InternetNZ

Internet New Zealand
PO Box 11-881, Manners Street
Wellington 6142, New Zealand
+64 4 495 2119
office@internetnz.net.nz
internetnz.net.nz

New Zealand National CSIRT Establishment: CSIRT Profiles and Case Studies

For a long time, many in the online security industry have been asking why New Zealand does not have a Computer Security Incident Response Team (CSIRT).

The National Cyber Police Office (a department of the Department of Prime Minister and Cabinet created to develop cyber security policy advice for government) has a cyber-plan. Within that cyber plan, NCPO has looked at various models for a CSIRT option.

InternetNZ commissioned this report to provide an analysis of the different models.

This paper does not offer an opinion on whether New Zealand does in fact need a CSIRT, but rather looks at the options available for such a group.

New Zealand National CSIRT Establishment: CSIRT Profiles and Case Studies

Prepared for InternetNZ

26 September 2014

Release version 1

Prepared by
CSIRT Foundry
Chris Horsley
chris.horsley@csirtfoundry.com
Tel: 0402 646 653
ABN: 59 151 819 135

Table of Contents

1. Executive summary 5

2. Preface 6

3. CSIRT introduction 8
3.1. Terminology 8
3.2. Nature of national CSIRTs 8

4. Organisation models and missions 9
4.1. Focus, mission 9
4.2. Authority 9
4.3. CSIRT trust model 10
4.4. CSIRT relationships 10
4.5. CSIRT structure 11
4.5.1. Size 11
4.5.2. Parent organisation / sponsor 12
4.5.3. Government support 13
4.5.4. Law enforcement relationships 14
4.5.5. Executive 15
4.6. Launching 15
4.7. Organisational threats 16
4.7.1. Competitors to assume role of the national CSIRT 16
4.7.2. Remaining neutral while offering services 16
4.7.3. Changes to revenue from external factors 16

5. Funding models 17
5.1. Sponsored / cost centre 17
5.2. Government funded 17
5.2.1. Non-government organisation (NGO) 18
5.2.2. Government-based team 18
5.3. Membership / subscription 19
5.4. Product / service funded 20

6. Target constituency 21
6.1. Enterprises 21
6.2. Home users 22
6.3. Small / medium enterprise (SMEs) 22
6.4. Government 23

7. Marketing and awareness 23
7.1. Gaining visibility with constituents 23
7.2. Face time at conferences 24
7.3. Original research 24
7.4. Work with the media 24
7.5. Get feedback early and often 24

8. Potential service offerings 25
8.1. Reactive services 25
8.1.1. Incident response 25
8.1.2. Technical analysis services 29
8.1.3. Takedown service 29
8.1.4. Malware analysis 30
8.1.5. Forensics 31
8.1.6. Expert witness 31

8.2. Proactive services ... 32
8.2.1. Vulnerability and threat bulletin publishing ... 32
8.2.2. Vulnerability co-ordination ... 32
8.2.3. Data clearing house (a.k.a. the funnel) ... 33
8.2.4. Blacklist publication ... 35
8.2.5. Sensor networks and threat detection ... 35
8.2.6. Penetration testing and audits ... 35
8.3. Hosted / automated services ... 36
8.4. National "common good" projects ... 36
8.5. Conferences ... 37
8.6. Consulting ... 37
8.7. Education ... 37
8.7.1. Training ... 37
8.7.2. Media ... 38
8.7.3. Teachable moments ... 39

9. Support functions ... 39
9.1. Software development ... 39
9.2. Liaison ... 39
9.3. System administration ... 40
9.4. Admin ... 40

10. Personnel and environment ... 40
10.1. Operational teams and environment ... 40
10.2. Technical skills to hire for ... 42
10.3. Personality types and soft skills to hire for ... 43
10.4. Staff considerations and staff retention ... 44

11. Co-operative efforts ... 45
11.1. FIRST ... 45
11.2. APCERT ... 45
11.3. Operational mailing lists ... 45
11.4. Other national and organisational CSIRTs ... 46
11.5. Domestic CSIRT associations ... 46
11.6. Joint operations centre ... 46

1. Executive summary

The formation of a national CSIRT for New Zealand presents many choices and parameters. This report considers several existing national CSIRTs: specifically, the constituencies they serve, their organisational models, their funding models, their services, and how they operate.

Key recommendations and factors to consider:

- A new national CSIRT should look to initially focus on constituencies not already served by existing government bodies or commercial providers. Identify unfilled niches, and potentially refocus energies elsewhere if and when those niches later become more widely serviced.
- The information security industry and the threats it faces shift rapidly. The CSIRT must be prepared to periodically review and refine its constituency, services, and mission.
- Incident response (IR) is the essential service a CSIRT must supply. This report describes IR operations as well as a diverse variety of supplementary services. These supplementary services may either be in the national interest, or to support the CSIRT's other operations.
- When deciding on the capabilities and powers of the national CSIRT, carefully consider the amount of authority it actually needs, and how that might adversely impact its approachability.
- The greatest asset of a national CSIRT is the trust others place in it. It should seek to provide balanced and independent advice, free of any commercial or political influences.
- Whether government or independently funded, getting government support and acceptance for the national CSIRT is crucial for its long-term viability.
- Existing outside of the government or as an NGO may give the national CSIRT the extra flexibility it needs to adapt to new threats, build new services quickly, liaise more readily, and adapt to changing conditions.
- A small team of highly motivated, skilled practitioners is recommended. Increased size may create too much bureaucracy to keep the national CSIRT flexible and responsive.
- A national CSIRT needs a close relationship with law enforcement to stop incidents at their ultimate source.
- Seek to engage a wide cross-section of industry, academia, and government when considering the strategic direction of the national CSIRT. A board may be one way to gain this input.
- A team of highly capable, technical staff is necessary, but without promotion and liaison, the CSIRT cannot be effective at domestic and international co-ordination.
- There are certain personality types that tend to thrive at a national CSIRT, over and above the desirable traits for any technical role. Soft skills are particularly valuable.
- Care must be taken to avoid burnout in staff. Thoughtful role rotation and the internal structure of teams can often have a large bearing on this.

2. Preface

New Zealand currently has several public, national-level entities involved in with cyber-security matters:

- NCSC is a government bureau that "provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats".
- NZTIF is a co-operative, non-profit industry group bringing together security practitioners from across New Zealand. National incident response and co-ordination is currently outside its purview.
- NCPO exists under Department of the Prime Minister and Cabinet, and "lead(s) the development of cyber security policy advice for government and… advise(s) on investing government resources in cyber security activities". They also lead the Connect Smart initiative.
- Netsafe is "an independent non-profit organisation that promotes confident, safe, and responsible use of online technologies", working with partners from many sectors.

From most accounts, these organisations perform their respective roles well. However, groups in New Zealand such as home users, small / medium businesses, and enterprises with non-critical infrastructure remain under-serviced for incident response and recovery from security incidents. If a small business or home user experiences a serious computer security incident, where may they receive assistance? Where should they go to receive advisory information? How should they receive impartial information and educational materials? These are services that may be served by a national body, serving all citizens of New Zealand.

Accordingly, New Zealand would greatly benefit from a single, national point of computer security incident co-ordination and advisory services, in the form of a national Computer Security Incident Response Team (CSIRT). A national CSIRT would complement and co-operate with existing organisations in the space, to fill needs that are not presently fulfilled.

Before beginning the process of establishing a new CSIRT, it is worth considering the services, structures and operational parameters of existing, similar organisations in comparative economies to review the strengths and challenges of each of these models.

This report does not seek to make firm recommendations about which choices a newly forming New Zealand national CSIRT should make, but presents options for the consideration of those who know the local environment best.

About the author

Chris Horsley has over six years of experience working in national CSIRTs (AusCERT and JPCERT/CC), three years consulting to national and organisational CSIRTs, as well as five years experience as a software developer and sysadmin before that.

He joined AusCERT in 2003, where he developed a strong interest in automation and visualisation, particularly for processing phishing sites and log files. The small but very active AusCERT analyst team did everything: tackling online financial fraud, building tools, talking on the phone to victims of compromise, interacting with the international security community, and providing security training courses.

After almost three years at AusCERT, he moved to Japan to work for JPCERT/CC, the Japanese national CSIRT. This led to tasks as varied as phishing site monitoring system development, dashboard development, international training, malware analysis, and sensor network visualisations. After four years and a great amount of cultural broadening in Japan, he moved back to Australia to start CSIRT Foundry.

Chris is now the principal consultant at CSIRT Foundry, specialising in activities related to CSIRTs of a national, organisational, or industry-based focus. It performs CSIRT and incident response consulting, CSIRT systems and software development, and CSIRT training services. Clients include CERT Australia, HKCERT, AusCERT, Rio Tinto, National Bank of Australia, IMPACT, NZITF, and JPCERT.

Chris has presented at various international security conferences, speaking about online financial fraud, CSIRT automation and software development, data visualisation, and malware. He has instructed CSIRT and IR training courses for governments and the private sector in Chile, Peru, New Zealand, Japan, Vietnam, Australia, Malaysia, and for international delegations.

Acknowledgement and referenced CSIRT profiles

The author would like to sincerely thank our panel of national CSIRT experts who contributed their advice and expertise:

- Koichiro Komiyama, JPCERT/CC (Japan)
    - JPCERT/CC profile
        - 50-60 staff members
        - Established in 1992
        - Non-government organisation (NGO)
- Matthew McGlashan, Context IS (formerly AusCERT and CERT Australia)
    - AusCERT profile
        - 12-15 staff members
        - Established in 1993
        - Not-for-profit organisation hosted at University of Queensland, funded by membership and conference
    - CERT Australia profile
        - 20-30 staff members
        - Established in 2011
        - Government entity
- Lakshan Soysa, AusCERT (formerly SLCERT (Sri Lanka))
    - SLCERT profile

- 12-15 staff members
- Established in 2006
- Non government organisation (NGO)

3. CSIRT introduction

3.1. Terminology

"CERT" is a registered trademark.

Throughout this document, we'll refer to an information security team with national responsibility or otherwise as a "CSIRT" (Computer Security Incident Response Team).

It's important to note that the oft-used "CERT" (Computer Emergency Response Team) is a registered trademark of Carnegie Mellon University, who founded the first national CSIRT, CERT/CC. If a team wishes to use the term "CERT" in their name, they must apply to CERT/CC for usage rights. Such requests are often granted to new national CSIRTs who make their case, and also make sure the name is globally unique.

Incident response will also be frequently referred to in this document as "IR".

"ISAC" stands for Information Sharing and Analysis Centre, which provide the data broking and sharing facilities of a CSIRT, often for a specific sector.

3.2. Nature of national CSIRTs

Incident response is fundamental; everything else is highly negotiable.

The core service requirement of any CSIRT is incident response. If the CSIRT does not offer some kind of a hotline or service for incident handling, it cannot be classed as a CSIRT.

A national CSIRT has the additional requirement of having responsibility for a country or territory. What "responsible for" means is a matter of debate, depending on the powers granted to it, its stated mission, existing agencies in the same space, and what it is practically capable of.

Beyond an ISP or organisational CSIRT's core functions, a national CSIRT may deal with the following:

- National and international incident co-ordination (multiple ISPs / registrars / service providers involved);
- Assistance to international CSIRTs by streamlining important incidents through back channels and local contacts;
- Translation of requests to local network operators (in non-English as a first language countries, particularly);
- Development of national incident response initiatives;
- Development of sector-specific CSIRTs and ISACs;
- Otherwise being the "default" abuse mailbox of a country.

National CSIRT roles may at times be in dispute. A number of notable national CSIRTs have begun as self-proclaimed to this role, only for a rival to emerge years later. It is often timing, first-to-market, and eventual official recognition by a government that determines an eventual outcome.

4. Organisation models and missions

4.1. Focus, mission

A national CSIRT's focus should be constantly reviewed and adjusted.

The first decision for any national CSIRT is its mission. What should it, and can it, set out to achieve?

It's important to not let this mission constrict the CSIRT further down the track. The nature of threats, and the way we respond to them, has shifted significantly multiple times over the last twenty years. Stating the CSIRT's mission in terms of a technical class of threat may prove limiting later.

