usezer

RESPOND RECOVER REPEAT

A Practical Guide to Cyber Incident Response

WWW.USEZER.COM.AU

Why Incident Response Matters

01. Faster Response Means Less Damage

Cybercrime reports in Australia have surged to over **87,000** incidents in FY2022–23, with one report **every 6 minutes.**
An IR plan enables fast detection and containment — preventing incidents from escalating.

02. Reduce Financial & Operational Risk

The average cost per cybercrime report:

- **$46,000** for small businesses
- **$97,200** for medium businesses

(Source: ASD Annual Cyber Threat Report)
A well-executed response reduces financial losses and limits downtime.

03. Stay Compliant

Australia's privacy and cyber security laws demand fast, transparent action when incidents occur. Under the **Privacy Act 1988,** organisations must report eligible data breaches to the Office of the Australian Information Commissioner (OAIC) and affected individuals without delay.

For businesses in energy, healthcare, transport, and other key sectors, the **Security of Critical Infrastructure (SOCI) Act** enforces even stricter obligations

04. Protect reputation and Trust

Business Email Compromise (BEC) remains the most reported cybercrime in Australia, averaging **$39,000** loss per incident.
How you respond directly impacts customer confidence and public trust.

🔍 Common Cybersecurity Incidents

1

📨 Phishing & Business Email Compromise (BEC)

Attackers trick users into clicking malicious links or sharing credentials. Often leads to email account takeover, invoice fraud, or data exposure.

2

💻 Ransomware Attacks

Files and systems are encrypted by attackers demanding a ransom payment. These can halt business operations and cause major financial damage.

3

🛠 Insider Threats

Malicious or negligent users (staff or contractors) misuse their access—intentionally or accidentally—to leak, delete, or steal data.

4

🕵 Credential Theft & Account Compromise

Stolen passwords (from phishing, reuse, or brute-force attacks) allow unauthorised access to internal systems.

5

📁 Data Exfiltration

Sensitive or regulated data is copied and removed from the organisation without authorisation—often quietly and over time.

