Software Engineering Institute
Carnegie Mellon

New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)

Robin Ruefle
Ken van Wyk
Lana Tosic

May 2013

New Zealand National Cyber Security Centre
Government Communication Security Bureau

Developed in cooperation with the CERT® Division of the Software Engineering Institute at Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0000416

Table of Contents

List of Figures

1 Introduction

1.1 Background

Cyber attacks are becoming more advanced and sophisticated, and are increasingly targeting intellectual property and other proprietary information held by businesses as well as individuals, government organisations, and critical infrastructures. Such attacks are seen across the globe.

Along with the increasing stealth, sophistication, and prevalence of attacks, changes in organisational data protection requirements, institutional regulations and local or national laws, and intruder technology have made it imperative to address security concerns at an enterprise level. If recognised as a business issue, enterprise security can be measured as an investment rather than an expensive business solution.

Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen. When cyber security incidents or attacks occur, it is critical that organisations can respond effectively. The speed with which an organisation can recognise, analyse, and respond to an incident will limit the damage and lower the cost of recovery. These types of activities and functions make up an organisation's incident management process. Such processes involve defining, prioritising, and synchronising the security actions and measures necessary to protect the integrity, confidentiality, and availability of an organisation's critical assets and infrastructures.

Many organisations have formalised their incident management capability and supporting processes as part of an over-arching cyber risk management activity. Such formalisation ensures a level of consistency, quality, and resilience that can withstand staff turnover and the dynamic changes in the cyber security arena. Other motivators driving the establishment or formalisation of incident management processes within organisations include:

- a general increase in the number of cyber security or information technology incidents being reported.
- a general increase in the number and type of organisations being affected by such incidents.
- a more focused awareness on the need for security policies and practices as part of organisational risk-management strategies.

The New Zealand government has responded to this increasingly hostile cyber environment by building strategies and supporting resources to help New Zealand organisations develop and implement better information security defences and practices. Documented guidance for organisations has been published in the *New Zealand Information Security Manual*, whose purpose is to "ensure that a risk managed approach to cyber security is applied within government" [New Zealand Government 2011b]. The New Zealand government has also developed the *New Zealand Cyber Security Strategy*. Both documents include sections on building an incident response (management) capacity. One of the key objectives of the *National Cyber Security Strategy* is to improve the level of cyber security across the government.

Incident Response and Planning is called out in the document as one of the *Strategy's* three priority areas or initiatives [New Zealand Government 2011a]:

> *The preparedness of New Zealand businesses to respond to cyber attacks is critical to New Zealand's cyber resilience. As new and more sophisticated malware and attack tools are developed, it is increasingly important for businesses to have measures in place to identify, assess and respond to incidents and threats.*
>
> *The Government will work with critical national infrastructure providers and other businesses to support them to further develop their cyber security responses.*

The desired outcome is a New Zealand government that is prepared to effectively and comprehensively manage and coordinate responses to, and recovery from, major incidents, regardless of their nature, origin, scale, complexity, intensity, and duration.

The National Cyber Security Centre (NCSC) is leading an initiative to develop an incident management programme specifically for New Zealand to support government and critical infrastructure organisations. This initiative includes developing a standardised method and format for responding to suspected threats, as well as setting up trusted communication channels and collaboration across New Zealand. The initiative also involves developing training and mentoring to ensure the expertise and skill base within these organisations is expanded and matured. One focus of the initiative is to assist government ministries, local government organisations, and critical infrastructure organisations in the development and sustainment of a formalised incident management capability. Such a capability is often institutionalised as a Computer Security Incident Response Team (CSIRT). One of the outcomes of this initiative is the development of this Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)

1.2 The Security Incident Management Guide for CSIRTs

NCSC has developed this *guide* in partnership with the CERT® Division of the Software Engineering Institute (SEI) at Carnegie Mellon University. Using the best practices model developed by the SEI, this guide directly supports the *New Zealand National Cyber Security Strategy* and the *New Zealand Information Security Plan* and is based on NCSC research and coordination of cyber security incidents across New Zealand government, critical infrastructures, and NCSC international partners.

The purpose of this guide is to enable organisations to understand what generic incident management processes, procedures, and resources they must establish to protect their critical assets and meet their business requirements. The guide

- provides best practices and a basic framework for most organisations establishing a security incident management capability or reinforcing an existing one,
- reviews and explains what constitutes an incident management capability,
- describes CSIRT structure and operation, including services, authority, and organisational model, and

® CERT® is a registered mark owned by Carnegie Mellon University.

- provides general guidance on the process of planning and implementing a CSIRT or other incident management capability.

NCSC is part of the Government Communications Security Bureau (GCSB), whose role is to protect government systems and information and to help critical infrastructure operators improve their computer and network security. The CERT Division's primary goals are to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services after attacks, accidents, or failures. The CERT Division has built partnerships around the world to increase cyber security awareness, education, and responsiveness.

This guide is an effort to help government and critical infrastructures identify what type of incident management capability they require and to provide guidance on how they might build such capability. The guide focuses on the CSIRT as an incident management capability structure. However, all the information presented also applies to other incident management structures or capabilities.

This guide is a high-level, introductory document. It is not comprehensive, but it but will serve as a basic starting point for developing an organisational incident management capability. For more detailed information, see the resources in Appendix B.

Questions about this guide should be addressed to the NCSC at info@ncsc.govt.nz.

1.3 Audience

The primary audience of this guide includes CSIRT managers, security managers, and personnel performing incident management tasks. It is particularly geared to the project team within the organisation that will be making decisions on how to stand up or improve the team or capability.

The guide may be of interest to other parts of the organisation that may have oversight or interaction with the CSIRT. It can provide some basic introductory material to business units not familiar with CSIRT services and operations or the concept of incident management such as Human Resources, Legal Counsel, Information Technology (IT), Risk Management, Physical Security, or specific lines of business. This guide may also be of interest to related C-level executives within the organisation such as the chief information officer (CIO), chief information security officer (CISO), or chief risk officer (CRO) if these positions exist.

This document is intended to provide a valuable resource to both newly forming teams and existing teams whose services, policies, and procedures are not clearly defined or documented. Ideally, an organisation should use this document at the early stages of CSIRT formation, after management has provided support and funding to form a CSIRT and prior to the team becoming operational. However, operational teams may find the guide to be a useful reference document.

1.4 Overview of Structure

This guide is broken down into five distinct sections:

- Section 1, Introduction, this section, that provides an overview of the guide, its audience, purpose and how it supports New Zealand cyber security initiatives.
- Section 2, Foundational Overview, defines and provides the context for incident management capability, including how it is instantiated. It reviews the incident handling life cycle, incident management processes and how they relate, and the general components of an incident management capability. It also discusses one particular type of incident management function or structure: the CSIRT, what it does, and what services it can provide.
- Section 3, Specific Guidance for New Zealand Government and Critical Infrastructure CSIRTs, provides more specifics on New Zealand incident response capabilities. It reviews the thought process for choosing how to develop or implement a particular CSIRT component. This section can be read as a whole or with a focus on just the component of interest.
- Section 4, Creating a CSIRT or Incident Management Capability, provides a list of steps for planning the creation of a CSIRT or incident management capability, important caveats, and information on help available from NCSC.
- Appendices, the appendices provide resources to extend understanding and provide further reading.

1.5 How to Use This Guide

Users can read this guide in a sequential manner or choose a particular component or aspect that best meets organisational needs and requirements. If the foundational information is already known, the reader can skip to the New Zealand guidance section directly (Section 3).

Newly forming teams can use the guide as the basis for understanding the issues involved in establishing a CSIRT. They can then use the information to develop detailed domain- or organisation-specific service definitions, policies, procedures, and to identify organisational operational issues. After applying the guidance in this document, an organisation should be on a fast track to a documented, reliable, effective, and responsible incident handling service and over-arching incident management process and function.

Existing teams can use this document to ensure they have covered the main issues and options that are appropriate for their organisation when developing their incident management capability.

Where applicable, the guide identifies approaches that have proved successful and pitfalls to avoid.

1.6 Feedback

Should you identify any corrections, modifications or improvements that should be made to this document, please contact the NCSC at info@ncsc.govt.nz

2 Foundational Overview

This section explains the mission, function, purpose, and activities related to incident management and CSIRT operations.

2.1 What Is Incident Management?

The ability to provide end-to-end, cross-enterprise management of events and incidents that affect information and technology assets within an organisation.

Organisations require a multi-layered strategy to secure and protect their critical assets and infrastructures. That strategy requires technical, organisational, and procedural approaches to manage computer security incidents as part of the overall goal of achieving business or mission objectives in the face of risks and attacks. Organisations do not want to just survive attacks; they want to be resilient.

As a defence against risks and threats from the cyber domain, organisations can:

- identify their key assets and data and their location, business owners, and criticality.
- perform risk assessments.
- keep up to date with the latest operating system patches and product updates.
- install perimeter and internal defences such as routers, firewalls, scanners, and network monitoring and analysis systems.
- update and expand information technology and security policies and procedures.
- provide security awareness training to employees, customers, supply chain partners, and constituents.
- formalise an incident management capability and corresponding processes.

An incident management capability provides coordination and resolution of computer security events and incidents. It implies end-to-end management for controlling or directing how security events and incidents should be handled. This involves defining a process and supporting policies and procedures; assigning roles and responsibilities; having appropriate equipment, infrastructure, tools, and supporting materials; and having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way.

Incident management is different but inclusive of incident handling and incident response. Incident handling is one service covering all the processes, tasks, or functions associated with handling events and incidents:

- detecting and reporting—the ability to receive and review event information, incident reports, and alerts.
- triage—the actions taken to categorise, prioritise, and assign events and incidents.

- analysis—the attempt to determine what has happened; what impact, threat, or damage has resulted; and what recovery or mitigation steps should be followed. This can include characterising new threats that may impact the infrastructure.
- incident response—the actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to stop the incident from happening again.

Incident response, as noted in the list above, is the last step, in incident handling. It is the process that encompasses the planning, coordination, and execution of any appropriate mitigation and recovery strategies and actions. Because the term *incident response* was developed first, many in the community still use it to refer to more than just the response functions, even to the full range of incident management processes.

Incident management is the larger process that includes incident handling, but it also encompasses the functions of preparing for incident handling work, building protections into the infrastructure to help detect, analyse, and respond to events and incidents, evaluating and sustaining the functions, and interfacing with other security and risk management activities.

There are many aspects to successfully managing computer security incidents in an organisation. Frequently, organisations focus primarily on response and fail to adequately consider the other aspects of incident management including preparing the organisation to manage incidents (e.g., gathering the right people, technology, and funding) and sustaining the incident management function over time.

Because incident management includes detecting and responding to computer security incidents as well as preventing them, many different parts of the organisation might be involved. Responding to computer security incidents does not happen in isolation. Actions taken to prevent or mitigate on-going and potential computer security events and incidents can involve a wide range of participants across the enterprise: security analysts, incident handlers, network and system administrators, human resources and public affairs staff, information security officers (ISOs), C-level managers (such as CIOs, CSOs, and CROs), other managers, product developers, and even end users.

To ensure that computer security incident response is effective and successful, all the tasks and processes being performed must be viewed from an enterprise perspective. In other words, an organisation must identify how tasks and processes relate, how information is exchanged, and how actions are coordinated. The term *incident management* refers to this bigger picture.

2.1.1 Incident Management Process

To build effective incident management and CSIRT capabilities, it is essential to identify the processes involved. This guide is based on the best practices model developed by the CSIRT Development Team at the CERT Division of the SEI [Alberts 2004]. This model documents a set of processes that outline various incident management functions. The process model includes the following high-level processes:

1. Prepare/Improve/Sustain (Prepare)

2. Protect Infrastructure (Protect)
3. Detect Events (Detect)
4. Triage Events (Triage)
5. Respond

The purpose of mapping an incident management process is to help agencies understand and document all relevant activities involved. Using the processes as a guide, an organisation can map its own workflows to determine current capabilities and dependencies, as well to identify weaknesses.

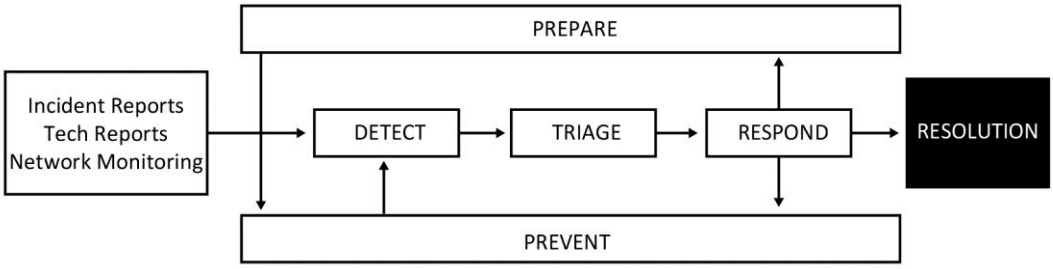

Figure 1: High-Level Incident Management Process Workflow

The following describes all five processes and provides their workflow diagrams.[1]

1. The *Prepare* process outlines requirements for implementing an effective, new incident management programme or improving an existing one. The general requirements for this process are to define the roles and responsibilities of designated incident management personnel and to establish a supporting infrastructure, as well as apply relevant standards and practices. The following is a non-exhaustive example of the activities:
   - establishing security policies, procedures, categories, and severity lists
   - building of initial incident management capability or CSIRT or reinforcing an existing one
   - identifying incident management key roles and management responsibilities within agencies
   - implementing a supporting infrastructure (i.e., incident recording data base, analysis tools, communication channels, and reporting forms)

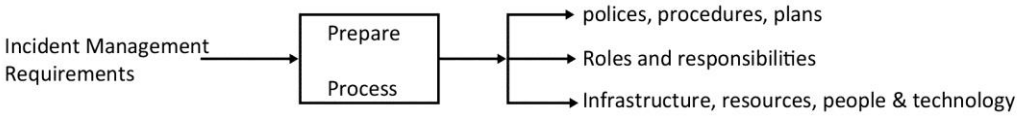

Figure 2: Prepare *Process Workflow*

2. The *Prevent and Protect* process involves actions to contain incidents by making changes in the infrastructure after detection and during response, including filtering, blocking, and eradication activities. This process also involves preventing incidents from recurring by

[1] Some of the diagrams have been customised for NZ NCSC activities.

implementing infrastructure changes based on previous incidents or experience. This process may include but is not limited to

- performing security audit and vulnerability scans and assessments
- following industry standards and best practices for defence-in-depth
- updating perimeter and internal boundary controls (IDS, firewalls, AV, etc.)
- establishing incident management processes as part of change control management

Continuing from the *Prepare* process:

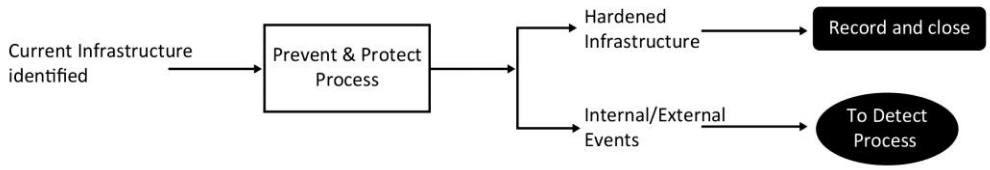

Figure 3: Prevent and Protect Process Workflow

3. The *Detect* Process involves identifying unusual internal or external activity or events that may compromise the availability, confidentiality, and integrity of the organisation's information and systems. Each organisation should have a clear definition of what constitutes a potential threat. Event detection can be either proactive or reactive:

   - proactive detection—receiving information that might suggest potential malicious activity or vulnerability, such as vulnerability alerts and reports, technology watch, and IDS alerts.
   - reactive detection—reporting of unusual activity from internal or external sources, such as system users or information security experts.

   It is essential that all incident details and data have been property recorded, documented, and passed to the *Triage* process for further processing of potentially malicious activity.

   Continuing from the *Prevent* process:

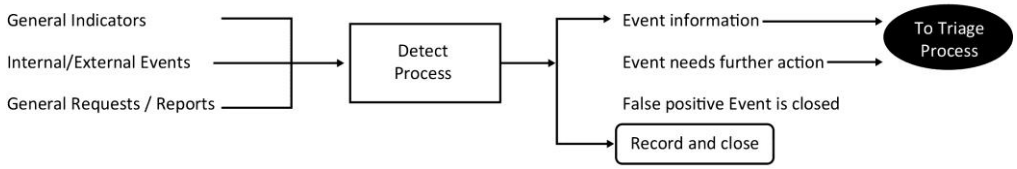

Figure 4: Detect *Process Workflow*

4. The *Triage* process is a critical point in any incident management capability. It is where all information flows into a single point of contact in order to be:

   - categorised
   - prioritised
   - assigned
   - correlated with incoming events

   The *Triage* process collects all available information on an incident to determine the scope of the incident, its impact, and what assets are affected. It then passes the results to the

Respond process. In upcoming CERT documents, the triage process will become the first step of a larger *Analysis* process. For now it will be called *Analysis (Triage)*.