A helpful starting point to define the focus and mission of the CSIRT may be this: what gaps exist in information security services nationally? What is the commercial sector not providing? One of our experts spoke of their selection criteria for CSIRT services being:

- Is there a niche not being addressed by the commercial sector yet?
- Is this a loss-making venture, likely not ever in the interest of the commercial sector?
- Is there some special sensitivity around this activity that would prevent domestic organisations working with international vendors? For example, nation state-targeted malware attacks may be too sensitive to share with an anti-virus vendor in Finland or the United States.

A service not being provided by the commercial sector today may be provided later. In 2004 in Australia, AusCERT focused heavily on phishing and financial fraud malware, which has not been observed before. Several years later, many financial institutions had their own internal teams alongside services from commercial vendors, and so the focus from AusCERT was reduced in response. Services should be anticipated to scale up or down as necessary in the future.

4.2. Authority

Authority and approachability can be a trade-off.

A national CSIRT with officially sanctioned authority has several advantages. Some national CSIRTs who are situated in the government telecommunications authority have the legislative power to demand action from tardy network operators or domain name registrars. This can certainly accelerate the incident response process, and may be valuable to have. Additionally, a national CSIRT with authority may have organisations required by law to report to them regarding certain classes of incident, such as consumer data breaches.

However, having this authority comes with a possible cost. Those reporting incidents may hesitate to work with an organisation with strong powers, such as a regulator able to impose financial penalties for non-compliance. Much as lawyers advise not to volunteer information when talking to police officers, organisations accountable to a regulator may not wish to incriminate themselves in incident reports, fearing a higher burden and potentially, penalties. Often when trying to not just close an incident, but understand its causes and operation, supplementary information (e.g. logs) offered by benevolent service operators is highly valuable.

At the other end of the spectrum, a CSIRT with no authority relies on goodwill when co-ordinating incidents. Incident reporters, not having any requirement to report incidents, are often driven by the motivation to resolve an incident for their own ends, though reports are also offered by community-minded souls. A CSIRT in this position will often experience a lack of response from co-ordination requests, but some reporters may end up being valuable allies as they offer logs and valuable intelligence post-incident.

4.3. CSIRT trust model

A CSIRT's number one asset is its reputation.

So the saying goes, trust takes a long time to build, and is quickly destroyed. There are a few initial steps in positioning a national CSIRT to maximise its trust.

Firstly, the national CSIRT should be impartial and vendor neutral. A CSIRT seen to have vested political or commercial interests risks their assessments, vulnerability notifications, and threat alerts as potentially biased. Software vendors have a tendency to downplay the impacts of software vulnerabilities; security companies have a tendency to talk up threats that their products solve. An impartial national CSIRT's job is to assess reported vulnerabilities and threats as a neutral party, and independently verify and report them.

Secondly, the CSIRT's incident response data handling processes should be public, clear, and strictly enforced. For example, AusCERT's default policy is that incident data received strictly remains within AusCERT. The reporter must explicitly grant permission for any external notifications to ISPs, foreign organisations, or law enforcement agencies.

This ties into the balance between authority and approachability. If an incident reporter thinks that an incident being reported to the CSIRT may be passed on to law enforcement without their knowledge, it may not be reported at all. The CSIRT's guarantee to let the reporter control how information is handled must be explicit, public, and strictly followed.

4.4. CSIRT relationships

We live in a globally networked world, but geography and culture is still a big factor.

We may contact any CSIRT in the world in seconds, but our effectiveness at co-operating with other national CSIRTs and network operators still come down to basic factors:

- *Time zone and region*. The simple factor of overlapping office hours still drives many close relationships. Much collaboration happens between 9-5, which naturally leads to being closest to those in our own region.
- *Face-to-face contact is still critical*. Trust is often built over meetings, conferences, and social gatherings. What happens over dinner at a conference is usually much more important that what happens during a day of presentations.
- *Language and culture*. National CSIRTs with common language and culture naturally gravitate together. One of the key things a national CSIRT can often offer is a translation layer for other international parties when co-ordinating with domestic entities.

There are a few lessons from this. The national CSIRT must connect to the major ICT hubs in their country, preferably with as much face-to-face contact as possible. Attend as many international conferences as resources allow, as this is where trust relationships are formed. Make a conscious effort to work with national organisations outside of your region, which can also allow for a "follow the sun" approach to distributed 24 hour incident handling.

The national CSIRT is the face of the country for incident response, and must make a conscious effort to connect domestic players to each other, and domestic players to the international community.

4.5. CSIRT structure

4.5.1. Size

Small organisations with low overhead allow the flexibility required for effective IR.

Many national CSIRTs run with a minimal number of staff. JPCERT is one of the larger non-government national CSIRTs at 50-60 staff, with AusCERT between 15-20, and SLCERT around 12-15 staff. There are some larger examples, typically situated in governments, as well as smaller teams with just 2-3 very busy staffers.

According to our experts, keeping operations lean and small is a good thing. A small team of passionate practitioners may have a high level of team cohesion and keeps costs down. As any organisation grows, it loses cohesion and the high levels of trust between its members and teams.

A small team can also keep things flexible. An incident response team has to alter its activities daily based on current incidents, change and develop processes rapidly in response to new threats, and modifying priorities based on medium and long-term incident trends. As an organisation gets bigger headcounts, it inevitably gains more bureaucracy and management layers, reducing the flexibility and creativity staff members may be permitted.

In private conversations with CSIRT staff that had worked for a small team and then a larger team, the greatest source of frustration in the transition to the larger team was the many layers of management approval needed for ad-hoc improvements to their processes. New ideas to better handle and detect incidents could also be kyboshed by any one of the several layers of management approval they required to proceed. Many of these staff then left this second, larger team, and left the national CSIRT space altogether.

4.5.2. Parent organisation / sponsor

An established sponsor organisation offering high autonomy for the CSIRT can be ideal.

The administrative overheads running a national CSIRT are much like any other organisation. If we wish to keep our team small, then it can make good sense to rely on the administrative processes of an established organisation.

How much support we can expect depends on what type of relationship the CSIRT and sponsor will have. The CSIRT may be embedded within the parent organisation, or may be stood up as a separate entity from its parent. We'll examine some existing CSIRTs to consider each approach.

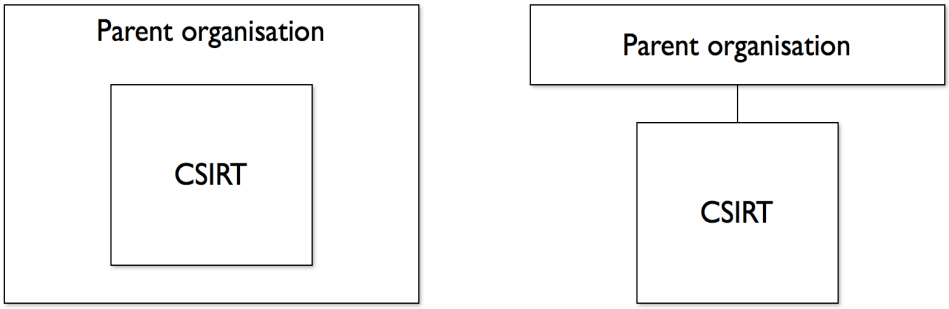


Figure 1: Common sponsor / CSIRT relationships. AusCERT and CERT Australia are embedded in their respective sponsoring organisations as shown on the left, while JPCERT and SLCERT exist independently as shown on the right.

AusCERT exists within the University of Queensland, which acts as a sponsor of sorts for administrative services. AusCERT staff members are actually University of Queensland employees. This allows AusCERT to use the university's infrastructure, services, and processes, and it is given some additional flexibility to arrange its affairs differently to the departments and units around it. As a downside, it also binds AusCERT staff to comparatively lower university pay grades, which can make it difficult to compete with the commercial sector for staff. Additionally, changes in senior management beyond AusCERT's control may have an impact on their own operations.

JPCERT takes this separation from the sponsor one step further. The Japanese Ministry for Economy, Trade and Industry (METI) provides the vast majority of JPCERT's funding, but JPCERT exists as a stand-alone NGO, with its own management and board. This has allowed JPCERT to establish its own procedures independently of METI, at the cost of needing to develop some

administrative procedures internally. Although not day-to-day operated by METI, METI still provides oversight via audits and approvals for some expenditure (e.g. international travel, annual budgeting, large scale projects).

SLCERT uses a somewhat similar approach to JPCERT. SLCERT is an independent organisation from its sponsor, Sri Lanka's Information and Communication Technology Agency (ICTA). A notable difference here was that SLCERT was initially funded via World Bank, with a deadline to become self-sustaining in three years.

4.5.3. Government support

Government support is (eventually) critical.

The difference between AusCERT's and JPCERT's parent organisations and sponsorship approaches also highlights an important benefit of having a strong government sponsor.

AusCERT had for many years been the "recognised" Australian national CSIRT, in lieu of any official government agency. The Australian government wished to bring some of the national CSIRT function back into the government, nominally so that government officials could represent Australia internationally, rather than the university employees of a not-for-profit.

Negotiations for AusCERT to supply technical "back end" services to the federal government's new national CSIRT collapsed, in a well-reported event. The Australian government went on to establish CERT Australia as a branch of the Attorney-General's Department. Many of AusCERT's staff moved to CERT Australia, wanting to continue working for the national CSIRT.

Consequently, AusCERT has been somewhat sidelined. Reports of CERT Australia's effectiveness vary, as they operate more with critical infrastructure providers rather than the public at large. The situation in Australia may have some way to go before it finds equilibrium.

This pattern of an incumbent national CSIRT being replaced by a government equivalent has been repeated elsewhere:

- In the United States, US-CERT took the national CSIRT mantle from CERT/CC.
- In Sri Lanka, SLCERT took over from TechCERT, run by the national domain registry.
- In Switzerland, GovCERT.ch became national CSIRT after the Swiss academic CSIRT SWITCH.ch's stewardship.

In each case, the original organisation remains and keeps close ties with the new national CSIRT, after an often rocky beginning to the relationship.

JPCERT, on the other hand, is one of the few original national CSIRTs founded in the early-mid 1990s which has largely retained its model through to today. A critical factor in this has been the Japanese government's strong involvement and funding of JPCERT via METI.

A national CSIRT without strong government backing seems to be likely to lose this role in the long-term. Governments have shown a preference to take more direct control over an organisation that may have critical strategic value for a country's infrastructure and services.

If direct support from the government is not possible, a non-government national CSIRT may also like to investigate gaining civilian clearances for one or more of their staff. This will at least help in being able to work more closely with government agencies on more sensitive incidents, should the occasion arise.

4.5.4. Law enforcement relationships

Law enforcement involvement is ultimately needed to stop a series of incidents, and CSIRTs must be highly conscious to align efforts with them.

CSIRTs play the "whack-a-mole" game of taking down malicious attacks and infrastructure as they pop up, but it takes the involvement of law enforcement to tackle the offenders behind such attacks. A tight relationship with law enforcement officers (LEOs) should be fostered early. Some CSIRTs even have a secondee LEO on-site to liaise between CSIRT staff and their agency on critical incidents.

CSIRTs and law enforcement agencies (LEAs) often have approaches with mutually exclusive objectives. A CSIRT may work on cases for just minutes or hours, with just enough evidence to satisfy that a site or host is indeed malicious and worthy of taking down. Typically, a CSIRT has little interest in attribution. Conversely, a LEA needs to gather comprehensive evidence that will stand up in court, often over weeks or months, with attribution a primary goal. A CSIRT swiftly taking action on a host being investigated by a LEA may interrupt a long-running investigation underway, or prevent an investigation from ever starting.

It's recommended that for any incidents where there is an especially high level of impact, or a strong suggestion of domestic actors, that the relevant LEA be consulted first to check if there's an investigation already underway, or the possibility of beginning one exists. Some CSIRTs go to the point of building a technical dossier on a target, so they might help accelerate any police investigation.

4.5.5. Executive

A national CSIRT needs input from many sectors.

