness training for all personnel.

Appendix A: Terminology and definitions

Use of consistent and pre-defined terminology to describe cybersecurity incidents and their effects can be helpful as part of cybersecurity incident response planning.

Cyberthreat

A cyberthreat is any circumstance or event with the potential to harm systems or data.

Examples of cyberthreats include (but are not limited to):

- business email compromise
- cybercrime
- cyber supply chain compromise
- exploitation of vulnerabilities
- phishing emails and scams
- ransomware.

Cybersecurity alert

A cybersecurity alert is a notification generated in response to a deviation from normal behaviour. Cybersecurity alerts are used to highlight cybersecurity events.

Cybersecurity event

A cybersecurity event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.

Examples of cybersecurity events include (but are not limited to):

- a user has disabled the antivirus on their computer
- a user has deleted or modified system files
- a user restarted a server
- unauthorised access to a server or computer.

Cybersecurity incident

An unwanted or unexpected cybersecurity event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations.

Examples of cybersecurity incidents include (but are not limited to):

- denial-of-service attacks

- unauthorised access or attempts to access a system
- compromise of sensitive data
- virus or malware outbreak (including ransomware).

Appendix B: Cybersecurity incident response readiness checklist

This checklist is provided to aid the initial assessment of an organisation's readiness to respond to a cybersecurity incident. This checklist is not an exhaustive list of all readiness activities.

	PREPARATION
☐	Your organisation has a cybersecurity policy or strategy that outlines your organisation's approach to prevention, preparedness, detection, response, recovery, review and improvement. For example, your organisation has a position on not paying ransoms, reporting cybersecurity incidents to government, publicly acknowledging cybersecurity incidents, and sharing information about cybersecurity incidents with trusted industry and government partners.
☐	A CIRP has been developed which: ▪ aligns with your organisation's operating environment, including emergency management and business continuity processes and procedures ▪ has been reviewed or tested in an exercise to ensure it is current and responsible personnel are aware of their roles and responsibilities ▪ includes supporting templates, for example situation reports.
☐	Personnel involved in managing cybersecurity incidents have received cybersecurity incident response training.
☐	Up-to-date hard copy versions of the CIRP and playbooks are stored in a secure location (in case of electronic or hardware failure) and are accessible to authorised personnel.
☐	Specific playbooks to supplement the CIRP have been developed and define step-by-step guidance for response actions to common cybersecurity incidents.
☐	A CIRT and SEMT, or equivalents, have been identified to manage any responses to cybersecurity incidents.
☐	All relevant IT and OT SOPs are documented and have been reviewed or tested in an exercise to ensure they are current and responsible personnel are aware of their roles and responsibilities.
☐	Arrangements for service providers, including cloud and managed services, to provide and retain logs have been established and tested to ensure they include useful data which can be provided in a timely manner.
☐	Log retention mechanisms for critical systems, services and networks have been adequately configured and tested to ensure that they capture useful data.
☐	Your organisation has internal or third party arrangements and capabilities to detect and analyse cybersecurity events/incidents. If these capabilities are outsourced, your organisation has an active service agreement/contract.

☐	Critical assets (systems, services and networks) have been identified and documented.
☐	SOPs have been developed, and roles and responsibilities assigned, for use of facilities and communications technologies in response to cybersecurity incidents, and these resources are confirmed as available. This includes for alternative/backup IT-based communication channels.
☐	Cybersecurity incident logging/records and tracking technologies used to manage any response to cybersecurity incidents are confirmed as available and have been tested.
☐	Role cards have been developed for personnel involved in the CIRT and the SEMT.
☐	Your organisation has internal or third party arrangements and capabilities to monitor cyberthreats. Situational awareness information is collected from internal and external data sources, including: ▪ local system and network traffic and activity logs ▪ news concerning political, social or economic activities that might impact cybersecurity incident activity ▪ external feeds on cybersecurity incident trends, new attack vectors, current attack indicators and new mitigation strategies and technologies.