Continuing from the *Detect* process:

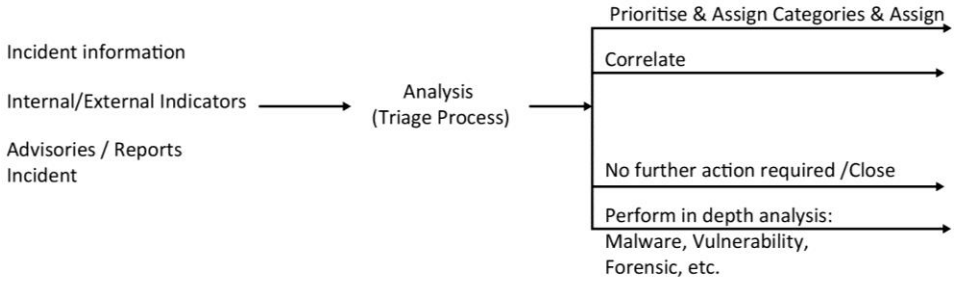

Figure 5: Analysis (Triage) *Process Workflow*

5. The *Respond* process involves actions taken to resolve or mitigate an incident by analysing, coordinating, and distributing information. The response process can actually entail more than just technical response; management and legal response may also be required and should be coordinated with the technical response.
   - Technical response can include analysing incoming events, planning the appropriate response, coordinating actions internally and externally, containing any on-going malicious activity, corresponding mitigation strategies, repairing or recovering any affected systems, performing post-mortem analysis reports and recommendations, and performing incident closure.
   - Management response focuses on activities such as notifications, organisational interactions, escalation, approval, and public relations.
   - Legal response includes actions associated with an incident where an interpretation of law and regulations is needed, such as those that involve privacy issues, nondisclosure, copyright, and other legal matters.

These responses may occur simultaneously and must be coordinated and communicated to achieve the most effect. This may include third-party cooperation and information sharing where possible and appropriate. It should be noted that, according to the *New Zealand Information Security Manual*, a New Zealand government agency must report any significant cyber security incidents [New Zealand Government 2011b].

Continuing from the *Analysis (Triage)* process:

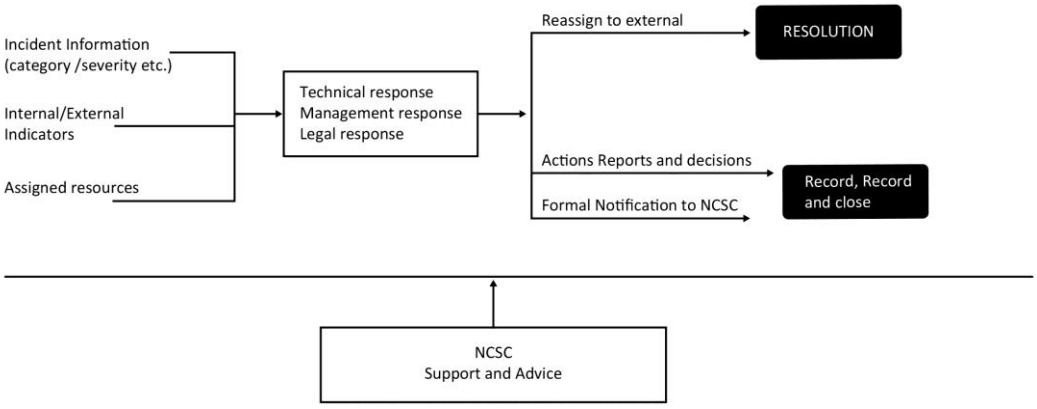

Figure 6: Respond *Process Workflow*

2.1.2 Incident Handling Life Cycle

The incident handling life cycle provides a more in-depth look at the interrelationships between the *Detect*, *Analyse (Triage)*, and *Respond* processes. The life cycle is circular: what is learned throughout the processes can be leveraged to improve the state of the practice in defending against future attacks.

Figure 7 shows how an event is received via monitoring or submitted report and then matched against the incident criteria that have been established. If the event meets the criteria, then an incident is declared, triggering further analysis and remediation. Lessons learned are then fed back into the life cycle to improve analysis and response strategies. The lessons are also shared with the protection and sustainment functions to help prevent incidents and prepare staff and infrastructure for better detection and response.

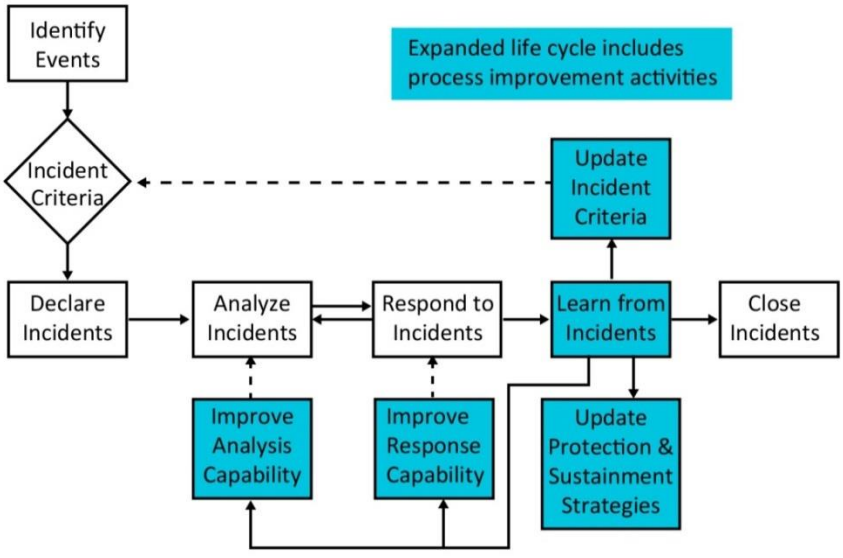

Figure 7: Incident Handling Life Cycle[2]

[2] Source: CERT Resilience Management Model (CERT®-RMM) Version 1.1 available at http://www.cert.org/resilience/rmm.html

Many of the functions and services associated with incident handling occur in parallel rather than sequentially. Some are even iterated, particularly analysis activities. Figure 8 breaks down the various incident handling activities and displays an example of their possible chronological relationships.

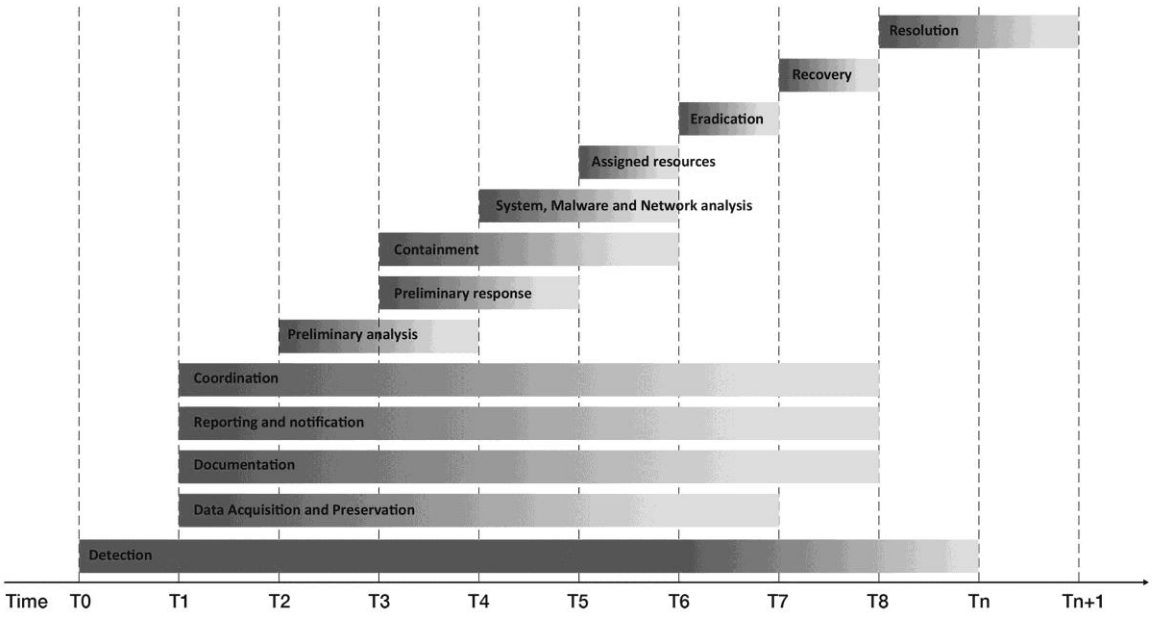

Figure 8: Incident Handling Activity Timeline

Some key supporting activities occur across much of the life cycle and should be recognised:

- Reporting and notification—providing the right information at the right time enables effective incident response. Those responsible for incident handling activities must constantly refine their ability to assess an incident as it unfolds and rapidly provide accurate and accessible information to decision makers. This includes the submission of the initial incident report and any updates that result from analysis or response actions taken. This also includes any notification to other organisations, constituencies, and stakeholders. Reporting and notification happen throughout the entire incident handling process rather than just one time. As more information is obtained or learned, it is passed on to relevant stakeholders.
- Documentation—this is not limited to the initial documentation of the incident in an incident reporting form, but also includes documentation of additional information gathered during analysis and response. This documentation process may also include response actions, including preliminary response actions, first responder actions, or actions taken to preserve and protect incident artefacts, evidence, or chain of custody.
- Coordination—this includes coordination between organisational components, outside experts, and other stakeholders to:
  - gather information, such as log and artefact collection.
  - share information, such as situational awareness, intelligence reports, and law enforcement activities.

- plan and implement response strategies across affected components.

2.2 Benefit of a Formalised Incident Management Capability

Any organisation that has networked systems connected to the internet must be able to manage events and incidents—even if the service is outsourced to a third party. The organisation must be able to understand the types of threats, events, and incidents that affect its overall wellness; lacking such a function can increase the risk to the organisation's business, products, services, finances, and trust.

Defining the capability helps ensure that there is a focused response effort staffed by people with expertise and experience. This allows a more rapid, standardised, and coordinated response rather than an ad hoc response. Instead of figuring it out as they go, a stable cadre of staff with incident handling expertise, combined with functional business knowledge, will know whom to contact and what steps to take to resolve and coordinate issues.

Formalising an incident handling capability also allows trust to evolve in the organisation and provides a point of collaboration with others in security community. More importantly it provides a centralised point of incident reporting and analysis, response coordination, and information dissemination. By having such a centralised, continuously operating point of presence, an organisation can take a more proactive, preventative approach and employ a more predictive analysis framework.

One of NCSC's goals in establishing this guidance document is to help build consistent incident management points of presence throughout New Zealand government and critical infrastructure organisations. Such points will act as partners, collaborators, and stakeholders in securing New Zealand's infrastructure and businesses and for responding to significant cyber incidents. It is hoped that a trusted network of experts will develop who know each other and can work together to resolve critical problems and issues related to cyber threats and attacks. Local points of presence understand their organisation's business missions and processes better than an outside presence (such as NCSC) and are better able to work with their colleagues to solve the problems. However, because some organisations may be small and not have expertise in all areas of incident management, having relationships with other incident management capabilities can provide surge and backup support, mentoring, or shared knowledge when needed.

2.3 Building an Incident Management Plan

Incident management is not just the application of technology to resolve computer security events. It requires the development of a plan of action and set of processes that are:

- consistent
- repeatable
- quality-driven
- measurable
- understood across the constituency or enterprise

It also requires the establishment of processes for:

- notification and communication,
- analysis and response,
- escalation,
- collaboration and coordination, and
- maintenance and tracking of records

Organisations should document their incident management processes in an incident response or incident management plan. This plan outlines activities, roles, and responsibilities for reporting, detecting, analysing, responding to, and recovering from computer security incidents. This is needed to ensure that the incident management process is institutionalised or, known by and followed throughout the organisation.

Having such a plan or documented guidance in place provides the organisation with a standard operating procedure for handling incidents and vulnerabilities that may threaten or impact critical business operations and information. It also enables the organisation to proactively engage the process immediately when an attack or other malicious activity is detected, rather than trying to figure out what steps need to be taken while already in the middle of an incident. Being prepared and knowing what steps to follow, what resources are available, whom to contact, and what policies and procedures to follow enable the organisation to respond in a timely manner which can result in quicker containment, eradication, and response and lower the incident's impact and damage.

An incident management plan should include at least the following components:[3]

- defined purpose and structure of the incident management function.
- outlined workflow for handling incidents across the incident management function and other parts of the organisation.
- description of the services performed by the incident management function.
- defined goals for the outcome of the response (e.g., collected evidence, coordinated information sharing, resolved incident).
- defined scope of the type of incidents handled and not handled.
- key people responsible for initiating and executing the plan.
- defined roles and responsibilities across the organisation for reporting, detecting, analysing, and responding to incidents.
- authority for performing various incident management and response activities.
- guidelines for determining who coordinates the incident response.
- high-level guidelines for what type of incidents to report and how to report them.
- guidelines for managing incidents throughout their life cycle, including closing incidents and conducting post-mortem analysis.

[3] This list represents the high-level, overall plan. Specific aspects of an incident management plan may entail additional detailed plans and policies.

- guidelines for whom to notify and in what timeframe (could also be in a communications plan).
- key data handling guidance that calls out the levels of sensitivity of data and how it should be shared, stored, or transmitted and to whom.
- guidance for contacting and working with human resources, legal counsel, business units, management, and other parts of the organisation.
- guidance for contacting external stakeholders or collaborators.
- guidance for pulling in additional staff or surge support to assist in times of crisis or when normal resources cannot scale.

Some incident response plans contain specific steps for handling specific types of incidents; these may be documented in incident scenarios and potential mitigations.

To be successful the incident response plan should:

- integrate into the existing processes and organisational structures so that it enables rather than hinders critical business functions.
- strengthen and improve the capability of the constituency to effectively manage security events and thereby keep intact the availability, integrity, and confidentiality of an organisation's systems and critical assets, where required.
- support, complement, and link to any existing business continuity or disaster recovery plans where and when appropriate.
- support, complement, and provide input into existing business and IT policies that impact the security of an organisation's infrastructure.
- implement a command and control structure, clearly defining responsibilities and accountability for decisions and actions.
- be part of an overall strategy to protect and secure critical business functions and assets.

2.4 Models for Institutionalising Incident Management Capability

How computer security incident management capabilities are implemented in different organisations can vary greatly. The choice of model may depend on the organisation's business security needs, size, or funding.

Some organisations may perform this function as part of security, IT, risk management, or business continuity functions. This is common in commercial industry, where this function may be served by:

- security teams
- security operation centre (SOCs)
- network operations centres (NOCs)
- crisis management teams
- resiliency teams
- IT helpdesk tiered team of experts (usually a level 3 or level 4 team)

- an outsourced team

Some organisations may assign responsibility for this function to a defined group of people or a designated unit such as a CSIRT.

Incident management, as a complete function, may be performed by both a formal CSIRT along with other groups in the organisation. Several groups, each with distinct or overlapping responsibilities, may manage cyber security events and incidents. This can include groups that manage firewalls, patch management systems, or even perform vulnerability analysis and response, if these functions are not handled by the CSIRT.

Organisational CSIRTs usually perform incident handling activities and are generally the focal point for coordinating and supporting incident response. How a particular organisation's incident management capability is structured and how the tasks are assigned across the enterprise depend on the organisation's mission, culture, and expertise.

2.5 What Is a CSIRT?

A CSIRT is a concrete organisational entity or capability (i.e., one or more staff members) that is assigned the responsibility of providing part of the incident management capability for a particular organisation. CSIRT incident handling activities may include:

- determining the impact, scope, and nature of the event or incident.
- understanding the technical cause of the event or incident.
- identifying what else may have happened or other potential threats resulting from the event or incident.
- researching and recommending solutions and workarounds.
- coordinating and supporting the implementation of the response strategies with other parts of the enterprise or constituency, including IT groups and specialists, physical security groups, information security officers (ISOs), business managers, executive managers, public relations, human resources, and legal counsel.
- disseminating information on current risks, threats, attacks, exploits, and corresponding mitigation strategies through alerts, advisories, web pages, and other technical publications.
- coordinating and collaborating with external parties such as vendors, ISPs, other security groups and CSIRTs, and law enforcement.
- maintaining a repository of incident and vulnerability data and activity related to the constituency that can be used for correlation, trending, and developing lessons learned to improve the security posture and incident management processes of an organisation.

A CSIRT has specialised knowledge of intruder attacks, threats, and mitigation and resolution strategies. It understands the escalation process and works to communicate relevant information to stakeholders and customers in a timely and effective manner. In addition, a CSIRT may:

- recommend best practices regarding secure configurations; defence-in-depth strategies for protecting systems, networks, and critical data and assets; and incident prevention.[4]
- perform or participate in vulnerability assessment and handling, malware analysis, computer forensics evidence collection and analysis, systems and network monitoring, security policy development, and security and awareness training and education.
- provide input into or participate in security audits or assessments such as infrastructure reviews, best practice reviews, vulnerability scanning, or penetration testing.
- conduct public monitoring or technology watch activities such as reviewing security websites, mailing lists, or general news and vendor sites to identify new or emerging technical developments, intruder activities, future threats, legal and legislative rulings, social or political threats, or new defensive strategies.
- support legal and law enforcement efforts through the collection and analysis of forensic evidence (provided that staff have the appropriate expertise, training, and tools).

The goal of a CSIRT is to minimise and control the damage resulting from incidents, provide effective response and recovery, and work to prevent future incidents. However, a CSIRT also can—and should—provide true business intelligence to its parent organisation or constituency by virtue of:

- the information it collects on the types of threats and attacks that currently impact or could potentially threaten the enterprise.
- its expertise in general intruder attacks and trends and corresponding mitigation strategies.
- its understanding of infrastructure and policy weaknesses and strengths based on performed incident post mortems.

CSIRT staff require skills and expertise in understanding intruder attacks and mitigation strategies, the incident management processes, and how to respond to events and incidents and coordinate their resolution.

Many organisations also assign the CSIRT responsibilities for protecting the infrastructure and detecting and triaging events. Each organisation must determine which of the incident management capabilities its CSIRT will provide.

An on-site CSIRT can rapidly respond to and contain a contain computer security incident, as well as help the organisation recover. CSIRTs may also be familiar with the compromised systems and therefore be more able to coordinate their recovery and propose mitigation and response strategies in a more effective manner.

A CSIRT's relationships with other CSIRTs and security organisations can facilitate the sharing of response strategies and early alerts to potential problems. CSIRTs can work proactively with other areas of the organisation to ensure new systems are developed and deployed with security in mind and in conformance with any site security policies. CSIRTs can also provide expert preventive and predictive analysis to help mitigate future threats.

