DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

New Zealand's Cyber Security Emergency Response Plan

Version 5, July 2021

Glossary

Term or acronym	Description
CERT NZ	New Zealand's CERT (Computer Emergency Response Team)
CIMS	Coordinated Incident Management System
CSERP	Cyber Security Emergency Response Plan
DPMC	Department of the Prime Minister and Cabinet
GCSB	Government Communications Security Bureau
NCPO	National Cyber Policy Office (a unit in DPMC)
NCSC	National Cyber Security Centre (a unit in GCSB)
NSS	National Security System
ODESC	Officials' Committee for Domestic and External Security Coordination

Version history

	Version	Authorised by	Date
	NZ CSIRP Version 1 NZ CSIRP Version 1	ODESC Cabinet	12 October 2012 23 January 2013
	CSIRP Version 2	ODESC	6 September 2013
	CSERP Version 3	SIB	10 August 2016
	CSERP Version 4	SIB	8 March 2017
	CSERP Version 5	SIB	14 July 2021

Contents

Introduction

Purpose

1. The Cyber Security Emergency Response Plan (CSERP) sets the framework for the government's response to a cyber security emergency to ensure that:
    - agencies and officials understand their roles and responsibilities in the event of a cyber security emergency;
    - the private sector understands the government's approach;
    - the response is coordinated, appropriate and effective during a cyber security emergency; and
    - following a cyber security emergency, services and operations are restored swiftly and appropriate lessons are identified and acted upon.

Definition

2. A **cyber security incident** is an event that impacts on the confidentiality, integrity or availability of digital systems and requires a response from the affected organisation(s). The response may involve specialist assistance.
3. A **cyber security emergency** is an incident or combination of incidents, which cause significant or sustained disruption to digital systems critical to health and safety, New Zealand's economic well-being, international reputation or democratic institutions, and requires a significant and coordinated response.

Scope

4. The processes and structures in the CSERP are intended to provide guidance to support response to cyber security emergencies.

Audience

5. The primary audience for the CSERP are officials from New Zealand's National Security System, specifically:
    - chief executives who are likely to be involved in the Officials' Committee for Domestic and External Security Coordination (ODESC);
    - senior officials who will be involved in coordination groups or watch groups;
    - officials who will have to brief senior officials or chief executives;
    - departmental communications staff; and
    - officials who have responsibilities relating to cyber security emergency response.
6. Other audiences for the CSERP (or components of it) include broader government agencies, the Office of the Privacy Commissioner, international partners and private sector companies affected by, or contributing to the response.

Background

7. The CSERP has informed New Zealand's response to cyber security emergencies since 2013. Throughout its existence, it has been updated to deliver the goals of the Cyber Security Strategy, adapt to the changing environment and reflect lessons learned from incidents and exercises.
8. Cyber security is a vital part of the government's responsibility to advance the seven key objectives[1] that underpin the "all hazards – all risks" approach New Zealand takes to national security. The CSERP is part of New Zealand's broader National Security System (NSS) and should be read alongside the NSS Handbook[2].
9. The CSERP is maintained by the Department of the Prime Minister and Cabinet (DPMC) and is authored in collaboration with other agencies with a role in cyber security.

Principles

10. The response to a cyber security emergency should be a joint team approach focusing on remediating the event and guided by the following principles:
    - **Cooperation**. Information sharing between agencies and the private sector is effective and enables the best use of resources.
    - **Coordination**. Roles and responsibilities are defined and ensure that all response functions are performed, and duplication is avoided.
    - **Sustainability**. Resource needs are anticipated and can deal with additional contingencies, whilst still maintaining an appropriate level of response activity.
    - **Timeliness**. Processes for triage, notification, response structure establishment and decision-making are efficient.
    - **Trust**. Government maintains the trust, consent and confidence of victims and stakeholders, and speaks with a single voice.

[1] The seven objectives are: ensuring public safety, preserving sovereignty and territorial integrity, protecting lines of communication, strengthening international order to promote security, sustaining economic prosperity, maintaining democratic institutions and national values, and protecting the natural environment.

[2] National Security System Handbook, August 2016, https://www.dpmc.govt.nz/sites/all/files/dpmc-nss-handbook-aug-2016.pdf

Activation of The Plan

11. Activation of the CSERP occurs when a cyber security incident is identified as meeting the threshold of a cyber security emergency. If there are different views from agencies on whether the threshold for an emergency has been met, or not met, the CSERP is activated and a coordinated categorisation process is undertaken.

