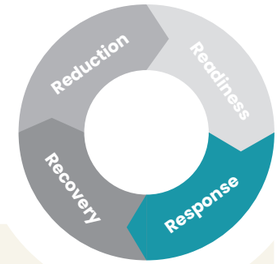
2.3 Response

Use this process flow for a step by step guide to respond to a cyber security incident.

This response process can be used as a pull out for ease of reference in an active incident



Business Response Steps

If you have cyber incident insurance and legal counsel engage your provider(s) early.

You should notify the Office of the Privacy Commissioner (OPC) within 72 hours if you believe you have had a data breach that could cause serious harm.

Notify CERT NZ for support in responding to the incident.

Incident Detected

1. Notify your IT provider and validate whether this is a cyber incident
2. Activate your Incident Response Plan
3. Assess the impact on the business to determine the severity of the incident
   - Has data been stolen or breached?
   - Are critical systems or devices unavailable?

Is this a critical incident?

- **No** → Manage internally with IT provider
- **Yes**

4. Decide who you need to support the response
   - Decide who can support your response. This could include your cyber insurance provider, legal advisor and CERT
5. Initiate your Business Continuity Plan (BCP)
   - A prolonged incident could stretch your manual processes
   - Consider what additional resource and support your staff may need
6. Assess whether you need to notify any external stakeholders or regulatory bodies. Deliver communication messages as appropriate
   - Keep messaging factual and balanced
   - Avoid promising resolution before the incident is understood
   - Remember that internal communications could be leaked to the public

Has the threat been remediated?

- **No** → Repeat from step 4 (re-investigate)
- **Yes**

7. Debrief and identify lessons learnt
   - Create an action plan to improve readiness and response
   - Involve everyone who assisted with the response when identifying lessons learnt

Incident Closed

Technical Response Steps

Keep communication open between the business and IT response to understand impact, where additional help may be needed and who else may need to be communicated with as the response develops

4. Investigate the extent of the incident
   - Find out why and how the incident happened
   - Preserve evidence and keep any valuable information
5. Stop the spread/mitigate the impact
   - Mitigating actions could include:
   - Shutting down systems and changing passwords
   - Disconnecting from compromised networks
   - Make decisions with awareness of the impact this will have on service availability for you and external stakeholders
   - Communicate to those impacted
6. Remediate the source of the incident
   - Fix vulnerabilities by patching any weaknesses or security threats
   - Remove any harmful elements such as malicious files or malware
   - Increase monitoring to make sure you are not reinfected
7. Recover systems, devices and data
   - Initiate applicable disaster recovery plan(s)
   - Restore systems in a prioritised, risk based way

Business
Technical

Te Whatu Ora
Health New Zealand