DETECTION, INVESTIGATION, ANALYSIS AND ACTIVATION

SOPs have been developed, and roles and responsibilities assigned, for:

☐	Detection mechanisms which can be used to identify cybersecurity events/incidents, such as scanning, sensor and logging mechanisms. These mechanisms require monitoring processes to identify unusual or suspicious activity commensurate with the potential impact of a cybersecurity incident. Common monitoring techniques include: ▪ network and user profiling that establishes a baseline of normal activity which, when combined with logging and alerting mechanisms, can enable detection of anomalous activity ▪ scanning for the introduction of unauthorised hardware and software ▪ scanning for unauthorised changes to hardware and software configurations ▪ sensors that provide an alert when a measure breaches a defined threshold(s) (e.g. device, server and network activity) ▪ logging and alerting of access to sensitive data or unsuccessful logon attempts to identify potential unauthorised access ▪ users with privileged access accounts subject to a greater level of monitoring in light of the heightened risks involved.
☐	Cybersecurity incident detection, including self-detected cybersecurity incidents, notifications received from service providers or vendors, and notifications received from trusted third parties (e.g. ASD).
☐	Cybersecurity incident analysis, including how cybersecurity incidents are to be categorised, classified and prioritised, and controls related to how data is stored and transmitted.
☐	Activating a CIRT to manage cybersecurity incidents, with roles and responsibilities assigned.

☐	Activating a SEMT to manage cybersecurity incidents, with roles and responsibilities assigned.
CONTAINMENT, EVIDENCE COLLECTION AND REMEDIATION	
☐	SOPs, playbooks and templates have been developed, and roles and responsibilities assigned, for containment, evidence collection and remediation.
☐	A secure location is available for storing data captured during cybersecurity incidents, which could be used as evidence of the malicious actor's tradecraft, and is ready to be provided to third-party stakeholders if requested.
COMMUNICATIONS	
☐	SOPs, playbooks and templates have been developed to support communicating with internal and external stakeholders.
☐	SOPs, playbooks and templates for media and communications professionals have been developed, and roles and responsibilities assigned, to support public and media messaging.
☐	You organisation has assigned a public and media spokesperson who is supported by technical subject matter experts.
☐	Personnel have been trained to implement communications processes and execute their roles and responsibilities.
☐	All personnel are cognisant of your organisation's policy, and their responsibilities, when a cybersecurity incident occurs (e.g. exercising discretion, using approved talking points, referring enquiries to the designated public and media spokesperson).
CYBERSECURITY INCIDENT NOTIFICATION AND REPORTING	
☐	Processes and procedures are documented to support your organisation to meet its legal and regulatory requirements on cybersecurity incident notification and reporting with roles and responsibilities within your organisation assigned. This includes the processes for obtaining authority to release and share information.
☐	Processes and procedures are documented for communicating with any cyber insurance providers.
POST CYBERSECURITY INCIDENT REVIEW	
☐	Processes are procedures are documented to support post cybersecurity incident reviews following the resolution of cybersecurity incidents, with post cybersecurity incident review reports submitted to management for endorsement.
☐	Processes and procedures are documented to ensure actions following cybersecurity incidents and/or exercises are tracked and completed (e.g. within an action register).

Appendix C: ASD cybersecurity incident triage questions

Where applicable, personnel reporting cybersecurity incidents to ASD on behalf of their organisation should try to have information available to answer the following questions:

- Who is reporting the cybersecurity incident? (e.g. CISO, SOC Manager)
- Who/what is the affected organisation/entity?
- What type of cybersecurity incident is being reported? (e.g. ransomware, denial of service, data breach, malware)
- Is the cybersecurity incident still active?
- When was the cybersecurity incident first identified?
- Is reporting for ASD awareness or is ASD assistance required?
    - If ASD assistance is required, what assistance is required?
- What type of system, service or network has been affected?
- What was observed (e.g. the sequence of events)?
    - date/time
    - effect/event
- Who or what identified the problem?
- Has a data breach occurred?
    - What type of data was exposed?
    - What volume of data was exposed?
    - What impact will this have on your organisation?
    - What impact (if any) will the data breach have on public safety or services?
    - Was it a misconfiguration/error, or was a malicious exfiltration or theft of data identified?
    - If applicable under the *Notifiable Data Breaches scheme*, has it been reported to the OAIC?
- What actions have been taken to rectify the issue?
    - Are internal or external cybersecurity incident response providers involved?
    - Are business as usual operations interrupted? If so, how long before operations will be back to normal?

- Will information about the cybersecurity incident be communicating publicly (e.g. with customers and/or the media)?
    - If so, please notify ASD beforehand if you will be referencing ASD.

