SACSF/T1.0

GOVERNMENT TEMPLATE ON CYBER SECURITY

**Cyber Security Incident Response Plan (Template)**

**Table of Contents**

[Introduction 3](#_Toc148995424)

[Purpose 3](#_Toc148995425)

[Objectives 3](#_Toc148995426)

[High Level Incident Response Process 4](#_Toc148995427)

[Preparation 5](#_Toc148995428)

[Roles and Responsibilities 5](#_Toc148995429)

[Incident Classifications 8](#_Toc148995430)

[Escalation and De-escalation 10](#_Toc148995431)

[Evidence Acquisition and Preservation 11](#_Toc148995432)

[Detection and Analysis 11](#_Toc148995433)

[Signs of an Incident 11](#_Toc148995434)

[Common Cyber Security Incident Types 12](#_Toc148995435)

[Containment 14](#_Toc148995436)

[Eradication and Recovery 14](#_Toc148995437)

[Reporting and Notification 15](#_Toc148995438)

[Communication Plans 16](#_Toc148995439)

[Post-incident Activity 17](#_Toc148995440)

[Post Incident Review 17](#_Toc148995441)

[Lesson Learned 17](#_Toc148995442)

[Appendices 19](#_Toc148995443)

[Appendix A - Cyber Incident Response Readiness Checklist 19](#_Toc148995444)

[Appendix B - Incident Triage Questions 22](#_Toc148995445)

[Appendix C – Financial Impact Assessment 23](#_Toc148995446)

[Appendix D - Situation Report Template 24](#_Toc148995447)

[Appendix E - Sample Evidence Chain of Custody Form 25](#_Toc148995448)

[Appendix F - Evidence Register Template 26](#_Toc148995449)

[Appendix G - Remediation Action Plan Template 27](#_Toc148995450)

[Appendix H - Post Incident Review Analysis Template 28](#_Toc148995451)

[Appendix I – Incident Response Playbook Template 34](#_Toc148995452)

[Aboriginal Impact Statement 40](#_Toc148995453)

[Related documents 40](#_Toc148995454)

[References 40](#_Toc148995455)

[Definitions 40](#_Toc148995456)

[Acronyms 41](#_Toc148995457)

[Document Control 41](#_Toc148995458)

Introduction

This template contains instructions for use in grey italics. Delete these before finalising.

This document was built to align with the key stages of a standard cyber security incident response process, which contains the following four major sections:

1. Preparation – document the internal and external resources required for the cyber security incident response, define the structure of incident response teams, clarify the roles and responsibilities during incident response, define the common cyber security incident types and criticality / response priority levels, and the evidence collection and preservation requirements

2. Incident Handling – outline the detailed requirements and related security capabilities for the Detection, Analysis, Containment, Eradication and Recovery stages of cyber security incident management

3. Reporting and Notification – define the internal and external communication plans, reporting / notification requirements and channels

4. Post-incident Improvement – learn from incidents and continually improve the cyber security incident prevention and handling capabilities.

This document also contains relevant tools and templates in the **Appendices**.

Purpose

The purpose of this document is to formalise the processes across the key stages of cyber security incident response process to support a swift and effective response to cyber incidents, aligned with the agency’s security and business objectives, to minimise the impact of a cyber security incident and enhance security capability and business resilience.

Objectives

This document seeks to support cyber security incident response and enable the following information security management and business objectives:

* To provide guidance on the steps required to respond to cyber security incidents
* To outline the roles, responsibilities, accountabilities and authorities of personnel and teams required to manage responses to cyber security incidents
* To outline legal and regulatory compliance requirements during incident response
* To outline internal and external communication processes when responding to cyber incidents
* To provide guidance on post incident activities to support continuous improvement
* Protect agency’s information assets, sensitive data and incident evidence
* Limit immediate incident impact within agency’s information assets, customers and business partners.

High Level Incident Response Process

The cyber security incident response process should be defined by the agency, based on the business objectives, organisational structure, and information security policies and procedures.



Preparation

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).

Points of Contact for Reporting Cyber Incidents

Include details about primary and secondary (backup) internal points of contact for your staff or stakeholders to report cyber incidents to over a 24/7 period.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Hours of Operation** | **Contact Details** | **Role Title** | **Responsibilities** |
|  | 0700–1900  hrs AEST | Phone Number  Email Address | On-Call Point of Contact | Primary point of contact |
|  | 1900–0700  hrs AEST | Phone Number  Email Address | Backup point of contact | Secondary (backup) internal points of Contact |

Cyber Incident Response Team (CIRT)

This section should Include details of the CIRT responsible for managing responses to cyber incidents. The composition of agency CIRT will vary depending on the size of the agency and available skills and resources. In addition, also include details of any 3rd party vendors that provide or manage your ICT systems/applications. If applicable, include details of your external incident response providers and the services they provide.