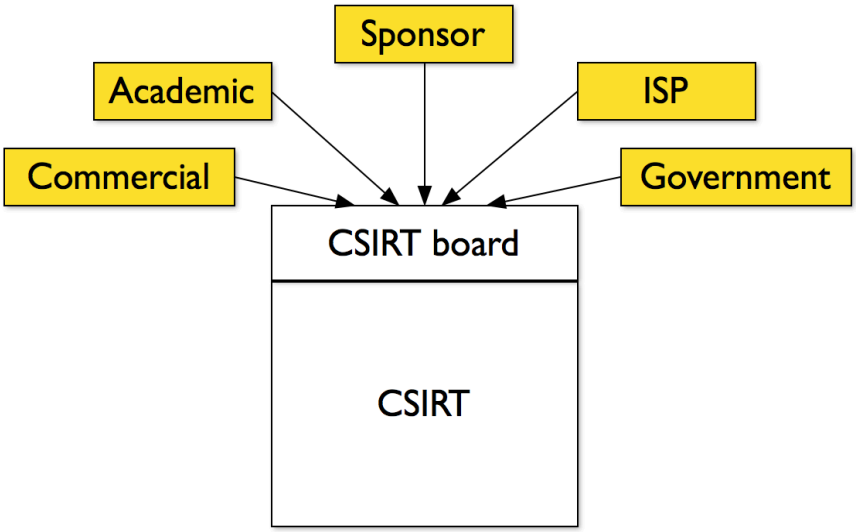


Figure 2: CSIRT board for strategic direction, gathered from multiple sectors

JPCERT uses the model of an executive board. The board is invited from a variety of industries in Japan, primarily ISPs, telecoms, government, and research / academia. The board provides a variety of views from different perspectives, and helps contributes to the strategic direction of JPCERT.

SLCERT also has a board. As an NGO, it reserves two places on its board for its government sponsor. Additionally, a board helped SLCERT to be inclusive of incumbent CSIRTs when it was founded. TechCERT, an existing CSIRT operation from a university, had been founded before SLCERT, and had assumed the role of de-facto national CSIRT. This created a level of tension, with the two organisations vying against one another. To increase cohesion, TechCERT was given a place on the SLCERT board, which also improved the range of opinions when forming the strategic direction for SLCERT.

4.6. Launching

Don't wait too long to tell people you exist.

In the Internet startup world, there is a concept known as the Minimum Viable Product (MVP). This widely followed philosophy states that as soon as a product is usable, it should be released, even if imperfect. This lets the startup assess whether there is base demand for the product, which features are most useful and which unnecessary, and whether the product as a whole must be redesigned or scrapped altogether.

One of our experts noted this same factor with national CSIRTs. Do not wait until you have perfect services with all the technical capabilities you envisage. Let people know you exist and are available as soon as you are operational in some

capacity. This lets you assess the demand for incident response services in your country, and tells you what needs to be advanced, adjusted, or rethought.

The initial public announcement may even be branded as a limited "beta" trial. This is a signal that you're actively looking for feedback and going through an initial growth phase.

4.7. Organisational threats

4.7.1. Competitors to assume role of the national CSIRT

The CSIRT world is fast moving; embrace others interested in the national CSIRT role.

The first generation of national CSIRTs internationally have seen considerable changes in their domestic situations over the last twenty years. CERT Australia replaced AusCERT as national CSIRT in Australia, SLCERT replaced TechCERT as national CSIRT in Sri Lanka, and US-CERT replaced CERT/CC as national CSIRT in the US.

In most of these cases, an existing group of enthusiasts (often from a university) was supplanted by a new government agency or NGO. This isn't necessarily a bad thing from a national perspective, as there are many sectors to be serviced. However, for any newly established team, there needs to be careful consideration:

- What is your constituency?
- Does anyone already have a responsibility for this constituency, or is likely to claim it?
- Are any government agencies likely to stand up a similar organisation? Common candidates would be regulators and intelligence organisations.
- Is it possible to get official recognition from the government for your role as national CSIRT?

4.7.2. Remaining neutral while offering services

If the CSIRT chooses to offer commercial services, care must be taken to avoid bias in its other operations. For example, if the CSIRT was to offer software, and a vulnerability was discovered, the vulnerability should be reported as impartially as one from a third party vendor. Or, if the CSIRT offered a web vulnerability monitoring system, the natural urge to highlight web vulnerabilities over other threats should be carefully managed.

4.7.3. Changes to revenue from external factors

One of the largest threats to a CSIRT can come from a shifting situation in the local economy or security market. Competitors may move into a commercial space that supplies the national CSIRT with its funding; conference spending may fall with a contracting economy; or the government may sharply curtail their sponsorship. Like any organisation, the CSIRT must have a good sense of the stability and likely changes to their revenue.

5. Funding models

A new CSIRT has many subtle flavours of funding model to select from. A funding model may be changed later, but naturally, a change can be very disruptive, so the feasibility of each option must be carefully assessed. Hybrid approaches are also possible.

5.1. Sponsored / cost centre

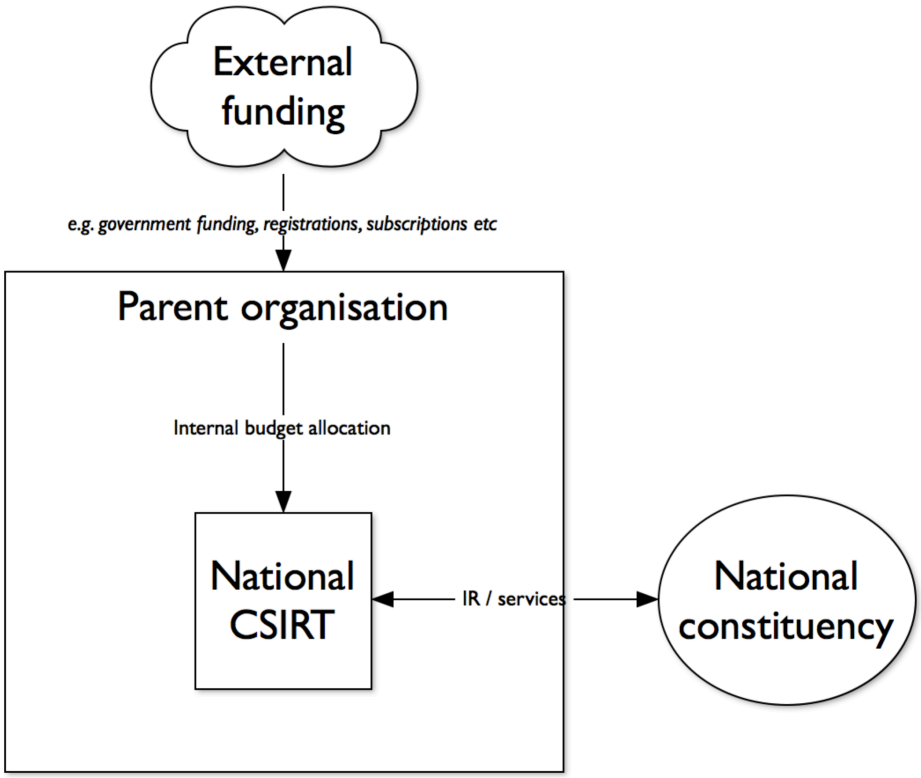


Figure 3: Sponsored / cost centre model

One option used successfully is to host the CSIRT in another established organisation, which operates the CSIRT as a cost centre. CERT.br uses such a model, by hosting the CSIRT inside the national domain registry, NIC.br. The budget for the national CSIRT comes from domain name registrations, a relatively stable source of income, helping to ensure ongoing operations. CERT.br are a long-standing CSIRT that is able to fund innovative research and software development projects in addition to its daily IR operations.

5.2. Government funded

Government funding may be attractive, depending on the model employed. A single source of funding means that the national CSIRT must carefully manage its relationship with its sponsor, but it possibly offers a higher level of stability.

A major decision to make is whether to seat the national CSIRT within the government proper, or stand it up as an independent, government-funded entity.

5.2.1. Non-government organisation (NGO)

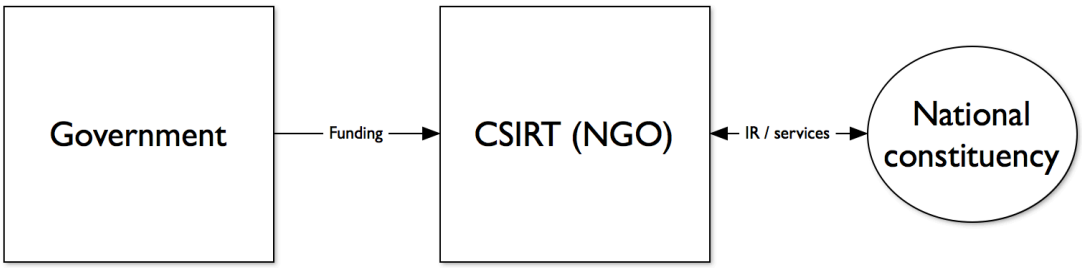


Figure 4: NGO model

Employed by JPCERT and SLCERT among others, this model allows for the relative stability of government funding, while allowing the CSIRT a degree of independence from bureaucracy and politics. The main risks to such a model are changing government priorities, internal restructures, or the expansion of empire-building departments prompting a move to bring the national CSIRT back inside the government proper, either by subsuming the existing team, or standing up a new team to replace it.

5.2.2. Government-based team

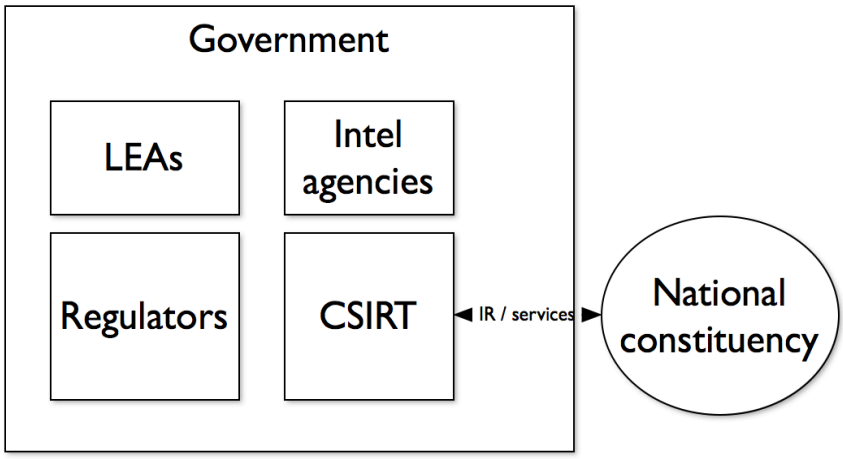


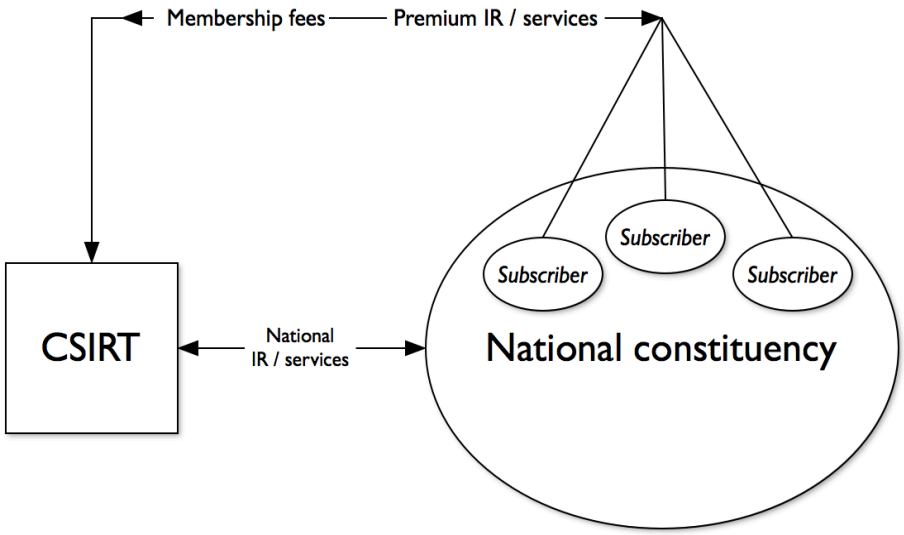
Figure 5: Government model

Employed by CERT Australia and US-CERT among others, the national CSIRT may be a government bureau. This offers advantages such as the ability to represent the country in an official capacity, potentially more stable funding, and a closer relationship with existing government agencies like regulators, signals intelligence organisations, and law enforcement agencies. It may also offer the CSIRT some official clout if desired.