Appendix D: Situation report template

Date of Entry:	**Time of Entry:**	**Author:**
Date/time cybersecurity incident was detected		
Current cybersecurity incident status	*New, In Progress, Resolved*	
Cybersecurity incident type		
Cybersecurity incident classification	*Critical, High, Medium, Low*	
Cybersecurity incident scope	*List the affected systems, services and/or networks; highlight any change to scope since the previous log.*	
Cybersecurity incident impact	*List the affected stakeholder(s); highlight any change in impact since the previous log entry.*	
Cybersecurity incident severity	*Outline the impact of the cybersecurity incident on your organisation(s) and public safety or services; highlight any change to severity since the previous log entry.*	
Notifications Actioned/Pending	*What other organisations need to be notified? (e.g. ASD, law enforcement, OAIC, customers, media)*	
Assistance required	*What assistance is required from other organisations? (e.g. ASD, law enforcement)*	
Actions being taken to resolve the cybersecurity incident		
Additional notes		
Contact details for the cybersecurity incident manager (and others if required)		
Date and time of the next update		

Appendix E: Cybersecurity incident log template

Date/Time	**Notes** (relevant facts, decisions, rationale)
20220330 – 0835hrs	*SOC identified phishing that resulted in the successful deployment of ransomware to the system.*
20220331 – 1455hrs	*CIRT collected forensic artefacts (listed in the evidence register). An initial investigation has assessed the cybersecurity incident as 'High'.* *The following systems are currently offline: ...*
20220401 – 1150hrs	*SEMT voted to escalate the cybersecurity incident to 'Critical'.* *Next actions were agreed to as follows: …*

Appendix F: Evidence register template

Date/Time and Location of Collection	**Collected by** (name, title, contact and phone number)	**Item Details** (quantity, serial number, model number, hostname, MAC address, IP addresses and hash values)	**Storage Location and Label Number**	**Access**
20220402 – 1200hrs – Head Office	*Jane Doe – CIRT – Contact Details*	*1 x disk and memory image, XYZ Desktop, ABC Model Number, IP ###.###.###.###, ...*	*Stored on hard drive asset number ####, in IT Security Office and on network drive H:\...*	*CIRT team, law enforcement, ASD*

Appendix G: Remediation action plan template

Date/Time	**Category** (Contain, Eradicate, Recover)	**Action**	**Action Owner**	**Status** (Unallocated, In Progress, Closed)
20220425 – 0900hrs	*Contain*	*Isolated hosts identified as infected per CIRT investigation.*	*CIRT Team Leader*	*In Progress*

Appendix H: Post cybersecurity incident reviews

A post cybersecurity incident review is a detailed review conducted after an organisation has experienced a cybersecurity incident. The content of the review will vary for each organisation, but primarily focuses on establishing learnings and providing recommended actions to mitigate future cybersecurity incidents. The purpose of this guide is to provide organisations that have experienced a cybersecurity incident with tools and techniques to conduct a post cybersecurity incident review.

How to use this guide

This guide contains high level steps recommended for organisations to follow after experiencing a cybersecurity incident. The guide should be used as a resource, and will need to be further tailored by organisations to suit their individual requirements. The templates provided are generic and will need to be tailored to suit specific organisational requirements.

Post cybersecurity incident review steps

Step 1 – Hold cybersecurity incident debriefs

Post cybersecurity incident debriefs are useful for capturing observations from personnel directly involved in managing a cybersecurity incident and identifying actions to improve how their organisation managed its response, as well as how the cybersecurity incident could have been prevented. There are two types of debriefs organisations may hold after experiencing a cybersecurity incident: a hot debrief and a formal debrief (also known as a cold debrief).

A hot debrief is held immediately after an organisation has recovered its systems, services or networks from a cybersecurity incident. The benefits of holding a hot debrief include:

- the team involved in responding to the cybersecurity incident can provide instant feedback and lessons learned
- any urgent issues identified during the cybersecurity incident can be addressed immediately
- personnel involved in the cybersecurity incident are more likely to recall information and detail as it is still fresh in their minds.

A formal debrief is held days to weeks after an organisation has recovered its systems, services or networks from a cybersecurity incident. The benefits of holding a formal debrief include:

- it provides an opportunity to discuss the cybersecurity incident in detail after it is resolved to gather key insights, learnings and opportunities for improvement
- it provides time between the cybersecurity incident and debrief allowing emotions to settle, particularly for stressful cybersecurity incidents
- it ensures all key personnel required for discussions are present, especially senior management who will need to drive the implementation of actions.