Below is an example CIRT roles and responsibilities table:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Organisation Role** | **Contact Details** | **CIRT Role** | **CIRT Responsibilities** | |
|  |  | | Phone Number  Email Address | CIRT Team Lead | * Response planning * CIRT Operations * Escalation and de-escalation of incident classification * Containment strategy decision |
|  |  | | Phone Number  Email Address | Deputy CIRT Team Lead | * Situational analysis * Threat intelligence * Technical advice |
|  |  | | Phone Number  Email Address | First Responders | * Incident logging * Initial triage, resolution or escalation * Notify cyber incident point of contact |
|  |  | | Phone Number  Email Address | Incident Responder | * Technical investigation (collection and processing of network and host data) * Containment, eradication and recovery efforts * Investigation findings report |
|  |  | | Phone Number  Email Address | Security Manager | * Investigation (if suspected internal threat) * Law enforcement liaison |

Other CIRT roles could include system administrators, network engineers, auditing and change management. For more significant cyber security incidents the CIRT could be expanded to include:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Organisation Role** | **Contact Details** | **CIRT Role** | **CIRT Responsibilities** | |
|  |  | | Phone Number  Email Address | Communications, engagement and media advisor | * Information and warnings * Internal communications * Media and community liaison/ spokesperson |
|  |  | | Phone Number  Email Address | Human resources | * Investigate corporate policy violations |
|  |  | | Phone Number  Email Address | Business continuity advisor | * Facilities support * Business and community consequence analysis/ management |
|  |  | | Phone Number  Email Address | Legal advisor | * Legal advisory services (incl. regulatory compliance) |
|  |  | | Phone Number  Email Address | Finance and procurement advisor | * Facilities and finance support |
|  |  | | Phone Number  Email Address | Administration and record keeping | * Administration support, incl. Incident Log, Evidence and Situation Reporting |

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:

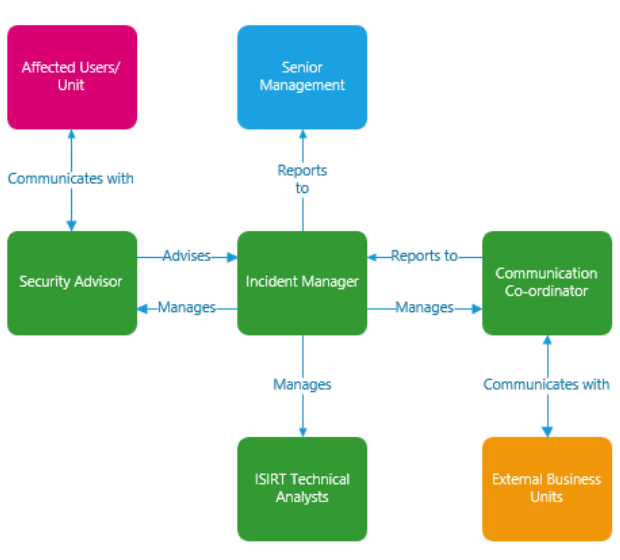
* Strategic issues identification and management
* Stakeholder engagement and communications (including Board and ministerial liaison, if applicable)
* Resource and capability demand (including urgent logistics or finance requirements, and human resources considerations during response effort).

Include details of the SEMT responsible for managing responses to cyber incidents. The composition and roles of the SEMT may vary depending on the incident impacts and size and structure of the agency, as some roles may not be relevant or multiple roles may be held by the same individual. Below is an example of SEMT table:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Contact Details** | **Title** | **SEMT Role** |
|  | Phone Number  Email Address | Chief Executive Officer | SEMT Chair |
|  | Phone Number  Email Address | Chief Information Officer | SEMT Deputy Chair |
|  | Phone Number  Email Address | Chief Information Security Officer | SEMT Deputy |
|  | Phone Number  Email Address | Chief Operating Officer | Operational functions of the business |
|  | Phone Number  Email Address | Chief Financial Officer/ Procurement Manager | Emergency procurement and expenditure oversight |
|  | Phone Number  Email Address | Legal Council | Regulatory compliance, cyber insurance |
|  | Phone Number  Email Address | Media and Communications Manager | Public relations and stakeholder engagement |
|  | Phone Number  Email Address | People and Culture Manager | Staff welfare management |

Roles and Relationships

A simple diagram could be added to reflect the relationship between the key personnel and teams involved in the response, which also indicate the escalation path. An example diagram is provided below.



Incident Classifications

This section includes the agency’s framework and decision making process for classifying a cyber incident. This can assist with prioritising resources and escalation. Classification factors could include:

* Effects of the incident (confidentiality, integrity and availability of information and systems)
* Stakeholders affected (internal and external)
* Incident type
* Impact on the business and community.

Agency should build the incident classification based on the internal service level expectations and the external service level agreements with managed service providers and incident containers. Consider any incident classifications already used by ICT services and if they should align. Below is an example of the incident classification table:

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident Classification** | **Description** | **Response Time** | **Restoration Time** |
| Critical  (Priority 1) | * Over 80% of staff (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. | 10 Minutes | 4 Hours |
| High  (Priority 2) | * 50% of staff 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. | 30 Minutes | 1 Day |
| Medium  (Priority 3) | * 20% of staff 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. | 1 Hour | 2 Days |
| Low  (Priority 4) | * <10% of non-critical staff 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. | 4 Hours | 3 Days |
| Informational  (Priority 5) | * A security event with no impact to information asset and business continuity. Examples include:   + Spam email with no embedded URL’s or attachments   + Automated malware detection alert requiring no further action. Single device, infection cleaned   + General cyber security advice   + False positive security alerts. | 7.5 Hours | N/A |