However, a government-housed national CSIRT may also be prone to the rigidity of the public service, which may reduce its effectiveness in the quickly changing environment of incident response. It may also result in the national CSIRT being overly government-centric, putting too much emphasis on other branches of government and critical infrastructure, and not enough on other sectors of the economy. Naturally, this will depend on the remit and management of the national CSIRT.

Finally, where incident reporters may be willing to work with an independent organisation, they may be hesitant to share information with a government agency. The risk of incriminating themselves for non-compliance or regulatory lapses may outweigh the perceived benefit of reporting a breach. However, a government agency may be able to legally require its constituency to report incidents.

5.3. Membership / subscription



A national CSIRT may secure its funding by asking its potential constituents to donate an annual fee for special services, such as priority or 24 hour incident support, feeds of bulletins and vulnerability reports, premium services like web site defacement checking, and discounts to training and conferences. AusCERT is one of the more notable CSIRTs in the Asia Pacific that is membership funded.

A key factor when running a membership-funded organisation is the creation of visible value for members. Quietly soldiering away on defending national networks is noble work, but it does not necessarily encourage re-subscriptions. Weight must be given to work with visible, useful output.

The advantage of a subscribed member base is that it keeps the national CSIRT strongly motivated to listen to the needs of its constituents. In order to get new members, it must work out where there is demand in the market, and develop

new services to suit. Additionally, a wide membership base means that funding is not concentrated to a single entity like a government, meaning that a higher level of independence is possible.

Funding from subscribers results in a number of disadvantages. The balance between the needs of members and the needs of a country are difficult to balance at times. Spend too much time on altruistic national activities that are not of direct benefit to members and they may not subscribe next year; spend too much time on member activities and your effectiveness as the national CSIRT becomes somewhat weaker.

A further factor to consider is that trying to increase membership numbers requires effort that may be outside the comfort zone of a technical team. Traditionally, this would be achieved with the same techniques that any subscription organisation would use: marketing; awareness campaigns; and subscription drives. This work may not come naturally to a small team of technically minded staffers, so a small marketing team or external service may need to be engaged.

In AusCERT's case, its vulnerability bulletin service is delivered on a daily basis to its members, making it a valuable and highly visible daily reminder of AusCERT's work. Memberships are driven in several other ways too. One factor is likely the hefty discount for members to its successful annual conference, paying for the subscription fee almost immediately. Additionally, providing valuable services in the national interest at no charge, such as stolen credential repatriation services, often prompts memberships almost as a donation of sorts for the work that AusCERT does for all Australian organisations.

5.4. Product / service funded

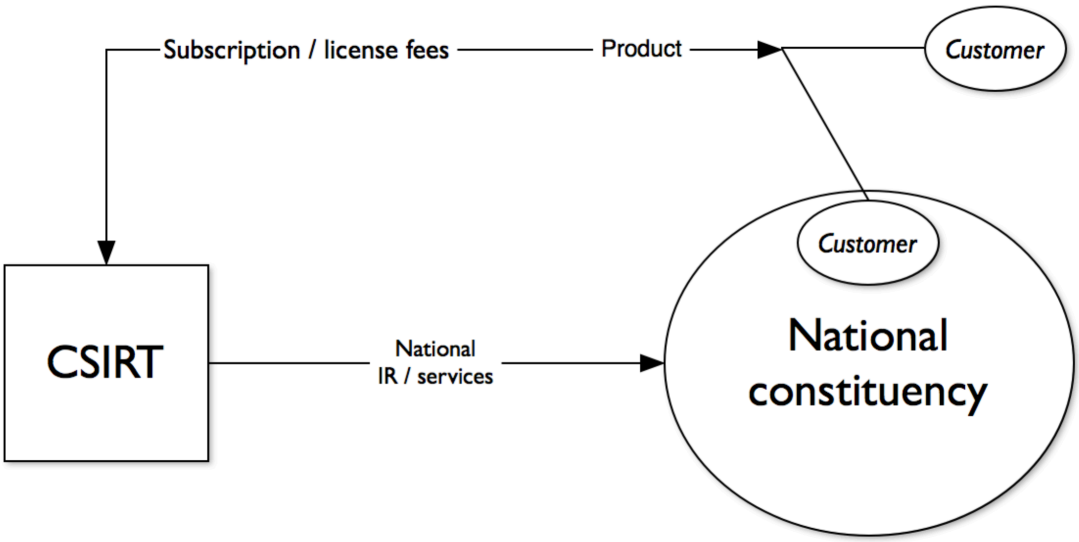


Figure 6: Product / service funded CSIRT model

A national CSIRT may be purely funded by commercially available services, or these may be used in combination with any of the above models. "Potential service offerings" contains more details of possibilities here.

Once again, a balance must be struck between providing commercial services and services in the national interest, all while retaining a standard of impartiality.

6. Target constituency

6.1. Enterprises

Medium and large enterprises will likely be an obvious target constituency for a national CSIRT, given their influence over the economy and critical services.

Each industry may have very different cultures, regulations, histories, terminology, and priorities. For example, the financial industry may treat integrity as their top priority, whereas a critical infrastructure provider may place their priority on availability.

Having a liaison that specialises in a particular industry, ideally having worked with that industry previously, can help the CSIRT to speak with authority and understanding.

SLCERT uses an interesting "umbrella CSIRT" model for their national CSIRT. Sector-specific CSIRTs have been spun off for the banking, ISP, and educational sectors. This may be visualised as:

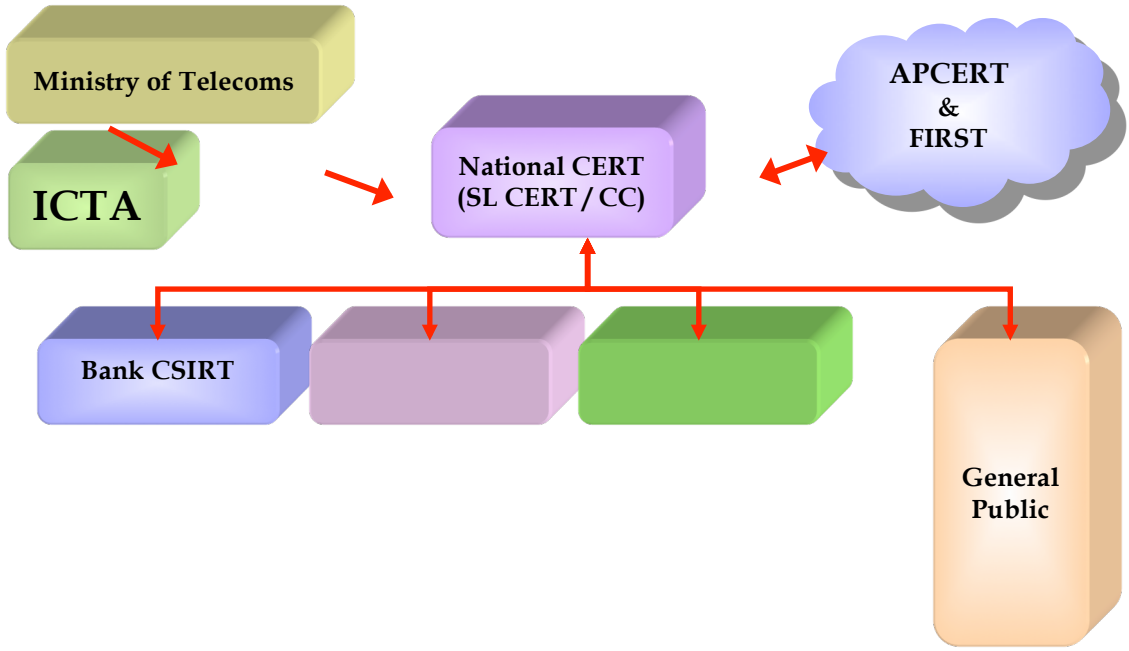


Figure 7: "Umbrella CSIRT" model. Source: SLCERT.

Under this model, SLCERT works with the sector CSIRTs, and the sector CSIRTs work with the sectors themselves. Very often, a sector CSIRT may have the involvement or membership of the regulator itself.

Where individual organisations may be hesitant to share threat information and details of compromises, they may be more willing to do so anonymously. The

sector CSIRTs and SLCERT can provide this function, publishing threat advisories or indicators of compromise in a non-attributable manner. Data may be shared just within a particular sector by the sector CSIRT, or between multiple sectors by SLCERT.

6.2. Home users

Home users are the largest constituency by volume, but often the last to be targeted for national CSIRT projects. While neglected by some national CSIRTs, often due to funding constraints, the security of home users impacts on their confidence in electronic transactions, which impacts upon the uptake of commercial and government services.

Supporting home users can take multiple forms, at various scales of operation. At a high level, this may involve awareness campaigns. The value of educating end users generally is hotly debated in information security circles, with some believing constraining and making systems more secure by default is the only valuable place to invest money.

However, awareness campaigns can suit any level of budget. At the no-budget end, the CSIRT may be able to get the message out to home constituents via media reporting. However, the message sent is somewhat at the mercy of the journalist. At the higher budgeted end of the spectrum, the CSIRT may choose to employ or contract PR professionals to design an awareness campaign with educational materials and events.

Aside from awareness campaigns, a CSIRT may choose to be more direct in their support of home user incidents. The Cyber Clean Project (CCC) (https://www.active.go.jp/en/) in Japan and Anti-Botnet Advisory Centre in Germany (https://www.botfrei.de/en/) both offer bot disinfection tools to reduce the instance of bots hosted on home systems. The German project was based on the Japanese CCC project, and as well as providing a free disinfection tool, also offers a direct helpdesk to end-users. This naturally requires a significant budget, but is arguably of direct benefit.

SLCERT have also been tasked with targeting home users. As Sri Lankans increase their use of e-government services, further priority has been placed on the idea of trying to secure home systems.

6.3. Small / medium enterprise (SMEs)

Small and medium enterprises can be numerous in any country, especially when "mom and pop" stores and home businesses are considered. This sector is a challenging mix of small business owners with middling or no technology training, who often run software found in larger enterprises. Once a technology provider has installed systems in an SME, they are often minimally administered from that point on.

The most interesting model to follow in this sector is Nominet's Cyber Assist project, which readers of this report may already be familiar with. Certainly, results from the initial pilot of the scheme should be most instructive.

Polling our expert panel about SME CSIRT services revealed that:

- SLCERT gives SMEs a low weighting compared to government and large enterprise, due to a high volume of potential support required, as well as the damage from any particular incident likely being lower.
- CERT Australia appears to put little emphasis on SMEs, focussing more on large enterprise and critical infrastructure providers.
- JPCERT similarly works more closely with large enterprises and critical infrastructure providers. Home user and small business security is a focus for another organisation, the Information-Technology Promotion Agency Japan (IPA).
- AusCERT likely deals more with SMEs than the other teams listed, either having SMEs as subscribed members, or having SME incidents referred to them by other agencies.

6.4. Government

A national CSIRT may deal with government departments, but their interaction may differ from the other sections we've talked about. Many developed countries already have a dedicated government incident response function, which may include forensic examinations and on-site incident response. This role is filled in Japan by the National Information Security Center (NISC), and in Australia by the Australian Signals Directorate (ASD).

SLCERT have been mandated to provide government incident response and encourage best practice. Uptake is reported to be quite good amongst government departments, with a couple of limiting factors. Some departments are hesitant to report incidents, as they fear the airing of improper practices. Departments are also at times unable to comply with best practice due to budget constraints, compounding this hesitancy.

Whether the government constituency is served by a government-wide CSIRT or the national CSIRT, government security operations can likely benefit from the co-operation of the national CSIRT. Governments may often be more constrained by official international relationship channels and information classification levels, which may not apply to a CSIRT operating outside of government. Government CSIRTs may be able to co-operate with national CSIRTs at such times, as well as benefiting from the diverse and unofficial intelligence channels the national CSIRT may have access to.

7. Marketing and awareness

A new national CSIRT may not have any resources available for PR and outreach. We'll explore some options for improving awareness of the CSIRT using the team's technical resources.

7.1. Gaining visibility with constituents

Tell people about problems they never knew they had.

A new CSIRT has a primary focus of incident response. Without knowledge of events in the constituency or incident reports, the team can face a proverbial case of sitting by the telephone, waiting for someone to call.