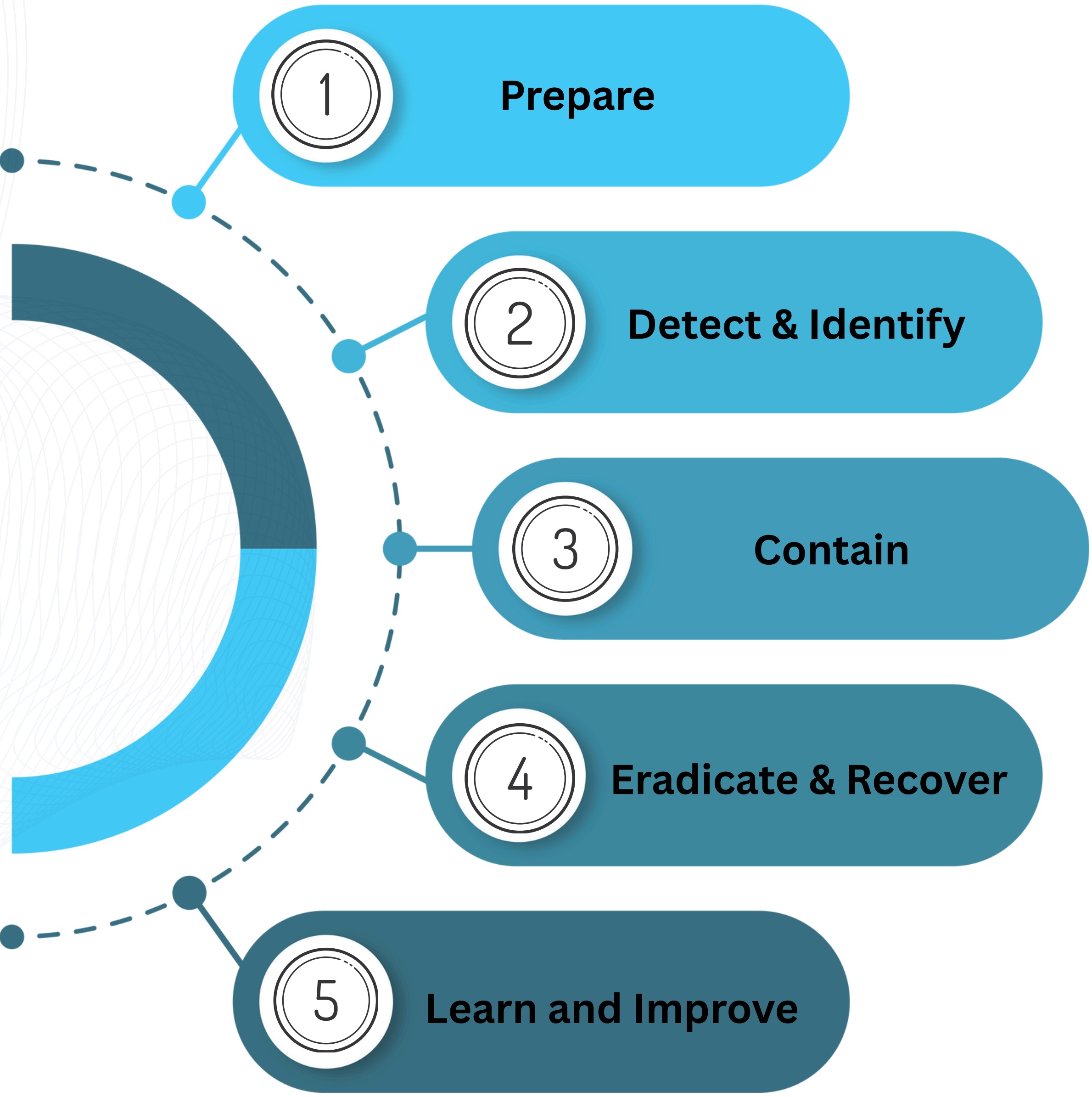
6

☁ System / Cloud Misconfigurations

Improperly secured systems and cloud services expose sensitive data publicly or allow unauthorised access.

🧭 The 5-Step Incident Response Process

This 5-step Incident Response process is adapted from the globally recognised **NIST Special Publication 800-61**. By structuring the response into clear phases — from preparation to post-incident improvement — it aligns with best practices recommended by both **International Standards** and **Australian Cyber Authority (ACSC).**



01. Prepare

Define Incident Types, Severity and Escalation Paths

Establish what qualifies as an incident, how severe it is, and who should be involved at each level of escalation.

Assign roles and responsibilities across IT, security, and leadership

Everyone involved should have clearly defined responsibilities to ensure swift and coordinated action.

Develop and document response playbooks and communication plans

Standardised response procedures and communication flows help avoid delays and confusion during real incidents.

Train staff on how to recognise and report suspicious activity

Employees play a critical role in early detection — training them improves the likelihood of fast, accurate reporting.

Conduct tabletop exercises to test and refine response readiness

Simulated incidents validate your plan and help teams build confidence and muscle memory.

Tools Used:

- Incident Response Playbooks
- Policy and Knowledge Documentation Systems
- Security Awareness and Simulation Platforms
- Case / Ticket management Systems

02. Detect and Identify

Monitor systems, logs, and networks for unusual activity

Proactive monitoring is the first step in identifying abnormal behaviours or potential threats.

Validate alerts to confirm a real incident is occurring

Filtering false positives ensures teams focus on actual threats without wasting resources.

Develop and document response playbooks and communication plans

Understanding the blast radius allows teams to prioritise actions and reduce the impact.

Determine the type and severity of the incident

Classifying incidents provides structure to the response and determines urgency

Begin internal communication and logging of the event

Documenting details from the start supports investigation, compliance, and lessons learned.