Identification

12. The responsibility for identifying a cyber security emergency resides within the operational cyber security agencies:
    - CERT NZ
    - NCSC
13. These agencies receive reports from the public, from their partnerships (including the New Zealand Police) or from technical capabilities that identify vulnerabilities or threats, which may lead to a cyber security emergency.

Categorisation

14. Categorisation occurs initially through a triage process performed by the operational cyber security agencies. The triage process is designed to ensure that resources dedicated to the response is commensurate to the severity and considers potential impacts as well as realised impact. Operational cyber security agencies undertake regular meetings that provide a basis of common understanding for incident severity.
15. The Coordinated Incident Management System (CIMS)[3] is used when dealing with events managed by the National Security System – such as cyber security emergencies. The cyber incident categorisation matrix has been mapped to CIMS.
16. Categorisation is valuable to quickly inform and guide an appropriate response but given the dynamic nature of cyber security incidents and emergencies, the categorisation may change over time. The lead agency, in consultation with the coordination group, or a watch group will be responsible for reviewing the categorisation.

Coordination

17. Cyber security emergencies categorised as SEVERE would be expected to activate the National Security System including establishment of a watch group and possibly ODESC.
18. Where a cyber security emergency is categorised as having a MAJOR severity rating, the identifying agency must consider whether broader discussion or interagency response is required. In such cases a Cyber Emergency Coordination Group may be held.
19. The identifying agency may also assess that the impacts of a MAJOR severity cyber emergency do not warrant the establishment of a Cyber Security Emergency Coordination Group. Where this occurs, the operational lead agency will coordinate the response and

[3] The New Zealand Coordinated Incident Management System (CIMS) 3rd edition, https://www.civildefence.govt.nz/resources/coordinated-incident-management-system-cims-third-edition/

notify the other cyber security agencies. The process is represented below (Figure 1) and in all cases the responses are in accordance with the principles in paragraph 10.

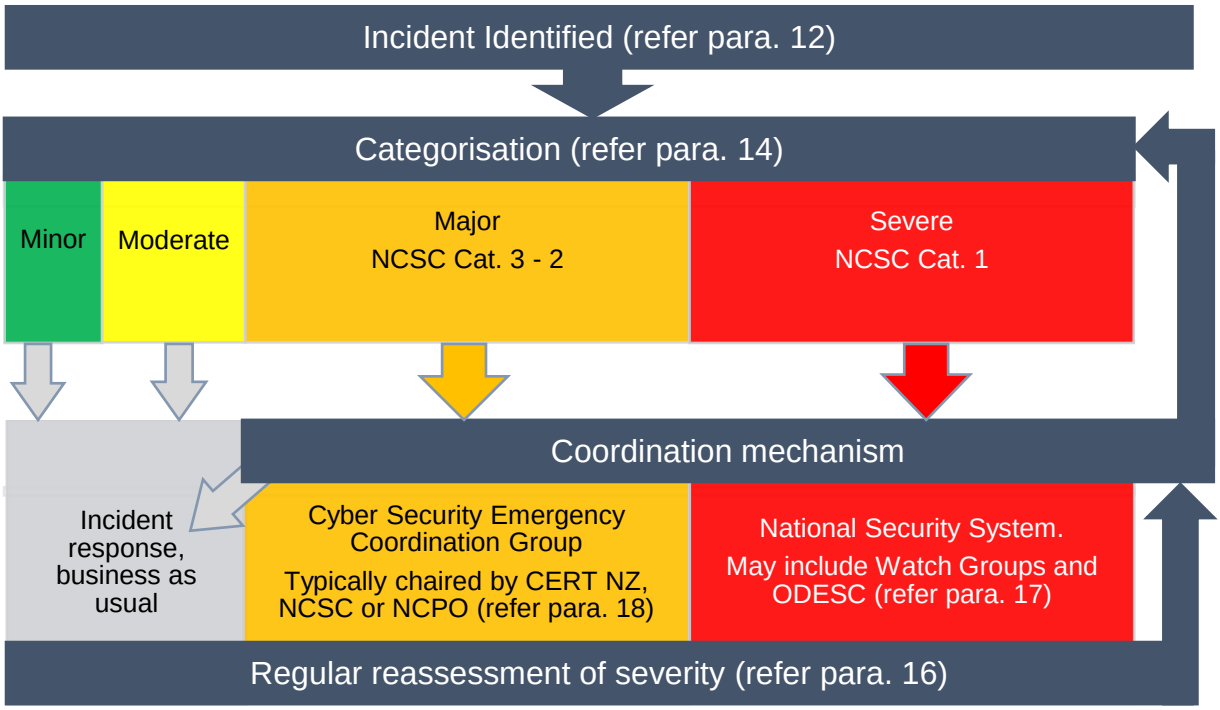

Figure 1: Indicative severity and corresponding coordination mechanism

20. When activated, the Cyber Security Emergency Coordination Group will typically be convened and chaired by a senior representative from the agency leading the response and operates without activating the National Security System. The group will be comprised of sufficiently senior officials to enable decision making, representing relevant policy and operational agencies. Quorum for the group requires attendance of CERT NZ, DIA, DPMC, NCSC and the New Zealand Police. Other agencies and organisations may be invited as required.

