

**CYBER INCIDENT**

**RESPONSE PLAN**

**TEMPLATE**

**cyber**.gov.au

**Table of Contents**

[1. Authority and Review 4](#_Toc107824822)

[2. Purpose and Objectives 5](#_Toc107824823)

[3. Standards and Frameworks 5](#_Toc107824824)

[4. High Level Incident Response Process 6](#_Toc107824825)

[5. Common Security Incidents and Responses 7](#_Toc107824826)

[5.1. Common Threat Vectors 7](#_Toc107824827)

[5.2. Common Cyber Incidents 8](#_Toc107824828)

[6. Roles and Responsibilities 9](#_Toc107824829)

[6.1. Points of Contact for Reporting Cyber Incidents 9](#_Toc107824830)

[6.2. Cyber Incident Response Team (CIRT) 9](#_Toc107824831)

[6.3. Senior Executive Management Team (SEMT) 10](#_Toc107824832)

[6.4. Roles and Relationships 10](#_Toc107824833)

[7. Communications 11](#_Toc107824834)

[7.1. Internal Communications 11](#_Toc107824835)

[7.2. External Communications 11](#_Toc107824836)

[8. Supporting Procedures and Playbooks 12](#_Toc107824837)

[8.1. Supporting Standard Operating Procedures (SOPs) 12](#_Toc107824838)

[8.2. Supporting Playbooks 12](#_Toc107824839)

[9. Sector, Jurisdictional and National Incident Response Arrangements 13](#_Toc107824840)

[9.1. Sector Arrangements 13](#_Toc107824841)

[9.2. Jurisdictional Arrangements 13](#_Toc107824842)

[9.3. National Arrangements 13](#_Toc107824843)

[10. Incident Notification and Reporting 14](#_Toc107824844)

[10.1. Legal and Regulatory Requirements 14](#_Toc107824845)

[10.2. Insurance 14](#_Toc107824846)

[INCIDENT RESPONSE PROCESS 15](file:///\\d85userdata.dpe.protected.mil.au\ol\olivia.gardiner\My%20Documents\Projects\CIRP\Final%20documents\26%20MAY%202022%20-%20Cyber%20Incident%20Response%20Plan%20Template%20-%20FINAL.docx#_Toc107824847)

[11. Detection, Investigation, Analysis and Activation 16](#_Toc107824848)

[11.1. Incident Classification 16](#_Toc107824849)

[11.2. Cyber Incident Response Team (CIRT) Activation 16](#_Toc107824850)

[11.3. Investigation Questions 17](#_Toc107824851)

[11.4. Escalation and De-escalation 17](#_Toc107824852)

[12. Containment, Evidence Collection & Remediation 18](#_Toc107824853)

[12.1. Containment 18](#_Toc107824854)

[12.2. Documentation 18](#_Toc107824855)

[12.3. Evidence Collection and Preservation 18](#_Toc107824856)

[12.4. Remediation Action Plan 19](#_Toc107824857)

[13. Recovery 20](#_Toc107824858)

[13.1. Stand Down 20](#_Toc107824859)

[14. Learn and Improve 21](#_Toc107824860)

[14.1. Post Incident Review 21](#_Toc107824861)

[14.2. Update and Test Cyber Incident Response Plan 22](#_Toc107824862)

[14.3. Training 22](#_Toc107824863)

[APPENDICES 23](file:///\\d85userdata.dpe.protected.mil.au\ol\olivia.gardiner\My%20Documents\Projects\CIRP\Final%20documents\26%20MAY%202022%20-%20Cyber%20Incident%20Response%20Plan%20Template%20-%20FINAL.docx#_Toc107824864)

[Terminology and Definitions 24](#_Toc107824865)

[Cyber Incident Response Readiness Checklist 25](#_Toc107824866)

[ACSC Incident Triage Questions 28](#_Toc107824867)

[Situation Report Template 29](#_Toc107824868)

[Incident Log Template 30](#_Toc107824869)

[Evidence Register Template 31](file:///\\d85userdata.dpe.protected.mil.au\ol\olivia.gardiner\My%20Documents\Projects\CIRP\Final%20documents\26%20MAY%202022%20-%20Cyber%20Incident%20Response%20Plan%20Template%20-%20FINAL.docx#_Toc107824870)