Escalation and De-escalation

Incident classification levels could change during the incident response process due to the further investigation and understanding of the impact. Agency should determine the escalation and de-escalation criteria and decision making methods. The following example includes the escalation and de-escalation triggers and/or thresholds, and decision making authorities:

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident**  **Classification** | **Action** | **Triggers and/or thresholds for escalation and de-escalation** | **Minimum level**  **authority** |
| Critical  (Priority 1) | De-escalate to High level incident | The senior management group determines that the critical incident can be de-escalated and recovered without long-term impact to the agency. | CE |
| High  (Priority 2) | Escalate to Critical level incident | The incident is realised to be critical, that a crisis or emergency response plan should be triggered. | Cyber Incident Manager |
| De-escalate to Medium level incident | CIRT determines the incident has lower impact than first estimation, that no critical systems or business operations are affected. | Cyber Incident Manager |
| Medium  (Priority 3) | Escalate to High level incident | The incident spread to wider user groups and devices, with potential fines or reputational damages to the agency. | First Responders |
| De-escalate to Low level incident | The incident is contained and limited impact caused to the agency. | Cyber Incident Manager |
| Low  (Priority 4) | Escalate to Medium level incident | CIRT discovers the impact of the incident increases and/or there is sensitive information involved. | First Responders |
| De-escalate to Informational level incident | CIRT determines the incident has no impact to information assets or it turns out to be a false positive alert. | Security Manager |
| Informational  (Priority 5) | Escalate to Low level incident | Help Desk team determines the security event may impact BAU activity, which should be handled as an incident | Help Desk Team Lead |

Evidence Acquisition and Preservation

Evidence needs to be acquired and maintained during an incident for analysis and response to the incident. It may also be needed for follow up digital forensics and legal proceedings.

It is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court. Examples of commonly collected evidence include:

* Disk/hard drive/host images
* Network packet captures and flows
* IP addresses
* Log files
* Network diagrams
* Configuration files
* Databases
* IR/investigation notes
* Screenshots
* Social media posts
* CCTV, video and audio recordings
* Documents detailing the monetary cost of remediation or loss of business activity
* Memory/RAM images.

In addition, evidence should be accounted during the incident response process. Whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party’s signature (*see Appendices F and G*). A detailed log should be kept for all evidence, including the following:

* Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
* Name, title, and phone number of each individual who collected or handled the evidence during the investigation
* Time and date (including time zone) of each occurrence of evidence handling
* Locations where the evidence was stored.

Detection and Analysis

This phase deals with the detection and determination of whether a deviation from normal operations within an agency is a cyber security incident, and its scope assuming that the deviation is indeed an incident.

Signs of an Incident

Agency should determine the signs of an incident based on the detection and monitoring capabilities within the agency. The events and alerts from various sources such as log files, error messages, and other resources, such as intrusion detection systems (IDS) and firewalls, that may produce evidence as to determine whether an event is an incident. Examples are listed below.

|  |  |
| --- | --- |
| **Sources of security event information** | **Signs of an incident** |
| * System Alerts: IDS, IPS, SIEM, Anti-virus, Anti-spam, File integrity checking, third-party monitoring services * Logs: OS logs, app logs, network device logs, network flows * Publicly available information: Vulnerability disclosure platform, NVD, rapid 7, exploit DB, vendor notifications * People: users, system administrators, security team, external auditors, suppliers, managed service providers. | * Web server log entries that show the usage of a vulnerability scanner * An announcement of a new exploit that targets a vulnerability of the mail server * A threat from a group stating that the group will attack the agency. * A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server * Antivirus software alerts when it detects that a host is infected with malware * A system administrator sees a filename with unusual characters * A host records an auditing configuration change in its log * An application logs multiple failed login attempts from an unfamiliar remote system * An email administrator sees a large number of bounced emails with suspicious content * A network administrator notices an unusual deviation from typical network traffic flows. |

Common Cyber Security Incident Types

Incidents can occur in various scenarios. Agency should identify and prepare to handle the cyber security incident that are common to their environments and use the common attack vectors. Following table is an example of common cyber security incident types.

If a particular event is determined to be an incident, and then it should be reported as soon as possible in order to allow the CIRT enough time to collect evidence and prepare for the preceding steps.