21. Responsibilities of the chair include secretariat services. Where required this may include providing briefs and updates to senior officials and relevant Ministers. Location and facilities of the group rests with the chair. Guidance for members and a draft agenda is included in Annex A and Annex B.

Escalation to the National Security System

22. The Cyber Security Emergency Coordination Group enables quick consultation across agencies and considers whether an incident categorisation accurately reflects national security risk and whether the operational response is sufficient. Its two primary functions are to:

    - assist or expedite the process of activating the CSERP;
    - consider the necessity of escalating the response and activating the NSS.

Roles and Accountabilities

23. In a cyber security emergency, the following roles need to be fulfilled. These roles reflect established best practice in cyber security incident management. It is often desirable for a single agency to have responsibility for all roles, but roles may be delegated. Most critical in an emergency is that a lead agency is quickly identified.

Lead agency

24. The lead agency has overall responsibility for managing a cyber security emergency and is accountable to their Minister for overall performance. It is required to manage response and recovery; need to have overall situational awareness of all work streams; and will likely be required to provide regular briefings to Ministers, senior officials and other supporting entities.
25. The NSS Handbook (2016) prescribes NCSC as the lead agency for cyber emergencies.
26. The lead agency can be reassigned by the Cyber Emergency Coordination Group. Instances where a cyber security emergency may be led by other agencies include:
    - Where the primary victim of a cyber security emergency is a government agency or industry organisation that has the capability to respond appropriately.
    - The most significant impacts of the emergency are more appropriately dealt with by another organisation, such as the National Emergency Management Agency.

A Cyber Security Emergency Controller

27. This role, if not performed by the lead agency, supports the lead agency coordinating the cyber security response and recovery activities. The cyber security emergency controller draws on access to technical specialists, partners resources and service provider relationships and involves oversight of all the aspects of the cyber security components of the emergency, including technical aspects of detection and analysis of malicious activity, as well as recommendations on containment and eradication.

Service Owners

28. Service owners affected by a cyber security emergency will be involved in the response and will need to understand the impact of the cyber security emergency and make decisions regarding impact on service delivery.

Technical Specialists

29. Experts play a critical role in understanding and responding to the cyber security components of the emergency. They will be required to restore and protect infrastructure that supports services impacted in a cyber security emergency. These may be public or private experts with the skills and capabilities to perform detection, disruption of cyber security threats as well as response; which includes the capability to deploy detection capabilities, perform analysis, that supports recommendations and measurement of the efficacy of containment, eradication and recovery of systems.

30. Technical specialists may come from the cyber security emergency controller agency, other agencies, or the private sector.

Law Enforcement Advisor

31. A cyber security incident or emergency will commonly involve a criminal act. The law enforcement advisor is an operational function that works with the cyber security emergency controller at an early stage to ensure deconfliction occurs in the event a criminal complaint is made by the service owners.
32. Complaints by service owners should be encouraged to be reported to Police. Frequently international partners are actively investigating related cases and evidence sharing is critical to attribution and holding offenders to account.
33. Where appropriate, Police will adapt their technical response to capture evidential material prior or in parallel to the recovery of systems, ensuring any destruction of evidential material via remediation is minimised. This is achieved through a deconfliction process with the technical specialists.

Communications

34. Effective communication is key to ensuring a coherent response to a cyber security emergency. It is vital that government provides information and speaks with one voice including when issuing public advisories that support the cyber security emergency response or reassure wider industry. Communications need to be coordinated through the lead agency to ensure consistency with overall response.
35. It will be necessary to identify the appropriate channels for communications and a dedicated spokesperson to lead any press briefings and coordinate across agencies acknowledging that the selected channel is likely to become the focus for follow-up enquiries from both the public and private sectors as well as the wider public.

International Liaison

36. Often cyber security emergency response requires international liaison. Responsibility for international liaison will depend on the specific cyber security emergency and type of liaison required.

Third Parties and Service Providers

37. Most cyber security emergencies will involve engaging with managed service providers. Government requires assurance from providers of cyber security services that their response to an emergency is adequate and that service recovery is aligned with national security imperatives.