Hot debrief guidance

Time

30 minutes – 1 hour.

Aim

The aim of the hot debrief is to review the cybersecurity incident, receive feedback on personnel observations and insights, and identify any urgent issues requiring immediate action.

Participants

The hot debrief should be led by a facilitator (such as a manager who was involved during the cybersecurity incident) and supported by a scribe whose role is to document attendance, key insights and immediate actions. It is recommended that hot debrief participants include all personnel involved during the detection, response and recovery phases of the cybersecurity incident, with upper management excluded (e.g. chief executive officers and general managers). This will ensure personnel involved in the cybersecurity incident can speak openly without fear of repercussion.

Content

The facilitator could guide discussion using the following questions:

- What went well?
- What could we do differently next time to improve?
- What action has been taken to remediate immediate risk?
- Are there any further issues that require immediate resolution?

Note, it is essential for the facilitator to remain objective during the discussion, and treat the cybersecurity incident as a learning point for all involved, without attributing blame to an individual or team.

Conclusion

At the end of the hot debrief, the facilitator should provide a summary of the discussions to participants who can confirm whether the key issues and actions were captured. The facilitator should explain the next steps and the expected timeframes for these.

Formal debrief guidance

Time

1–2 hours.

Aim

The aim of the formal debrief is to review the cybersecurity incident, validate what worked, and produce actions and assigned responsibilities to improve current arrangements.

Participants

The formal debrief should be led by a facilitator who asks key questions, supported by a scribe to document attendance, key insights and actions.

It is recommended that formal debrief participants include:

- technical personnel who were involved in detecting, responding to and resolving the cybersecurity incident

- non-technical personnel who were involved during the cybersecurity incident
- communications/media personnel involved in the cybersecurity incident.

Content

Questions to consider in the formal debrief can be found in the post cybersecurity incident review analysis Template. The facilitator can use this guidance to lead the conversation with the participants while the scribe documents the discussion directly into the template. The scribe can also use the action register template to document any actions resulting from the discussion.

Conclusion

At the end of the debrief, a decision should be made about whether additional discussions are required, or if finalisation of the cybersecurity incident documentation can be completed. If email correspondence is selected to disseminate the documentation, an action officer will need to be identified for completing them and circulating them to staff for endorsement.

Step 2 – Complete cybersecurity incident documentation

Based on the findings of the debriefs, the action officer should complete a draft of the post cybersecurity incident review analysis and the action register and circulate them to the personnel involved in the debrief for their feedback and endorsement. Note, it is important that the action register details an assigned lead (action officer) for closing out each action.

Once feedback is received and incorporated, documentation should be sent to an executive staff member (e.g. a chief executive officer or general manager) for endorsement. The executive staff member may advise their expectations on the frequency of progress reporting of agreed actions and nominate a person to lead tracking and reporting.

Step 3 – Cybersecurity incident tracking and reporting

The identified actions should be tracked and reported at agreed frequencies.

Post cybersecurity incident review analysis template

CYBERSECURITY INCIDENT SUMMARY	
Cybersecurity incident name	
Date of cybersecurity incident	*dd/mm/yyyy*
Cybersecurity incident priority	*Low/Medium/High* *Established from the impact and/or risk to the business.*
Time cybersecurity incident occurred	

Time cybersecurity incident was resolved	
Cybersecurity incident type	
Personnel involved	*Names of the individuals involved in resolving the cybersecurity incident and their functions(s), including any service providers.*
Cybersecurity incident impact	*What impact did the cybersecurity incident have (e.g. loss of systems, services or networks).*
Brief summary	*What happened?*

Cybersecurity incident analysis

Cybersecurity incident analysis is broken into the following categories:

- **Timeline:** Summary of what happened and when. Provides high level areas for improvement.
- **Protection:** Identifies the control mechanisms that were in place at the time of the cybersecurity incident and their effectiveness. Establishes how to improve the protection of systems, services and networks.
- **Detection:** Establishes how to reduce the time to identify a cybersecurity incident. Addresses what detection mechanisms were in place and how those mechanisms could be improved.
- **Response:** Identifies improvements for the cybersecurity incident response.
- **Recovery:** Addresses improvements for cybersecurity incident recovery.