[Remediation Action Plan Template 32](file:///\\d85userdata.dpe.protected.mil.au\ol\olivia.gardiner\My%20Documents\Projects\CIRP\Final%20documents\26%20MAY%202022%20-%20Cyber%20Incident%20Response%20Plan%20Template%20-%20FINAL.docx#_Toc107824871)

[Post Incident Review Analysis Template 33](#_Toc107824872)

[Action Register Template 39](file:///\\d85userdata.dpe.protected.mil.au\ol\olivia.gardiner\My%20Documents\Projects\CIRP\Final%20documents\26%20MAY%202022%20-%20Cyber%20Incident%20Response%20Plan%20Template%20-%20FINAL.docx#_Toc107824873)

[Role Cards 40](#_Toc107824874)

[ACSC Incident Categorisation Matrix 2022 41](#_Toc107824875)

# Authority and Review

Document Control and Review

|  |  |
| --- | --- |
| **Document Control** |  |
| Author |  |
| Owner |  |
| 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** |
|  |  |  |  |

# Purpose and Objectives

**Purpose of the CIRP**

**Objectives of the CIRP**

# Standards and Frameworks

# High Level Incident Response Process

# Common Security Incidents and Responses

A list of commonly used terms and definitions is provided at [Appendix A](#_Terminology_and_Definitions).

### Common Threat Vectors

The following table contains common threat vectors from the NIST Computer Security Incident Handling Guide.

|  |  |
| --- | --- |
| **Type** | **Description** |
| **External/Removable Media** | An attack executed from removable media or a peripheral device (e.g. malicious code spreading onto a system from an infected USB flash drive). |
| **Attrition** | An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g. a DDoS intended to impair or deny access to a service or application or a brute force attack against an authentication mechanism, such as passwords). |
| **Web** | An attack executed from a website or web-based application (e.g. a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware). |
| **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). |
| **Supply Chain Interdiction** | An antagonistic attack on hardware or software assets utilising physical implants, Trojans or backdoors, by intercepting and modifying an asset in transit from the vendor or retailer. |
| **Impersonation** | An attack involving replacement of something benign with something malicious (e.g. spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation). |
| **Improper usage** | Any incident resulting from violation of an organisation’s acceptable usage policies by an authorised user, excluding the above categories (e.g. a user installs file sharing software, leading to the loss of sensitive data). |
| **Loss or Theft of Equipment** | The loss or theft of a computing device or media used by an organisation (e.g. a laptop, smartphone or authentication token). |

### Common Cyber Incidents

The following table provides a list of common cyber incident types and corresponding initial response activities.

|  |  |
| --- | --- |
| **Type/Description** | **Response** |
| **Denial of Service (DoS) and Distributed Denial of Service (DDoS):** overwhelming a service with traffic, sometimes impacting availability. |  |
| **Phishing:** deceptive messaging designed to elicit users’ sensitive information (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. |  |
| **Malware:** a Trojan, virus, worm, or any other malicious software that can harm a computer system or network. |  |
| **Data breach:** unauthorised access and disclosure of information. |  |
| **Industrial Control System compromise:** unauthorised access to ICS. |  |

# Roles and Responsibilities

This section includes details of the roles and responsibilities of core individuals and teams responsible for incident response and decision making, including the operational level Cyber Incident Response Team (CIRT) and the strategic level Senior Executive Management Team (SEMT).

All personnel listed here should be familiar with their responsibilities in this plan and practise their response.

### Points of Contact for Reporting Cyber Incidents

Primary and secondary (backup) internal points of contact to report cyber incidents to over a 24/7 period.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Hours of Operation** | **Contact Details** | **Role Title** | **Responsibilities** |
|  |  |  |  |  |

### Cyber Incident Response Team (CIRT)

CIRT members responsible for managing responses to cyber incidents:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Organisation Role** | **Contact Details** | **CIRT Role Title** | **CIRT Responsibilities** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

For more significant cyber security incidents the CIRT could be expanded to include:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Organisation Role** | **Contact Details** | **CIRT Role Title** | **CIRT Responsibilities** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

#### Surge Arrangements

### Senior Executive Management Team (SEMT)

Significant cyber 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).

SEMT members responsible for managing responses to cyber incidents:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Contact Details** | **Title** | **SEMT Role** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Roles and Relationships

The following diagram reflects the relationship between the key personnel and teams involved in the response.