One strategy to accelerate awareness is not to tell people what you can do for them; show them. There is an ocean of incident and event data available from many public feeds. If the CSIRT can harness all this data and notify users before they are aware of the problem themselves, the value of the CSIRT can be quickly demonstrated. Once relationships with reporters have strengthened, more incidents will be reported, and it will have a self-reinforcing effect on the CSIRT's awareness of activity in their constituency.

There is such a volume of data available that some kind of automated handling is recommended. A detailed explanation of tools is beyond the scope of this report, but a few open source solutions are CIF, Abusehelper, and IFAS (disclaimer: the author is involved in IFAS development).

7.2. Face time at conferences

Make your team available to the constituency.

Considerable budget may be allocated to conferences, security days, and workshops to ensure that the national CSIRT's staff members are mainstays of the local information security community.

One approach that may be worth exploring is assigning each staff member one or more communities to specialise in. By having different staffers focus on a particular community, they more easily build deeper trust relationships.

7.3. Original research

Breaking news creates reputation.

If you have the resources, publishing original security research is a fast and constructive way to enhance the reputation of the team. Good research, such as new vulnerabilities or threat analyses, gets reported elsewhere, in mailing lists and by media, so it's a potentially cost-effective way to increase awareness of services the team offers.

7.4. Work with the media

The media has wide, cost-effective reach.

This is covered in more depth in Media, but being available to and working closely with media outlets can be a cost-effective way to reach a wide audience.

7.5. Get feedback early and often

Don't wait until you're perfect.

Don't wait until your CSIRT is "mature" before letting people know you exist; announce early. Don't focus on any one particular way of increasing awareness; try lots of different ideas and see what is most effective.

8. Potential service offerings

A CSIRT's core services can be broken into two broad categories: reactive and proactive. The CSIRT may also offer a variety of supplementary services, as illustrated below.

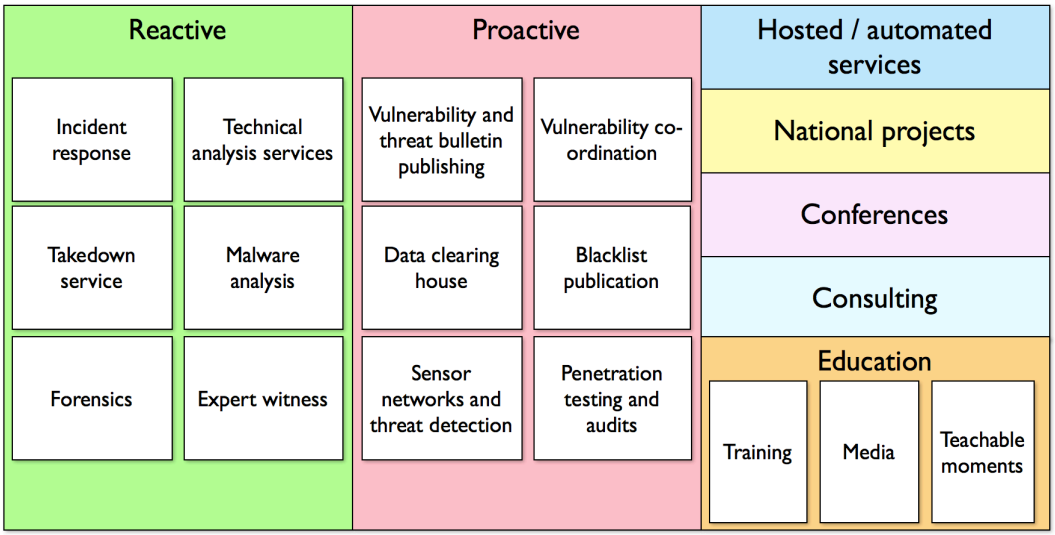


Figure 8: CSIRT service options

We will now explore each of these service offerings in more depth.

8.1. Reactive services

8.1.1. Incident response

As the critical service that defines a CSIRT, incident response should be considered before anything else. There are a number of decisions to make which defines the nature of the services you'll provide.

24-hour service

Offering a 24-hour service is often a function of budget and staffing levels.

Factors to consider:

- Being on-call after hours can significantly impact on staffers' personal life, even if no calls are received. Typical impacts are that on-call staff cannot be out of network range, need to carry multiple phones and laptops, cannot drink alcohol after work, cannot travel, and may have interrupted sleep patterns.
- Being on-call normally comes with salary loading, which requires additional budget.
- How often will you rotate on-call duties? If you have a small team, will members be on-call most of the time?

- Will the team be operational on Christmas and other public holidays? The announcement of major software vulnerabilities has happened on Boxing Day in the past, requiring immediate response.
- If a remote VPN was an option for the CSIRT previously, it's essential for a 24-hour service.

Triage

Consider:

- Many reports received by a CSIRT are either relatively unimportant, unable to be acted upon with the data supplied, or outside the mandate of the organisation (contacting the CSIRT as a last resort for the theft of virtual game items is not unheard of). Processing such reports is time consuming and often repetitive.
- Each morning and afternoon, consider a first pass of all incident reports to remove noise and prioritise any reports. This allows batch processing of some types of reports, and efficient delegation of notable incidents.
- Create prioritisation criteria for incidents, creating consistent triage between incident handlers. You may consider: the potential for loss of life; size and criticality of the affected party; potential impact of the reported incident (single attack versus widespread vulnerability); reporter's connection to core constituency (e.g. direct constituents get priority, then domestic reports, then international reports); estimated cost to repair (possibly given a low weighting due to inaccuracy of estimates).

Software

Software to manage incident reports (an incident management system, or IMS) is essential – it is likely the most important piece of software the CSIRT will use.

A good IMS should:

- Allow the import of reports from a variety of sources like email, phone, and a web reporting form;
- Allow flexible operational reporting (how many open tickets, how many tickets added today, how many tickets closed today);
- Allow flexible management reports (who is reporting the most incidents, what type of incidents are trending up and down, which networks have the highest count of incidents);
- Allow a programmatic / extensible interface to allow custom and automated behaviour;
- Have an easy to use web interface that can be reliably and quickly accessed over a slow, remote connections (e.g. bandwidth-optimised web site), or possibly a mobile device;
- Allow for a variety of incident data and metadata such as priority, reporter details, network addresses, domain names, and file attachments;
- Allows for access control so that incidents may be restricted to certain teams or staff members;
- Allows a search interface to correlate current activity against historical activity;

- Allow for automated escalation or reminders for incidents that are not closed after a preset time.

When choosing an IMS, consider:

- An Excel spreadsheet or an inbox alone might seem good enough for an initial, quick solution. However, the team quickly becomes locked into using it as data is accumulated and workflows adapt to it. Over time, migrating to a more robust system gets more and more complex and expensive.

  It's been known for some teams to reluctantly use ancient, hastily assembled Access databases for years, long after they've been outgrown. So, consider a robust, mature solution from day one, even with a small initial volume of incidents.
- A critical initial decision is whether to use existing software, or develop your own in-house solution. An IMS may seem deceptively simple at first, like an enhanced email client, but it usually tends to include a lot of complex functionality that makes the development effort much higher than expected. *Therefore, it's highly recommended to evaluate and comprehensively discount all existing software options before writing a new IMS from scratch.* Many teams have ended up writing their own IMS, and end up needing to dedicate a full-time employee or more worth of effort to maintaining it. These resources could be much more effectively used in handling incidents themselves or developing other niche tools.
- The decision to write a custom IMS often starts when existing options lack several features deemed critical or desirable to the team. Consider contributing to existing open source projects by adding necessary features.
- There are several well-used pieces of open source IMS software, as well as commercial options. A full evaluation is beyond the scope of this report, but RTIR and OTRS are popular open source options, and RSA Archer is a well-used commercial product.

Reporting mechanisms

You may wish to offer flexible reporting mechanisms to your constituents:

- *Phone hotline.* You may opt to have multiple phone numbers; a public number for incident reports from the public; and a priority hotline only given to constituents.
- *Web site form.* The key balance here is demanding enough information to enable incident response to commence, but without an overwhelming number of form fields that causes reporters to give up in frustration. Judicious use of carefully selected mandatory and optional fields is crucial.
- *Web site API.* Some reporters will wish to send large volumes of automatically generated incident reports. By adding a programmatically-accessible API to your website which validates and stores incident data,

this may encourage additional incident reports, enhancing the national CSIRT's visibility of malicious activity.

- *Structured email.* Some reporters will wish to automatically send you incidents pulled from their IDS or logs. If you support processing structured incident data such as IODEF or STIX/TAXII, you can automate the handling of many incidents and save valuable analyst time.
- *Freeform email.* A CSIRT needs to handle unstructured requests, which begin as "Have you ever seen activity like…", and possibly escalating into a full-blown incident. An IMAP mailbox is essential here to make sure efforts to process email reports are synchronised between team members.

Specialised category incident handlers

Rather than letting a single incident handler battle through each and every incident in sequence, you may like to have a group of staff members who are fully or partially dedicated to a particular type of incident. This allows the team member performing initial incident triage to delegate specialised, time-consuming, or time-critical incidents to others. Some examples would include:

- *Incident triage*: first pass through all inbound correspondence, follow up on any incidents that have short, documented procedures.
- *General incident secondary support*: the incident triage officer may delegate any complex or time-critical incidents to a second staff member. For example, if a report concerning a DDoS from a large number of domestic bots was received by the CSIRT, the handling for this incident may be passed along to the secondary support handler so that the incident triage may continue their work.
- *Takedown handler*: many of the reports a CSIRT receives identify malicious content, often a website or infected host. These incidents require the handler to verify the report, identify the relevant ISP / registrar / CSIRT, locate contact details, draft and send an email takedown request with supporting evidence, and finally, follow up to make sure the identified site or host has been disabled. This workflow may be more efficient when performed by a dedicated handler assisted by software tools.
- *Malware analysis handler*: malware analysis often requires a different analysis environment and different skills sets, so dedicating a staff member to this role may also prove useful.
- *Vulnerability / threat bulletin publisher*: as new threats and vulnerabilities are received, this staff member is responsible for triaging, analysing, and publishing them to constituents. It's often important to have a second staff member to vet drafts and provide an independent analysis.

Rotation

Incident response often involves days of intensely interesting work, followed by weeks of routine, "seen it all before" trench digging. For this reason, rotating staff through the different roles often helps to avoid feelings of the hopelessness that can come with continually responding to problems, but never having time to deal

with the underlying causes (e.g. deeper analysis, building automated systems to reduce manual effort). A rotation of one or two weeks is a good initial interval time to consider.

Additionally, this rotation provides other natural advantages such as: cross-skilling; redundancy when staff members are sick or away at conferences; and good documentation on incidents and procedures since a new handler needs to continue handling incidents the following week.

8.1.2. Technical analysis services

In a similar vein to incident response, the CSIRT may offer more in-depth technical analysis services to constituents. For example, following a successfully executed attack, a company with few security officers may send a web application log to the national CSIRT for their expert advice on determining how the attack was performed and which vulnerabilities were exploited.

This service may be especially desirable for a national CSIRT looking to gain revenue with some or all of its services. Deep analysis may be only open to subscribers or a subset of members rather than the public at large, given its resource-intensive nature.

It may also be desirable if the team is seen as independent and vendor neutral, so the recommendation following the report will considered impartial and not promoting any particular commercial service, software, or appliance.

8.1.3. Takedown service

Given the large volume of fraud-oriented sites, drive-by downloads, and web site defacements, a national CSIRT may consider a specialised service to request takedowns on behalf of its constituents. There are pros and cons to offering this as a service:

Pros:

- Malicious and fraudulent sites are a highly visible incident type, increasing the CSIRT's relevancy along with perceived effectiveness of the CSIRT's activities;
- Constituents can make a reasonable estimate of financial damage avoided by disabling a phishing or fraud site, clearly demonstrating the value of subscription to the CSIRT;
- Successfully analysing novel new countermeasures to attacks make good case studies / research, bolstering the CSIRT's reputation as an expert authority;
- Takedown activities encourage close co-operative relationships with different sectors such as finance, retail, and government, allowing the CSIRT to become an important hub of activity.

Cons:

- Much takedown work is highly repetitive, necessitating a level of automation to avoid staff fatigue and burnout;

- There are a number of commercial vendors who have offered such services for a number of years. Care must be taken that domestic constituents are not already using and satisfied with these services;
- Takedown work can be highly resource intensive, so ensure that staff levels are sufficient before advertising this as a dedicated service.