TIMELINE	
Date and time of detection	
When was the cybersecurity incident acknowledged?	*When did the organisation identify that a cybersecurity incident was occurring?*
Date and time of cybersecurity incident response	
Date and time of cybersecurity incident recovery	
Who discovered the cybersecurity incident first and how?	*Or who was alerted to it first? How did the discovery or alert happen?*

Was the cybersecurity incident reported externally? If yes, when?	*For example, did the organisation report it to ASD or the OAIC?*
Who supported resolving the cybersecurity incident? When did they provide support?	*List the names of personnel involved in resolving the cybersecurity incident and the time (and date if not all on the same day) they joined in.*
What activities were conducted to resolved the cybersecurity incident? When were they conducted and what was their impact?	*It is easier to do this in a list. For example: Time > Task > Impact.*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the action register.* *Brief description of action > Proposed action officer.*
PROTECTION	
What controls were in place that were expected to stop a cybersecurity incident similar to this?	
How effective were those controls?	*Did they work? Why/why not?* *How could they be improved?*
Are there other controls considered better for protecting against a similar cybersecurity incident?	*What are they?*
What business processes and procedures were in place to prevent this type of cybersecurity incident from occurring?	
How effective were those business processes and procedures?	*Did they work? Why/why not?* *How could they be improved?*
Any other findings and/or suggestions for improvement?	*See the PPOSTTE model for guidance.*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the action register.* *Brief description of action > Proposed action officer.*

DETECTION	
How was the cybersecurity incident detected?	*How did the organisation know a cybersecurity incident was happening?*
What controls were in place to detect the cybersecurity incident?	
Were those controls effective?	*Did they work? Why/why not?* *How could they be improved?*
Are there any ways to improve the 'time to detection'?	*How could the organisation reduce that time?*
Are there any indicators that can be used to detect similar cybersecurity incidents in the future?	
Are there any additional tools or resources that are required in the future to detect similar cybersecurity incidents?	*Is there anything from a detection perspective that would help mitigate future cybersecurity incidents?*
Any other findings and/or suggestions for improvement?	*What activities worked well? What activities did not work so well? What could be changed with hindsight?* *See the PPOSTTE model for guidance.*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the action register.* *Brief description of action > Proposed action officer.*
RESPONSE	
What was the cause of the cybersecurity incident?	
How was the cybersecurity incident resolved?	*What needed to happen for the cybersecurity incident to be resolved?*
What obstacles were faced when responding to the cybersecurity incident?	

Were any business processes and procedures used in responding to the cybersecurity incident?	*For example, does the organisation have a CIRP, and was this followed?*
Were those business processes and procedures effective?	*Did they work? Why/why not?*
What delays and obstacles were experienced when responding?	
Were there any escalation points?	*Were there any escalation points that the cybersecurity incident went through?*
If there were escalation points, did they hamper the response or were they at the appropriate level?	*For example, having to escalate to a chief operating officer to take action on an ongoing cybersecurity incident had severe timeline impacts for the response.*
How well did the information sharing and communications work within your organisation?	*What worked well/what did not work well? How could it be improved?* *Was there any information that was needed sooner?* *How did the organisation communicate within the IR team, across jurisdictions, across time zones, legal teams and external comms teams?*
Were there any media enquiries received during the cybersecurity incident?	*If yes, how did the organisation respond?*
Was media produced during the cybersecurity incident?	*If yes, what was the media that was produced?*
Were stakeholders and/or customers notified during the cybersecurity incident?	*Why/why not? When? How?* *Was it effective? How could it be improved?*
Were trained personnel available to respond?	*Are there any personnel knowledge and/or skills gaps? What are they?* *Were there enough resources available to respond?*
Any other findings and/or suggestions for improvement?	*See the PPOSTTE model for guidance.*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the action register.* *Brief description of action > Proposed action officer.*
RECOVERY	

How long did it take for all systems, services and networks to recover?	
How could this time be improved?	*For example, how could the recovery time be reduced?*
Are there any obligations to report externally about the cybersecurity incident?	*If yes, to who?*
Were there any media enquiries after the cybersecurity incident?	*If yes, how did the organisation respond?*
Were stakeholders and/or customers notified following the cybersecurity incident?	*Why/why not? When? How?* *Was it effective? How could it be improved?*
Any other findings and/or suggestions for improvement?	*See the PPOSTTE model for guidance.*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the action register.* *Brief description of action > Proposed action officer.*

Appendix I: Action register template

ID	Action	Action Officer	Date Expected to Completed	Status	Updates	Comments
01	*Describe the action in detail.*	*Name of the person who will be leading the action.*	*Date the action is expected to be completed.*	*Complete* *In progress* *Not yet started*	*Insert date, and any updates to progressing the action.* *Detail any blockers here.*	*Any relevant information relating to closing out the action.*

Appendix J: Role cards

Example of a role card:

ROLE CARD – CYBER SECURITY INCIDENT

INCIDENT MANAGER

RESPONSIBILITIES

- Activate the CSIRP.
- Coordinate operations room setup.
- Manage a team of incident responders including preparing for, and tracking, daily investigation tasks.
- Provide administrative and logistical support for incident responders.
- Manage the passage of relevant operational information to the SEMT.