|  |  |  |
| --- | --- | --- |
| **Category** | | **Description** |
| Data breaches | Unauthorised access or theft of sensitive information, such as customer data, personal identifiable information (PII), financial records, or intellectual property. | |
| Phishing attacks | Deceptive emails, messages, or websites designed to trick users into revealing sensitive information, such as usernames, passwords, or credit card details. | |
| Social engineering attacks | Manipulation of individuals or employees through psychological manipulation to disclose sensitive information, perform certain actions, or gain unauthorised access to systems. | |
| Insider threats | Malicious activities or data breaches initiated by employees or trusted individuals within an organisation, either intentionally or unintentionally. | |
| Malware infections | Installation or execution of malicious software, such as viruses, worms, Trojans, or spyware, that can disrupt systems, steal data, or provide unauthorised access. | |
| Advanced Persistent Threats (APTs) | Sophisticated and prolonged cyber attacks by well-resourced adversaries targeting specific organisations or industries to gain unauthorised access, steal data, or perform espionage. | |
| Credential theft | Theft or compromise of usernames, passwords, or authentication tokens, leading to unauthorised access to systems or accounts. | |
| Website defacement | Unauthorised changes made to a website's appearance or function, often to display political or ideological messages, indicating a breach of security controls. | |
| Supply chain attacks | Exploitation of vulnerabilities within the supply chain to compromise systems or introduce malicious components into software or hardware. | |
| Mobile device security breaches | Compromise of smartphones, tablets, or other mobile devices, leading to unauthorised access to personal data, location tracking, or financial fraud. | |
| Internet of Things (IoT) attacks | Compromising IoT devices, such as smart home appliances, medical devices, or industrial control systems, to gain unauthorised access, disrupt operations, or conduct surveillance. | |
| Data exfiltration | Unauthorised extraction or theft of data from an organisation's network, often involving sensitive or proprietary information. | |
| Ransomware attacks | Infection of systems with malicious software that encrypts data, making it inaccessible to the user. Attackers demand a ransom payment in exchange for the decryption key. | |
| Distributed Denial of Service (DDoS) attacks | Coordinated efforts to overwhelm a network, server, or website with a flood of traffic, rendering it inaccessible to legitimate users. | |
| Cyber espionage | The unauthorised access, theft, or surveillance of sensitive information or intellectual property for strategic, political, or economic gain. | |
| Business email compromise (BEC) | A type of phishing attack where attackers impersonate executives or trusted individuals to deceive employees into transferring funds or disclosing sensitive information. | |
| Cryptojacking | Unauthorised use of a victim's computer or device to mine cryptocurrencies without their knowledge or consent. | |
| Zero-day exploits | Exploitation of software vulnerabilities that are unknown to the software vendor, leaving systems exposed to attacks until a patch or fix is released. | |
| Insider trading breaches | Unauthorised access or use of confidential information by insiders, such as employees or contractors. | |

Containment

The primary purpose of containment phase is to limit the damage and prevent any further damage from happening. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Agency should define acceptable risks in dealing with incidents and develop strategies accordingly. Below is an example of containment strategy.

|  |  |  |
| --- | --- | --- |
| **Containment plan** | **Triggers and/or thresholds for containment** | **Minimum level**  **authority** |
| Shut down the system, stop operation of the IT services from the spread of the impact | The administrator account is compromised, website defacement, | System Owner |
| Disconnect the affected network from the central networks, e.g. unplug the network cable from the routers and switches | Malware outbreak is spreading through the internal networks | Chief Information Officer |
| Disable the account that has been compromised to prevent it from accessing the resources | The account user credentials are compromised, unauthorised access to the system | System Administrator |
| Erase / re-image the devices, rebuild the system | The accounts and/or backdoors left by attackers on affected systems need to be removed completely | Security Manager |

Criteria for determining the appropriate strategy include:

* Potential damage to and theft of resources
* Need for evidence preservation
* Business impact assessments and business continuity plans in place
* Service availability (e.g., network connectivity, services provided to external parties)
* Time and resources needed to implement the strategy
* Effectiveness of the strategy (e.g., partial containment, full containment, short term / long term)
* Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

Eradication and Recovery

Eradication phase is aiming to remove the cause and components of the incident, such as deleting malicious code, reimaging of a system’s hard drive(s), and decommissioning a cloud service. This phase is also the point where defences should be improved after learning what caused the incident and ensure that the system cannot be compromised again (e.g. installing patches to fix vulnerabilities that were exploited by the attacker, etc).

Some examples of actions performed during the eradication phase:

* using the original disk images that were created prior to a system being deployed into production to restore the system and then installing patches and disabling unused services to harden the system against further attacks.
* scan affected systems and/or files with anti-malware software to ensure any malware that is latent is removed (i.e. using an anti-virus program combined with CCleaner to disinfect systems and scan the Windows registry for keys that may initiate any latent malware).

The purpose of Recovery phase is to bring affected systems back into the production environment carefully, as to ensure that it will not lead another incident. *Agency* should test, monitor, and validate the systems that are being put back into production to verify that they are not being reinfected by malware or compromised by some other means.

Some of the important decisions to make during this phase are:

* Time and date to restore operations – it is vital to have the system operators/owners make the final decision based upon the advice of the CIRT
* How to test and verify that the compromised systems are clean and fully functional
* The duration of monitoring to observe for abnormal behaviours
* The tools to test, monitor, and validate system behaviour.

Reporting and Notification

Agencies should determine and document the reporting channels and communication plans for cyber security incidents. Below are some examples for reporting and communicating on the cyber security incidents.

|  |  |  |  |
| --- | --- | --- | --- |
| **Organisation / agency to receive notification or report** | **Contact details for the notifying organisation / agency** | **Key notifying / reporting requirements and information (e.g. incident type, severity, deadlines)** | **Personnel responsible** |
| Watch Desk | Email: WatchDesk@sa.gov.au  Phone: 1300 244 168 (press 2)  Watch Desk Duty Officer | • the date and time the cyber security incident occurred  • the date and time the cyber security incident was discovered  • a description of the cyber security incident  • any actions taken in response to the cyber security incident  • to whom the cyber security incident was reported  • if assistance is required for incident response.  Refer to [SACSF Guideline 4.0: Cyber security event and incident reporting](https://www.security.sa.gov.au/documents/documents/SACSF-G4-0-Cyber-Security-Event-and-Incident-Reporting.pdf)  Note that the DPC Watch Desk is the single point of contact for the ACSC, SAPOL and the Australian Federal Police. |  |
| Privacy Committee of South Australia | E: PrivacyCommittee@sa.gov.au | See details on how to report privacy breaches here.  <https://www.archives.sa.gov.au/privacy-committee/privacy-breach-notification> |  |
| Office of the Australian Information Commissioner (OAIC) | See contact details at https://www.oaic.gov.au/about-us/contact-us/ | Refer to <https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach>  (Only relevant for breaches of Tax File Numbers) |  |
| Cyber Security Insurance | Name:  Email:  Phone: | • Insurance provider should be contacted as soon as it is suspected that a claim may be made.  • Documentation of all expenditure relating to the incident must be kept. |  |