# Communications

### Internal Communications

### External Communications

A picture containing icon

Description automatically generated

# Supporting Procedures and Playbooks

### Supporting Standard Operating Procedures (SOPs)

The Standard Operating Procedures (SOPs) available to support incident response efforts include:

### Supporting Playbooks

The playbooks available to provide step-by-step guidance for responses to common incidents include:

Icon

Description automatically generated

# Sector, Jurisdictional and National Incident Response Arrangements

The relevant sector, state and/or territory and national arrangements are detailed in this section.

### Sector Arrangements

### Jurisdictional Arrangements

### National Arrangements

[Appendix C](#_ACSC_Incident_Triage) provides the ACSC’s incident triage questions.

# Incident Notification and Reporting

Processes for internal and external incident notification and reporting include:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Incident type/**  **threshold** | **Organisation/agency to receive notification or report** | **Contact details for the notifying organisation/agency** | **Key notifying/reporting requirements and link to organisation/agency information** | **Personnel responsible** |
|  |  |  |  |  |
|  |  |  |  |  |

### Legal and Regulatory Requirements

### Insurance

Diagram

Description automatically generated

INCIDENT  
RESPONSE PROCESS

# Detection, Investigation, Analysis and Activation

### Incident Classification

For example:

|  |  |
| --- | --- |
| **Incident Classification** | **Descriptions** |
| **Critical** |  |
| **High** |  |
| **Medium** |  |
| **Low** |  |

For information about the ACSC Incident Categorisation Matrix see [Appendix K](#_ACSC_Incident_Categorisation).

### Cyber Incident Response Team (CIRT) Activation

#### Logistics and Communications

### Investigation Questions

To guide the incident response efforts and understanding of the scope and impact of the incident, develop a list of investigation questions for each incident. Not all questions may be answerable with the data available and questions may change as your investigation progresses.

Possible initial investigation questions include:

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

### Escalation and De-escalation

The triggers and/or thresholds and decision making authorities for incident escalation and de-escalation include:

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident Classification** | **Action** | **Triggers and/or thresholds for escalation and de-escalation** | **Minimum level authority** |
| **Critical** | De-escalate to High |  |  |
| **High** | Escalate to Critical |  |  |
| De-escalate to Medium |  |  |
| **Medium** | Escalate to High |  |  |
| De-escalate to Low |  |  |
| **Low** | Escalate to Medium |  |  |

# Containment, Evidence Collection & Remediation

### Containment

Containment actions are implemented in order to minimise the damage, prevent the incident from spreading or escalating, and prevent the attacker from destroying evidence of their attack.

When planning containment actions, consider:

* Any additional impacts there could be to systems/services
* Time and resources required to contain the incident
* Effectiveness of the containment solution (e.g. partial vs full containment)
* Duration that the solution will remain in place (e.g. temporary vs permanent solution)

### Documentation

All incidents should be documented. For each incident, identify the responsible personnel, recipients of the information, and timeframes. Refer to [Appendix D](#_Situation_Report_Template) for a Situation Report template and [Appendix E](#_Incident_Log_Template) for an Incident Log template.

Situation reports may contain the following information:

* Incident date and time
* Status of the incident
* Incident type and classification
* Scope and Impact
* Severity
* External assistance required
* Actions taken to resolve the incident
* Contact details for incident manager and key CIRT personnel
* Date and time of the next update

### Evidence Collection and Preservation

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, IP address and hash values). See the Evidence Register template at [Appendix F](#_Evidence_Register_Template) to capture this information.

### Remediation Action Plan

A Remediation Action Plan is to be developed and implemented for eradicating and resolving the incident following successful containment and evidence collection. See [Appendix G](#_Remediation_Action_Plan) for a template.

When developing the Remediation Action Plan, consider:

* What actions are required to eradicate/resolve the incident?
* What resources are required to resolve the incident (if not already included in the CIRT)?
  + Are there additional external resources you may require?
* Who is responsible for remediation actions?
* What systems/services should be prioritised?
* What systems/services will be affected during the remediation process? How will these systems be affected?
* What is the expected resolution time?

# Recovery

Develop a recovery plan that details the approach to recovering IT and/or OT networks, systems and applications once containment and eradication is complete.

When developing the Recovery Plan, consider:

* How systems will be restored to normal operation and expected timeframes?
* How systems will be monitored to ensure they are no longer compromised and are functioning as expected?
* How identified vulnerabilities will be managed to prevent similar incidents?