[4] These recommendations are usually provided to the IT group charged with building and maintaining the security infrastructure.

2.5.1 CSIRT Purpose

CSIRTs can vary in purpose based on sector. For example, law enforcement CSIRTs may focus on prosecuting cybercrime incidents by collecting and analysing computer forensic data from affected or involved systems. Government CSIRTs, on the other hand, may be involved in security awareness training and general incident handling activities but never perform any forensics activities, which may instead be handled by special investigators within the government agency.

Whatever special tasking a CSIRT might have, their main function is incident handling.

2.6 Components of a CSIRT Capability

This section describes a CSIRT's generic components that need to be defined when planning and implementing a CSIRT. The Following sections describe the components in more detail.

The components of a CSIRT include:

- constituency—whom the CSIRT provide services to/for
- mission—what the CSIRT does at the highest level (i.e., purpose)
- services—how the CSIRT accomplishes its mission, defined in part by
  - functions provided
  - types of incidents handled
  - types of activities performed
- organisational structure—how the CSIRT is organised, and how the CSIRT connects with other parts of the organisation
- resources—staff, equipment, and infrastructure needed to operate and perform the CSIRT's mission
- funding—how all of the components are financed and sustained

A key element in the success of the CSIRT components is achieving management and constituent buy-in to the idea and operational processes of the team. Without buy-in, the team will not succeed. To gain such buy-in, management and constituent requirements, expectations, desires, and problems need to be understood and addressed during CSIRT development. The group planning and designing the CSIRT must meet with representatives from these entities to collect this information. These representatives should also participate in the planning and design phases.

It is particularly important to understand what incident management activities are already occurring and who is performing them. If the activities are already being satisfactorily performed by others, the CSIRT can incorporate them or develop coordination channels to work together. This might free up the CSIRT to perform other key functions.

The components of a CSIRT influence each other and therefore influence the design of the whole. For example, the constituency and needs will influence the mission. The resources and

how they are dispersed will influence the organisational model needed, the services the team can provide, and how well the mission can be executed.

2.6.1 CSIRT Constituency

During its operation, every CSIRT will interact with a wide range of entities. The most important of these is the specific community that the CSIRT was established to serve; its constituency. A CSIRT constituency can be unbounded (the CSIRT will provide service to anyone requesting it), or it can be bound by some constraints. Most commonly, CSIRTs have bounded constituencies that tend to reflect the CSIRT's funding source. The most common constraints are determined by nation, geography, political divisions (e.g., government departments), technical specifications (e.g., use of a specific operating system), the organisation (e.g., within a given corporation or company), the network service provider (e.g., connection to a specific network), or contracts (e.g., the customers of a fee-for-service team).

A CSIRT cannot operate effectively without gaining and maintaining the constituency's trust and respect. Even a CSIRT that has total authority over its constituency cannot assume it has its constituency's trust and respect, which must be earned and nurtured. Experience indicates that it takes about a year from the time that a team commences operations and announces itself before the constituency may feel comfortable reporting incidents or asking for assistance on a regular basis.

Understanding the CSIRT's constituency will help determine their needs, the assets that need to be protected, and the requirements for the CSIRT. This information will, in turn, help the team determine what services it can offer and what organisational model will fit the needed service delivery.

Defining the CSIRT's constituency will also help scope the team's work when it becomes operational. It will help determine what requests the team will handle and what requests will be passed on to other CSIRTs or other relevant parties.

Some teams may have their constituency already defined. For example, the constituency of a CSIRT in a small commercial business will mostly likely be the business's employees; while the constituency for a government agency may be the government agency employees. However, defining a constituency may not be so easy. A CSIRT at a university could have as its constituency the systems and networks administrators in the various departments or the entire university population, including all faculty and students. This distinction is important. For a university CSIRT, it will determine the level of alerts and advisories the team will write and what type of responses they will make.

Examples of constituencies include:

- CSIRT parent organisation
- government ministries, authorities, and institutions
- embassies and other government bodies worldwide
- military organisations
- critical infrastructures

  - banks
  - oil and gas organisations
  - telecommunication organisations
  - transport and logistics organisations
- education and research organisations
- the private sector
- members via subscriptions
- the general public

2.6.2 CSIRT Mission

The CSIRT's mission should explain the purpose of the team and highlight its core objectives and goals. The mission statement should

- be unambiguous.
- consist of at least three or four sentences specifying the mission with which the CSIRT is charged.
- complement the mission of any larger organisation that houses the team or any external bodies that fund it.

The Internet Engineering Task Force's RFC 2350, *Expectations for Computer Security Incident Response*, is a best practices document that provides information on general topics and issues that need to be clearly defined and articulated to a CSIRT constituency and the general internet community [Brownlee 1998]. The RFC document lists the various components of a CSIRT charter, which provides some recommendations for what should be included in the mission.

2.6.3 CSIRT Services

Not all CSIRTs provide the same set of services. The services provided depend on the needs of the constituency, the expertise available, and the funding and resources allotted. CSIRTs should strive to choose a small set of services that are most needed and ensure they are operational before expanding. One of the biggest problems a team can have is to try to offer too many services at once.

The services a team can potentially provide cover a broad range of activities. The CSIRT services list shown in Figure 9 was jointly created by the CERT CSIRT Development Team and the Trusted Introducer for European CSIRTs service. Appendix C defines each service and explains the different categories of services. It should be remembered that this list is not a list of what a CSIRT *should* offer. It is a list of potential services that a team might offer. No single CSIRT should try to offer all services.

Security quality management services refer to services normally performed by other organisational entities. The CSIRT might provide input to the service deliverer but does not usually perform the service itself. CSIRTs do, however, often provide security consulting, awareness building, and education and training.

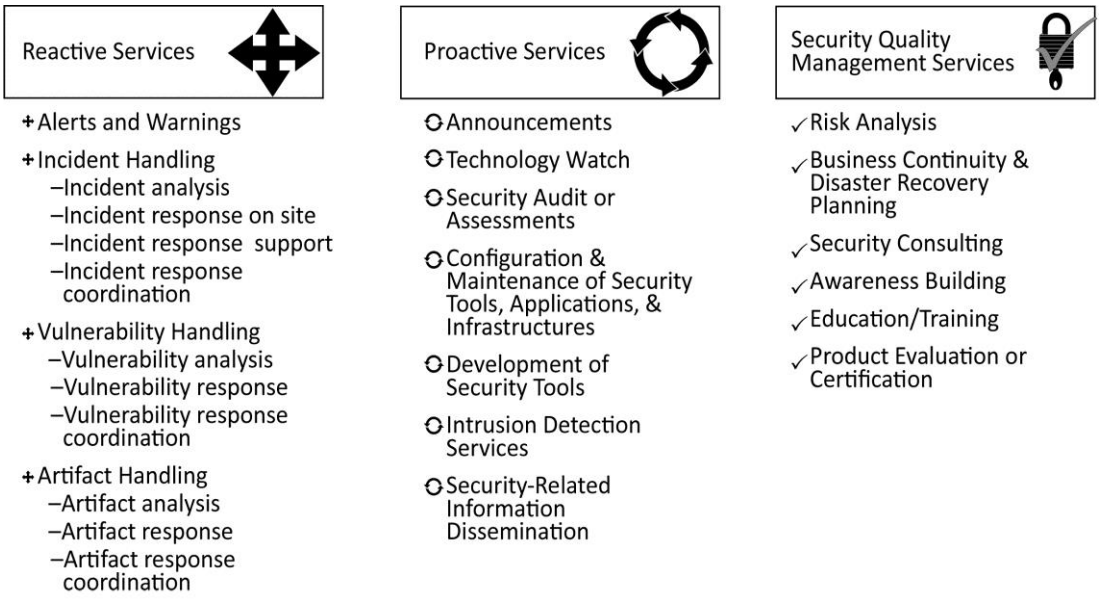

Figure 9: CSIRT Services List

For a team to be considered a CSIRT, it must perform at least one of the following incident handling services:

- incident analysis
- incident response on-site
- incident response support
- incident response coordination

Different types of CSIRTs will offer different sets of services. A national team may spend a lot of time doing collaboration and coordination work but no artifact (malware) analysis or vulnerability handling. Many CSIRTs do not do artifact (malware) analysis and vulnerability handling because it requires more expertise and time.

Once a team has chosen its services, it must define how each service operates within the CSIRT and for the constituency. This includes developing service descriptions, rules of engagement, triggers or approvals for execution, methods of request, and supporting policies and procedures.

The need for well-defined services, policies, and procedures does not diminish once the CSIRT is operational. Existing CSIRTs lacking clearly defined services commonly suffer from recurring operational problems. For example, they rely on their existing staff to pass on their operational experience to new staff. All too frequently, the consistency, reliability, and levels of service exhibited by such CSIRTs fluctuate dramatically due to the varied perceptions of each of the team members. As a consequence, the constituency served by these CSIRTs may have a false impression of the services offered, which jeopardises essential rapport between the CSIRT and its constituency. Clearly defined and documented services will help the team and, more importantly, will provide guidance for the team's constituency, enabling them to understand the services offered by the CSIRT and how those services should be accessed and used.

2.6.4 Policies and Procedures

All services and CSIRT functions should be supported by well-defined policies and procedures. These offer guidance for:

- roles and responsibilities
- priorities
- escalation criteria
- the nature of responses given
- new CSIRT staff members

As a CSIRT is established, the organisation should establish the essential policies, procedures, or process guidance. The organisation will not be able to create them all before the team is implemented, but it should create the key pieces. Specifically, the incident management plan and any supporting concept of operations (CONOPS) or charter that defines the purpose and operation of the team should be in place, approved by management, and disseminated to the constituency.

Other policies, procedures, and guidance that should be in place include the:

- security policy—outlines the general security actions and protections for the organisation.
- incident reporting policy—outlines the type of incidents that should be reported by the constituency, to whom they should be reported, and by what mechanisms.
- external communications policy—defines whom they can talk with (e.g., other CSIRTs, law enforcement, and victims of attacks) and what type of information can be shared outside the CSIRT and parent organisation. This policy is often created in conjunction with an information disclosure policy that outlines what type of information can be released by the CSIRT and to whom.
- communication plan or policy—identifies requirements for notification or communication of potential threats and detected incidents, or mitigation and resolution strategies, within the constituency or to designated stakeholders, partners, or oversight agencies. The communication plan should also cover who should receive the information and in what timeframe.
- media relations policy—defines how to handle questions from the media and what might be talked about in media interviews. This includes any process for facilitating media access to designated CSIRT staff through organisational media relations personnel.
- data sensitivity policy—defines a schema for determining the level of sensitivity to be used to categorise data and assets and the required labelling and protection for each level.
- data storage and handling policy—determines how long data and logs and artifacts related to incident handling are retained and how they are stored and protected.
- acceptable use policy—defines, for the constituency and the CSIRT members, acceptable behaviour and use of organisational equipment and assets along with consequences for violating the policy.

Supporting procedures for how to conduct the policies should also be in place. The remaining procedures for all other CSIRT activities will be developed as the team gains operational experience.

Key procedures that also might need to be set up initially include but are not limited to:

- receiving, analysing, and remediating incident reports
- gathering, securing, and preserving evidence
- configuring CSIRT networks and systems
- performing system and network monitoring and intrusion detection and handling alerts
- handling incidents perpetrated by organisational insiders[5]

All of these policies and procedures should be supported by:

- definitions for what a computer security or cyber incident entails for the CSIRT or constituency
- categories of incident types
- criteria or triggers for declaring an incident and engaging the incident response process

2.6.5 Organisational CSIRT Structure

A CSIRT can take many forms or organisational structures. It can be a separate entity with staff assigned to perform incident handling and related activities 100 percent of the time, or it can be an ad hoc group, pulled together based on members' expertise and responsibility when a computer security incident occurs. Participating in proactive activities such as security and awareness training, security assessments, security information dissemination, and network monitoring is more difficult for members of ad hoc CSIRTs because their day-to-day activities are not necessarily related to incident response.

CSIRTs come in all shapes and sizes and serve diverse constituencies. Some CSIRTs, such as the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), support an entire country. Other CSIRTs may provide support to a particular university such as Oxford, a commercial organisation such as Boeing or SUN Microsystems, or a particular domain or IP range such as the one in Brazil (CERT.br). There are also corporate teams and organisations that provide CSIRT services to clients for a fee.

General categories of CSIRTs include:

- internal or organisational CSIRTs—provide incident handling services to their parent organisation. This could be a CSIRT for a bank, a university, or a federal agency.
- national CSIRTs—coordinate and facilitate the handling of incidents for a particular country or economy. They will usually have a broader scope and a more diverse constituency.

---

[5] An insider is defined as *Current or former employee, contractor, or other business partner who has or had authorized access to an organisation's network, system or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organisation's information or information systems.*

- analysis centres—focus on synthesising data from various sources to determine trends and patterns in incident activity. This information can then be used to help predict future activity or provide early warning when current activity matches a set of previously determined characteristics.
- vendor teams—coordinate with organisations who report and track vulnerabilities. Another type of vendor team may provide internal incident handling services for their own organisation.
- incident response providers—provide incident handling services as a product to other organisations. These are sometimes referred to as managed security service providers (MSSPs).

Various global and regional organisations devoted to incident management collaboration and coordination have been created. This includes organisations such as the Forum of Incident Response and Security Teams.[6]

The size and geographical distribution of an organisation can shape a CSIRT's organisational model or structure. Models include but are not limited to:

- security team
- internal distributed team
- internal centralised team
- combined distributed and centralised team
- coordinating CSIRT

Security Team

When an organisation has no identified CSIRT, system and network administrators usually perform incident handling activities as part of their other duties.

Maintaining responsibility for incident response at the local system and network administrator level has several consequences. This localised strategy does not allow the security team to collect security data across the organisation, analyse that data to identify current and future threats, and alert the organisation and distribute preventive and remedial actions.

Internal Distributed Team

In this model, existing staff provide a virtual, distributed CSIRT. A manager or team lead oversees and coordinates activities affecting the virtual team. Individuals across the organisation are identified as the appropriate points of contact for particular functional areas or divisions, based on their experience and expertise with various operating-system platforms, technologies, and applications. These staff members may perform incident handling on a full-time or part-time basis.

[6] http://www.first.org/

This virtual organisation executes the organisation-wide incident response activity. Such a model also allows information to flow across the organisation, including incident reports and response strategies.

If the team is composed of individuals with only part-time CSIRT responsibility, finding individuals with the appropriate experience, skills, and training, and who are willing and able to take on these tasks, may be problematic. Once found and trained, these individuals need to be allowed to invest the time and energy to keep their skills and abilities current, raising the possibility that the CSIRT members' operating units may not be able to sustain their appropriate commitments.

Effective management and coordination of this virtual organisation may become a problem. It will take a strong, central leader to develop a team spirit and keep all sites operating according to general standards.

Internal Centralised CSIRT

In this model, a fully staffed, dedicated CSIRT is given the resources to provide the services outlined in its mission. All team members spend 100 percent of their time working for the CSIRT. The team leader reports directly to high-level management, and the team is centrally located.

This dedicated CSIRT model provides a very stable structure for building manageable, predictable incident handling capabilities. It provides the organisation a clear mechanism for proactively managing its computer security risks. The organisation can now analyse potential threats and risks and determine the appropriate levels of prevention and mitigation necessary to provide adequate levels of response.

This model requires that a new, specialised unit be created, staffed, and integrated into the organisation's operations.

The main weakness of the internal centralised CSIRT is that the incident handling capability is separate and distinct from the operational units. In a small organisation, this should not be a problem. This might be an optimal model for a small organisation. In a large organisation, it may be difficult for the CSIRT to keep up to date with changing technologies across geographically dispersed sites. It may also become difficult for the dedicated team to integrate and coordinate across a large organisation. There is also no mechanism to ensure that response efforts are being carried out in a consistent, correct manner at the local level.

Combined Distributed and Centralised Team

This model is an attempt to combine the best features of the distributed model with the best features of the centralised model. It maximises the utilisation of existing staff in strategic locations throughout the organisation with the centrally located coordinating capabilities of the dedicated team to provide a broader understanding of the security threats and activity affecting the constituency.

The strength of this model is that it provides a stable core of full-time CSIRT professionals along with a network of part-time affiliated members from the operating units. The full-time members

provide the stability, expertise, and permanent infrastructure, while the part-time members provide the operational knowledge and ability to involve appropriate personnel from their business units. This arrangement can increase acceptance or buy-in from all parts of the organisation.

The greatest weakness of this approach is that two systems must be managed and coordinated. If this is not handled well, the dedicated team will be disconnected from the rest of the organisation and the distributed component ineffectual. This model doesn't necessarily work well for small organisations, as they do not usually have the needed expertise distributed across the organisation.

Coordinating CSIRT

A CSIRT can also be organised as a coordinating centre rather than a direct incident response service. The coordinating CSIRT helps organise response efforts across geographically dispersed CSIRTs or even across an organisation's business units that have their own CSIRTs. These dispersed groups carry out the actual incident response steps and mitigation strategies. The coordinating CSIRT synthesises incident reports and statistics from all areas to determine the general security position of the organisation and its vulnerability to attack. It also consolidates the information so that an accurate picture of incident activity across the organisation can be relayed as needed.

As a coordinating centre, a CSIRT might also act as a major reporting for a number of constituencies or other CSIRTs. It may also coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broader community.

The CSIRT of a country, state, or province would most likely follow this model.

Other Alternative CSIRT Organisational Models

Often an organisation may be too small to support a CSIRT structure. In that case the CSIRT function might be outsourced, or it may be reduced in scope. A reduced scope can mean that the CSIRT might only be a point of information sharing, with someone assigned as a liaison between the organisation's system administrators, network administrators, and relevant managers and a larger coordinating CSIRT or national coordination centre

Whatever model is chosen must fit the environment, culture, and need of the parent organisation. These models can apply across the CSIRT types.