Communication Plans

Detailed communication plans should also be developed based on the agency’s process for managing internal and external communications. The communication plans should outline how agency is prepared to communicate and the details for backup communication channels to communicate with staff and stakeholders. Below is an example of communication plan.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Communication Plan** | **Stakeholders / audience** | **Information / materials for communication** | **Communication Channels** | **Primary responsible personnel** |
| Internal Communications | * Agency employees * Business functions and units * Board * Senior executives * Affected users * CIRT and SEMT | * + A brief summary of the incident and business impact   + Actions currently being undertaken to resolve the incident   + Actions staff can take to assist   + Business continuity options for staff who are affected by the incident   + Messaging for external stakeholders   + Key points of contact for enquiries   + Expected timeframes for further updates | * Helpdesk hotline * Group emails * Intranet * Website |  |
| External Communications | * Agencies * Third party service providers * Law enforcement * Customers * Clients * Suppliers * Media * General public * Insurance providers | * + Incident information (based on need to know principle) * System/services affected * Steps being taken to resolve the incident * Third parties that agency is working with to support incident remediation   + Options for stakeholders affected by the incident (customers)   + Key points of contact for enquiries   + Expected timeframes for further updates | * Phone number * Hotline * Email * Website * Social media * News |  |

Post-incident Activity

Post Incident Review

A Post Incident Review (PIR) should be held and documented immediately after agency has recovered its networks and systems from a cyber security incident and a formal debrief held after the incident report has been completed within short period of time (e.g. two weeks).

Key questions to consider in a 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?

Refer to ***Appendix H*** for more detailed questions to consider in the PIR.

Lesson Learned

The purpose of Lesson Learned exercise is to learn from the incidents that occurred to improve the team’s performance and provide reference materials in the event of a similar incident. This can also be used as training material for new team members or as a benchmark to be used in uplifting security controls.

The lessons learned exercise should go through the incident response report with the consideration of following areas and agendas:

* When was the problem was first detected and by whom
* The scope of the incident
* How it was contained and eradicated
* Worked performed during recovery
* Areas where the CIRT teams were effective
* Areas that need improvement.

It should also include time for suggestions and discussion between members of how to improve the overall team. Information from the reporting and tracking of cyber security events and incidents is used to identify recurring or high impact incidents. The information is also used in the continuous improvement of the Cyber Security Incident Response Plan and relevant documents.

Appendices

Appendix A - 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. |
|  | 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 cyber 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. |
|  | Incident detection, including self-detected incidents, notifications received from service providers or vendors, and notifications received from trusted third parties |
|  | 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 B - Incident Triage Questions

Where applicable, personnel reporting cyber security incidents 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?
* 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 South Australian Privacy Committee?
    - 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 Watch Desk beforehand if you will be referencing the SA Government.

Appendix C – Financial Impact Assessment

|  |  |
| --- | --- |
| **Financial Impact Assessment** | |
| Below are a list of example costs that may be incurred. Not all of these costs may be recoverable, but they will provide a comprehensive picture of the financial impact for agency. The list is not intended to be exhaustive and other financial impacts may also be experienced (add to as required). | |
| Productivity losses:   * Normal wages for staff directly involved with incident response and remediation (IT, media/communications, legal, administrative, etc.) * Wages for executives diverted from normal duties to oversee incident management * Wages for staff unable to perform their normal duties due to loss of access to required hardware, applications or information * Cost of customer service inquiries resulting from incident * Other\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Approximate Total:  $ |
| Staff costs in addition to normal wages:   * Overtime * Allowances * Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Approximate Total:  $ |
| Technology / Infrastructure:   * Repair * Replacement * New technology/tools used for incident response & remediation * Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Approximate Total:  $ |
| External Consultants:   * Data restoration * Digital forensics * Post incident review * Legal advice * Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Approximate Total:  $ |
| Liabilities:   * Claims from organisations or individuals for the costs associated with the impact of the incident on the community * Compliance related notifications and fines * Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Approximate Total:  $ |
| Other costs:   * Loss of IP or other information assets with monetary value to the agency * Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Approximate Total:  $ |
| Approximate total cost of incident: | $ |

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? |  | |
| **Actions taken to resolve incident** |  | |
| **Additional notes** |  | |
| **Contact details for incident manager and others if required** |  | |
| **Date and Time of next update** |  | |