### Stand Down

A picture containing text, electronics

Description automatically generated

# Learn and Improve

### Post Incident Review

A Post Incident Review (PIR) is a detailed review conducted after a cyber security incident.

Key questions to consider in the PIR:

* What were the root causes of the incident and any incident response issues?
* Could the incident have been prevented? How?
* What worked well in the response to the incident?
* How can our response be improved for future incidents?

The PIR Guide and Template with more detailed questions to consider is available at [Appendix H](#_Post_Incident_Review). Recommendations that arise from the review can be documented in a corresponding Action Register.  
Use the template at [Appendix I](#_Action_Register_Template).

#### PPOSTTE Model

The PPOSTTE model can assist to reflect on key elements of the 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**  *This only applies to exercises* | Exercise development, structure, management, conduct |

### Update and Test Cyber Incident Response Plan

The PIR may result in changes to the CIRP, Playbooks and Templates. Changes should be communicated  
to the relevant personnel.

### Training

Icon

Description automatically generated

****

APPENDICES

**Appendix A**

### Terminology and Definitions

Use of consistent and pre-defined terminology to describe incidents and their effects can be helpful during a response. In your CIRP, include commonly used terms used in your organisation. ACSC defines cyber threats, events, alerts and incidents as follows:

**Cyber threat**

A cyber threat is any circumstance or event with the potential to harm systems or information. Other threats are listed on [cyber.gov.au](https://www.cyber.gov.au/acsc/view-all-content/threats/large-organisations-and-infrastructure). Organisations can include a list of cyber threats of concern. The ACSC Annual Cyber Threat Report (2021) outlines the following threat environment and key cyber security trends:

* COVID-19 themed malicious activity including phishing emails and scams
* Ransomware
* Exploitation of security vulnerabilities
* Software supply chain compromise
* Business Email Compromise
* Cybercrime

**Cyber security event**

A cyber security 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.

A cyber security event has the potential to become, but is not confirmed to be, a cyber incident.

Examples of cyber security 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 system.

**Cyber security alert**

A cyber security alert is a notification generated in response to a deviation from normal behaviour.  
Cyber security alerts are used to highlight cyber security events.

**Cyber incident**

A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that have  
a significant probability of compromising business operations. A cyber incident requires corrective action.

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

* Denial-of-service attacks (DoS)
* Unauthorised access or attempts to access a system
* Compromise of sensitive information
* Virus or malware outbreak (including ransomware).

**Appendix B**

### Cyber Incident Response Readiness Checklist

This checklist is to aid your organisation’s initial assessment of its readiness to respond to a cyber security incident. This checklist is not an exhaustive list of all readiness activities.