8.1.4. Malware analysis

Malware analysis can go from a service the national CSIRT performs as needed, to a central focus. Here, we look at a few levels of operation ordered from few to high resource requirements.

AV industry liaison

If few internal malware analysts are available to a national CSIRT, it may find it beneficial to develop strong relationships to the anti-virus industry. After receiving a malware sample from a constituents and receiving permission to forward it on to third parties, the team may submit it to many anti-virus teams on behalf of the constituent, requesting a summary analysis of its functionality.

Ideally, this is win-win-win for the anti-virus vendors, the constituent, and the CSIRT. Anti-virus industry vendors receive new and interesting samples and increase their detection rate; the constituent has a chance to gain greater insight into the sample and receives better AV protection; and the CSIRT becomes a valuable intermediary, increasing the strength of its ties to both the constituent and AV vendors.

AusCERT has used this technique very effectively in the past. With a minimal number of staff resources available for detailed malware analysis, this effort was requested of expert analysts in AV companies. Some AV companies would prioritise such requests, as the samples received from AusCERT were already vetted as somehow interesting, as well as being used in a significant incident. Only a minority of AV vendors would reply with analysis, and there was no obligation for them to do so, but at the very least, detection would eventually be added for constituents' AV products, regardless of the product they used.

Surface and runtime analysis

Much can be achieved with automated runtime analysis in a CSIRT. For the investment of setting up an isolated malware lab, newly received samples can be queued to be analysed both on a surface level (file size, file hash, other metadata) and by a runtime analysis system (execute the malware and observe its behaviour). There are a variety of both open source and commercial runtime analysis systems, both locally hosted, or available via web interface or API.

There are limitations to this approach. Modern malware can be quite sophisticated in its detection of the environment it operates in, and may not execute if it determines it's running in a virtualised or isolated lab environment. However, for a relatively small investment in hardware and software, there may be a high benefit for constituents and the CSIRT's awareness of domestic malware attacks.

SLCERT uses a combination of a basic runtime analysis environment and good industry connections to provide malware analysis service to its constituents.

Full malware analysis lab

A CSIRT may opt to essentially replicate many of the analytical services an AV vendor lab would typically provide. As well as the surface and runtime analysis services detailed previously, this adds a layer of static analysis, involving a detailed deconstruction of the malware's instructions and operation.

The major downside of this approach is the expense and human expertise required. To competently perform static or reverse analysis requires a high level of technical expertise, which is already in high demand in the commercial sector.

JPCERT has a dedicated malware team that would be larger than some smaller national CSIRTs in their entirety. The driving force for this is the increasing instance of malware-borne targeted attacks (sometimes known as APTs) against government agencies and institutions in Japan. As many antivirus vendors are located outside Japan, there is a hesitation or legislative constraint not to send such highly sensitive malware samples to international, commercial organisations.

JPCERT's malware team operates under high levels of confidentiality regarding its clients and operations, even offering access-controlled facilities and very limited operational visibility to other teams within JPCERT. This team is highly regarded, and attracts stable funding from the domestic institutions that use their services.

8.1.5. Forensics

Digital forensics is another area in demand, especially amongst law enforcement agencies and large organisations performing internal fraud and HR investigations.

This is a resource-intensive service, and needs experienced and trained investigators to properly offer such a service. This may not be a service every constituent will want, and is possibly a service for a later maturity level, but it may be worth surveying your constituency to determine demand.

SLCERT offers a forensic analysis service on a limited basis to law enforcement agencies with a valid warrant.

8.1.6. Expert witness

A CSIRT may also be able to supply expert witnesses in the event of court cases with an information security facet. This is likely not a regular service, but may be very helpful to law enforcement agencies.

Some factors to consider here:

- Will the CSIRT charge for its expert witnesses, or offer such services gratis?

- Will CSIRT expert witnesses appear in court, or only supply reports that may be submitted as evidence? There may be some safety concerns when appearing as an expert witness.

8.2. Proactive services

8.2.1. Vulnerability and threat bulletin publishing

Teams like AusCERT, JPCERT and CERT/CC offer a stream of alerts to their constituents. These typically fall into two categories: vulnerability announcements, and threat warnings (e.g. current widespread exploitation of a vulnerability).

This type of alert publishing service is one of the core proactive services a CSIRT can offer to their constituents. Alerts may either be drafted by the CSIRT, or republished with permission from the original publisher, likely a researcher or vendor.

If much of the information we'll republish is in the public domain, why send this to our constituents at all? An initial reason is to avoid duplication of curation efforts. Information security officers in any organisation are under their own resource constraints, so a national CSIRT service that eliminates duplicated effort will be welcome. Additionally, raw vulnerability bulletins may be enhanced with standardised metadata, such as platforms and version affected, publication date, and priority. This allows both searching an archive of previous alerts, as well as a chance to tailor the alert feed to a constituent based on the platforms and software they use. If resources permit, you may like to offer constituents a web application that allows them to check off vulnerability bulletins that have been assessed, mitigated, or patched.

The original alerts the national CSIRT publishes are of increased value. Constituents benefit from a novel, impartial analysis of a new vulnerability or threat, especially one that's tailored for local conditions in New Zealand.

Publishing such a vulnerability service is not a light undertaking, and may require at least one full-time employee worth of effort, as well as a publishing workflow system to support this.

Despite this, impartial, well-researched, and factual CSIRT publications are highly valuable during a high profile chain of incidents, or the emergence of a new threat. It is also a service that is a highly visible daily reminder to constituents of the value that the CSIRT is creating.

8.2.2. Vulnerability co-ordination

Vulnerability co-ordination is not necessarily a service that will create revenue for the national CSIRT, if revenue is a concern at all, but may be deemed as a service in the national interest.

The core of vulnerability co-ordination is receiving raw vulnerability reports from researchers, verifying their validity, determining an initial set of impacted platforms, and then notifying the vendor responsible. Once the vendor has been

notified, it's the national CSIRT's job to stay in close contact, determine the progress of patches and/or temporary mitigations, incorporate additional threat information from the vendor into any calculations of impact and risk, and keep them accountable to disclosure timelines.

This type of co-ordination is beneficial to the major parties: researchers; vendors; and software users. Researchers may at times want to keep their identity secret, for reasons of organisational non-attribution, or fear of litigation from the vendor (even if unfounded). So, they may use the national CSIRT as a proxy, with assurances that the researcher's identity is only revealed publicly with their permission. Vendors benefit from a pre-vetted supply of new vulnerability reports, co-ordinated by a responsible organisation with a formal policy of disclosure deadlines and policies. Software users, too, benefit from the use of a "co-ordinated vulnerability disclosure" policy, which allows countermeasures to be developed before a public announcement, ideally lowering the risk of exploitation.

JPCERT runs a long-standing vulnerability co-ordination team, endorsed by the Japanese government. Over many years, JPCERT has created close ties with many software and hardware vendors in Japan, as well as the domestic researcher community. This service is particularly important in Japan, which has a great amount of software that is only used domestically.

In New Zealand, the strong information security researcher community is an argument for providing a dedicated vulnerability disclosure service. However, there are several arguments against standing up such a service, at least initially. Firstly, CERT/CC has a very mature vulnerability disclosure team, and this can potentially handle vulnerability co-ordination for much of the software used in the English-speaking world. A second factor is the rise of commercial vulnerability handling services along with vendors that pay significant money for new vulnerabilities, potentially reducing the number of vulnerabilities reported to a national CSIRT or vendor altruistically.

However, even if no dedicated vulnerability software co-ordination team is stood up, the new national CSIRT should at least be aware of the protocols involved should this need arise on an ad-hoc basis. CERT/CC has a wealth of knowledge on the subject, and is an excellent place to begin.

8.2.3. Data clearing house (a.k.a. the funnel)

One important role a CSIRT performs is that of an information broker. Being a clearinghouse of incident and event data is a highly useful role for any national CSIRT.

We may visualise this model as a funnel of sorts, turning noisy raw data feeds into highly targeted, highly relevant feeds for domestic organisations:

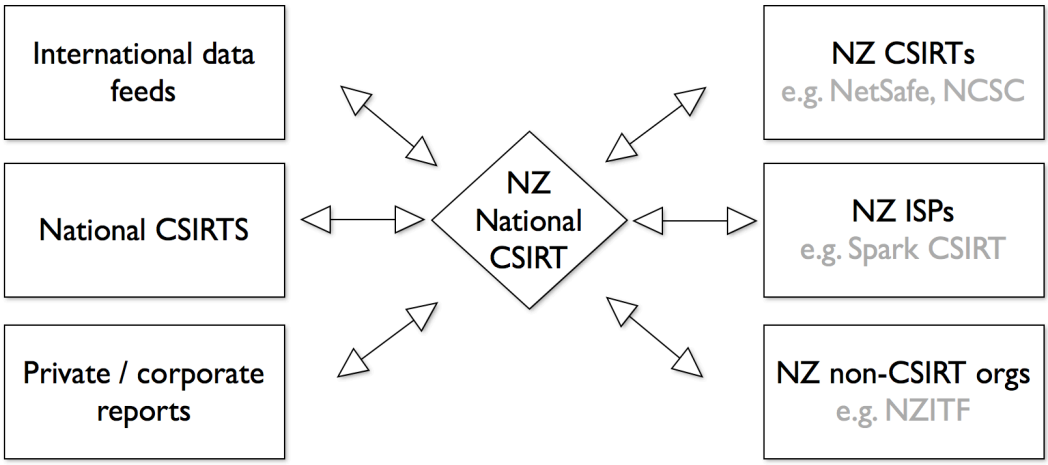


Figure 9: Model of CSIRT as an information broker

A few points to note about being an effective data broker:

- Key to success is cultivating the international and domestic partnerships you have.
- Make sure you're highly responsive on reports received, providing feedback to the original reporter when asked. The feeling of having a report ignored rarely produces subsequent reports.
- Make outgoing reports highly relevant to their recipients, verifying that there's enough data to take action on. NTP-synchronised timestamps with a time zone are critical if available.
- The volume of data feeds can be overwhelming: automate where possible. Not all of this software needs to be developed in house, but having at least one developer on-hand to assist may make a world of difference.
- Commercial storage tools for indexing and processing large amounts of data can be very good quality, but require a healthy budget. Open source solutions are also available and advantageous from a budgeting stance, but sometimes require more expertise to configure and get desired functionality.
- In some ways, data you can contribute to other organisations can be seen as something of a currency. Original data you can produce can have compounding effects, such as invitations to receive other data feeds, or inviting analysis from third parties that can be shared back.
- Confidentiality is key: be very careful before using and re-sharing data, making sure the original publisher is comfortable with your use. The international information security community is tight-knit, and word of abusing or reselling such feeds spreads quickly.
- Software is available to manage such volumes of feeds: CIF, Abusehelper and IFAS are some options (disclosure: author is a developer for IFAS).

8.2.4. Blacklist publication

As well as using your data broker capability to send incident alerts to your constituents, you may like to refine this data into something more immediately consumable.

The national CSIRT may like to publish blacklists of IP address blocks, malicious URLs, and known bad hosts. These lists can be made available in a variety of formats and imported into popular open source and commercial tools, such as firewalls and IDSes.

It's important not to overstate the coverage of such lists. Comprehensively tracking and storing data for worldwide networks is a massive undertaking, so you might like to state that this supplements existing rule sets, but is specifically focused on New Zealand-targeted threats and networks.

8.2.5. Sensor networks and threat detection

Tying into the desire to detect and announce emerging threats to the national CSIRT's constituency, the CSIRT may decide to run network sensors. These sensors may be developed in-house, or deployed as part of an existing sensor network. JPCERT (Tsubame), Dragon Research Group, and the Honeynet Project run some of the sensor networks available in the Asia Pacific region. For the investment of some rack space, it can significantly improve a CSIRT's awareness.

One requirement for running a successful sensor network is good sensor placement. A simple passive sensor may be placed on an otherwise unused ADSL connection, while massive volumes of flow data may be collected and analysed from a busy ISP or educational network router. Good domestic contacts with ISPs and universities will help greatly here.

Running a sensor network is a specialised topic beyond the scope of this report, but it may be worth investigating early on. Finding a home for sensors of international research groups is often a good way to forge relationships with other organisations, access the global data of the rest of the sensor network, and more proactively detect emerging network threats.

8.2.6. Penetration testing and audits

The national CSIRT may decide to run penetration tests or audits as a source of revenue, or may be mandated to do so for certain sectors. This is a service that more directly overlaps with widely offered commercial services, so care needs to be taken that establish penetration services does not arrive on an already saturated market.

Penetration testing also has its risks, particularly when running exploit tools like Metasploit. Adversely affecting the production systems of a client or constituent is not unlikely, and so legal and contractual protection should be built in. SLCERT in fact opted not to offer such services because of the heightened risks. However, in the right circumstances, penetration testing and audits may be a lucrative source of revenue and a directly useful service for a CSIRT's constituents.

8.3. Hosted / automated services

Whether the CSIRT wishes to run automated services to fund other operations or run at a loss for the common good, the options for services the CSIRT can provide are almost as widespread those of a mainstream security vendor.

Sample services may be: website defacement and drive-by-download monitoring; infrastructure uptime monitoring; SSL certificate validity and expiry monitoring; PKI services; automated web site log analysis; blacklist filtering; and automated malware analysis.

Building and advertising such software from scratch is large investment, much akin to founding a startup company, and beyond the scope of this report. A more practical, initial option may be "white labelling" an existing online service. A national CSIRT may negotiate with an existing security service to rebrand their service with the CSIRT's name. The CSIRT may then advertise and offer this service to their members as being their own. The CSIRT either takes a small commission from the white label service provider for every paying constituent they bring to the service, or the CSIRT pays a discounted wholesale price to supply this service to their existing members.

Such an outsourced service may be quick to get up and running. At the same time, care must be chosen that the vendor is a reputable one, since the CSIRT will have little to no control about the performance and stability of the service or the conduct of the company behind it. Additionally, the CSIRT will likely not expect an overwhelming revenue stream this way, as commissions are typically modest.

8.4. National "common good" projects

As well as commercial services, a national CSIRT may take it upon themselves or be commissioned to build a loss-making project in the national interest. Co-ordinating a domestic or international drill such as Cyber Storm would be such a project.

One significant, novel example of a national project this was the Cyber Clean Center (CCC) project in Japan. The aim of this project was to detect malware infections on Japanese networks using honeypots, develop free malware removal tools akin to lightweight anti-virus, and notify users of infection, with instructions on how to clean their machine. CCC was notable for its large-scale collaboration between two government departments, JPCERT, Trend Micro, the telecom ISAC, an IT promotion agency (IPA Japan), and over 70 Japanese ISPs. As well as attempting to improve the standard of security for Japanese Internet users, ISPs also expected to save on their user support costs via CCC's centralised, automated approach.

The project ran for five years, finishing in 2011, and has since been rolled into a new, restructured project known as ACTIVE. The CCC model has also been emulated in other countries.

SLCERT, on request of the Sri Lankan government, assisted in the development of a national PKI infrastructure known as the National Certificate Authority

(NCA), designed for citizens to access e-government and financial services. This service was determined as not being commercially attractive for development by a vendor, and so it was determined that it should be built as a national project by SLCERT and their parent organisation, ICTA.

8.5. Conferences

Running an information security conference is a way a national CSIRT can bolster their reputation and potentially gain revenue to subsidise other loss-making services.

AusCERT runs one of the more successful commercial conferences in Australia and New Zealand, taking place in May each year. A combination of "commercial" conference admission fees and heavy vendor participation make this one of the major revenue earners for AusCERT each year. While AusCERT is the brand behind the conference, and the program and much of the conference design is a result of AusCERT's input, the logistics themselves are assisted by venue and event management staff.

The AusCERT conference has had a largely positive reputation boost for the AusCERT team, to the point that some conference goers associate the name "AusCERT" more with the conference than they do with the CSIRT operation. AusCERT's position as a non-government entity makes this possible – it would be difficult to imagine a government entity having the latitude to host a similar event.

SLCERT also runs a Cyber Security Week conference, which involves a fee-based conference, along with a hacking challenge, training courses and awareness sessions. The revenue derived from this is lucrative to SLCERT, and it also gives a very good return in terms of awareness and reputation for SLCERT.

8.6. Consulting

The national CSIRT may also opt to offer traditional security consulting. SLCERT offers network architecture reviews, audits, and policy development as a commercial service.

8.7. Education

8.7.1. Training

Training is time and resource intensive, both in preparation and delivery, but can be advantageous for a national CSIRT to improve the standard of practice in a constituency, to potentially raise revenue, and for establishing its expert credentials. Even if training courses can be run at cost, sponsored, or subsidised by other services, this may be seen as desirable for a national CSIRT.

Finding subject matter for a training course depends on several factors: the skills sets of the CSIRT's team, the demand for a particular topic, and competition in the market offering similar courses. All of the CSIRTs surveyed offered training courses that were quite diverse.

JPCERT

JPCERT has a special situation, in that their constituency may not feel comfortable operating in the English language that many training providers offer. One unique course they offer domestically is the CERT/CC "Secure Coding" course, a translation of the original English content. They have a specialised team with software development experience that has performed this training at many large corporations such as Nintendo and Sony. By offering such training, they hope to raise the standard of secure software development, and ultimately reduce the number of vulnerabilities introduced into software.

AusCERT

AusCERT has offered many courses over the years, depending on demand and the specialities of the analyst team. In the past, this has included Windows server security, the LAMP stack (Linux + Apache + MySQL + Perl/PHP), and CSIRT establishment. These courses have been toured around Australia, with one to two courses in each capital city.

SLCERT

SLCERT offer a range of both technical and management-level courses.

On the technical level, they have run courses on network security implementation, security in virtualized environments, malware analysis, and secure web application development. On the management level, they have run courses on end-user security best practises, the use of encryption, use of digital signatures, policies and procedures, social engineering, and after changes in laws regarding electronic crime, the cyber crimes act and its provisions.

8.7.2. Media

Media is critical for a national CSIRT to get word out about emerging threats to a mainstream audience, in addition to creating awareness about the CSIRT and its activities. The national CSIRT needs to be the impartial "voice of reason" when new threats are hyped by parties with vested interests. Shying away from the media creates a vacuum that others will fill.

Media can be a double-edged sword, as anyone who has been taken out of context or asked inflammatory questions will attest. Media training is critical to understand how journalists work, how to prepare remarks, and how to handle interviews. In fact, AusCERT requires its staff to go through a one-day media training course before being able to talk to the media directly.

Speaking to the media may be more difficult for a government or regulatory organisation, where comments to the media are treated as official government positions. For those other national CSIRTs who can and wish to speak to the media, staying in journalists' list of go-to experts when widespread incidents occur may help to boost the CSIRT's message and profile.

8.7.3. Teachable moments

A method believed highly effective at imparting knowledge is to deliver it at the moment it is needed. Broad information focused on future prevention and worst-case scenarios may be easily dismissed or forgotten, but presenting information security training information at the moment of a real or simulated impact is said to greatly improve retention.

One example of this is the Anti-Phishing Working Group's landing page project. This seeks to replace active phishing sites with information for victims about the fraudulent nature of the page they just tried to visit, and how to avoid such falling for such scams in the future. Naturally, this relies on willing ISP staff or web site owners to upload the page on to the previously compromised server. However, it is a good example of not just remediating a problem, but exploiting the opportunity to educate and improve the root cause at the same time.

9. Support functions

9.1. Software development

Internal software development is a sometimes overlooked, but important role in any CSIRT. The ability to develop ad-hoc scripts to support incident response, as well as develop major systems to automate CSIRT operations, is a major asset. Potentially, a full or part-time developer should be one of your first hires.

The national CSIRT and IR space tends to heavily favour open source server software running on any flavour of Linux. Python is currently widely used for both lightweight scripting and complex systems, followed by Java and C/C++. The early hire of a Python-fluent developer is recommended to give enough flexibility to handle most software development needs when starting out. Having domain knowledge of incident response, security, and networking is naturally highly advantageous.

The physical environment for software developers in a CSIRT can be a difficult one. A CSIRT operations room can be a noisy environment, and unconducive to the extended concentration required for software development. You may wish to consider allowing an isolated area that software developers can focus, away from the constant bustle of incident response. It may also be useful to establish a policy of guaranteed, interrupt-free time for the development team, in which they cannot be casually approached with requests.

9.2. Liaison

Solving deep technical problems, as opposed to encouraging inter-organisational co-operation, are very different skill sets. With any luck, some of your initial staff members may be able to do both, but you may wish to hire staff with the explicit objective of liaising between players in an industry to bring them together. CERT Australia has had some successes here in their focus on critical infrastructure-related industries, which bridge the gap between traditionally secretive sections of the government and industry.

9.3. System administration

CSIRTs are not quite ready (or willing) for the cloud

Outsourcing systems hosting and management might have increased dramatically in popularity of late, but an unscientific poll of national CSIRTs shows that most still employ their own system administrators and have their own small data centre for most functions (web sites and DDoS mitigation possibly being exceptions to this).

CSIRTs, as "leading lights" in information security, are especially conservative when it comes to relinquishing control of their own systems. The highly sensitive nature of incident data received, and resultant loss of trust that would result from a data breach, means that data is often secured more tightly than is available from an outsourced provider. Finally, securing and administrating systems in-house ensures that the team maintains a practical knowledge of technology choices and threats, rather than outsourcing this expertise elsewhere.

9.4. Admin

Like any organisation, a new CSIRT will need all the administrative functions of any organisation, like human resources, budgeting, procurement, and hiring. This might be done by standing up an administration section within the CSIRT proper, or relying on a parent organisation to supply this for you.

10. Personnel and environment

10.1. Operational teams and environment

Setting up a shared operations room allows great communication, but gets harder with growth. Non-operational staff may find an operations room unproductive to work in.

In the author's experience, CSIRT technical staff members are often highly independent, and can benefit from a free-flowing environment that provides space for interaction.

AusCERT case study

AusCERT, being a small, monolithic team (approx. 15 people total, with around 5-7 analysts), is able to have all analysts in a single room. This comes with the major advantage of analysts of different functions being aware of all ongoing incidents, with the downside of a lot of environmental noise.

On the whole though, this approached worked quite well, and was fundamental in being able to perform role rotation (to be covered further in "Personnel").

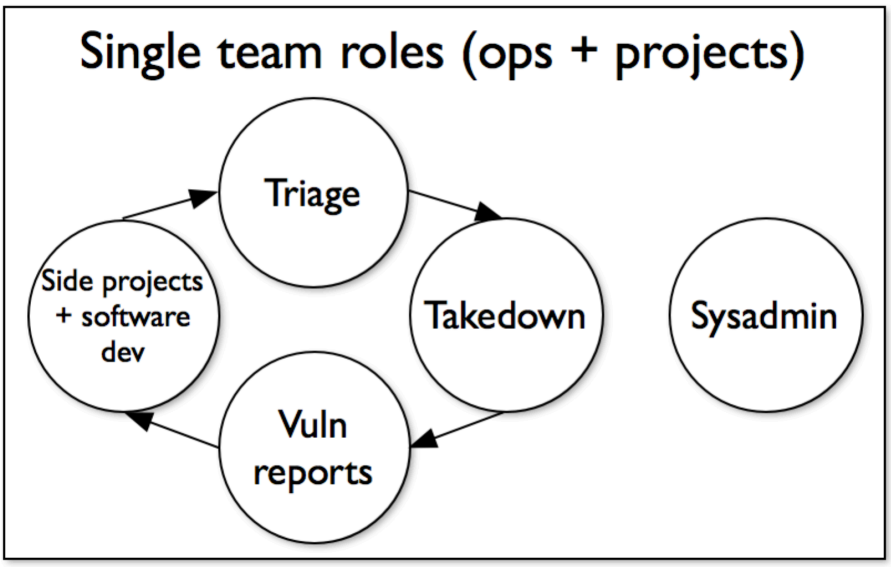


Figure 10: Monolithic, single pool model, with rotating roles

AusCERT has experimented with multiple models since this monolithic model. It employed a "pool" system previously; pool 1 being operational roles (incident response, vulnerability bulletin publishing) and pool 2 being short to medium term projects (software development or research). This model allowed the flexibility of rotating people off project roles and back on to operational roles as absence or demand changed. However, the fact that favoured project time could not be guaranteed sometimes caused resentment as a project was put on hold to refocus on IR triage.

The current AusCERT model uses two dedicated teams: an operations team, and a development / sysadmin team. Both of these teams are in close proximity, but this division still creates a gap in understanding between the needs and conditions each team operates under. This situation is common for any growing organisation, however.

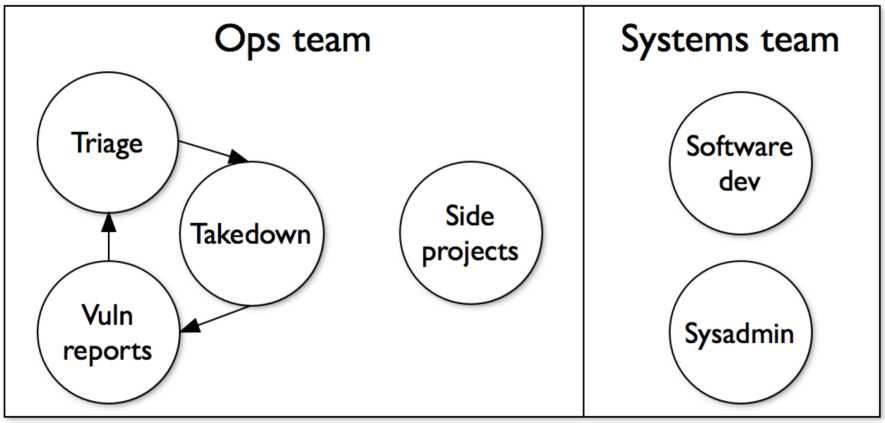


Figure 11: Ops team and systems team model

JPCERT case study

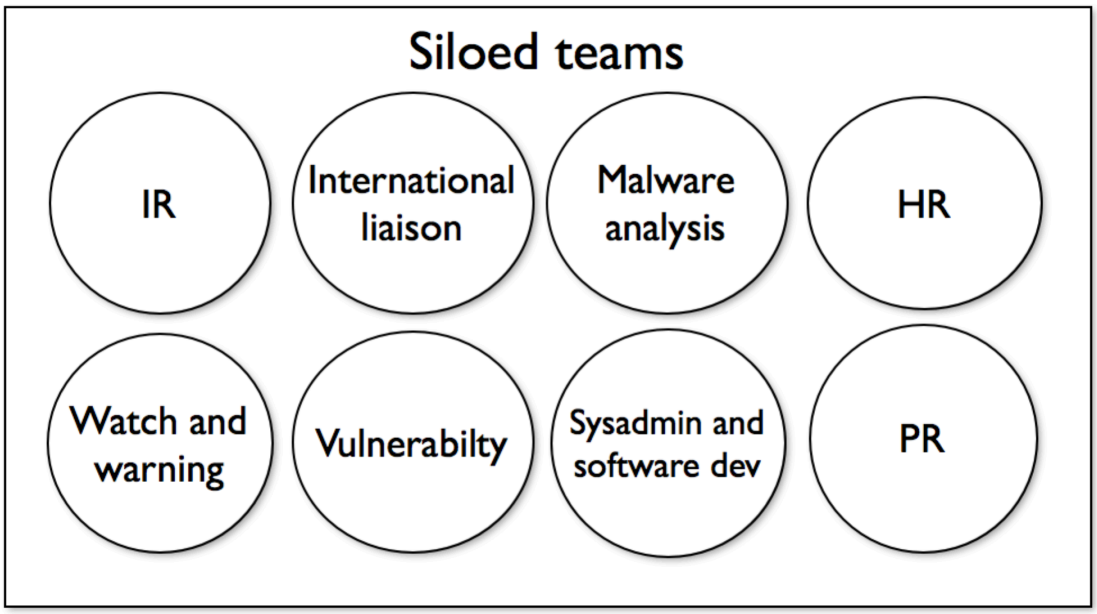


Figure 12: Siloed team model

As an organisation of over fifty people, JPCERT faces different operational team issues. JPCERT at one point embraced a strict silo culture. Each technical team was strictly segregated both geographically and culturally, by virtue of some of the teams operating under heavy confidentiality. This created the conditions of being almost a cluster of micro-organisations, rather than teams in the same organisation.

JPCERT has since moved to a model with all technical staff being located in the same large room, allowing cross-pollination between teams. Some confidentiality constraints necessarily remain, but higher levels of professional and social interaction between teams is encouraged.

SLCERT case study

SLCERT divides their staff into three teams: proactive (essentially consultancy), responsive (IR and forensics), training and awareness. This helps prevent the more chaotic IR team environment from affecting the more single-focused consultancy team.

10.2. Technical skills to hire for

Generalists with one or two specialist domains make good candidates.

One of our experts stated that if they could hire five analysts for a new CSIRT, they would prioritise:

- *Three analysts.* These analysts should be versatile generalists, as a small CSIRT team is expected to cover a multitude of technical and non-technical domains. They should have strong backgrounds in networking, and range of ecosystems on one or more major operating systems.
    - Ideally, one of these analysts will have worked at an ISP. As well as having a strong networking background, this will help the team

understand incidents from the perspective of network providers, along with bringing in pre-formed relationships with ISPs.
    - Another of these analysts should have strong web application or web application security skills. Many modern attacks target the browser, and being able to analyse and disable web site attacks is a highly visible, high worth activity.
- *Developer.* CSIRT need endless amounts of scripting, tools, and systems to improve automation, and so having a developer in-house who understands the IR environment can be very helpful. It may also be helpful to cross-train the developer in incident response, both for redundancy of roles, as well as the developer having a first-hand understanding of the team's operations.
- *Malware analyst.* Malware analysis has become a highly valuable skill for a CSIRT's constituents, who may not have such skills in-house. Many attacks hinge on sophisticated malware, and deep analysis is crucial for effective mitigation. Any malware analyst hired should ideally have static analysis skills, as well as experience with targeted attacks / APTs.

10.3. Personality types and soft skills to hire for

You can arm someone with knowledge, but it's difficult to teach independence and creativity.

If we work with the model of a CSIRT being a relatively small and flat organisation, we need to be very careful in our hiring. A single bad choice can drastically change the cultural balance of an organisation, so you might say that the first thing we often subconsciously hire for is a cultural fit.

Here are some attributes observed in successful CSIRT staff members by our expert panel:

- *Creativity*. It's easy enough to train someone to manually process one hundred web site defacement incidents, but you really want to hire the person that develops a far more efficient, automated way to get to the same outcome. Creativity often ties in very well with problem solving, and looking into the underlying malicious techniques used in incidents beyond just resolving them.
- *Problem identification and analytical thinking.* Some classes of incidents aren't reported, but come from a realisation following a new vulnerability report or seemingly unrelated incident observation.
- *Independence.* Successful CSIRT staff often work under very little supervision, and are given high autonomy to solve problems with a loose set of constraints. They are often motivated by the intrinsic challenge of resolving incidents and problems, or by the mission of improving network security.
- *Someone who will "have a go".* Many of the techniques and tools used in CSIRTs are immature, and are constantly being developed. The ability to experiment with new ideas and techniques to improve the art of incident response is highly prized. Many ideas won't be used long term, but each small step takes a team closer to a workable solution.

- *Willingness to learn.* As anyone working in the information security field may attest, the new threats for we focus on now are different to those we focused on five years ago, which are different again to ten years ago. CSIRT staffers must continually retrain, read widely, and keep learning.
- *Practicality.* Much of incident response is a "best effort" basis. Few incidents are resolved to a perfect conclusion, so an incident handler needs to know when further efforts will only produce diminishing returns. A perfectionist may become quite frustrated with the frequent lack of closure and ambiguity.
- *Personable with soft skills.* Incident response necessitates working with other parties such as reporters, ISPs, and other CSIRTs. Technical skills are essential, but high communication skills in writing and presenting, as well as the ability to co-operate well with others, turns a solid technologist into a very effective CSIRT staffer.
- *Ability to task switch.* In a small CSIRT operations group, tasks may change from hour to hour, given priorities. The ability to change from writing training materials, to taking down phishing sites, to assisting in co-ordinating an international incident, is crucial.
- *Community-mindedness.* A high proportion of national CSIRT staffers tend to value community projects and co-operation highly.
- *Interest / passion for work.* CSIRT work swings between the deeply interesting and the mundane and routine. To get through the patches of routine work, a passion for information security and incident response are crucial.
- *Trustworthiness.* If the critically important reputation of a CSIRT is only as good as its staff members, this is possibly the most important characteristic for any new staff member.

10.4. Staff considerations and staff retention

Avoid burnout, foster personal growth.

One of our experts observed that CSIRT staff members tend to prioritise their job satisfaction by:

1. Liking and respecting the people they work with;
2. The substance and meaning of the work they do;
3. Money.

Given that many national CSIRTs pay less than positions in the commercial sector, CSIRT staffers are often more driven by doing work they care about with like-minded people they respect.

Many CSIRTs have long-tenured staff, but retention can sometimes be an issue. Burnout and a perceived lack of growth is perhaps a leading issue for those leaving a CSIRT. Incident response can sometimes be thankless, routine work, producing little in the way of measureable, tangible outcomes. One of our experts suggested that all staff members have not only incident response work, but are encouraged to pursue long-term projects with concrete, visible outputs.

Another way to prevent high turnover is emphasising personal growth for staff members. Training and certifications are one way to do this, but offering an annual training budget, or offering to pay for certification costs on a successful result are also attractive.

Additionally, regular conference attendance allows for an increase in personal standing in the international incident response community. These trips may be rotated around to staff members, while trying to get particular staff members to be a fixture in particular communities.

11. Co-operative efforts

International co-ordination is a core function of national CSIRTs. Here, we list some suggestions for groups a New Zealand national CSIRT may want to be involved with.

11.1. FIRST

FIRST is likely well known to many information security practitioners in New Zealand. It has become a fairly broad church in recent years, and is a little North American-centric, but is the premiere international community for CSIRTs. Their annual conference is valuable, and the national CSIRT workshop that often takes place in the same week is especially relevant.

11.2. APCERT

APCERT takes its membership from the Asia Pacific, and the New Zealand national CSIRT will likely want to actively participate. As well as running an annual conference, there are also a variety of research projects (e.g. Tsubame passive sensor network, IFAS data feed aggregation project, incident report sharing project) that are conducted between APCERT members.

11.3. Operational mailing lists

There are a variety of operational mailing lists run by the international incident response community, which are often highly vetted. Compared to public information security groups, these groups often have an excellent yield of highly relevant incident response information, as well as being a great place to know influential network operators, CSIRT personnel, and researchers around the world.

Vetting is usually performed on a personal rather than organisational level, meaning that membership transfers after job movements. A healthy proportion of potential national CSIRT staff member candidates in New Zealand already have membership to some of these lists, and if not, may confer with international colleagues to ask for vetting.

11.4. Other national and organisational CSIRTs

Outside of formal organisations like FIRST and APCERT, many CSIRT to CSIRT trust relationships are peer to peer. Often, they are formed as a result of meeting at conferences and finding shared project objectives, or as a result of successful or ongoing incident response.

When responding to incidents internationally, never feel shy about CC-ing the relevant national CSIRT into the request. As well as keeping other national CSIRTs in the loop of incidents in their own constituencies, they may also be able to assist with language translation or the most effective local contacts, as well as continuing to foster relationships that will be useful during high-priority events.

11.5. Domestic CSIRT associations

A domestic CSIRT association is a valuable resource, and New Zealand has been ahead of the curve for some time here with the NZITF.

The geographic centralisation of a group's members is key, according to one of our experts. Face to face time is vital, and so regular meetings and social events in cities where members reside helps to keep the group relevant.

11.6. Joint operations centre

Housing representatives from multiple agencies and organisations in one room can be an excellent way to break down barriers. The Australian High Tech Crime Centre did some pioneering work in Australia by bringing together the Australian Federal Police and technical staff from financial institutions, and today, the Cyber Security Operations Centre (CSOC) brings together staff from many federal agencies, including CERT Australia and the Australian Signals Directorate (ASD).

Establishing such a centre can be expensive and require a degree of political will, but daily face-to-face contact is a highly effective way to increase inter-agency cohesion.