2.6.5.1 Coordination and Collaboration

Incident handling is not a self-contained process. Relationships, communication channels, data-sharing agreements, and policies and procedures must be established across the organisation to support this activity.

Because a CSIRT may only perform some of the organisation's incident management tasks, it is important to identify who else is involved. This may include management, other technical and

legal personnel, or investigative personnel. Defining the interfaces between groups and establishing a standard and consistent process for them to work together will make or break an incident management capability.

An internal team should define how to work with:

- business managers—They need to understand what the CSIRT is and how it can help support their business processes. Agreements must be made concerning the CSIRT's authority over business systems and who will make decisions if critical business systems must be disconnected from the network or shut down.
- representatives from IT—How will the IT staff and the CSIRT interact? What actions will be taken by IT staff, and what actions are taken by CSIRT members? What information can the IT staff provide to the CSIRT, and what information the CSIRT can provide to the IT team? What roles and authority does each have?
- representatives from the legal department—When and how is the legal department involved in incident response efforts?
- representatives from human resources—They will need to be involved in developing policies and procedures for removing internal employees found engaging in unauthorised or illegal computer activity.
- representatives from public relations—They must be prepared to handle any media inquiries and help develop information disclosure policies and practices.
- any existing security groups, including physical security—The CSIRT will need to exchange information with these groups about computer incidents and may share responsibility with them for resolving issues involving computer or data theft.
- audit and risk management specialists—They can help develop threat metrics and potential risks to constituency systems.
- any law enforcement liaisons or investigators—They will understand how the team should work with law enforcement, when to contact them, and who will do the investigations or even forensic analysis.
- general representatives from the constituency—They can provide insight into their needs and requirements.

Identifying areas of expertise, defining roles and responsibilities, and outlining rules of engagement for any interface between groups are key steps to begin building an effective capability. Rules of engagement might include determining if a CSIRT incident tracking or ticketing systems needs to interface with any existing trouble ticket databases or determining if the CSIRT will need service level agreements with the constituent business units.

To whom the CSIRT reports will depend on where it is located in the organisation and vice versa. In today's organisational structures, the CSIRT would not normally be part of the IT department, but would be outside that area, in an independent capacity. This may mean that they report to the:

- chief security officer (CSO), if this is where cyber security issues are handled.

- chief information security officer (CISO), if physical and cyber security are combined.
- chief risk officer (CRO), if the risk management area has incorporated security risks into its domain.

The CSIRT could be an independent unit reporting to a specific business manager or directly to the executive manager or agency head.

Wherever it is located, the CSIRT should be at a level where it can achieve organisation-wide collaboration and information sharing and, when necessary, enforce its mandate. It is important to think about what actions the CSIRT will need to take and what type of management support will be required to facilitate those actions during incident handling and response. Identifying such issues may suggest the right reporting or management structure. Experience shows that the higher up the management chain the CSIRT is positioned, the better situated it will be to perform its function.

Any contractual or legal obligation may impact the CSIRT reporting structure. For example, the CSIRT may be contracted to support a specific constituency or organisation. This contract may require specific decisions makers to be involved in CSIRT actions or for the CSIRT to report specific information on a periodic basis to designated management. Management may also require periodic updates on CSIRT activity, or department heads and other managers may want to be involved in CSIRT response decisions.

2.6.5.2 Authority

Authority describes the control that the CSIRT has over its own actions and the actions of its constituents, related to computer security and incident response. Authority is the basic relationship the CSIRT has to the organisation it serves. Authority goes hand in hand with the location of the CSIRT in any organisation.

There are three distinct levels of authority or relationships that a CSIRT can have with its constituency:

- full—The CSIRT can make decisions, without management approval, to implement response and recovery actions. For example: A CSIRT with full authority would be able to tell a system administrator to disconnect a system from the network during an intruder attack, or the CSIRT itself could disconnect the system.
- shared–The CSIRT participates in the decision process regarding what actions to take during a computer security incident but can only influence, not make, the decision.
- no authority—The CSIRT cannot make any decisions or take any actions on its own. The CSIRT can only act as an advisor to an organisation, providing suggestions, mitigation strategies, or recommendations. The CSIRT cannot enforce any actions. The key to success in this case is the ability to influence which will depend on the trust given to the CSIRT based on its performance and ability.

Another type of authority is indirect authority, in which the CSIRT may be able to exert pressure on the constituency to take a specific action. For example, an ISP may be able to force its constituents to take a specific action or face discontinuation of internet services.

For a CSIRT to be successful in its mission, it is critical that management approves and supports the team's level of authority; otherwise, the team will lose credibility within the organisation and will not be successful. Management—particularly division managers, system and network administrators, and any other groups within the organisation—should also adequately and clearly convey the CSIRT's authority to the constituency. This is often done by sending out an executive memo that designates the CSIRT as having authority for a specific set of incident management activities.

2.7 CSIRT Resources

CSIRT resources include the staff, equipment, and infrastructure needed to successfully operate the team and fulfil the mission.

2.7.1 Staffing

Hiring or obtaining the right staff is critical to the success of a CSIRT team. The best staff embodies a variety of skills. They are dedicated, innovative, detail-oriented, flexible, analytical, problem-solvers, good communicators, and able to handle stressful situations. One of the most traits of a team member is integrity. Team members must also have a good sense of being part of a working team. Staff must be able to deal with the slow days and the hectic days.

Skills can include:

- personal
  - people skills
  - communication skills
- technical
  - system and network administration experience
  - platform expertise: UNIX, Windows, Macintosh
  - basic understanding of internet protocols
  - basic understanding of common computer attacks and vulnerabilities
- security training
  - incident handling experience
  - problem-solving abilities
  - critical thinking and analysis abilities
  - cyber threats and attack knowledge
  - digital media analysis (forensics) and malware analysis skills

When hiring CSIRT staff, requirements for certifications and/or background checks should also be considered.

2.7.2 Infrastructure

A CSIRT infrastructure should incorporate all known precautions that are physically and financially possible. CSIRTs should serve as a model to other organisations. They must ensure that their operations are secure and all incident and sensitive data are protected. Their purview

should include both physical and network infrastructures. Access to CSIRT staff should be protected as stringently as access to the data they are working with.

To perform their functions, CSIRT staff will need access to basic computing and communications systems. These include, as needed, home and office equipment for production work and also test labs or equipment for analysis work, including vulnerability analysis and malware analysis where appropriate.

A support infrastructure for the operation of the CSIRT and its various activities is also highly recommended rather than using the existing parent organisation's network. However, this is not always possible due to funding, logistics, or available expertise.

Recommendations and considerations for a supporting CSIRT infrastructure include but are not limited to:

- separate CSIRT network
- secure network and system configurations
- separate email, web, DNS, and other appropriate servers and services
- up-to-date and consistent software versions and patches as an archive for recovery and patching
- standardised method for updating software on staff devices (patch management)
- test network, lab, or devices
- secure intranet for CSIRT staff internal communication and actions
- robust tracking system for incident handling
- secure communications mechanism
- secure remote access
- phone bridges and teleconferencing capabilities
- analysis, correlation, visualization, and trending tools

2.8 Summary

Some guiding principles of CSIRT development should be considered and recognised when building a team:

- *All teams are different*. Each CSIRT must recognise that other teams may not do things the same way they do or even categorise incidents in the same way or at the same priority. These differences must be respected at all times.
- *Know your constituency and their service mission.* The CSIRT processes and capability implemented will depend on the defined mission, key assets or lines of business to be protected, funding, and expertise available.
- *Leverage what already exists.* This can mean understanding who is already doing incident management within the organisation and incorporating their applicable ideas and processes, or using tools and templates such as incident reporting forms from other CSIRTs (with approval and appropriate citations).

- *Learn from others*. Many members of the CSIRT community have tackled the logistical issues and problems associated with standing up a team. Organisations should get to know them and meet with them to see what lessons they have learned that may apply to the organisational CSIRT's situation.

The CERT Division has learned specific lessons:

- Trustworthiness is paramount to success.
  - A CSIRT's staff is its main external interface.
  - Their attitude, actions, and responses are key to the team's success.
- Train for a marathon, not a sprint.
  - CSIRTS will be responding to incidents for many years to come.
  - Many new CSIRT staff initially think their efforts will result in immediate security improvement, but it may take time.
  - CSIRTs have the opportunity to increase security awareness in their constituency.
- Many CSIRTs
  - have no authority over their constituency and must be effective through influence.
  - are a third party to an incident: not the victim, not the perpetrator, not the investigator.
- CSIRTs need to understand their role and not intrude on the role of others.
- No two CSIRTs are identical.

3 Specific Guidance for New Zealand Government and Critical Infrastructure CSIRTs

3.1 Introduction

The NCSC Security Incident Management Guide is designed to provide assistance to NZ Government and critical Infrastructure organisations in defining, prioritising and synchronising the security actions and measures necessary to protect their organisation's integrity, confidentiality and availability of critical information assets.

3.2 Vision

To empower NZ Government agency and critical Infrastructure by enabling them to establish sufficient and appropriate internal CSIRTs to meet the growing need to protect their critical assets from cyber security threats.

3.3 Mission

The New Zealand government is establishing a New Zealand -wide Computer Security Incident Response Team capability. Its mission is to enable all NZ government agencies and critical infrastructures to better plan for and respond to information security incidents as they occur, and to do so in a consistent and business-like manner that reduces the negative impact of security incidents enables the team to learn from mistakes, both personal and systemic.

3.4 Purpose

The purpose of the Security Incident Management Guide is to provide best practices and basic framework for NZ Government and critical infrastructure organisations when establishing or reinforcing existing incident management and response capability. This document will assist NZ Government and critical Infrastructure organisations in establishing effective internal CSIRTs to improve their services and operations through education, mentoring and collaboration.

3.5 Benefits

- Effective protection of NZ Government and critical Infrastructure critical assets.
- Centralised and effective cyber incident coordination and response on a national level.
- Effective identification of critical information.
- Development of resilient NZ Government and critical Infrastructure.
- Establishment of a NZ standardised cyber security incident response method and format.
- Establishment of trusted communication channels and collaboration across NZ Government agencies and critical Infrastructure.

3.6 Constituency

This guide describes how New Zealand government agencies and critical infrastructures should implement their various localised portions of the overall government incident response program.

The New Zealand government CSIRT is being implemented as an internal CSIRT, meaning its focus is principally on detecting and responding to incidents within the New Zealand government. As such, its purpose is not to provide incident response services to New Zealand private citizens, businesses, or any such entities outside of New Zealand.

3.7 Supporting Functions for Services and Processes

Individual government agency level and critical infrastructure organisations will provide essential CSIRT services internally. Certain incidents are then reported to NCSC which coordinates where nationally significant.

Each government agency and critical infrastructure local CSIRT will provide a service level commensurate with its size and available resources.

To the extent feasible and appropriate, ministries and critical infrastructures may benefit from economies of scale by sharing some of their CSIRT services and supporting functions, such as monitoring and notification. The following list defines the typical functions of a government agency or critical infrastructure CSIRT organisation. Note that these functions support the incident management process model previously discussed in Section 2 and also support many of the services from the CSIRT Services List.

This guide and any related training is provided on a self-help basis. In the sections below compliance level is given to help understand which functions are critical for an agency or organization to be effective. How and if an agency chooses to implement and structure a service will be up to that agency.

Supporting functions include but are not limited to:

- **Monitoring (supports Detect, Protect, and Network Monitoring such as IDS)**

  Compliance: must

  Each government agency or critical infrastructure organisation will ensure the operational security of its data systems is adequately monitored for security anomalies. The systems monitored should include essential infrastructure elements (e.g., internet gateways and firewalls, domain name servers), production data services (e.g., web/network servers providing mission-critical services), and application/database servers (e.g., servers providing mission-critical business processing services). Desktop systems and other non-mission-critical systems should be monitored en masse via centralised monitoring services.

- **Notification (supports Alerts and Warning)**

  Compliance: must

  Each government agency or critical infrastructure will provide a means for security event notification via appropriate channels (e.g., help desk, security hotline, email address, web portal reporting form, fax, intrusion detection alerts) so that employees and automated security entities can alert security operations staff of potential security incidents.

- **Identification (supports Detect and Triage and Analysis)**

  Compliance: must

  Each government agency or critical infrastructure must ensure its CSIRT is capable of identifying the basic nature of reported security events.

- **Prioritization (supports Triage)**

  Compliance: must

  Each government agency or critical infrastructure CSIRT must ensure it is able to prioritise security events and incidents with a view to determining if the incident may be of national significance and therefore reported to the NCSC.

- **Triage (supports Triage and Analysis)**

  Compliance: should

  Each government agency or critical infrastructure CSIRT should be able to perform triage on security incident reports as they arrive. The triage process should prioritise each incident and its handling to ensure appropriate attention is paid to each reported incident. Triage should also assign each incident and inquiry to the appropriate CSIRT staff.

- **Analysis (supports Triage and Analysis and Response)**

  Compliance: must

  Each government agency or critical infrastructure CSIRT must be able to perform the initial analysis of all reported incidents. The initial analysis should assess all feasibly available information related to the incident and determine a preliminary recommended course of action. For significant incidents, the NCSC will assume operational responsibility for handling the incident, but initial analysis will typically reside with the government agency or critical infrastructure CSIRT organisations.

  The developed course of action should include all relevant plans to collect data, perform deeper technical analysis of information, and contain the impact of the incident, and so on.

- **Containment (supports Response)**

  Compliance: must

  Each government agency or critical infrastructure CSIRT must be able to isolate and contain security incidents. Different types of incidents will require different measures to isolate and contain their impact, but the CSIRT should have the ability to carry out the containment process.

- **Eradication (supports Response)**

  Compliance: must

  Each government agency or critical infrastructure CSIRT must be able to eradicate from its systems any malicious software or other residue of security incidents.

- **Recovery(supports Response)**

  Compliance: must

  Each government agency or critical infrastructure CSIRT must be able to recover and restore data processing systems back to a production-ready status following a security incident.

- **Feedback, learn, and improve (supports Prepare/Improve/Sustain)**

  Compliance: should

  Upon successful closure of a security incident, each government agency or critical infrastructure CSIRT should be able to conduct an after-action critical analysis of the steps taken. The purpose of this analysis is to study and learn from any mistakes that were made, or to further optimize and continuously improve the CSIRT's operational processes and procedures.

3.8 Organisational Issues

It is expected that New Zealand government agencies and critical infrastructure CSIRT organisations will be internal CSIRTS. This means that their focus is principally inward, to ensure the proper functioning of their own IT systems (in contrast to an external team that might provide security and incident response services to those outside of their own government agency or critical infrastructure).

The purpose of each CSIRT is to be the single focal point for managing incident response operations. The CSIRT will perform all incident response activities as appropriate and as described in its own incident response plan (per section 4.6 of the New Zealand Information Security Manual, version 1.01, June 2011).

Internal CSIRTs perform numerous functions in support of incident management. Their principal function is to be their parent organisation's primary focal point for handling security incidents.

Note that depending on the resources and expertise available within the government agency or critical infrastructure, the organization may not be able to provide these functions on its own. It might need to contract out the service, share the service with another organization, or look to a coordinating centre for assistance.

3.8.1 Organisational Structure Alternatives

CSIRT organisations can be implemented in different shapes and sizes to suit a government agency's or critical infrastructure's needs and available resources. These can range from little more than a plan of action with each participant being assigned various roles and responsibilities in addition to his or her normal job duties, all the way to a formal CSIRT organisation with full-time staffing.

How to implement a CSIRT is at the discretion of each government agency or critical infrastructure. Factors going into the decision should include the size and relative resources available to a government agency or critical infrastructure, as well as the strategic nature of the mission performed by the organisation.

Informal Capability: Incident Response Plan Only, with Defined Roles and Responsibilities

In this type of CSIRT, no full-time CSIRT staffing is provided to the organisation. Instead, a CSIRT plan is developed (and periodically tested through exercises and or real events). The plan should outline the various roles and responsibilities necessary to perform the CSIRT's functions prior to, during, and after incidents.

Rather than staffing each role or responsibility in the CSIRT plan, extant staff members are assigned to each, ensuring that the organisation has explicit personnel assigned in the event of a security incident.

In this sort of CSIRT structure, it is vital that the organisation test its plan from time to time, preferably twice per year. Testing should include a thorough invocation of the CSIRT processes, including off-hours notifications and interdepartmental coordination of actions.

Defined Function in SOC or Similar Body

Another option for a CSIRT organisation is to include minimum full-time staffing and use the extant resources of other related departments. Such CSIRTs will often use existing data centre operations, network operations centres, or security operations centres for CSIRT notifications and off-hours alerting. This ensures around-the-clock availability of CSIRT functionality without needing to fully staff a dedicated CSIRT operations facility.

Formal Structure: CSIRT

Larger ministries and critical infrastructures are likely to need full-time dedicated CSIRT staffing to adequately execute their responsibilities. But even for a full-time staffed CSIRT, several options exist.

1. A small CSIRT can include just one or some small number of full-time staff. These may be augmented by other staff as needed, but the full-time staff are considered the core team and are responsible for executing and overseeing all principal CSIRT functions.
2. A medium-sized CSIRT will likely include essential management as well as technical staff. It will largely be self-sufficient, but it may call upon other resources (e.g., help desk) for off-hour notifications to provide around-the-clock availability without full staffing.
3. The largest organisations will likely need a full complement of CSIRT staff for its around-the-clock needs.

3.8.1.1 Choosing the Right Structure

Deciding which sort of CSIRT to implement is never as simple as a straightforward budgeting exercise. Anticipating how many incidents a government agency or critical infrastructure will encounter is always problematic. As a general rule, it is advisable to start small and build as needed.