|  |  |
| --- | --- |
| **Preparation** | |
|  | Your organisation has a cyber security policy or strategy that outlines your organisation’s approach to prevention, preparedness, detection, response, recovery, review and improvement.   * For example, does your organisation have a position on, for example, paying ransom, reporting incidents to government, publicly acknowledging cyber incidents, sharing information about incidents with trusted industry and government partners? |
|  | A Cyber Incident Response Plan has been developed, which:   * Aligns with your organisation's operating environment and other processes, including emergency management and business continuity processes. * Has been reviewed or tested in an exercise to ensure it remains current and responsible personnel are aware of their roles, responsibilities and processes. * Templates have been prepared, for example Situation Reports. |
|  | Staff involved in managing an incident have received incident response training. |
|  | Up-to-date hard copy versions of the Cyber Incident Response Plan and playbooks are stored in a secure location (in case of electronic or hardware failure) and are accessible to authorised staff members. |
|  | Specific playbooks to supplement the Cyber Incident Response Plan have been developed, that define step-by-step guidance for response actions to common incidents, and roles and responsibilities. |
|  | A Cyber Incident Response Team (CIRT) and a Senior Executive Management Team (SEMT) – or equivalents - have been formed to manage the response, with approved authorities. |
|  | All relevant IT and OT Standard Operating Procedures (SOPs) are documented and have been reviewed or tested in an exercise to ensure they remain current and responsible personnel are aware of their roles, responsibilities and processes. |
|  | Arrangements for service providers, including cloud and software as a service, to provide and retain logs have been established and tested to ensure these include useful data and can be provided in a timely manner. |
|  | Log retention for critical systems have been configured adequately and tested to confirm that they capture useful data. Refer to the [ACSC publications](https://www.cyber.gov.au/publications) including [Windows Event Logging and Forwarding](https://www.cyber.gov.au/acsc/view-all-content/publications/windows-event-logging-and-forwarding) for specific guidance. |
|  | Your organisation has internal or third party arrangements and capabilities to detect and analyse incidents. If these capabilities are outsourced, your organisation has an active service agreement/contract. |
|  | Critical assets (data, applications and systems) have been identified and documented. |
|  | Standard Operating Procedures (SOPs) have been developed, and roles and responsibilities assigned for use of facilities and communications technologies in response to cyber incidents, and these resources are confirmed as available. This includes for alternative/back-up ICT-based channels. |
|  | Incident logging/records and tracking technologies used to manage a response are confirmed as available and have been tested. |
|  | Role cards have been developed for each person involved in the CIRT and the SEMT. Individual actions will depend on the type and severity of the incident. Example role card is available at [Appendix J](#_Role_Cards). |
|  | Your organisation has internal or third party arrangements and capabilities to monitor threats. Situational awareness information is collected from internal and external data sources, including:   * Local system and network traffic and activity logs * News feeds concerning ongoing political, social, or economic activities that might impact incident activity * External feeds on incident trends, new attack vectors, current attack indicators and new mitigation strategies and technologies. |
| **Detection, Investigation, Analysis and Activation** | |
| Standard Operating Procedures (SOPs) have been developed, and roles and responsibilities assigned for: | |
|  | Detection mechanisms which can be used to identify potential information security incidents, such as scanning, senses and logging mechanisms. These mechanisms require monitoring processes to identify unusual or suspicious activity, for example behaviour and logging, commensurate with the impact of an incident. Common monitoring techniques include:   1. 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; 2. scanning for unauthorised hardware, software and changes to configurations; 3. sensors that provide an alert when a measure breaches a defined threshold(s) (e.g. device, server and network activity); 4. logging and alerting of access to sensitive data or unsuccessful logon attempts to identify potential unauthorised access; and 5. users with privileged access accounts subject to a greater level of monitoring in light of the heightened risks involved.[[1]](#footnote-1) |
|  | Incident detection, including self-detected incidents, notifications received from service providers or vendors, and notifications received from trusted third parties (e.g. ACSC). |
|  | Incident analysis, including how incidents are to be categorised, classified and prioritised, and controls related to how data is stored and transmitted (i.e. if out-of-band transmission is required). |
|  | Activating a Cyber Incident Response Team (CIRT) to manage critical incidents, with roles and responsibilities assigned. |
|  | Activating a Senior Executive Management Team (SEMT) to manage critical incidents, with roles and responsibilities assigned. |
| **Containment, Evidence Collection and Remediation** | |
|  | Standard Operating Procedures (SOPs), playbooks and templates, have been developed, and roles and responsibilities assigned for containment, evidence collection and remediation. These can be included as appendices to the Cyber Incident Response Plan. |
|  | A secure location is available for storing data captured during an incident, which could be used as evidence of the incident and the adversary’s tradecraft, and ready to be provided to third-party stakeholders if needed. |
| **Communications** | |
|  | Policy, plans, Standard Operating Procedures (SOPs) and templates have been developed to support communicating with:   * Internal stakeholders (e.g. Board, staff) * External stakeholders (e.g. stakeholders to assist with the response and stakeholders with an interest in the response) |
|  | Policy, plans, Standard Operating Procedures (SOPs) 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 subject matter experts. |
|  | Staff have been trained to implement the communications processes and execute their roles and responsibilities. |
|  | Staff who are not involved in managing incidents are cognisant of your organisation’s policy and processes and their responsibilities when an incident occurs (e.g. exercising discretion, using approved talking points, referring enquiries to the designated officer). |
| **Incident Notification and Reporting** | |
|  | Processes and contact details are documented to support the organisation to meet its legal and regulatory requirements on cyber incident notification, reporting and response, with roles and responsibilities within your organisation are assigned. This includes the processes for obtaining authority to release and share information. |
|  | Processes are documented for insurance requirements. |
| **Post Incident Review** | |
|  | A process is documented to conduct Post Incident Reviews (PIR) following conclusion of an incident and PIR reports with recommendations are submitted to management for endorsement. |
|  | A process is documented to ensure actions following incidents and/or exercises are tracked and completed (e.g. Action Register). |