Appendix E - Sample Evidence Chain of Custody Form

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Incident details: | | | | | |
| Incident no: |  | | Investigator’s  name: |  | Date: / /  Time: |
| Location item(s) obtained from: | |  | | | | |
| Purposes for which items were obtained: | |  | | | | |
| Items currently assigned to: | |  | | | | |
| Items currently used by: | |  | | | | |

**Item record:**

|  |  |
| --- | --- |
| Item | **Description of item**, e.g. the location (if different to above), serial number, model number, hostname, and IP address of a computer 1 |
| 1 |  |
| 2 |  |
| 3 |  |

1. Includes controlled copies of data e.g. copied data used for analysis.

**Movement record:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item No.** | **Date** | **Time** | **Relinquished by** (name and business division) | **Received by** (name and business division) | **New storage location and reason for movement** |
|  | / / |  | Name:  Division:  Signed: | Name:  Division:  Signed: |  |
|  | / / |  | Name:  Division:  Signed: | Name:  Division:  Signed: |  |

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 Watch Desk* |
| **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?* |
| **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?* |
| **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?* |
| **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?** |  |
| **PROPOSED ACTIONS** | *Detail any resulting actions that can be incorporated into the Action Register.*  *Brief description of action > Proposed Action Officer* |

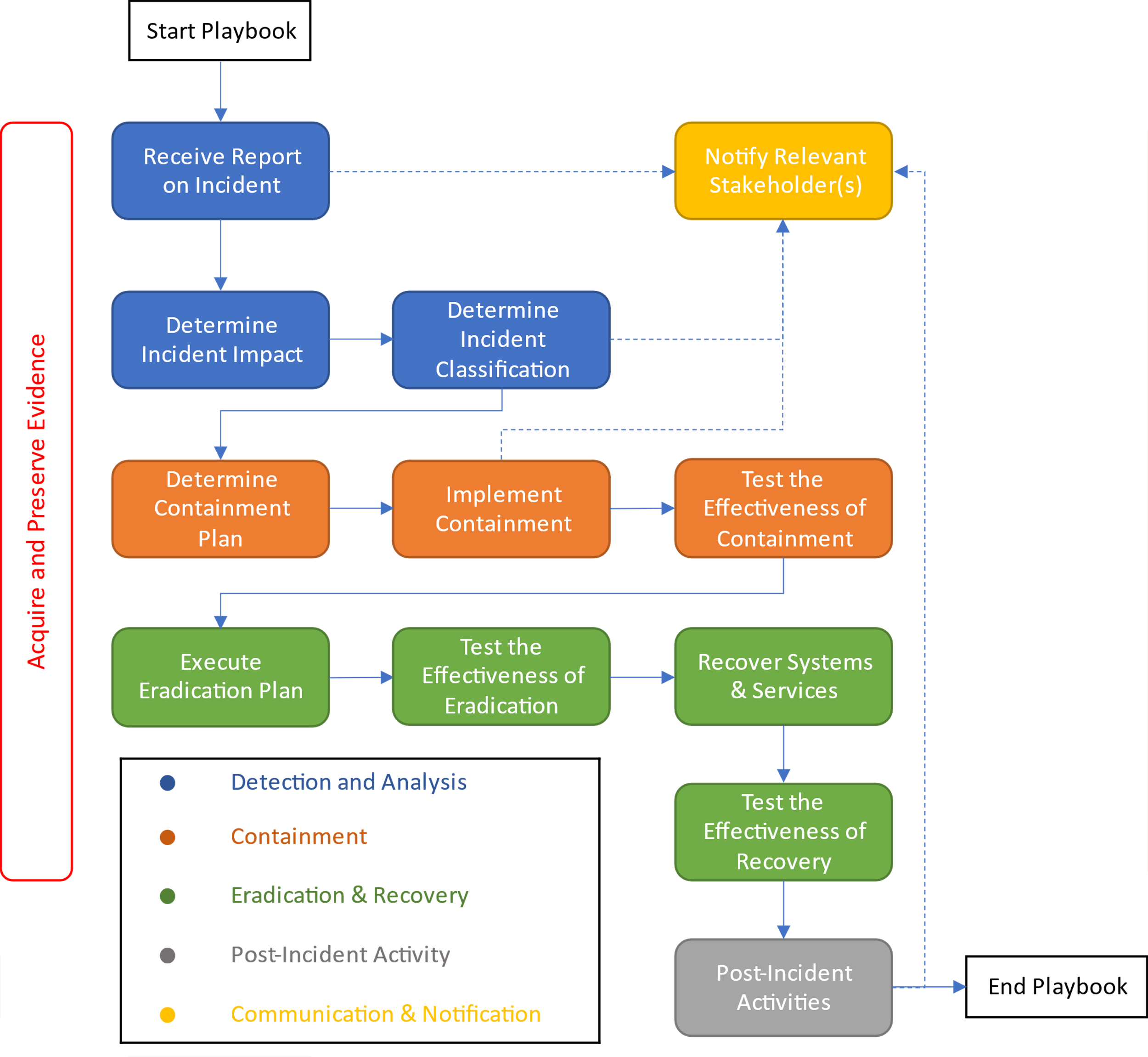
Appendix I – Incident Response Playbook Template

**Cyber Security Incident Response Playbooks (Template)**

Cyber security incident response playbooks can be developed for common or high-impact incident types so that staff responding to the incident have a simple, consistent approach to follow in potentially high-pressure situations.