One approach to choosing the right structure is to determine the number of security incidents the organisation has been involved in and use that to extrapolate how many they are likely to see over the next two or three years. The estimate can be used to determine how much labour would be required for each incident and perhaps even for each functional responsibility area. That estimate can then be balanced against available budgetary resources to find a feasible level of staffing and the right structure for an organisation's CSIRT capability.

3.8.2 Reporting Structure

The New Zealand Information Security Manual states that "agencies must direct personnel to report cyber security incidents to an ITSM as soon as possible after the cyber security incident is discovered in accordance with agency procedures" [New Zealand Government 2011b]. It further says that significant cyber security incidents must be reported to NCSC and recommends that non-significant cyber security incidents be reported via an ITSM and that the reporting should be in the Incident Object Description Exchange Format (IODEF) data standard[7]. These reporting requirements principally regard reporting incidents externally to a government agency or critical infrastructure. However, at present the NCSC website contains an incident reporting form that should be used in the first instance.

Internal matters are not the same. For internal reporting, personnel should report incidents to their CSIRT via their own local ITSM or similar process or procedure.

Organisational alignment and reporting of the CSIRT itself is yet another matter. As is often the case, a reporting structure that ensures a degree of check and balance is an industry best practice. Though the CSIRT function is inherently related to IT, it may not be best to have the CSIRT report through the same reporting structure as an agency's IT department. Consider

[7] IODEF The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by (CSIRTs) about computer security incidents. Source: http://www.ietf.org/rfc/rfc5070.txt

instead having the CSIRT report to the appropriate operational executive staff, such as a COO organisation that is responsible for mission operations or a CISO within a general security organisation. This ensures that the business needs of the government agency or critical infrastructure are treated with due care.

3.8.3 Authority

In most cases, CSIRTs are not given operational authority over the systems in their constituency. As with reporting structures, this is normally done as a check and balance in the process. Most CSIRTs operate as advocates for the agency's business function, but in an advisory capacity by reporting to the business executive management.

However, significant incidents may require that a CSIRT be given temporary operational authority over certain systems to ensure the most expeditious handling of the incident.

3.8.4 Operations

Depending on the nature of each CSIRT, and in particular whether or not it provides hands-on incident handling support to its parent government agency or critical infrastructure, it will have the ability to carry out incident handling operations.

In other words, it will have both a plan and capability of providing operational support to its constituency. This can range from a basic ability to offer technical guidance through to hands-on "fingers on keyboard" support to incident affected constituents. The support will include typically assistance throughout an incident's life cycle, from identification through analysis, containment, eradication, and recovery.

Each government agency or critical infrastructure will need to evaluate its needs and its resources to determine what an appropriate level of operational incident support would be.

3.8.5 Communications Plan

Of vital concern during a security incident is an organisation's ability to effectively communicate between all key stakeholders. Every CSIRT will have a plan and ability to communicate during security incidents. The plan should provide for secure and reliable communications among all of the active participants, ranging from executive decision makers through CSIRT and other technology staff.

A key point in any emergency communications is to ensure communications availability and confidentiality, even during crises. The plan should include who to contact, their contact information, when to contact them (i.e., timeframe), and what to tell them. The plan may also include any action to be taken once contacted, if applicable.

3.8.6 Staffing

3.8.6.1 Defined Roles and Responsibilities

Each government agency or critical infrastructure CSIRT organisation, no matter how big or small, should clearly define all of its members' (including extended members') roles and

responsibilities. Further, these roles should be clearly communicated to all the relevant members.

3.8.6.2 Competencies: Skills and Abilities

Each CSIRT should assess its needs for technical as well as non-technical skills and abilities amongst its staff members, again including extended staff. These requirements should be driven first and foremost by the technologies that the parent government agency or critical infrastructure has deployed into production environments.

For CSIRT operations, deep and low-level technical understanding of supported systems is often required. Knowledge of data networks, file structures, and computer architectures are often necessary in order to conduct investigative or forensics tasks. These use cases should be thoroughly considered in defining a CSIRT's skills.

Similarly, it is often necessary for a CSIRT to be able to call upon non-technical professional skills, such as lawyers, human resources, and public affairs.

3.8.6.2.1 Training and Professional Development Issues

Each government agency or critical infrastructure should ensure its CSIRT staff are adequately trained on incident response generally and specifically on their own CSIRT processes, procedures, and policies.

Additionally, training on the technical and non-technical skills described above is likely to be necessary. Technical training is something that must keep up with technology trends as well. As new technologies are being deployed, so too must the CSIRT staff be trained to be able to handle incidents effectively.

3.8.6.2.2 Supporting Policies and Procedures

In addition to the customary complement of policies and procedures each government agency and critical infrastructure must maintain, there should be a series of incident response related ones. These should include policies on handling incident information (including evidence) and decision authority during crises (including operational authority).

Standard operating procedures (SOPs) should then be written to cover most operational aspects of each CSIRT. Notably, SOPs should be developed for emergency communications, handling media interactions, incident reporting, sensitive data storage, and record keeping/incident tracking.

3.8.6.2.3 Surge Support

From time to time, every CSIRT experiences incident loads that overwhelm its ability to effectively respond. These surge conditions should be carefully planned for so that the parent organisation's business needs can still be properly handled. Of special concern are the following topics.

- Staff augmentation – the organisation should have defined staff with needed expertise, identified and trained to help the CSIRT perform its functions in times of stress or when normal operational staffing will not suffice.

- Triage procedures and incident prioritization – the organisation should have criteria and triggers established for times of stress, that will keep key operational tasks running but focus on high priority incidents related to any on-going crisis.

3.8.6.2.4 Methods for Obtaining/Sharing Staff

To handle incident surges, most CSIRTs make use of existing organisational IT staff. As described above, planning for these situations is vital, and perhaps the most vital aspect is how to bring on board additional, temporary CSIRT staff.

Each CSIRT will need to find the right solution within its parent government agency or critical infrastructure for this eventuality. Organisations that have done this successfully have generally put in place intra-management agreements such as memoranda of understanding (MOUs) that describe clearly how and when staff augmentation procedures will be used.

Having these understandings in place and understood by all key stakeholders is vital to the process. When surge conditions exist, there can be no question or hesitation among the key management stakeholders. A best practice is to have management agree in writing to how and when the surge support or staff sharing occurs.

3.8.6.3 Equipment and Infrastructure

No matter how large or small a CSIRT is, some basic and dedicated equipment is essential. Because CSIRTs often handle sensitive data during incidents, it is advisable that their systems be isolated from those in the parent organisation. Other requirements and considerations include the following list

- Incident tracking

  All CSIRTs must keep records of their incident operations for reporting and record keeping purposes. These systems needn't be enormous databases, but dedicated hardware and software are generally advisable. Because an organisation's incident records are among its most sensitive data, the incident tracking system should be in a facility and network that is isolated from the parent organisation. At a minimum, a firewall-isolated network segment with a dedicated incident tracking system is prudent.

- Incident handler communications

  A vital aspect of incident handling is day-to-day communications with affected parties. As such, a CSIRT's staff should have adequate desktop computers equipped with all the software necessary. This should include the ability to email and otherwise communicate within the parent government agency or critical infrastructure. It is also highly likely the CSIRT staff will need to exchange email with external parties.

- Analysis and testing

  While handling incidents, collected data will frequently need to be analysed and studied in carefully controlled environments. This may include analysis of malware samples collected during an incident. As such, it is generally necessary to set up a lab environment that is isolated from external networks.

- Data and evidence collection

  Invariably, CSIRTs are required to collect incident information that may need to be used as evidence later on. Handling evidentiary information is something that requires considerable precautions and careful procedures. These include off-line secure storage of records, isolated analysis systems, and so on. All CSIRTs that are called on to support law enforcement and similar investigations must have these facilities ready to go.

3.8.6.4 Workflow: Information Flow

The CSIRT should determine what information is coming into the organisation for situational awareness and incident detection; along with what information is going out of the organisation and to whom.

Incoming information includes the types of reports received, the type of data feeds from network logging or monitoring appliance, or intelligence from other organisations including intelligence and law enforcement sectors. This might also include information sharing with other CSIRTs and security organisations within and outside the government agencies or critical infrastructure sector.

Outgoing information can include alerts, advisories, security guidance and documentation, awareness information, or formal briefings and reports going to management and business lines.

3.8.6.5 Incident Criteria

It is necessary to thoroughly consider New Zealand's policies and definitions for different types of incidents. As a start, the New Zealand government provides the following definitions

- 'cyber security incident' is defined as "an activity or event, or the threat of an activity or event, caused by humans (maliciously or accidentally) or by natural phenomena, that threatens or impacts:
  - the confidentiality, availability and integrity of data, information, and computer systems and networks; and
  - infrastructure and services that are enabled or supported by data, information and computer systems and networks".
- A 'major incident' is one where New Zealand's national security, economy, public institutions, or international relationships may be substantially harmed, or where law and order and public health and safety may be jeopardised.

When deciding what level to categorise any specific incident, there are numerous criteria to take into consideration. These include:

- The nature of the incident – its type, scale, complexity, intensity, and duration, including whether:
    - the impacted agency or agencies are finding it difficult to effectively respond.
    - the incident is occurring at, or is spreading to, multiple sites and organisations.
    - the situation is worsening, or could get worse rapidly.
    - there are multiple and cascading effects.
    - a hostile organisation, using sophisticated techniques, may be behind the incident.
    - there are indications that Government networks and classified or sensitive information has been compromised.
- The impact, or potential impact, of the incident, including on the following:
    - the Government's ability to control New Zealand territory, protect the physical security of citizens, maintain law and order, and uphold the nation's institutions and values;
    - the public's health, safety, and ability to go about daily affairs;
    - the nation's economic activity and prosperity; and
    - New Zealand's relationships with other countries.
- The degree of uncertainty about the incident, including potential second and third order effects.

3.8.6.6 Incident Reporting Mechanisms: NZ NCSC Reporting Form

All CSIRTs must enable their constituents to report incidents in a consistent and user-friendly manner. Standardized reporting forms can be helpful, and should be available to constituents in a variety of formats and delivery options, including PDF, paper, fax, web site form page, and so on. CSIRTs should also allow for constituents to report incidents via telephone. Larger CSIRT organisations will generally operate a CSIRT hotline service, while smaller CSIRTs will allow incident reporting via agency IT help desks and similar.

For reporting incidents among New Zealand CSIRTs, including to the NCSC, the Internet standard IODEF format is used, so all incident tracking database tools should have the ability to import and export IODEF formatted incident data. At present the NCSC reporting form should be used in the first instance.

3.8.6.7 Incident Reporting Guidance

The New Zealand Information Security Manual sets forth clear guidance on incident reporting, as follows:

- Reporting cyber security incidents
    - System Classification(s): R, C, S, TS; Compliance: must
    - Agencies must direct personnel to report cyber security incidents to an ITSM as soon as possible after the cyber security incident is discovered in accordance with agency procedures.

- Reporting cyber security incidents
    - System Classification(s): R, C, S, TS; Compliance: should
    - Agencies should:
        - encourage personnel to note and report any observed or suspected security weaknesses in, or threats to, systems or services,
        - establish and follow procedures for reporting software malfunctions,
        - put mechanisms in place to enable the types, volumes and costs of cyber security,
        - incidents and malfunctions to be quantified and monitored; and
        - deal with the violation of agency cyber security policies and procedures by personnel through a formal disciplinary process.

- Reporting significant cyber security incidents to NCSC
    - System Classification(s): R, C, S, TS; Compliance: must
    - Agencies, through an ITSM, must report significant cyber security incidents to NCSC.

- Reporting non-significant cyber security incidents to NCSC
    - System Classification(s): R, C, S, TS; Compliance: recommended
    - It is recommended that agencies, through an ITSM, report non-significant cyber security incidents to NCSC.

- How to report cyber security incidents to NCSC
    - System Classification(s): R, C, S, TS; Compliance: should
    - Agencies should formally report cyber security incidents using the New Zealand e-GIF adoption of the IODEF standard.

As such, all CSIRTs are to create policies and procedures for incident reporting, both within the agency among its constituents, as well as externally to NCSC. Note that the NCSC reporting form is the primary vehicle for reporting.

4 Creating a CSIRT or Incident Management Capability

When forming an incident management capability, organisations often discover that incident management activities are already occurring but are not identified as such. This critical piece of information should not be ignored. As part of the planning and design process of building an incident management capability, it is important to identify what types of incident management activities are already occurring and who is responsible for them. This knowledge can help shape and structure the needed services.

For example, if an organisation wants to create a CSIRT, it can define the required interfaces between the CSIRT and any other on-going incident management activities by determining what is already in place. If parts of the organisation are already handling certain functions successfully, then perhaps the CSIRT can instead focus on those activities that are not being done. For example, if configuration management, vulnerability scanning, and security awareness training are already being done by an organisation's IT department, it may be appropriate to have that area continue to provide those services while a new CSIRT concentrates on other services such as incident analysis, technology watch, vulnerability coordination, or incident response support and coordination. A formal mechanism or interface must be established between and agreed to by existing functions and any new CSIRT functions, to provide coordination and information exchange.

This kind of insight and other general steps for creating an incident management capability or a CSIRT can be found in the CERT A*ction List for Developing a Computer Security Incident Response Team (CSIRT)*.[8] This document provides a high-level overview of actions and topics for planning and implementing a CSIRT. It also identifies some common problems teams may encounter in their implementation. Remember that all teams are different. These steps are just a guide; following this list verbatim will not be appropriate for all situations. Each organisation should adapt the applicable pieces of the list to its own strategy.

4.1 Steps for Planning a CSIRT

The following list may be used as a starting point to plan a CSIRT. More detailed information can be found in the list of resources in Appendix B.

1. Identify stakeholders and participants.
    a. Determine who needs to be involved at each level of the CSIRT planning, implementation, and operation.
    b. Determine whom the CSIRT serves or supports.
    c. Identify people with whom the CSIRT will coordinate or share information, both inside and outside the organisation. (Consider talking with them during information-

[8] Developed by the CERT Division, available at: http://www.cert.org/csirts/action_list.html.

gathering. Consider asking them to participate in the development project or help review CSIRT design and implementation plans.)

d. Identify people already performing security or incident response functions and talk to them.

e. Identify which internal and external organisations might interface with or participate in the CSIRT.

Common problems: A full range of stakeholders and participants are not identified and included in the planning and development phase. The organisation fails to identify and understand where computer security incident response activities are performed and how this will change with any new plans for a CSIRT.

2. Obtain management support and sponsorship.

   a. Find an executive manager to sponsor and champion the CSIRT's establishment.

   b. This person can be a good liaison to other executive and business managers in the constituency or parent organisation.

   c. Present a business case to management outlining the benefits the CSIRT will bring to the organisation or constituency.

   d. Obtain management support for the time and resources the team will spend researching and gathering information during the planning process.

   e. If establishing a CSIRT within an organisation, explain the ideas, concepts, and benefits to other business function managers.

   f. If establishing a national team, explain the concepts and benefits to key organisations and potential strategic partners who will be supported by the CSIRT.

   g. Request that management announce the formation of the CSIRT project and ask people to provide information as needed during the planning and implementation phases.

   Common problems: Relevant stakeholders, participants, business managers, and strategic partners are not aware that a CSIRT is being planned.

3. Develop a CSIRT project plan.

   a. Form a project team to help plan and establish the CSIRT.

   b. Appoint a project leader. This person can inform management about the progress made in planning.

   c. Apply project management concepts to the task of setting up a CSIRT.

   Common problems: The project team does not involve a diverse set of stakeholders. A reasonable time frame is not established for the project's completion; time frames are often too short or are unrealistic for a CSIRT to become fully operational. A project leader is not established, and the project languishes without direction or completion.

4. Gather information.

a. Hold conversations with a variety of stakeholders to:
    i. determine the needs and requirements of the constituency and any parent or host organisation.
    ii. collect information about types of incidents already occurring to better understand the expertise and services the CSIRT will need to provide.
    iii. understand any incident management or response that is already occurring.
    iv. understand legal, political, business, or cultural issues that will define the environment in which the CSIRT will operate.
    v. understand data ownership and intellectual property (IP) issues and authority related to any type of publications, products, or information collected or developed by the CSIRT.
b. Define political and compliance issues, including any public, private, academic, government, or military rules, regulations, or policies that must be followed or addressed as the CSIRT is established.
c. Understand the previous history.
    i. Find out if anyone attempted to create a CSIRT in the organisation before. If so, find out what happened and check for any information you can use.
    ii. Based on the previous activity, identify any organisational expectations of the CSIRT that the team will need to correct.
    iii. Determine if the desired domain name is available (i.e., if the CSIRT will have its own domain name). If the name is available, obtain it as soon as possible.

Common problems: The CSIRT does not involve or gather input from all stakeholders. There are disagreements over who owns the data and IP, which can cause delays in providing CSIRT information to the constituency.

5. Identify the CSIRT constituency.
    a. Determine the initial group of individuals or organisations that the CSIRT will serve and support.
    b. Identify what types of services the CSIRT will provide to different segments of the constituency. For example, services provided to the general public may be different than services provided to government organisations or critical infrastructures. Understanding the constituency will also help define what groups to target for CSIRT service marketing.
    c. Identify and establish strategic partners, if applicable. Strategic partners can:
        i. help guide the priorities and direction of the CSIRT and help define and mature the CSIRT's capabilities and services.
        ii. engage in information sharing and research.
        iii. participate in customised interactions with the CSIRT.
        iv. help increase the visibility and influence of the team.

v. help promote the adoption and use of security best practices throughout the enterprise or constituency.

d. Identify how the constituency members obtain services from the CSIRT.

e. Identify constituents that the CSIRT may not initially support, but may support in the long term after the CSIRT has been operational and is ready to expand its services.

