Help us **defend** New Zealand

NZITF

CSIRT NZ

Partnership Information Pack

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

Help us **defend** New Zealand

We invite you to partner with us to help defend New Zealand.

We are creating a **ground-breaking** nationwide **Computer Security Incident Response Team (CSIRT).**

This CSIRT will be unique in New Zealand with a focus on supporting small and medium sized private sector companies and non-profit organisations.

New Zealand's **Problem**

New Zealand businesses want an independent, expert information security voice they can call on for help.

Most organisations, unless you are a government agency, critical national infrastructure or <u>really</u> large, **don't have anyone to turn to** when they have a cybersecurity incident.

NZITF

NEW ZEALAND INTERNET TASK FORCE

The **NZITF** is a not-for-profit organisation with the mission of improving the cybersecurity posture of New Zealand.

The Task Force is a forum based on mutual trust used for debating, information-sharing, collaborating and networking on matters relating to the cybersecurity of New Zealand.

Members come from the security community across government, law enforcement, academia and private sector industries, including telecommunications, information technology and financial services.

ANZIA
AUSTRALIA & NEW ZEALAND INTERNET AWARDS
2012 Security and Privacy - Highly Commended

connect SMART
Protect yourself online
PARTNER 2015/16

WINNER
AUSCERT 20 years
AWARDS 2013
Best Security Initiative

Does New Zealand need a CSIRT?

We think so.

The cybersecurity threat landscape is ever changing and growing. The GCSB saw a rise in computer security incidents reported from 147 in 2014 to 132 for the 1st half of 2015. Digital harm related incidents reported to Netsafe rose from 452 for January 2015 to 1210 for September 2015. The majority of which Netsafe dealt with as there was no other computer security experts to help the person in need.

According to Mandiant's Regional Advanced Threat Report: Asia Pacific 1H 2015, regional organizations are 45% more likely to be attacked than the global average.

+100%

Increase in reported incidents
2014 -2015
GCSB

+300%

Increase in reported incidents
Netsafe

NZITF

New Zealand **needs** a CSIRT

Most kiwi businesses **don't know who to contact** to help them figure out if they have been compromised and give them the advice they need to become more secure.

101 countries worldwide have national CSIRTs in operation[1].

New Zealand's top 10 trading partners[2] all have national CSIRTs able to help businesses and non-profit organisations.

[1] National CSIRTs
[2] Top 10 NZ Trading Partners

What is a CSIRT?

A **Computer Security Incident Response Team** (CSIRT) exists to help individuals and organisations that are impacted (or likely to be) by some type of cyber security incident. They may have been hacked by criminals, are suffering a denial of service attack or are dealing with any other kind of cybersecurity threat (e.g. ransomware).

CSIRTs come in all shapes and sizes and serve diverse constituencies. Some CSIRTs support an entire country, others may provide assistance to a particular region, and some provide support to a particular university or commercial organisation.

Proof of Concept

New Zealand Internet Task Force (NZITF) are building a proof-of-concept CSIRT that will help businesses and non-profit organisations defend themselves.

The NZITF has the expertise, relationships and trust-model to create a useful, operational team that can make a meaningful difference to New Zealand's cybersecurity.

Our members receive the collective benefits We want to build on our experience in coordinating nation-wide drives to address insecurity (e.g. open resolvers), conduct breach notification and leading on vulnerability disclosure.

We want your help to make a CSIRT a reality.

Starting with a **proof of concept CSIRT**

The best way to go about getting a national CSIRT that delivers incident response capability AND proactive security outreach is by doing it. Now.

Build off the NZITFs skills, experience and trust-relationships to create a small, dedicated, resource to find, and fix computer security incidents in NZ.

Focus on supporting small and medium sized organisations, including companies, NGOs and community organisations with under 200 employees[1].

This proof of concept CSIRT will run for up to a year, provide a core suite of defined services to small and medium sized organisations, and be governed by a set of agreed principles.

[1] ConnectSmart week 2015 was focussed on small-to-medium businesses. https://www.connectsmart.govt.nz/

Why a Proof of Concept?

A proof of concept allows us to find out:

- *What type of CSIRT does NZ need?*
- *What services should it offer?*
- *Which industries or sections of NZ need the most help?*

The results will be used to help NZ Government and industry identify what is required to run a permanent national CSIRT, and what cybersecurity services our small-to-medium organisations need.

CSIRTnz Principles

Our governing principles in seeking to set up CSIRTnz are:

- **Demonstrating the value of a CSIRT**
  Show the value that a dedicated CSIRT resource can bring to New Zealand's Internet-connected businesses and communities.
- **Partnership & transparency**
  Work with everyone who also wants to improve New Zealand's cyber security; be open and transparent about who, why and the nature of the working relationships; publicly share aggregated statistics on what types of threats are seen, what is being done, and the types of incidents occurring.
- **Confidentiality**
  We commit to the need for confidentiality. Incident report details and other private information will be protected and respected.
- **Lean and agile**
  Seek funding to launch CSIRTnz with a small, agile team, supported by NZITF members. Explore what happens next with sponsors and the New Zealand Internet community.
- **Automate**
  Work to automate as much threat information and enable automated information sharing between willing partners as much as possible.

CSIRTnz
Core Services

The following services (as a minimum) are proposed to be provided during the PoC:

- **Incident response**
  Help organisations respond to an incident and put them in touch with the right agencies, experts or organisations if further follow up is needed.

- **Advice**
  Provide advice to partners on common and collective problems. This includes vulnerability disclosure and coordination services to any security researcher.

- **Information & intelligence**
  share proactive intelligence and offer assistance on problems as well as useful information and assistance on how to respond.

- **Reporting**
  Measure, collate and report everything we possibly can.

Join **others**

To make CSIRTnz happen we need funding partners to get people to do the incident response, do the research and improve New Zealand's cyber security posture. There are companies already willing to help us improve New Zealand's cyber security.

If you:

- want to help defend New Zealand
- want to protect your customers
- understand the collective security benefits of a dedicated incident response capability
- have New Zealand based business and non-profits as customers
- want a public CSIRT a reality in New Zealand

…then we want to talk to you about becoming a Platinum, Gold or Silver partner with our proof-of-concept CSIRT.

What **you** will get out of it

Becoming a Platinum, Gold or Silver partner with our proof-of-concept CSIRT gives you multiple benefits:

- Your brand is associated with active security participation
- You can advertise your contribution
- You will get a seat on the Strategic Reference Board (Platinum only)
- You will get to take part in our Partner forums, working with the CSIRT team, and other partners to discuss current security threats and guide the CSIRTnz team's actions each quarter.
- You will help NZ industry defend itself
- We will all learn more about what attackers are doing within NZ
- We will all learn what we need to do to protect ourselves

Other forward thinking New Zealand companies have already signed up…. Will you?

Partnership **Options**

CSIRTnz benefits and expected contributions:

	Silver Partner (limit 10)	**Gold Partner** (limit 5)	**Platinum Partner** (limit 3)
Benefits			
Use of CSIRTnz branding on own collateral	CSIRT.NZ Silver Partner Logo	CSIRT.NZ Gold Partner Logo	CSIRT.NZ Platinum Partner Logo
Have your company's logo and link to your website on the CSIRTnz homepage	✓	✓	✓
Receive regular statistics and updates as well as aggregate customer feedback	✓	✓	✓
Attend and contribute to quarterly Partners Forums to guide CSIRTnz's actions over the next quarter	✓	✓	✓
Offer your business customers CSIRTnz's incident response services as a part of our first wave of private incident response services		✓	✓
Be given the opportunity to have branding at any public events held by CSIRT during the Proof of Concept		✓	✓
Be given the opportunity to speak at any public events held by the CSIRT during the PoC			✓
Able to nominate a member to CSIRTnz's Strategic Reference Group, enabling you to help guide and grow CSIRTnz			✓
Have your company's logo included in all CSIRTnz advisories, releases and publications			✓
Reserved seats at the official launch of CSIRTnz	2	5	10
Contribution			
Funding for the proof-of-concept CSIRT	$10,000 (excl GST)	$25,000 (excl GST)	$50,000 (excl GST)
Follow cyber security best practice and promote this through internal channels/materials including to staff	✓	✓	✓
Promtoe CSIRT messages throughout the proof of concept timeframe	✓	✓	✓
Support CSIRT promotions and messaging through social media	✓	✓	✓
Provide regular input into cyber security events and incidents			✓
Host, or provide the opportunity for, at least one CSIRT event during the proof of concept			✓

Strategic Reference Group

Is made up from Government, NZITF and Platinum sponsors.

Helps guide CSIRTnz, work with us to understand how it should grow and what should happen through a collaborative, multi-stakeholder approach.

SRG decisions are not binding for CSIRTnz, but recommendations are treated very seriously.

SRG members are highly experienced and highly valued so it would be remiss of CSIRTnz, and the NZITF Board, to ignore their counsel.

What happens **In a year?**

CSIRTnz is a proof-of-concept that runs for a **year starting quarter 4.**

NZITF can help support it for a short period of time, but we are a membership organisation, not a service provider.

So what happens at the end of the year when the proof of concept finishes?

It will depend on what we learn during the proof of concept and the value delivered to its constituents. Options will most likely include either continuing to incubate the CSIRT team in the NZITF, move capabilities established into another organisation or everything closed down.

We think that's a decision for industry, civil society, the technology sector, the information security community and government to take together. This is one of the key questions for the Strategic Reference Group to consider.


Help us defend New Zealand
NZITF
Help New Zealand small and medium enterprises and non-profit organisations protect themselves.
CSIRT NZ