The process and template below can be used to develop playbooks that consider your agency’s tools, processes and resources.

High Level Process



Detailed Playbook Procedure and Checklist

|  |  |  |
| --- | --- | --- |
| **Phase 1 – Detection and Analysis**  *Acquire and preserve evidence at this stage. Maintain the evidence register and keep the chain of custody form up to date.* | **Lead by (Contribute by)** | **Status** |
| **Receive Report on Incident**  Based on the details learned about the incident thus far, define the team structure required for the response. Relevant responders and SMEs should be assembled for the incident response activities.  Required resources should be identified and collected to support the following activities, *including the tools, devices, accounts, print outs, keys, maps, etc.*  Notify Relevant Stakeholder(s)  Notify and communicate to the relevant internal and external stakeholders. *This includes the DPC Watch Desk, SAPOL, cyber insurance providers, Cyber Incident Response Team (CIRT) leaders and members, affected users, third parties and suppliers.* | CIRT Team Lead (First Responders / affected users / help desk team / system administrator) |  |
| **Determine Incident Impact**  Analyse the criticality and scale of the incident, *including the number of users affected, systems and services outage due to the incident, sensitive information / data breaches, etc.*  Perform investigation and technical analysis, *this includes examining malicious emails and programs, reviewing logs, interviewing affected users, consulting legal and HR teams for compliance and policy violations.*  *Following are the example activities for phishing:*   * *Obtain a copy of the suspicious email* * *Examine the email headers (*[*https://toolbox.googleapps.com/apps/messageheader/*](https://toolbox.googleapps.com/apps/messageheader/)*) and answer the following questions:* * *Does the sender email and domain name match the display name?* * *Is the display name or sender email and domain name expected or known to the recipient?* * *Do the headers show the mail client that was used to send the email?* * *Do the headers show any signs of automated scripts (e.g. x-php-script)?* * *Do the headers show any unexpected hops (e.g. the email was relayed through an unexpected country before arriving at the recipient)?* * *Examine the email content and answer the following questions:* * ***Without clicking on them, examine any links present in the email.*** *Do they point to expected websites or addresses? Where are the destination IP addresses located? Do they match the text in the email?* * *Does the email match the expected look and feel of the particular sender (i.e. the email contains all the usual, expected content and formatting, logo and disclaimer)?* * *Does the email contain spelling or grammar errors?* * *Does the email try to convey a sense of urgency to the recipient? (e.g. request an immediate payment)* * *Does the email contain links, attachments or HTML? (e.g. potential phishing link, malicious attachment)* * *‘View the source’ of the email to examine it in plain text. Does it contain any scripts or obfuscated text (i.e. long strings of seemingly meaningless letters and numbers)?*   *By performing the analysis described above and speaking with affected users, the following questions should be answered:*   1. *Does the phishing attempt appear targeted?* 2. *Did the user reply to or forward the email?* 3. *Were links followed or attachments downloaded and/or executed?* 4. *Was personal or otherwise sensitive information disclosed by the user?* 5. *Did the user’s workstation exhibit any strange behaviour upon preview/reading of the email?* 6. *Is the phishing attempt widespread (affecting a large number of users)?*   *Note: the impact analysis at this stage should not delay the progress of incident response. It should be used for initial scoping of the investigation and prioritisation of resources. A detailed impact assessment could be performed at Eradication, Recovery and Post-incident Activity stage.* | CIRT Team Lead (Security Manager / SMEs / HR / Legal) |  |
| **Determine Incident Classification**  The criticality of the impact and priority of the incident determine the classification levels. Once the classification level is determined, relevant stakeholders should be notified, and relevant resources should be acquired to handle the cyber incident.  *Note: the classification level may change (escalate / de-escalate) during the incident response process, due to further realisation and observation of the incident.*  Notify Relevant Stakeholder(s)  Notify and communicate to the relevant internal and external stakeholders. *This includes the DPC Watch Desk, SAPOL, cyber insurance providers, Cyber Incident Response Team (CIRT) leaders and members, affected users, third parties and suppliers.* | CIRT Team Lead (Security Manager / SMEs) |  |
| **Phase 2 – Containment**  *Acquire and preserve evidence at this stage. Maintain the evidence register and keep the chain of custody form up to date.* | **Lead by** | **Status** |
| **Determine Containment Plan**  Select the containment plan to stop the spread and increase of impact, based on the pre-defined containment strategy and scenario of the incident.  *Following are example containment plans:*  ***Block the source***  *If the source address of the email can be identified, block all emails that originate from that address or domain (if possible) using:*   * *Office365 (block IP using a connection filter, or add to spam filter block list)* * *Email security solutions such as Mimecast, Proofpoint (add to spam filter block list)*   *If required, consider the following:*   * *Block emails written in specific languages* * *Block emails originating from specific countries or regions* * *Block emails that contain scripts*   ***Block URLs***  *If URLs or IP addresses are identified within the phishing emails, block access to them:*   * *On the edge firewalls* * *Within web proxy URL filter*   ***Reset exposed credentials***  *If any user credentials have been exposed (e.g. a user entered them into form after clicking a link within the phishing email), immediately force a password change for users’ passwords.*  ***Disable affected accounts***  *If the accounts credentials are compromised, the accounts should be disabled to prevent unauthorised access.*  ***Quarantine/remove phishing emails***  *Using the information gathered during the initial investigation, remove all identified phishing emails from all affected users’ mailboxes.*  *Note: to make decision on the containment plan, approval must be given by the minimum level authority.* | CIRT Team Lead (Security Manager / System Owner / System Administrator) |  |
| **Implement Containment**  Delegate containment activities to responsible persons with agreed upon timelines. *This includes actions such as quarantine an email, disable an account, unplug the network cable, shut down an IT services, direct the adversary to a sandbox, etc.*  Notify Relevant Stakeholder(s)  Relevant stakeholders should be notified to support or communicate the containment.  *For example, if a financial transaction is involved, inform finance department; or if an account needs to be deleted, inform the system administrator. Submit details of the phishing campaign to the following:*   * [*www.scamwatch.gov.au/report-a-scam*](http://www.scamwatch.gov.au/report-a-scam) | CIRT Team Lead (System Administrator / Security Manager) |  |
| **Test the Effectiveness of Containment**  Confirm effectiveness of containment. The containment must be effective before commencing the eradication and recovery phase. | CIRT Team Lead (System Administrator / Security Manager) |  |
| **Phase 3 – Eradication & Recovery**  *Acquire and preserve evidence at this stage. Maintain the evidence register and keep the chain of custody form up to date.* | **Lead by** | **Status** |
| **Execute Eradication Plan**  Analyse the sources and causes of the incident and remove them from the environment*. This includes removal of attack vectors and implementing additional security controls, such as blocking IP ranges / domains, re-imaging the systems, vulnerability scans and performing patches.*  *Following are example eradication plans:*  ***Remove attack vectors***   * *Blocking the source within Office 365 (IP, domain, language, country/region etc.)* * *Blocking emails with similar characteristics to the phishing email within Office 365* * *Blocking any malicious URLs or IPs that were detected at the edge firewalls* * *Blocking certain types of attachments (.exe, .zip, .docm, etc.)*   ***Reset affected accounts***  *Completely delete the compromised account and set up new accounts for the affected users and systems.* | CIRT Team Lead (System Administrator / Security Manager) |  |
| **Test the Effectiveness of Eradication**  Confirm effectiveness of eradication. The eradication must be effective before commencing the recovery activities. | CIRT Team Lead (System Administrator / Security Manager) |  |
| **Recover Systems & Services**  Bring affected systems back into the production environment. Return the affected services back to operational. *This includes recovery and restoration procedures, such as backup restoration, account reset / re-creation, re-open the website and APIs, etc.*  The Containment stage is meant for short term containment of the incident. Any blocks or containment strategies used should be revisited and/or removed (if no longer required) to restore the BAU / normal operations. *For example, the quarantine emails should be released if not identified as malicious, the disabled accounts should be re-activated if not compromised.* | CIRT Team Lead (System Administrator / Security Manager) |  |
| **Test the Effectiveness of Recovery**  Confirm effectiveness of recovery. The incident should be resolved by this stage. | CIRT Team Lead (System Administrator / Security Manager) |  |
| **Phase 4 - Post-Incident Activity** | **Lead by** | **Status** |
| **Post-Incident Activities**  Perform post incident review (PIR) and lesson learned exercises to improve the incident response process and cyber security controls.  Notify Relevant Stakeholder(s)  Relevant stakeholders should be notified that incident has been resolved and systems and services are back. Education and training should be delivered to the users, so that affected users will be aware of the signs of the incident if it occurs again. | CIRT Team Lead (Security Manager / SMEs / System Administrator) |  |