Common problems: Not all constituents are addressed or defined, so they have no formal interface with the CSIRT. The CSIRT does not properly create an understanding of the benefits its services can provide for the defined constituency. It is not made clear how the constituency should contact the CSIRT and obtain assistance. The CSIRT tries to support too many diverse constituencies during its start-up.

6. Define the CSIRT mission.

   a. Determine the mission of the CSIRT. This is a general, long-term process. The mission should not change much over time, so it should be written broadly enough to accommodate any change in services or functions while still succinctly defining the purpose and function of the CSIRT. The mission statement should provide value to both the constituency and the parent or host organisation.

   b. Determine the primary goals and objectives of the CSIRT. These will be more practical and may be changed as the CSIRT expands its scope or services.

   c. Obtain agreement on the mission from all relevant stakeholders (e.g., management, constituency, collaborators, and staff); ensure everyone understands the mission.

   Common problems: Staff do not understand the mission, and mission creep occurs (the CSIRT loses focus on its defined purpose and becomes less effective). Outside parties (such as politicians) have a perspective on the mission that does not match the CSIRT's mission; these parties may try to pull the team into activities it is not prepared to handle.

7. Secure funding for CSIRT operations.

   a. Obtain funding for start-up, short-term, and long-term operations.

      This will include:

      i. initial staffing, short-term and long-term professional development, and training.

      ii. equipment, tools, and network infrastructure for detecting, analysing, tracking, and responding to computer security incidents.

      iii. facilities for protecting and securing CSIRT data, systems, and staff.

   b. Decide what funding model will support the CSIRT. This could include fee-for-service, membership subscriptions, government sponsorship, or a parent organisation budget line.

   Common problems: CSIRTs can lose effectiveness by not funding efforts to keep staff up to date with emerging technologies or by not enabling staff to attend conferences and training to improve their skills, knowledge, and abilities. This can make the team less able to handle new threats, attacks, and risks that affect their constituency.

8. Decide on the range and level of services the CSIRT will offer.
    a. Start small and grow. Be realistic about the type and number of services the new CSIRT can provide given existing expertise and resources.
    b. Determine the services the CSIRT will provide and identify which parts of the constituency they will be offered to.
    c. Define the process for delivery of services (e.g., hours of operation, contact methods, methods for information dissemination, and related processes).
    d. Decide how the CSIRT will market its service.

    Common problems: The constituency wants the CSIRT to perform services before it is ready. The CSIRT tries to offer too many services at once and play too many roles. The CSIRT creates services that are not needed or that another organisation is offering. The CSIRT does not market needed services.

9. Determine the CSIRT's reporting structure, authority, and organisational model.
    a. Determine where the CSIRT will fit into the organisational structure. For instance, a national-level CSIRT may function within the government, as a separate national entity, or as part of another organisation. If placed within another organisation, how will the CSIRT be perceived by the constituency and how will those perceptions affect its operation?
    b. Create an organisation chart and keep it current.
    c. Determine if the CSIRT must report up the hierarchy to any other organisation or parent entity.
    d. Prepare to educate the constituency about the work the CSIRT will be able to do. Team members may need to diplomatically refuse some work requests and should prepare appropriate responses.

    Common problems: Non-CSIRT assignments are imposed by outside stakeholders that take staff away from the primary CSIRT functions and inhibit effective performance of normal services.

10. Identify required resources such as staff, equipment, and infrastructure.
    a. Determine how the CSIRT infrastructure will be protected, secured, and monitored, especially the physical premises and data repositories.
    b. Define processes for collecting, recording, tracking, and archiving information.
    c. Create job descriptions that list the required knowledge, skills, and abilities (KSAs) for each CSIRT position.
    d. Create a mentoring and training plan for staff and ensure they are cross-trained on unique expertise or services.
    e. Determine requirements for appropriate background checks, certifications, or security clearances.

Common problems: Staff is not cross-trained, resulting in single points of failure if someone performing a function requiring a unique skill leaves. Staff are not given opportunity and a path for professional or career development, resulting in burnout and high levels of job turnover.

11. Define interactions and interfaces.
    a. Identify interactions and interfaces with key parts of the constituency, stakeholders, and with any internal or external partners, collaborators, or contractors.
    b. Determine what other entities the CSIRT will coordinate with.
    c. Identify how information flows between these entities.
    d. Define and establish interfaces and methods of collaboration and communication with others as appropriate, including law enforcement, vendors, critical infrastructure components, internet service providers (ISPs), other security groups, and other CSIRTs.
    e. Ensure there are good methods for internal communication among the CSIRT staff.
    f. For all these interfaces, understand
        i. who owns the data that is shared.
        ii. who has authority and responsibility for data.
        iii. how the data is shared and with whom it is shared.
        iv. how the data is protected, controlled, and securely stored.
    g. Define methods to disseminate information to the constituency and relevant stakeholders.
    h. Develop and explain standard document types for disseminating information to the constituency.

    Common problems: Data is not shared in a controlled and secure manner, resulting in confidences being broken. CSIRT staff are not informed about CSIRT activities, reducing effectiveness in normal work roles. Defined interfaces are not established, causing a process breakdown when escalation or data sharing and coordination are required.

12. Define roles, responsibilities, and the corresponding authority.
    a. Develop roles and responsibilities for all CSIRT functions.
    b. Define and develop the interfaces between CSIRT functions and other external functions and collaborations.
    c. Identify areas where authority may be ambiguous or overlapping, and define functions and roles between groups.

    Common problems: Staff members do not know where their role ends and someone else's begins. More than one group is given the same responsibility. No one is given a specific responsibility, and the task is never completed.

13. Document the workflow.
    a. Create a diagram (swim-lane chart, flow chart, etc.) to document the CSIRT processes and corresponding interactions, including who performs the work and where in the process the interfaces and handoffs occur.
    b. Build quality assurance measures and components into the CSIRT processes and corresponding workflows.

    Common problems: Staff members are uncertain how to follow certain processes or perform various coordination and collaboration activities.

14. Develop policies and corresponding procedures.
    a. Establish definitions for terminology (e.g., "computer security event and incident") along with other terms unique to the organisation.
    b. Determine corresponding incident categories, priorities, and escalation criteria.
    c. Identify initial policies and procedures that need to be formalised before operation and those that can be created after the CSIRT is operational.
    d. Develop incident reporting guidelines for the constituency and ways to publicise them.
    e. Define and document criteria for providing CSIRT services to ensure that consistent, reliable, and repeatable processes are followed by staff.

    Common problems: Common definitions are not shared between the CSIRT and constituency, resulting in confusion and misunderstanding. The organisation is unable to summarise data on incident trends because there is no clear definition of terms. The lack of formalised policies can delay response time because processes must be defined each time an incident occurs.

15. Create an implementation plan and solicit feedback.
    a. Obtain input about the implementation plan from stakeholders and constituents (or other CSIRT experts), ask for their comments, and ensure the plan matches the mission.
    b. Update and improve the plan based on feedback.
    c. Obtain management and constituent support for the implementation.

    Common problems: The constituency is not informed about the CSIRT implementation and does not provide support, which may result in incidents not being reported to the CSIRT or CSIRT advice and recommendations not being followed. The implementation plan is not sent for review, resulting in a plan that is not supported or implemented.

16. Announce the CSIRT when it becomes operational.
    a. Ask management to make a formal announcement.
    b. Provide marketing materials and incident reporting guidelines explaining how the constituency should interact with the CSIRT.

c. Incorporate training about CSIRT services and interactions into staff orientation programs.

d. Find ways to disseminate information about CSIRT services such as organisational intranets, websites, brochures, seminars, and training classes.

Common problems: The CSIRT is not formally announced, and no one understands how or when to interface with the team. [Caveat: There may be cases where the team should not be announced publicly. If that is the case, then this step should be skipped. However, the organisation will still need to determine who needs to know about the team and how that information will be communicated.]

17. Define methods for evaluating the performance of the CSIRT.

    a. Define baselines for incident reporting and handling within the organisation before the CSIRT is implemented. Use the baselines to compare performance once the CSIRT is operational.

    b. Define measurement criteria and quality assurance parameters so that the CSIRT can be consistently measured.

    c. Define methods for obtaining constituency feedback.

    d. Implement reporting and auditing procedures to ensure that the CSIRT is performing efficiently and meets established service level agreements or performance metrics.

    Common problems: No methods are instituted for evaluating whether the CSIRT is accomplishing its mission. Methods for process improvement are not implemented. Performance metrics do not adequately measure CSIRT performance.

18. Have a backup plan for every element of the CSIRT.

    a. Identify key and critical CSIRT functions, services, and equipment.

    b. Design a disaster recovery and business continuity plan for critical CSIRT services and processes; these plans should tie into similar plans for the parent organisation.

    c. Plan what will happen if someone cannot fulfil their role or cannot provide space or equipment needed by the CSIRT.

    d. Institute mock exercises to test whether CSIRT functions and facilities can be operational during emergency situations.

    Common problems: The CSIRT has no reach-back capability ready if additional staffing is needed during peak or emergency situations. Key CSIRT systems and networks that provide critical functions and services are not backed up, resulting in the CSIRT not being able to function during an emergency situation.

19. Be flexible.

    a. Do not try to do too much at once. However, be ready to adapt and take advantage of good opportunities when they arise if they will not severely tax the CSIRT resources and cause problems delivering existing CSIRT services.

b. Understand that services may evolve over time, and be ready to learn new skill sets and gain new knowledge.

c. Keep learning about changing technologies to ensure response strategies can effectively deal with new threats and risks.

d. Look for ways to collaborate with others in the CSIRT and security fields.

Define your vision in a concept of operations (CONOPS) document. Clearly articulate the defined:

- constituency
- mission
- organisational home
- authority
- set of CSIRT services
- organisational model
- relationships (internal and external, such as IT, legal, law enforcement, human resources, critical infrastructures, academia, government, and other security organisations)
- workflow diagrams, descriptions, roles, and responsibilities
- CSIRT incident reporting categories and guidelines
- CSIRT contact information

4.2 Caveats

Each organisation must decide on the structure and operation that works for itself. There is no solution or recipe for creating a CSIRT. Doing so depends on each organisation's needs and requirements, mission and goals, and available resources and support.

Not all CSIRTs are created equal. Solutions that work for one team may not work for another because of various constraints and environmental situations.

- Recognise that some techniques and operational methodologies will only be learned with time and experience.
- Also recognise that it may take time for you to have an impact in your organisation or constituency. Remember, experience shows that it can take up to a year to gain the constituency's recognition and even more time to gain its trust.
- Once an incident management capability or CSIRT is in place, it may actually begin receiving more incidents because it provides better visibility for detecting and reporting incidents. This should be explained to management, and their expectations should be set accordingly.
- Recognise that the business climate or environment will impact the organisational framework, not only for how effective your CSIRT will be, but also what services you may be able to provide and the level of support for each service.
- The CERT Division's experiences have shown that most new teams:
  - need time to establish relationships with constituents, stakeholders, and collaborators
  - end up focusing on more reactive versus proactive services

- have less well defined interfaces and procedures

while more mature teams generally:

- have documented processes, policies, and procedures
- have well-defined interfaces and communication channels
- have instituted and enforced a training and mentoring plan
- have a quality assurance program in place
- have an evaluation mechanism in place to measure their success
- participate in more collaboration and data-sharing activities
- balance between reactive and proactive services
- provide input into quality management services
- understand their stakeholder's needs and collaborate with them
- focus on a more enterprise view involving a variety of stakeholders

4.3 Help Available from NCSC

The web page for NCSC provides access to resources and news concerning cyber security issues, including upcoming training, available cyber security documents, and incident reporting forms.

See: http://www.ncsc.govt.nz/

Government organisations that encounter or suspect a cyber security threat or incident should contact the National Cyber Security Centre (NCSC):

- speak directly with the NCSC on phone +64 (0)4 498 7654
- download an incident form from http://www.ncsc.govt.nz/incidents.html and complete and return it to info@ncsc.govt.nz or fax +64 (0)4 498 7655.

References

[Alberts 2004]
Alberts, Chris; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Defining Incident Management Processes for CSIRTs: A Work in Progress* (CMU/SEI-2004-TR-015). Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/library/abstracts/reports/04tr015.cfm

[Brownlee 1998]
Brownlee, N. & Guttman, E. *Expectations for Computer Security Incident Response* (RFP 2350). Internet Engineering Task Force, 1998. http://www.ietf.org/rfc/rfc2350.txt

[Caralli 2010]
Caralli, Richard A.; Allen, Julia H.; Curtis, Pamela D.; White, David W.; & Young, Lisa R. CERT® Resilience Management Model, v1.0 (CMU/SEI-2010-TR-012). Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr012.cfm

[Killcrece 2002]
Killcrece, Georgia; Kossakowski, Klaus Peter; Ruefle, Robin; & Zajicek, Mark. *CSIRT Services*. (2002). http://www.cert.org/csirts/services.html

[New Zealand Government 2011a]
New Zealand Government. *New Zealand's Cyber Security Strategy.* New Zealand Government, 2011. http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf

[New Zealand Government 2011b]
New Zealand Government. *New Zealand Information Security Manual.* New Zealand Government, 2011. http://www.gcsb.govt.nz/newsroom/nzism/NZISM_2011_Version_1.01.pdf

[NIST 2012]
National Institute of Technology and Standards (2012), *Computer Security Incident Handling Guide* (Publication No. 800-61 Revision 2) http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Appendix A: Acronym List and Glossary

Acronym List

AV	antivirus
C	Classification: Confidential
CRAMM	CCTA Risk Analysis and Management Method
CIO	chief information officer
CISO	chief information security officer
COO	chief operating officer
CRO	chief risk officer
CSO	chief security officer
CASPR	Commonly Accepted Security Practices and Regulations
CSIRT	Computer Security Incident Response Team
CONOPS	concept of operations
COBIT	Control Objectives for Information and Related Technology
DNS	domain name system
e-GIF	e-Government Interoperability Framework
ENISA	European Network and Information Security Agency
FIRM	Fundamental Information Risk Management
GCSB	Government Communications Security Bureau
IODEF	Incident Object Description Exchange Format
ISO	information security officer
ITSM	information technology service management
IT	Information Technology
IP	intellectual property
ITU	International Telecommunication Union

IP	Internet Protocol
ISP	internet service provider
IDS	intrusion detection system
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
KSAs	knowledge, skills, and abilities
MSSP	managed security service provider
MOU	memorandum of understanding
MELISA	Méthode d'Evaluation de la Vulnérabilité Résiduelle des Systèmes d'Information
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NOC	network operations centre
NZISM	*New Zealand Information Security Manual*
NZ	New Zealand
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PDA	personal digital assistant
R	Classification: Restricted
RFC	Request for Comments
S	Classification: Secret
SOC	security operation centre
SEI	Software Engineering Institute
SOP	standard operating procedure
TS	Classification: Top Secret
US-CERT	United States Computer Emergency Readiness Team
VPN	virtual private network

Glossary

This glossary lists terms that are used throughout this guide and contains a short list of definitions of the most important terms relevant to the objectives of the document.

Activity

An occurrence in a system that may be relevant to the security of the system. The term includes security events (and security incidents) and those that are not. Until an occurrence can be identified or confirmed as a security event, it may be referred to more generally as just an activity.

Advisory

A document that provides "mid-term and long-term information about problems and solutions suitable to raise awareness and help avoid incidents. They typically contain information about new vulnerabilities, but may also contain information about intruder activity."

Alert

Short-term notices about critical developments containing time-sensitive information about recent attacks, successful break-ins, or new vulnerabilities. There may already be complete information regarding the subject of an alert, but something may have changed to require the publication of new information.

Artefact

The remnants of an intruder attack or incident activity. These could be software used by intruder(s), a collection of tools, malicious code, logs, files, output from tools, status of a system after an attack or intrusion. Examples of artefacts range from Trojan-horse programs and computer viruses or worms to programs that exploit (or check for the existence of) vulnerabilities or objects of unknown type and purpose found on a compromised host.

Computer Security Incident

Any real or suspected adverse event in relation to the security of computer systems or computer networks. In the computer security arena, these events are often simply referred to as incidents.

CSIRT

An acronym for "computer security incident response team." This is a team providing services to a defined constituency. There are several acronyms used to describe teams providing similar types of services (e.g., CSIRC, CSRC, CIRC, CIRT, IHT, IRC, IRT, SERT, SIRT). We have chosen to use the generic term "CSIRT," as it has been widely adopted in the computer security community.

Depending on factors such as expertise and resources, the level and range of service provided might be different for various teams.

Constituency

A specific group of people and/or organisations that have access to specific services offered by a CSIRT.

Establish

To bring about or set into place something; to create and implement something.

Event

see “security event”

Event report

A detailed account of an occurrence in a system, typically a computer security event.

Executive manager

A person in a high management position, often one who administers other managers.

External

Outside or beyond the boundaries of a specified thing (For example, “external to the organisation” would mean that a person is not a member of that organisation but outside of it.)

General indicator

An identifying characteristic of something, at the broadest level.

Improvements

Desirable changes or advances in the quality of something.

Incident

In this text, the term implies a “security incident” or “computer security incident.”

Incident handling

The processes used for handing an incident; in this text, the term includes the processes for detecting, reporting, triaging, analysing, and responding to computer security incidents.

Incident management

The processes for controlling or administering tasks associated with computer security incidents; in this text, the term implies management of a computer security incident, and includes all of the

Detect, Triage, and Respond processes as well as the Prepare (improve, sustain) processes and the Protect processes outlined in this report. Incident management is the performance of reactive and proactive services to help prevent and handle computer security incidents. It can include security awareness and training functions, incident handling, vulnerability handling, assessment activities, IDS, and other services.