Recovery

38. The time to restoration of normal services and operations will depend on the nature of the cyber security emergency. When dealing with historical breaches, focus should be on identifying breadth of access and points of presence. In cases where a cyber security emergency affects availability of services, immediate restoration may be the priority.

Monitoring the implementation of entities' business continuity plans will be critical in order to:

- identify areas in which remedial action or additional assistance is required; and
- provide accurate advice to Ministers and senior officials.

39. Investigative work to determine the origins of a cyber security incident, which vulnerabilities were exploited, and which systems may have been compromised or degraded, will often continue after the immediate effects of a cyber security emergency have been resolved. Where the possibility for ambiguity within the recovery exists, the Cyber Security Emergency Coordination Group can identify the requirement for post-incident work and delegate the lead to the appropriate agency.

Debrief

40. In addition to technical investigative work, the Cyber Security Emergency Coordination Group will consider what post-incident briefing, review or reporting is necessary. This may include:

    - an immediate inter-agency review to inform a post-emergency brief for Ministers and senior officials (including ODESC) as required; and
    - a 'lessons identified' process to inform a full post-emergency report and
    - a post event operational debrief.

41. The Cyber Security Emergency Coordination Group will allocate responsibility for compiling of a post-emergency report to a single agency lead, with supporting agencies contributing specific material as required. The submission date for the report will be agreed between the contributing agencies.

Management of the Plan

Reviewing the CSERP

42. The responsibility for reviewing and updating the CSERP rests with the NCPO in consultation with other agencies with a role in cyber security. Updates to the CSERP will be synchronised with updates to the cyber risk profile and will incorporate lessons learned from cyber security incidents and exercises.

Exercising the CSERP

43. In addition to lessons learned from cyber security incidents and emergencies, the CSERP is tested by regular inter-agency exercises, including with the private sector and international partners. These exercises, which aim to test the government's readiness to manage a cyber security emergency, will be coordinated by the operational agencies.

(U) Annex A – Guide for Members of the Cyber Security Emergency Coordination Group

Purpose of a Cyber Security Emergency Coordination Group

The Cyber Security Emergency Coordination Group may be charged with coordinating the government response to a cyber security emergency with a MAJOR severity rating. Specifically, it is responsible for:

- confirming (or identifying) the strategic aim(s) and supporting objectives that will determine the government's response;
- identifying key risks;
- overseeing the implementation of an action plan (including communications material); and
- ensuring that appropriate recovery procedures are designed and implemented.

Composition of a Cyber Security Emergency Coordination Group

Depending on the nature of the incident, a Cyber Security Emergency Coordination Group will typically be chaired by the Director CERT NZ, the Director National Cyber Security Centre, the Director National Security Policy Directorate, DPMC, or a senior representative from NZ Police.

The membership of a Cyber Security Emergency Coordination Group is comprised of senior officials from government agencies with a role in incident response. Attendees reflect a balance of operational, communications and policy expertise. While the agencies involved are likely to vary on a case-by-case basis, the group will likely include the:

- Department of the Prime Minister and Cabinet;
- National Cyber Security Centre;
- CERT NZ;
- New Zealand Police and
- Department of Internal Affairs.

Other government agencies and private sector organisations may be involved as required.

Your role within the Cyber Security Emergency Coordination Group

The Cyber Security Emergency Coordination Group will look to you for current information on the impact of the emergency on your organisation, any measures that your organisation is taking in response to the incident (including communications) and any assistance that your organisation would like from government agencies.

Other groups which may be activated in response to this emergency

Depending on the impacts of the emergency, a Watch Group may be established. Details on the form and functions of a Watch Group are contained in the National Security System Handbook. A copy is available at: https://www.dpmc.govt.nz/sites/all/files/dpmc-nss-handbook-aug-2016.pdf.

(U) Annex B – Cyber Security Emergency Coordination Group agenda template

The Cyber Security Emergency Coordination Group Chair is responsible for producing and circulating the Cyber Security Emergency Coordination Group agenda and the meeting record – which should capture the decisions made, the rationale for those decisions, and any actions for follow up. The agenda for the first meeting will typically include:

1. **Introduction**
    a. Decisions that need to be made immediately
    b. Governance
        i. Lead Agency
        ii. Spokesperson(s)
2. **Situation update**
3. **Assessment**
4. Confirm **strategic purpose and priorities** (this will inform decisions)
5. Consideration of **key risks and implications**
6. **Communications** (public information)
7. **Support requirements and resources**
    a. Activation of appropriate plans and legislation
    b. Tasking of additional resources if required
    c. Activation of specialist support if required
    d. Support for Ministers
8. **Decisions and action items**
9. **Next meeting**