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this guideline. There is no specific impact on Aboriginal people.

Related documents

Tips: Agency could include the relevant incident response plans and scenario-based playbooks as below:

This plan supports, and is to be used in conjunction with the following incident response plans and playbooks:

1. Incident Response Procedures / Playbooks – describes the processes and responsibilities for managing a particular cyber security incident (e.g. ransomware attack, malware breakout, phishing email attack, DoS attack, etc.)
2. Major Incident / Crisis Management Procedure – describes the response processes and responsibilities during a major incident
3. Disaster Recovery Plan – defines the resources and actions to respond to and recover from a business continuity event impacting the department’s on-premise managed services.
4. Evidence collection and preservation procedure
5. Detailed Communication Plans

References

1. [NIST Computer Security Incident Handling Guide](https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf)
2. [SANS Incident Handler's Handbook](https://sansorg.egnyte.com/dl/6Btqoa63at)
3. [Cyber Incident Response Plan - Guidance - July 2022](https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf)

Document Control

|  |  |
| --- | --- |
| Approved by: CIO Steering Committee | |
| Contact: Chief Information Security Officer |  |
| Division: Office of the Chief Information Officer | Compliance: Optional |
| Review number: V1.0 | Date of approval: November 2023 |
| Next review date: November 2025 | Most recent approval: November 2023 |

|  |
| --- |
| Licence |
| http://i.creativecommons.org/l/by/2.5/au/88x31.png  With the exception of the Government of South Australia brand, logos and any images, this work is licensed under a [Creative Commons Attribution (CC BY) 4.0 Licence](http://creativecommons.org/licenses/by/4.0/). To attribute this material, cite the Office of the Chief Information Officer, Department of the Premier and Cabinet, Government of South Australia, 2023. |