Incident response

An answer given or action taken by people designated to react to an incident. It is the process that encompasses the planning, coordination, and execution of any appropriate mitigation and recovery strategies and actions.

Infrastructure

A set of underlying equipment (of a computer network).

Legal response

An answer given or action taken by people designated to react to any incident aspects related to or governed by the law.

Lessons learned

Knowledge that is gained or identified after a completed activity.

Management response

An answer given or action taken by a manager or higher ranking authority within an organisation; note that this response differs from “technical response”.

Mission

An assignment or duty, the purpose of an organisation. For a given organisation, this term is often identified or defined in a mission statement.

Organisation a body of people that is organised and recognisable by some identifiable characteristic(s). Examples: a small business, a company, a government agency, a university department.

Prioritisation

The ranking or sorting in order of importance or urgency.

Policy

A set of written statements directing the operation of an organisation or community in regard to specific topics such as security or dealing with the media.

Procedure

The implementation of a policy in the form of workflows, orders, or mechanisms.

Process

A series of actions or steps intended to bring about a desired result.

Quality assurance

A confirmation that the characteristics of an object, process, or procedure meet the specified (or expected) degree of excellence.

Rationale

A reason or justification for something

Reporting requirement

A mandatory instruction or guideline for submitting an account of some specified activity (security event or incident)

Resource

An available asset that can be used for help (to accomplish or produce an outcome)

Risk assessment

A process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and (optionally) recommends how to allocate resources to countermeasures so as to minimise total exposure.

Security event

An occurrence in a system that is relevant to the security of the system. (See: security incident.) [Comment] The term includes both events that are security incidents and those that are not.

Security incident

A security event that involves a security violation. [Comment] In other words, a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. See “computer security incident.”

Security Policy

A policy addressing security issues.

Site

Depending on the context in which this term is used, it might apply to computer system(s) that are grouped together by geographical location, organisational jurisdiction, or network addresses.

Sponsor

An individual or group who champions, assists, and supports an endeavour or initiative such as a CSIRT or incident management capability and its establishment and services.

Stakeholder

An individual or group, that is interested in (or may be affected by) the activities and services of a CSIRT or incident management capability or other type of organisation.

Technical response

An answer given, or action taken, by someone who is familiar with the technology-related aspects of a reported incident or vulnerability. This response typically could include a summary of their analysis of the incident, as well as recommendations or suggested steps for recovering from malicious activity or attacks or for hardening or securing the affected system(s). It can also include the execution of these actions. Note that this response differs from “management response.” Technical response is most often performed by CSIRT or IT or Security staff.

Triage

The process of receiving, initial sorting, and prioritising of information to facilitate its appropriate handling.

Vulnerability

The existence of a software weakness, such as a design or implementation error, that can lead to an unexpected, undesirable event compromising the security of a system, network, application, or protocol.

Vulnerability assessment

Activity or procedure intended to evaluate or identify the existence of known vulnerabilities (in a computer system or network). In a broader sense the assessment could also look for procedural or organisational weaknesses.

Appendix B: Resources and References

New Zealand Guidance

- *New Zealand's Cyber Security Strategy*, June 2011
  http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf
- *New Zealand Information Security Manual (NZISM) v 1.01*, June 2011
  http://www.gcsb.govt.nz/newsroom/nzism/NZISM_2011_Version_1.01.pdf
- *New Zealand National Cyber Security Centre*
  http://www.ncsc.govt.nz/
- *Security in the Government Sector*
  http://www.security.govt.nz/publications/security-in-the-government-sector/

The following websites offer additional information about organisations involved in the security of government systems:

- http://www.gcsb.govt.nz
- http://www.nzsis.govt.nz
- http://www.police.govt.nz
- http://www.mfat.govt.nz
- http://www.dia.govt.nz
- http://www.e.govt.nz
- http://www.standards.govt.nz
- http://www.privacy.org.nz
- http://www.dpmc.govt.nz
- http://www.auditnz.govt.nz
- http://www.oag.govt.nz
- http:// justice.govt.nz

http://dnc.org.nz/

General CSIRT Resources

CERT CSIRT Publications

- *Handbook for CSIRTs, Second Edition*
  http://www.sei.cmu.edu/library/abstracts/reports/03hb002.cfm
- *Defining Incident Management Processes for CSIRTs: A Work in Progress*
  http://www.sei.cmu.edu/library/abstracts/reports/04tr015.cfm
- *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*
  http://www.sei.cmu.edu/library/abstracts/reports/03tr001.cfm

- *Incident Management Capability Metrics, Version 0.1*
  http://www.sei.cmu.edu/library/abstracts/reports/07tr008.cfm
- *Incident Management Mission Diagnostic Method, Version 1.0*
  http://www.sei.cmu.edu/library/abstracts/reports/08tr007.cfm
- Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0
  http://www.sei.cmu.edu/library/abstracts/reports/11tr015.cfm
- *CERT CSIRT Services List*
  http://www.cert.org/csirts/services.html
- *Resources for National CSIRTs*
  http://www.cert.org/csirts/national/
- *Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?*
  http://www.cert.org/csirts/csirt-staffing.html
- *Organisational Models for Computer Security Incident Response Teams (CSIRTs)*
  http://www.sei.cmu.edu/library/abstracts/reports/03hb001.cfm

Other Resources

- *Expectations for Computer Security Incident Response (RFP 2350)*
  http://www.ietf.org/rfc/rfc2350.txt
- *Terena TF-CSIRT Guide to Setting up a CSIRT*
  http://www.terena.org/activities/tf-csirt/archive/acert7.html
- *ENISA Step-by-Step Guide to Setting Up a CSIRT*
  http://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide/
- *ENISA Good Practices for Running a CSIRT*
  http://www.enisa.europa.eu/activities/cert/support/guide2
- *Proactive Detection of Network Security Incidents, Report*
  http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report
- *Computer Security Incident Handling Guide (NIST SP 800-61)* rev 2.
  http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
- International Telecommunication Union
  - General Information
    http://www.itu.int/cybersecurity
  - *ITU National Cybersecurity/CIIP1 Self-Assessment Tool*
    http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf
- Team Cymru
  - *Resources for National CSIRTs*
    http://www.cert.org/csirts/national/
  - *CSIRT Assistance Program*
    http://www.team-cymru.org/Services/CAP/

- ShadowServer
  - *Get Reports on Your Network*
    http://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork
- Honeynet Project
  http://www.honeynet.org/

Appendix C: List of Services

Introduction

One of the primary issues to be addressed in creating a computer security incident response team (CSIRT) is deciding what services the CSIRT will provide to its constituency. This process also involves naming and defining each provided service, which is not always an easy task. Experience has shown that there is often great confusion about the names used for CSIRT services. The purpose of this document is to present a list of CSIRT services and their definitions.[9] This list provides a common framework for a consistent and comparable description of CSIRTs and their corresponding services.

Although this document focuses on services provided by CSIRTs, many of these same services can also be provided by system, network, and security administrators who perform ad hoc incident handling as part of their normal administrative work when there is no established CSIRT. We refer to this type of ad hoc team as a "security team." The enclosed service definitions can also be used by any of these organisational teams or others in the computer security field.

A CSIRT must take great care in choosing the services it will offer. The set of services provided will determine the resources, skill sets, and partnerships the team will need to function properly. The selection of services should first and foremost support and enable the business goals of the CSIRT's constituency or parent organisation. The services provided should be those that the team can realistically and honestly provide based on the team size and range of expertise. It is better to offer a few services well than a large range of services poorly. As a CSIRT gains the trust and respect of its constituency, it can look to expand its services as staff and funding permit.[10]

Service Categories

There are many services that a CSIRT can choose to offer. Each CSIRT is different and provides services based on the mission, purpose, and constituency of the team. Providing an incident handling service is the only prerequisite to be considered a CSIRT.

CSIRT services can be grouped into three categories:

- Reactive services. These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something

[9] The list was originally based on the example CSIRT services on page 20 of the *Handbook for Computer Security Incident Response Teams (CSIRTs)* [1]. An extended and updated list was developed by Klaus-Peter Kossakowski in the book *Information Technology Incident Response Capabilities* [2]. When Kossakowski became involved with the Trusted Introducer for CSIRTs in Europe [3], the new list was used to help teams describe themselves based on established service names. In an effort to consolidate CSIRT service terminology, the Trusted Introducer service worked with the CSIRT Development Team of the CERT Coordination Center, Pittsburgh, PA, to produce this updated and more comprehensive list of CSIRT services.

[10] More information on selecting services can be found in the Handbook for Computer Security Incident Response Teams (CSIRTs).

that was identified by an intrusion detection or logging system. Reactive services are the core component of CSIRT work.

- Proactive services. These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.
- Security quality management services. These services augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organisation such as the IT, audit, or training departments. If the CSIRT performs or assists with these services, the CSIRT's point of view and expertise can provide insight to help improve the overall security of the organisation and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

The services are listed in the following table and described in detail below.

It should be recognised that a CSIRT should look at performing only those functions that fit its mission and purpose. Not all of these services are expected to be provided by any team. Instead the CSIRT should choose a small set of services to initially provide and then grow as resources, demand, and need increase.

These are only a potential set of services. A CSIRT can choose one or more to implement.

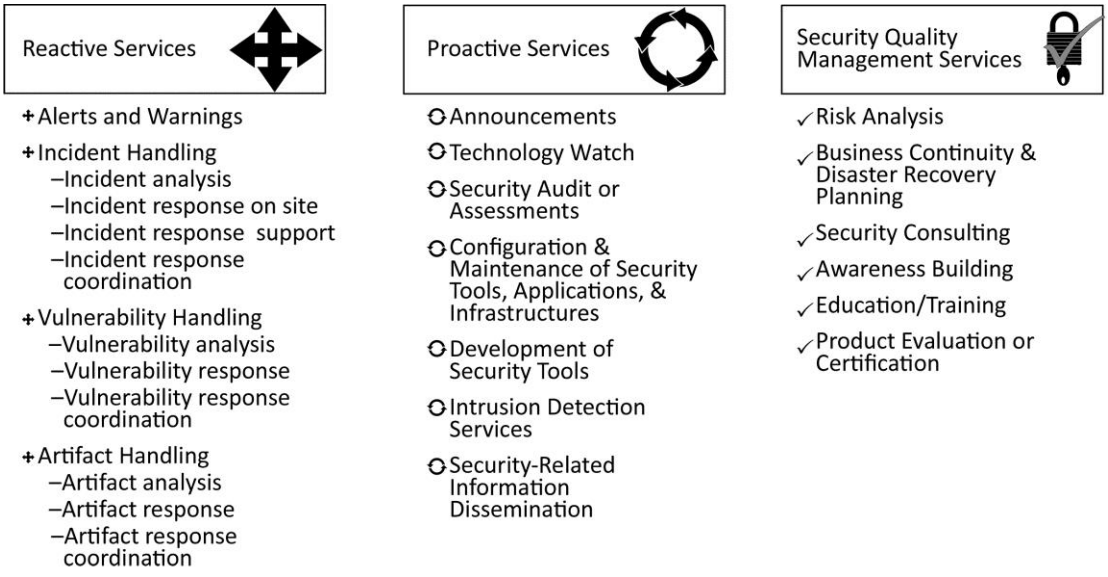

Figure 10: Description of CSIRT Services

It should be noted that some services have both a reactive and proactive side. For example, vulnerability handling can be done in response to the discovery of a software vulnerability that is being actively exploited. But it can also be done proactively by reviewing and testing code to determine where vulnerabilities exist, so the problems can be fixed before they are widely known or exploited.

Service Descriptions

Reactive Services

Reactive services are designed to respond to requests for assistance, reports of incidents from the CSIRT constituency, and any threats or attacks against CSIRT systems. Some services may be initiated by third-party notification or by viewing monitoring or IDS logs and alerts.

Alerts and Warnings

This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the CSIRT or may be redistributed from vendors, other CSIRTs or security experts, or other parts of the constituency.

Incident Handling

Incident handling involves receiving, triaging,[11] and responding to requests and reports, and analysing incidents and events. Particular response activities can include:

- taking action to protect systems and networks affected or threatened by intruder activity.
- providing solutions and mitigation strategies from relevant advisories or alerts.
- looking for intruder activity on other parts of the network.
- filtering network traffic.
- rebuilding systems.
- patching or repairing systems.
- developing other response or workaround strategies.

Since incident handling activities are implemented in various ways by different types of CSIRTs, this service is further categorised based on the type of activities performed and the type of assistance given as follows:

- Incident analysis. There are many levels of incident analysis and many sub-services. Essentially, incident analysis is an examination of all available information and supporting evidence or artefacts related to an incident or event. The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. The CSIRT may use the results of vulnerability and artefact analysis (described below) to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. The CSIRT correlates activity across incidents to determine any interrelations, trends, patterns,

[11] Triaging refers to sorting, categorizing, and prioritizing incoming incident reports or other CSIRT requests. It can be compared to triage in a hospital where patients who need to be seen immediately are separated from those who can wait for assistance.

or intruder signatures. Two sub-services that may be done as part of incident analysis, depending on the mission, goals, and processes of the CSIRT, are:

  - Forensic evidence collection: the collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. This gathering of information and evidence must be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; and checking for Trojan horse programs and toolkits. CSIRT staff performing this function may also have to be prepared to act as expert witnesses in court proceedings.
  - Tracking or tracing: the tracing of the origins of an intruder or identifying systems to which the intruder had access. This activity might involve tracking or tracing how the intruder entered the affected systems and related networks, which systems were used to gain that access, where the attack originated, and what other systems and networks were used as part of the attack. It might also involve trying to determine the identity of the intruder. This work might be done alone but usually involves working with law enforcement personnel, Internet service providers, or other involved organisations.

- Incident response[12] on site. The CSIRT provides direct, on-site assistance to help constituents recover from an incident. The CSIRT itself physically analyses the affected systems and conducts the repair and recovery of the systems, instead of only providing incident response support by telephone or email (see below). This service involves all actions taken on a local level that are necessary if an incident is suspected or occurs. If the CSIRT is not located at the affected site, team members would travel to the site and perform the response. In other cases a local team may already be on site, providing incident response as part of its routine work. This is especially true if incident handling is provided as part of the normal job function of system, network, or security administrators in lieu of an established CSIRT.
- Incident response support. The CSIRT assists and guides the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation. This can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies. It does not involve direct, on-site incident response actions as described above. The CSIRT instead provides guidance remotely so site personnel can perform the recovery themselves.
- Incident response coordination. The CSIRT coordinates the response effort among parties involved in the incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as Internet service providers, other CSIRTs, and system and network administrators at the site. The coordination work may

[12] The term "incident response" is used here to describe one type of CSIRT service. When used in team names such as "Incident Response Team," the term typically means incident handling.

involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. Part of the coordination work may involve notification and collaboration with an organisation's legal counsel, human resources or public relations departments. It would also include coordination with law enforcement. This service does not involve direct, on-site incident response.

Vulnerability Handling

Vulnerability handling involves receiving information and reports about hardware and software vulnerabilities[13]; analysing the nature, mechanics, and effects of the vulnerabilities; and developing response strategies for detecting and repairing the vulnerabilities. Since vulnerability handling activities are implemented in various ways by different types of CSIRTs, this service is further categorised based on the type of activities performed and the type of assistance given as follows:

- Vulnerability analysis. The CSIRT performs technical analysis and examination of vulnerabilities in hardware or software. This includes the verification of suspected vulnerabilities and the technical examination of the hardware or software vulnerability to determine where it is located and how it can be exploited. The analysis may include reviewing source code, using a debugger to determine where the vulnerability occurs, or trying to reproduce the problem on a test system.
- Vulnerability response. This service involves determining the appropriate response to mitigate or repair a vulnerability. This may involve developing or researching patches, fixes, and workarounds. It also involves notifying others of the mitigation strategy, possibly by creating and distributing advisories or alerts.[14] This service can include performing the response by installing patches, fixes, or workarounds.
- Vulnerability response coordination. The CSIRT notifies the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability. The CSIRT verifies that the vulnerability response strategy has been successfully implemented. This service can involve communicating with vendors, other CSIRTs, technical experts, constituent members, and the individuals or groups who initially discovered or reported the vulnerability. Activities include facilitating the analysis of a vulnerability or vulnerability report; coordinating the release schedules of corresponding documents, patches, or workarounds; and synthesizing technical analysis done by different parties. This service can also include maintaining a public or private archive or knowledgebase of vulnerability information and corresponding response strategies.

---

[13] A *vulnerability* is the existence of a flaw or weakness in hardware or software that can be exploited, resulting in a violation of an implicit or explicit security policy.

[14] Other CSIRTs might further redistribute these original advisories or alerts as part of their services.

Artefact Handling[15]

An artefact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artefacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

Artefact handling involves receiving information about and copies of artefacts that are used in intruder attacks, reconnaissance, and other unauthorized or disruptive activities. Once received, the artefact is reviewed. This includes analysing the nature, mechanics, version, and use of the artefacts; and developing (or suggesting) response strategies for detecting, removing, and defending against these artefacts. Since artefact handling activities are implemented in various ways by different types of CSIRTs, this service is further categorised based on the type of activities performed and the type of assistance given as follows:

- Artefact analysis. The CSIRT performs a technical examination and analysis of any artefact found on a system. The analysis done might include identifying the file type and structure of the artefact, comparing a new artefact against existing artefacts or other versions of the same artefact to see similarities and differences, or reverse engineering or disassembling code to determine the purpose and function of the artefact.
- Artefact response. This service involves determining the appropriate actions to detect and remove artefacts from a system, as well as actions to prevent artefacts from being installed. This may involve creating signatures that can be added to antivirus software or IDS.
- Artefact response coordination. This service involves sharing and synthesizing analysis results and response strategies pertaining to an artefact with other researchers, CSIRTs, vendors, and other security experts. Activities include notifying others and synthesizing technical analysis from a variety of sources. Activities can also include maintaining a public or constituent archive of known artefacts and their impact and corresponding response strategies.