Tools Used:

- SIEM (Security Information and Event Management)
- EDR (Endpoint Detection and Response)
- Log management systems
- Threat intelligence platforms
- Intrusion Detection Systems (IDS)

03. Contain

Isolate compromised systems, accounts, or segments

Stop lateral movement by immediately segmenting infected or exposed environments.

Apply short-term fixes to stop immediate spread

Initial containment actions — such as disabling user accounts — can buy time for longer-term responses.

Implement long-term containment measures to sustain operations

Strategic containment allows business continuity while managing risk.

Maintain business continuity where possible

Balance security with the need to keep critical functions online.

Preserve evidence for investigation and reporting

Secure logs and artifacts are vital for root cause analysis and reporting obligations.

Tools Used:

- Identity & Access Management (IAM)
- Network Segmentation & Firewall Management
- Endpoint Isolation Tools (EDR Tool)
- Mobile Device Management (MDM)
- SIEM - SOAR Automation

04. Eradicate and Recover

Remove malicious code, backdoors, or unauthorised access

Clean systems of all compromise indicators to ensure complete removal of threats.

Patch vulnerabilities and reset credentials

Fix the exploited entry points and prevent attackers from regaining access.

Restore clean versions of affected systems from backups

Bring systems back using known-good backups, verified and tested.

Monitor for signs of reinfection or residual threats

Continue monitoring for any trace of the original threat after recovery.

Gradually return systems to production with enhanced controls

Restore services methodically and apply updated protections to reduce future risk.

Tools Used:

- Backup and recovery platforms
- Vulnerability and patch management systems
- Endpoint Detection & Response (EDR)
- Threat Hunting & Forensics Platforms

05. Learn & Improve

Conduct a post-incident review with all stakeholders

Gather all involved parties to review what happened and how it was handled.

Identify root causes and breakdowns in detection or response

Analyse the incident timeline to find gaps or inefficiencies in the process.

Update playbooks, security controls, and training

Use findings to enhance your response materials, configurations, and awareness programs.

Share lessons learned with teams or industry groups

Sharing insights helps others and contributes to sector-wide improvement.

Use findings to improve overall cyber resilience

Refining your IR process strengthens defences against future incidents.

Tools Used:

- Threat Modelling and Risk Assessment Tools
- Training and Awareness platforms

How USEZER Can Help?

Our Services

MANAGED DETECTION SERVICES (EDR)

Managed Detection Services monitor and detect threats in real time, identifying and responding to security risks to strengthen overall protection.

24X7 SOC SERVICES

24x7 SOC services provide continuous threat monitoring, detection, and response to protect against security risks in real time.

MANAGED FIREWALL SERVICES

Managed Firewall services control and monitor network traffic, blocking unauthorized access and responding to potential threats to ensure network security.

IDENTITY AND APPLICATION CONTROL

IAM, PAM and application solutions secure access by managing user permissions, preventing unauthorized access to critical systems.

EMAIL PROTECTION SERVICES

Email Protection services filter and monitor email traffic, blocking phishing, malware, and other threats to safeguard communication and prevent data breaches.

VULNERABILITY MANAGEMENT

Vulnerability Management services identify, assess, and prioritize security weaknesses, enabling timely remediation to reduce exposure and improve overall security

MANAGED BACKUP SERVICES

Reliable, automated backup solutions with monitoring, testing, and recovery support—ensuring your critical data is always protected and recoverable.

COMPLIANCE

We ensure your organisation aligns with regulatory and industry standards—such as ISO 27001 and the Essential Eight—to strengthen data security, privacy, and risk management practices.

CONTACT US

Nuwan Fernando	Boniface Fernando	Grace Waldemar
Phone Number	Phone Number	Phone Number
+61 414 764 949	+61 2 9421 4755	+61 41 444 2485
+61 (02) 8007 5400	+61 (02) 8007 5400	+61 (02) 8007 5400

Email: soc@usezer.com.au

usezer.com.au

✉ connect@usezer.com.au

usezer