**Appendix C**

### ACSC Incident Triage Questions

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

* Who is reporting the incident? (include their position e.g. CISO, ITSA, SOC Manager etc.)
* Who/what is the affected organisation/entity?
* What type of incident is being reported? (e.g. ransomware, denial of service, data exposure, malware)
* Is the incident still active?
* When was the incident first identified?
* Are you reporting for ACSC awareness or is ACSC assistance required?
  + If ACSC assistance is required, what assistance is needed?
* What type of system or network has been affected?
  + Information Technology (IT)
    - Corporate systems/networks, databases, servers, VOIP systems.
  + Operational Technology (OT)
    - SCADA, Remote sensors, BMS/BAS, logic controllers.
* What was observed (the sequence of events)? E.g. was lateral movement observed?
  + Date/Time
  + Effect/Event
* Who or what identified the problem?
* Has a data breach occurred?
  + What type of information was exposed?
    - What impact will this have on the organisation?
    - What impact (if any) will the breach have on public safety or services?
  + What volume of records/data was exposed?
  + Was it a misconfiguration/error, or was a malicious exfiltration or theft of data identified?
  + Has it been reported to the Office of the Australian Information Commissioner (OAIC)?
    - If not, organisations need to consider if mandatory reporting obligations apply under the Notifiable Data Breach (NDB) scheme
* What actions have been taken to rectify the issue?
  + Does the organisation/entity have internal or external IT and/or cyber security incident response providers?
  + Are services/business as usual operations interrupted?
    - If so, how long do they expect before they are back at normal operating capability?
* Will you be communicating publicly about the incident and engaging with media?
  + If so, please notify the ACSC beforehand if you will be referencing the ACSC.

**Appendix D**

### Situation Report Template

|  |  |  |
| --- | --- | --- |
| **Date of entry:** | **Time of entry:** | **Author:** |
| **Date and Time incident detected** |  | |
| **Current Status** – New, In Progress, Resolved |  | |
| **Incident Type** |  | |
| **Incident Classification** |  | |
| **Scope** – list the affected networks, systems and/or applications; highlight any change to scope since the previous log |  | |
| **Impact** – list the affected stakeholder(s); highlight any change in impact since the previous log entry |  | |
| **Severity** – outline the impact of the incident on your organisation(s) and public safety or services; highlight any change to severity since the previous log entry |  | |
| **Notifications**  **Actioned/Pending** |  | |
| **Assistance required** – what assistance do we require from other organisations? (e.g. ACSC, law enforcement) |  | |
| **Actions taken to resolve incident** |  | |
| **Additional notes** |  | |
| **Contact details for incident manager and others if required** |  | |
| **Date and Time of next update** |  | |

**Appendix E**

### Incident Log Template

|  |  |
| --- | --- |
| **Date and Time** | **Notes**  (relevant facts, decisions, rationale) |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Appendix F**

### Evidence Register Template

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Access** |  |  |  |  |  |
| **Storage location and label number** |  |  |  |  |  |
| **Item Details**  (quantity, serial number, model number, hostname, media access control (MAC) address, IP addresses and hash values) |  |  |  |  |  |
| **Collected by**  (name, title, contact and phone number) |  |  |  |  |  |
| **Date, Time and Location of collection** |  |  |  |  |  |

**Appendix G**

### Remediation Action Plan Template

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Status**  (unallocated, In Progress, Completed) |  |  |  |  |  |
| **Action Owner** |  |  |  |  |  |
| **Action** |  |  |  |  |  |
| **Category**  (Contain, Eradicate, Recover) |  |  |  |  |  |
| **Date and Time** |  |  |  |  |  |

**Appendix H**

### Post Incident Review Analysis Template

**Incident Summary**

|  |  |
| --- | --- |
| Incident name |  |
| Date of incident | *dd/mm/yy* |
| Incident Priority | *Low/Medium/High*  *Established from the impact and/or risk to the business* |
| Time incident occurred |  |
| Time incident was resolved |  |
| Incident type | *Malware, etc.* |
| Personnel involved | *Names of the individuals involved in resolving the incident and their function(s), including any service providers* |
| Incident impact | *What impact did the incident have? I.e. loss of systems* |
| Brief summary | *What happened?* |

**Incident Analysis**

The Incident Analysis is broken into the following categories:

* **Incident timeline** – Summary of what happened and when. Provides high level areas for improvement.
* **Protection** – Identifies the protection mechanisms that were in place at the time of the incident and their effectiveness. Establishes how to improve the protection of our systems and networks.
* **Detection** – Establishes how to reduce the time to identify an incident is occurring. Addresses what detection mechanisms were in place, and how those mechanisms can be improved.
* **Response** – Identifies improvements for the incident response.
* **Recovery** – Addresses improvements for incident recovery (i.e. how to recover from an incident faster).

|  |  |
| --- | --- |
| **INCIDENT TIMELINE** | |
| **Date and time of detection** |  |
| **When was the incident acknowledged?** | *When did your organisation identify that an incident was occurring?* |
| **Date and time of incident response** |  |
| **Date and time of incident recovery** |  |
| **Who discovered the incident first and how?** | *Or who was alerted to it first? How did the discovery or alert happen?* |
| **Was the incident reported externally? If yes, when?** | *For example, did your organisation report it to the ACSC?* |
| **Who supported resolving the incident? When did they provide support?** | *List the names of personnel involved in resolving the incident, and the time (and date if not all on the same day) they joined in.* |
| **What activities were conducted to resolve the 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 an incident similar to this?** | *I.e. systems, networks, etc.* |
| **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 incident?** | *What are they?* |
| **What business processes were in place to prevent this type of incident from occurring?** | *I.e. Your organisation’s policies and procedures.* |
| **How effective were those business processes?** | *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* |

|  |  |
| --- | --- |
| **INCIDENT DETECTION** | |
| **How was the incident detected?** | *How did you know the incident was happening?* |
| **What controls were in place to detect the incident?** |  |
| **Were those controls effective?** | *Did they work? Why/why not?* |
| **What business processes were in place to detect the incident?** |  |
| **Were those business processes effective?** | *Did they work? Why/why not?* |
| **Are there any ways to improve the ‘time-to-detection’?** | *How could your organisation reduce that time?* |
| **Are there any indicators that can be used to detect similar incidents in the future?** |  |
| **Are there any additional tools or resources that are required in the future to detect similar incidents?** | *Is there anything (from a detection perspective) that will help mitigate future incidents?*  *Technology? Human resources with specific skills? Etc.* |
| **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?*  *\*\*Also 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* |

|  |  |
| --- | --- |
| **INCIDENT RESPONSE** | |
| **What was the cause of the incident?** |  |
| **How was the incident resolved?** | *What needed to happen for the issue to be resolved?* |
| **What obstacles were faced when responding to the incident?** |  |
| **Were any business policies and/or procedures used in responding to the incident?** | *For example, does your organisation have an Incident Response Plan, and was this followed?* |
| **Were those business policies and/or 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 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 (COO) to take action on an ongoing incident had severe timeline impacts on responding to an active incident.* |
| **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 your organisation communicate within the IR team, across jurisdictions, across time zones, legal teams, external comms teams, etc.?* |
| **Were there any media enquiries received during the incident?** | *If yes, WHAT was the media, and how did your organisation respond?* |
| **Was media produced during the incident?** | *If yes, WHAT was the media, and how did your organisation respond?* |
| **Was the customer notified during the incident?** | *Why/why not? When? How?* |
| **Were trained staff available to respond?** | *Are there any staff 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* |

|  |  |
| --- | --- |
| **INCIDENT RECOVERY** | |
| **How long did it take for all systems 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 incident?** |  |
| **Were there any media enquiries after the incident?** |  |
| **Were staff and/or customers notified of the incident?** | *Why/why not?*  *How was the notification completed? 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* |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Comments** | *Any relevant information relating to closing out he action* |  |  |  |  |
| **Updates**  **Appendix I** Action Register Template | *Insert date, and any updates to progressing the action*  *You can also detail any blockers here* |  |  |  |  |
| **Status** | *Complete*  *In Progress*  *Not yet started* |  |  |  |  |
| **Date expected to complete** | *Date the action is expected to be completed* |  |  |  |  |
| **Action Officer** | *Name of the person who will be leading the action* |  |  |  |  |
| **Action** | *Describe the action in detail* |  |  |  |  |
| **ID** | 01 | 02 | 03 | 04 | 05 |

**Appendix J**

### Role Cards

Example of a role card:

**ROLE CARD – CYBER INCIDENT RESPONSE**

**Virtual Meeting Room:**

XXXX

**Backup conference line:**

XXXX

**Media:**

XXXX

**Security:**

XXXX

**Legal:**

XXXX

**KEY CONTACTS**

**ROLE CARD – CYBER INCIDENT RESPONSE**

Reports to SEMT Chair

**RESPONSIBILITIES**

* Activate the CIRP
* 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

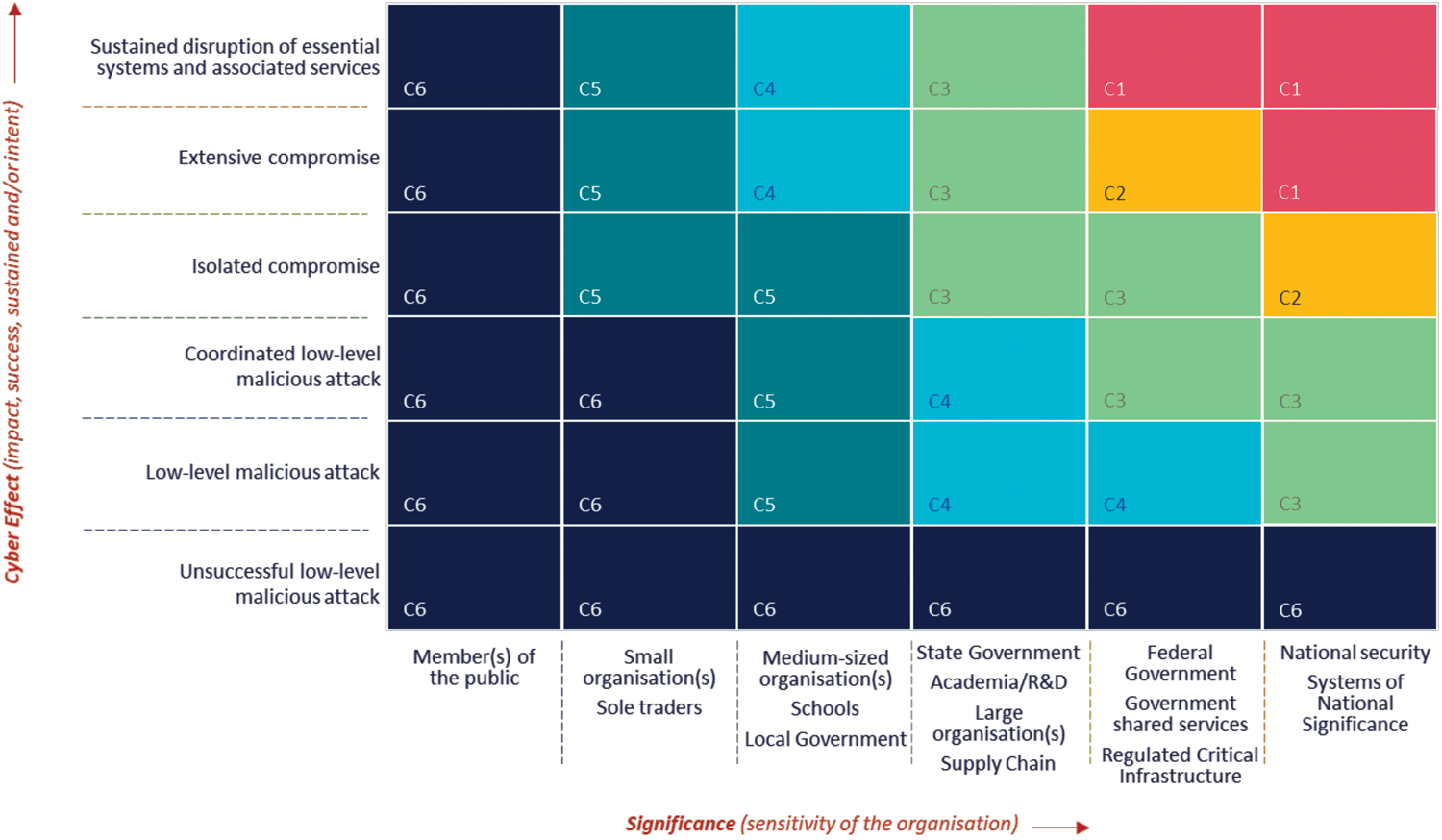
**INCIDENT MANAGER**

**Appendix K**

### ACSC Incident Categorisation Matrix 2022

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

1. APRA Prudential Practice Guide CPG 234 Information Security. [↑](#footnote-ref-1)