Proactive Services

Proactive services are designed to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur.

Announcements

This includes, but is not limited to, intrusion alerts, vulnerability warnings, and security advisories. Such announcements inform constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

---

[15] Artifact analysis is often referred to as malicious code analysis.

Technology Watch

The CSIRT monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. Topics reviewed can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies. This service involves reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks. This can include communicating with other parties that are authorities in these fields to ensure that the best and most accurate information or interpretation is obtained. The outcome of this service might be some type of announcement, guidelines, or recommendations focused at more medium- to long-term security issues.

Security Audits or Assessments

This service provides a detailed review and analysis of an organisation's security infrastructure, based on the requirements defined by the organisation or by other industry standards[16] that apply. It can also involve a review of the organisational security practices. There are many different types of audits or assessments that can be provided, including:

- infrastructure review—manually reviewing the hardware and software configurations, routers, firewalls, servers, and desktop devices to ensure that they match the organisational or industry best practice security policies and standard configurations.
- best practice review—interviewing employees and system and network administrators to determine if their security practices match the defined organisational security policy or some specific industry standards.
- scanning—using vulnerability or virus scanners to determine which systems and networks are vulnerable.
- penetration testing—testing the security of a site by purposefully attacking its systems and networks.

Obtaining upper management approval is required before conducting such audits or assessments. Some of these approaches may be prohibited by organisational policy. Providing this service can include developing a common set of practices against which the tests or assessments are conducted, along with developing a required skill set or certification requirements for staff that perform the testing, assessments, audits, or reviews. This service could also be outsourced to a third part contractor or managed security service provider with the appropriate expertise in conducting audits and assessments.

Configuration and Maintenance of Security Tools, Applications, Infrastructures, and Services

This service identifies or provides appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the CSIRT

[16] Industry standards and methodologies might include Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), CCTA Risk Analysis and Management Method (CRAMM), Information Security Forum's Fundamental Information Risk Management (FIRM), Commonly Accepted Security Practices and Regulations (CASPR), Control Objectives for Information and (Related) Technology (COBIT), Methode d' Evaluation de la Vulnerabilite Residuelle des Systemes d'Informa (MELISA), ISO 13335, ISO 17799, or ISO 15408.

constituency or the CSIRT itself. Besides providing guidance, the CSIRT may perform configuration updates and maintenance of security tools and services, such as IDS, network scanning or monitoring systems, filters, wrappers, firewalls, virtual private networks (VPN), or authentication mechanisms. The CSIRT may even provide these services as part of their main function. The CSIRT may also configure and maintain servers, desktops, laptops, personal digital assistants (PDAs), and other wireless devices according to security guidelines. This service includes escalating to management any issues or problems with configurations or the use of tools and applications that the CSIRT believes might leave a system vulnerable to attack.

Development of Security Tools

This service includes the development of any new, constituent-specific tools that are required or desired by the constituency or by the CSIRT itself. This can include, for example, developing security patches for customised software used by the constituency or secured software distributions that can be used to rebuild compromised hosts. It can also include developing tools or scripts that extend the functionality of existing security tools, such as a new plug-in for a vulnerability or network scanner, scripts that facilitate the use of encryption technology, or automated patch distribution mechanisms.

Intrusion Detection Services

CSIRTs that perform this service review existing IDS logs, analyse and initiate a response for any events that meet their defined threshold, or forward any alerts according to a pre-defined service level agreement or escalation strategy. Intrusion detection and analysis of the associated security logs can be a daunting task—not only in determining where to locate the sensors in the environment, but collecting and then analysing the large amounts of data captured. In many cases, specialised tools or expertise is required to synthesise and interpret the information to identify false alarms, attacks, or network events and to implement strategies to eliminate or minimise such events. Some organisations choose to outsource this activity to others who have more expertise in performing these services, such as managed security service providers.

Security-Related Information Dissemination

This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include:

- reporting guidelines and contact information for the CSIRT
- archives of alerts, warnings, and other announcements
- documentation about current best practices
- general computer security guidance
- policies, procedures, and checklists
- patch development and distribution information
- vendor links
- current statistics and trends in incident reporting
- other information that can improve overall security practices

This information can be developed and published by the CSIRT or by another part of the organisation (IT, human resources, or media relations), and can include information from external resources such as other CSIRTs, vendors, and security experts.

Security Quality Management Services

Services that fall into this category are not unique to incident handling or CSIRTs in particular. They are well-known, established services designed to improve the overall security of an organisation. By leveraging the experiences gained in providing the reactive and proactive services described above, a CSIRT can bring unique perspectives to these quality management services that might not otherwise be available. These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities, and attacks. Feeding such experiences into the established traditional services (described below) as part of a security quality management process can improve the long-term security efforts in an organisation.

Depending on organisational structures and responsibilities, a CSIRT may provide these services or participate as part of a larger organisational team effort.

The following descriptions explain how CSIRT expertise can benefit each of these security quality management services.

Risk Analysis

CSIRTs may be able to add value to risk analysis and assessments. This can improve the organisation's ability to assess real threats, to provide realistic qualitative and quantitative assessments of the risks to information assets, and to evaluate protection and response strategies. CSIRTs performing this service would conduct or assist with information security risk analysis activities for new systems and business processes or evaluate threats and attacks against constituent assets and systems.

Business Continuity and Disaster Recovery Planning

Based on past occurrences and future predictions of emerging incident or security trends, more and more incidents have the potential to result in serious degradation of business operations. Therefore, planning efforts should consider CSIRT experience and recommendations in determining how best to respond to such incidents to ensure the continuity of business operations. CSIRTs performing this service are involved in business continuity and disaster recovery planning for events related to computer security threats and attacks.

Security Consulting

CSIRTs can be used to provide advice and guidance on the best security practices to implement for constituents' business operations. A CSIRT providing this service is involved in preparing recommendations or identifying requirements for purchasing, installing, or securing new systems, network devices, software applications, or enterprise-wide business processes. This service includes providing guidance and assistance in developing organisational or constituency

security policies. It can also involve providing testimony or advice to legislative or other government bodies.

Awareness Building

CSIRTs may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organisational security policies. Increasing the general security awareness of the constituent population not only improves their understanding of security issues but also helps them perform their day-to-day operations in a more secure manner. This can reduce the occurrence of successful attacks and increase the probability that constituents will detect and report attacks, thereby decreasing recovery times and eliminating or minimising losses.

CSIRTs performing this service seek opportunities to increase security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to keep constituents up to date with on-going security procedures and potential threats to organisational systems.

Education/Training

This service involves providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials. Topics might include incident reporting guidelines, appropriate response methods, incident response tools, incident prevention methods, and other information necessary to protect, detect, report, and respond to computer security incidents.

Product Evaluation or Certification

For this service, the CSIRT may conduct product evaluations on tools, applications, or other services to ensure the security of the products and their conformance to acceptable CSIRT or organisational security practices. Tools and applications reviewed can be open source or commercial products. This service can be provided as an evaluation or through a certification program, depending on the standards that are applied by the organisation or by the CSIRT.

Summary

This document outlines and defines various incident handling services and several other services that can be provided by a CSIRT. Some teams may offer many services from this list; others may only be able to provide a few; still other teams may share the responsibility for providing these services with other parts of their parent or host organisation, or they may outsource some services to an incident response or managed security services provider. As mentioned at the beginning of this document, to be considered a CSIRT, a team must provide one or more of the incident handling services: incident analysis, incident response on site, incident response support, or incident response coordination.

Experience has shown that whatever services a CSIRT chooses to offer, the parent organisation or management must ensure that the team has the necessary resources (people, technical expertise, equipment, and infrastructure) to provide a valued service to their constituents, or the CSIRT will not be successful and their constituents will not report incidents to them.[17]

In addition, as changes occur in technology and Internet use, other services may emerge that need to be provided by CSIRTs. This list of services will therefore need to evolve and change over time.

References

[1] West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. Handbook for Computer Security Incident Response Teams (CSIRTs) (CMU/SEI-98-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1998. http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html.

[2] Kossakowski, Klaus-Peter. Information Technology Incident Response Capabilities. Hamburg: Books on Demand, 2001 (ISBN: 3-8311-0059-4).

[3] Kossakowski; Klaus-Peter & Stikvoort, Don. “A Trusted CSIRT Introducer in Europe.” Amersfoort, Netherlands: M&I/Stelvio, February, 2000. http://www.kossakowski.de/first-2001.pdf (see “Appendix E, Basic Set of Information”).

17 If the CSIRT does not provide the services but outsources the activities to another organisation such as a managed security services provider, it must still ensure that the same standards for staffing, equipment, and infrastructure are adhered to, in order to protect the CSIRT and organisational data and services.

Appendix D: Sample CSIRT Staff Roles and Descriptions

The following is a sample of the types of staffing, the range of positions, and the tasks for various positions that might be required for a CSIRT. Not all CSIRTs require all these roles. Each government agency or critical infrastructure organisation should choose those that best fit their needs and CSIRT structure and model. Roles include but are not limited to the following:

- manager or team lead
  - provides strategic direction,
  - enables and facilitates work of team members,
  - supervises team,
  - represents CSIRT to management and others, and
  - interviews and hires new team members.
- assistant managers, supervisors, or group leaders
  - support strategic direction of assigned functional area,
  - support the team lead as needed,
  - provide direction and mentoring to team members,
  - assign tasks and duties, and
  - participate in interviews with new team members.
- hotline, help desk, or triage staff
  - handle main CSIRT telephone(s) for incident or security reports,
  - provide initial assistance, depending on skills, and
  - undertake initial data entry and the sorting and prioritizing of incoming information.
- incident handlers
  - undertake incident analysis, tracking, recording, and response,
  - coordinate the reactive and proactive guidance that will be provided to the constituency (develop material such as documentation, checklists, best practices, and guidelines),
  - disseminate information,
  - interact with the CSIRT team, external experts, and others (such as sites, media, law enforcement, or legal personnel) as appropriate, by assignment from team lead or other management staff,
  - undertake technology-watch activities if assigned,
  - develop appropriate training materials (for CSIRT staff and/or the constituency),
  - mentor new CSIRT staff as assigned,
  - monitor intrusion detection systems, if this service is part of the CSIRT activities,
  - perform penetration testing if this service is part of the CSIRT activities, and
  - participate in interviews with new staff members as directed.
- vulnerability handlers
  - analyse, test, track and record vulnerability reports and vulnerability artefacts,

  - research or develop patches and fixes as part of the vulnerability response effort,
  - interact with the constituency, the CSIRT team, software application developers, external experts (CERT/CC, US-CERT, vendors) and others (media, law enforcement, or legal personnel) as required,
  - disseminate information on vulnerabilities and corresponding fixes, patches, or workarounds,
  - undertake technology-watch activities if assigned,
  - mentor new CSIRT staff as assigned, and
  - participate in interviews with new CSIRT staff.
- technical writers
  - assist and facilitate the CSIRT in the development of publications such as advisories, best practices, or technical tips.
- web developers
  - maintain CSIRT web site, and
  - create new content and corresponding designs for web site in conjunction with
  - CSIRT staff.
- trainers
  - develop and deliver curriculum for teaching new incident handlers within CSIRT,
  - develop and deliver curriculum for constituency members, and
  - provide security awareness training.
- network or system administrators
  - administer CSIRT equipment and peripheral devices, and
  - maintain the infrastructure for CSIRT products; this includes secure servers, the data repository, secure email, and any other internal systems required by the CSIRT.
- support staff
  - assist staff as needed with administrative support services, and
  - coordinate travel and conference arrangements as necessary.
- platform specialists
  - assist in analysis and response efforts by providing specific expertise in supported technologies or operating systems (e.g., UNIX, Windows, mainframes, applications, databases), and
  - may also perform incident handling, vulnerability handling, or infrastructure tasks if needed.

Appendix E: Incident Handling Discussion and Exercise Scenarios

Using scenarios of malicious activity or incidents is a good method for engaging new teams in discussion of what their process should be, or teaching them the basic steps for incident handling, or allowing them to apply what they've learned in a exercise.

The US National Institute of Standards and Technology (NIST) has included a set of scenarios and some general incident handling questions in its Special Publication 800-61rev2 document, *Computer Security Incident Handling Guide.* The general incident handling questions can be found in Appendix A of the NIST document, on pages 52-53. The questions are included below for ease of use.

Scenario Questions[18]

The following questions should be considered for each of the scenarios.

Preparation

1. Would the organization consider this activity to be an incident? If so, which of the organization's policies does this activity violate?
2. What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact?

Detection and Analysis

1. What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to take action before the incident occurred?
2. What indicators of the incident might the organization detect? Which indicators would cause someone to think that an incident might have occurred?
3. What additional tools might be needed to detect this particular incident?
4. How would the incident response team analyze and validate this incident? What personnel would be involved in the analysis and validation process?
5. To which people and groups within the organization would the team report the incident?
6. How would the team prioritize the handling of this incident?

[18] Source: National Institute of Standards and Technology Special Publication 800 61 Revision 2 (August 2002), available at: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Containment, Eradication, and Recovery

1. What strategy should the organization take to contain the incident? Why is this strategy preferable to others?
2. What could happen if the incident were not contained?
3. What additional tools might be needed to respond to this particular incident?
4. Which personnel would be involved in the containment, eradication, and/or recovery processes?
5. What sources of evidence, if any, should the organization acquire? How would the evidence be acquired? Where would it be stored? How long should it be retained?

Post-Incident Activity

1. Who would attend the lessons learned meeting regarding this incident?
2. What could be done to prevent similar incidents from occurring in the future?
3. What could be done to improve detection of similar incidents?

General Questions

1. How many incident response team members would participate in handling this incident?
2. Besides the incident response team, what groups within the organization would be involved in handling this incident?
3. To which external parties would the team report the incident? When would each report occur? How would each report be made? What information would you report or not report, and why?
4. What other communications with external parties may occur?
5. What tools and resources would the team use in handling this incident?
6. What aspects of the handling would have been different if the incident had occurred at a different day and time (on-hours versus off-hours)?
7. What aspects of the handling would have been different if the incident had occurred at a different physical location (onsite versus offsite)?

The scenarios included in Appendix A of the NIST publication are listed below. The actual scenario can be read in the NIST document:

- Scenario 1: Domain Name System (DNS) Server Denial of Service (DoS)
- Scenario 2: Worm and Distributed Denial of Service (DDoS) Agent Infestation
- Scenario 3: Stolen Documents
- Scenario 4: Compromised Database Server
- Scenario 5: Unknown Exfiltration
- Scenario 6: Unauthorized Access to Payroll Records
- Scenario 7: Disappearing Host

- Scenario 8: Telecommuting Compromise
- Scenario 9: Anonymous Threat
- Scenario 10: Peer-to-Peer File Sharing
- Scenario 11: Unknown Wireless Access Point

In addition to the NIST questions and scenarios, the following are some new scenarios and related questions for the New Zealand government and critical infrastructures to consider. These were developed as part of this *Security Incident Management Guide for CSIRTs*.

New Scenarios:

Scenario 12: Malware Infestation in relatively small NZ Government Agency

It's late on a Friday prior to a long holiday weekend, when a relatively small NZ Government agency ITSM receives a report of possible malware on a department-level PC. The incident began after an employee connected to a popular website and clicked his browser on an advertisement URL link. Within moments, the employee's PC began "misbehaving" -- generally running slowly and displaying pop-up messages and such. Even after rebooting the PC, the employee was unable to make the behavior go away, so he contacted the agency's ITSM and requested help.

1. Was the employee's PC targeted, or was it simply one of the many unlucky computers to connect to the advertising link?
2. Is the incident contained on that one PC, or is there reason to believe other computers could become affected? Have any anti-virus/malware products yet been run on the affected PC, and (if so) what did they find?
3. Has the advertiser or the site hosting the advertisement been notified?
4. Should the affected PC be isolated for the weekend by disconnecting it from the network and shutting it down, or should the CSIRT immediately make an image copy of the PC's storage media for possible further investigation?

Scenario 13: Targeted Malware Infestation in Critical Infrastructure

Several agency employees have recently started using a popular on-line portal aimed at helping government IT staff share information about their challenges and solutions. Unknown to them, this popular "watering hole" site has been compromised, causing malware to be injected on several web browser products/versions. The previously unseen malware has successfully infected dozens of agency users' desktop and laptop computers. Agency CSIRT staff are alerted to the problem via a warnings amongst a network of CSIRT operations professionals. They immediately check their firewall logs and discover that dozens of their users had been frequenting the affected watering hole site.

1. How did the watering hole become compromised?
2. Do any anti-malware products authoritatively identify the malware on the agency PCs?

3. How should the affected agency PCs be isolated?
4. Should the agency CSIRT perform artifact analysis on the malware samples? If so, how deeply should the malware be examined, or should it be shipped off (say) to a product vendor for deeper analysis?
5. Should the CSIRT follow standard procedures for restoring the affected PCs, or should additional measures be taken, as this appears to have been a targeted attack on government IT workers?

Scenario 14: BYO Device Malware Infestation

A agency has recently started allowing employees to bring their own iOS and Android tablet computers to work and use them on unclassified networks for official business purposes. Several Android BYOD users have discovered and shared a popular mobile office suite app, and the app has quickly gained acceptance as a de facto standard amongst the agency community. Several sensitive agency files show up on a hacker group's web site, and it is soon discovered that the attack was made possible because the office suite contained malware.

1. How should the CSIRT identify all of the users of the office suite?
2. What ownership issues are there for the BYO device owners and the data on their personal tablets?
3. How will the CSIRT isolate and contain the damage from this attack, and how will that response differ from a conventional desktop PC malware infestation?
4. What remedial policy changes and enforcement processes will result from this incident?