ROLE CARD – CYBER SECURITY INCIDENT

KEY CONTACTS

Virtual Meeting Room:
XXXX

Backup conference line:
XXXX

Media:
XXXX

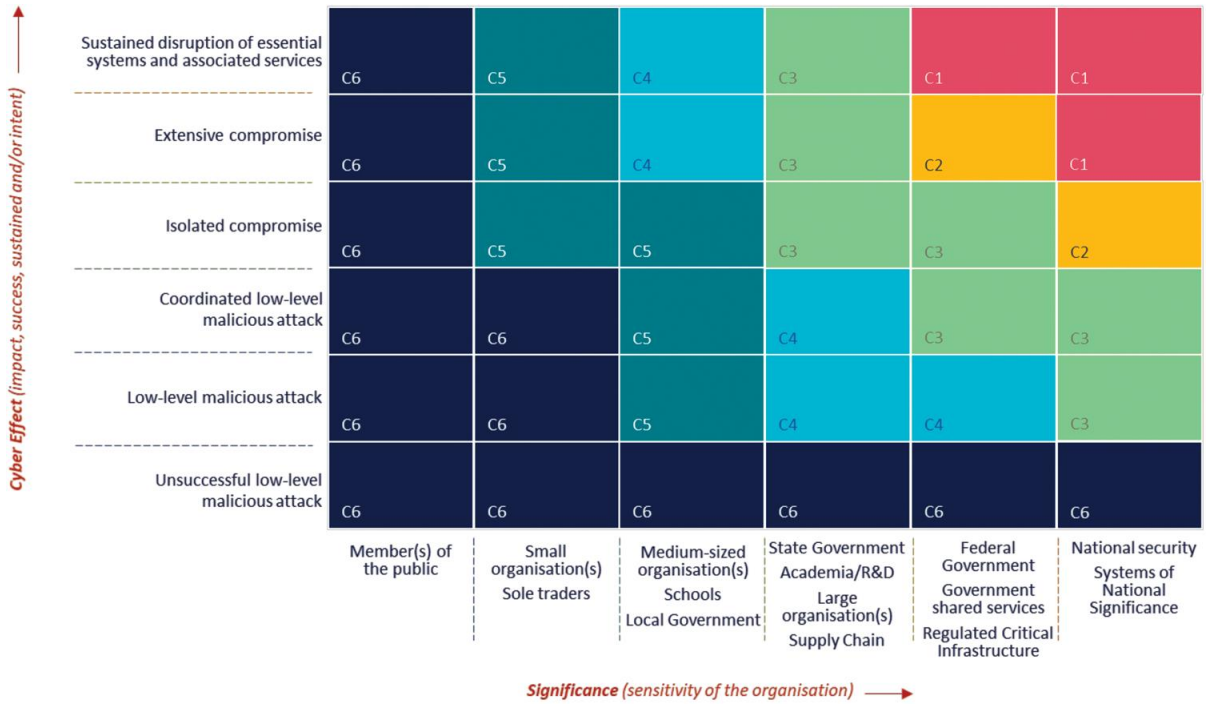
Security:
XXXX

Legal:
XXXX

Appendix K: ASD cybersecurity incident categorisation matrix

ASD categorises cybersecurity incidents by severity using a matrix that considers the:

- cyber effect (i.e. the impact, success, sustained and/or intent)
- significance (i.e. sensitivity of the organisation).



The severity of the cybersecurity incident informs the type and nature of cybersecurity incident response and crisis management arrangements that are activated. Depending on the severity of the cybersecurity incident, ASD has a suite of capabilities that it may deploy to support the affected parties. However, ASD determines which capabilities are appropriate and available given competing priorities. Organisations must not rely on ASD for their ability to respond to cybersecurity incidents in an appropriate and timely manner.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate