# New Zealand's Cyber Security Challenge

## Kestrel Group – 30 June 2015

**Paul Ash**

**Director, National Cyber Policy Office Department of the Prime Minister and Cabinet**

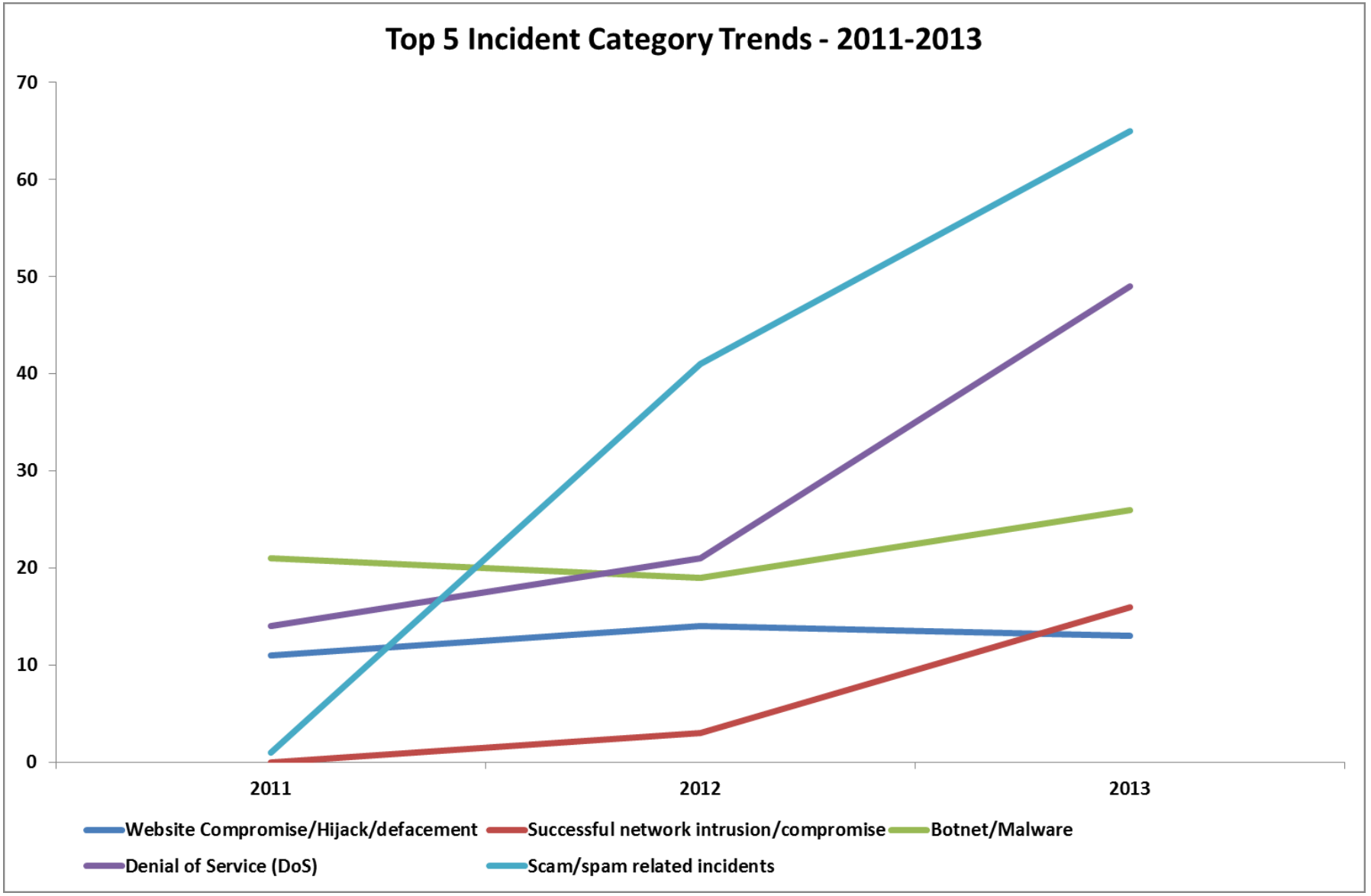
connect SMART
Protect yourself online

newzealand.govt.nz

# NCPO – who we are and what we do

- Small policy team located in the Department of the Prime Minister and Cabinet
- Lead the development of policy advice for government on cyber security
- Advise on investing government resources in cyber security
- Oversee the development of national strategy and policy on cyber security
- Lead international engagement on cyber policy
- Facilitate engagement with the private sector on cyber security issues.
- Lead the government's cyber security awareness programme: Connect Smart

# What's the problem? (1)




Source: NCSC 2013 Incident Summary

# What's the problem? (2)

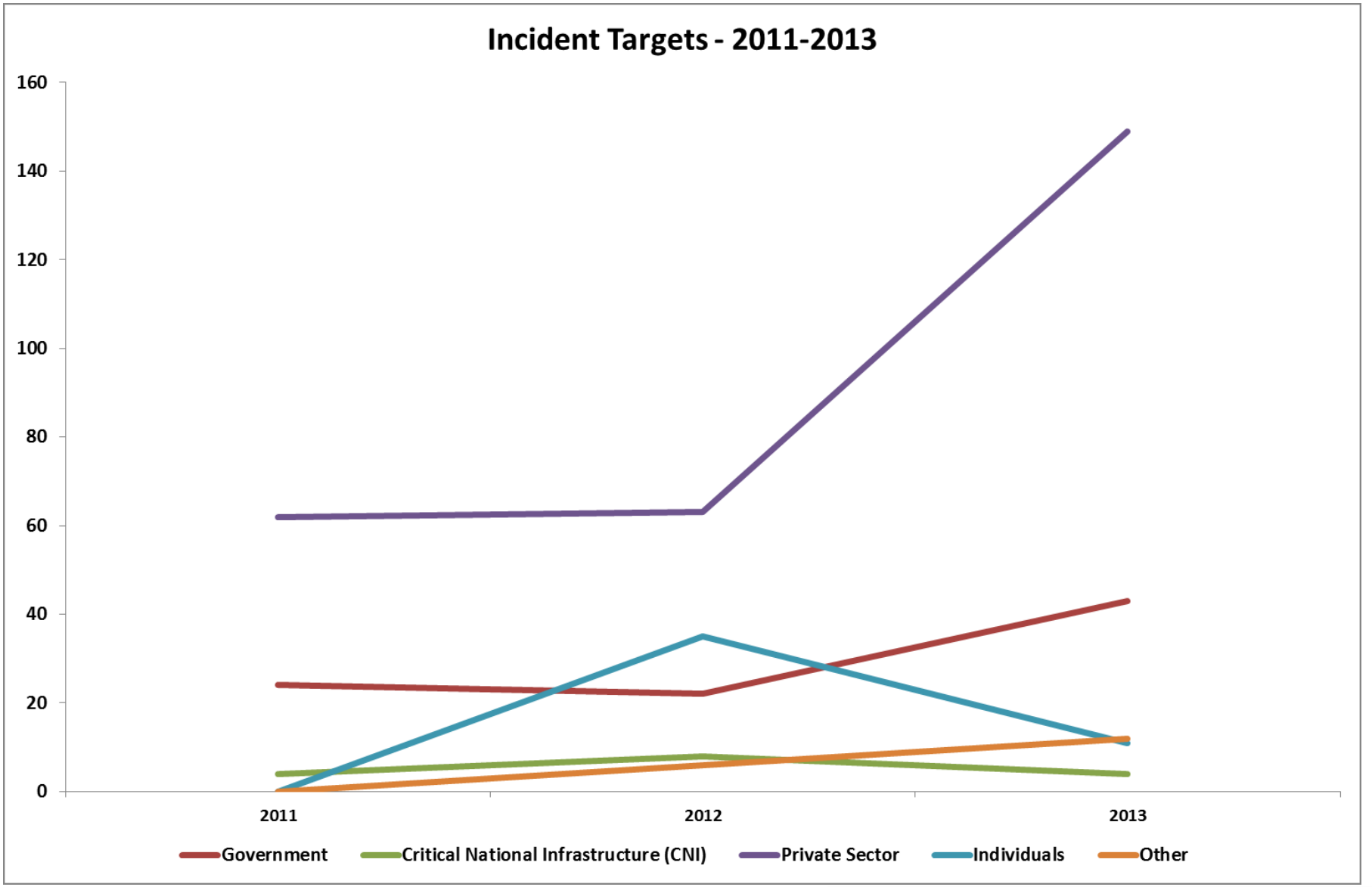
## Actors

- States
- Criminals
- Issue-motivated

## Impact

- Theft: IP or money
- Damage: systems or physical
- Manipulation: changing data
- Fraud, ransomware, DDoS

# Targets




Source: NCSC 2013 Incident Summary

# What's the government doing about it? (1)

- The 2011 Cyber Security Strategy had three priorities:

  1. Increasing awareness and online security
  2. Protecting government systems and information
  3. Incident response and planning

- Since then:

  - GCSB Act: cyber security role
  - TICS Act: network security
  - Establishment of the National Cyber Security Centre in the GCSB
  - CORTEX underway
  - National Cybercrime Centre in the Police
  - DIA and establishment of GCIO and GCPO
  - Emergency response exercises

# What's the government doing about it? (2)

- The threat is evolving and so are we.
- Increasingly working in partnership with the private sector – partnership approach set out in the 2011 Strategy and in establishing NCPO

## Connect Smart

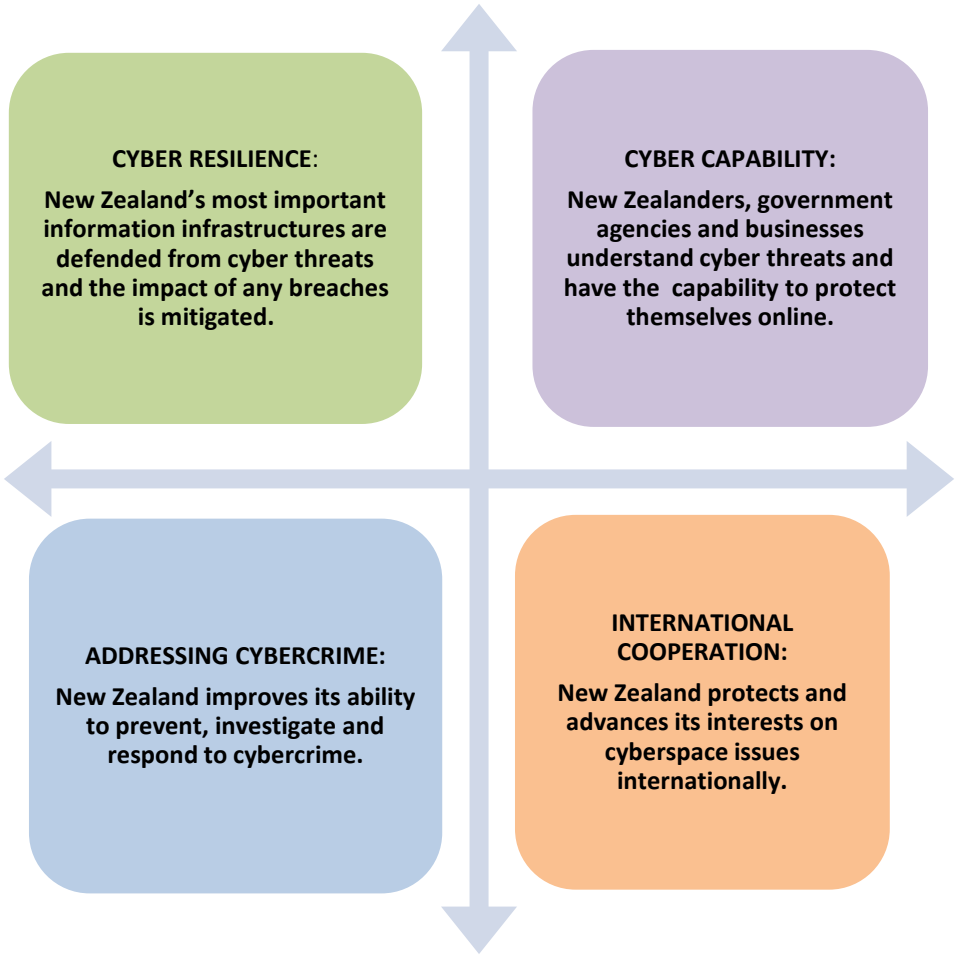
- A growing public-private partnership
- Tailored advice and outreach

## New Cyber Security Strategy

- Making our small size our competitive advantage
- Maximise the collective expertise of government, private sector, NGOs and international partners
- A multi-layered approach to cyber security

# New Cyber Security Strategy

Four intersecting goals:



# New Cyber Security Strategy

Some of the specifics:

## CORTEX

- Protecting New Zealand's critical national infrastructure from highly advanced threats

## A New Zealand CERT?

- A customer-focused entity
- Triage cyber incidents – a place for New Zealanders to go
- Brings together data and expertise from intelligence, international partners, private and NGO sectors
- A trusted clearing-house

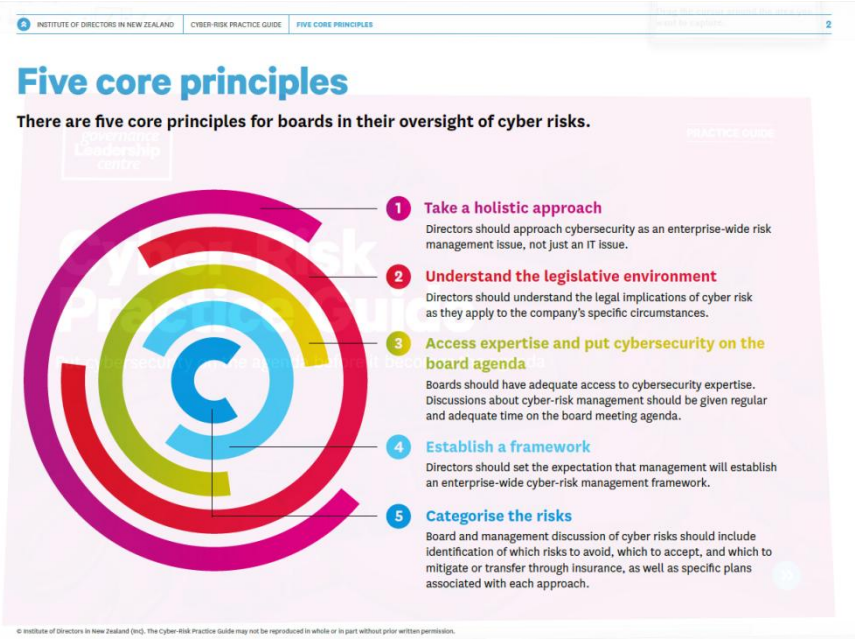
# What's on the horizon?

- The threat landscape will change – a given
- Possible establishment of a NZ CERT – a public private model
- Connect Smart – from an awareness week to a year-round programme
- A public-private cyber security summit?
- Cyber security a factor in economic competitiveness
- Emerging cyber security regulation in key markets:
  - NIST framework in the US;
  - NIS Directive in the EU; and
  - Cyber security legislation in China.

# What do you need to think about?

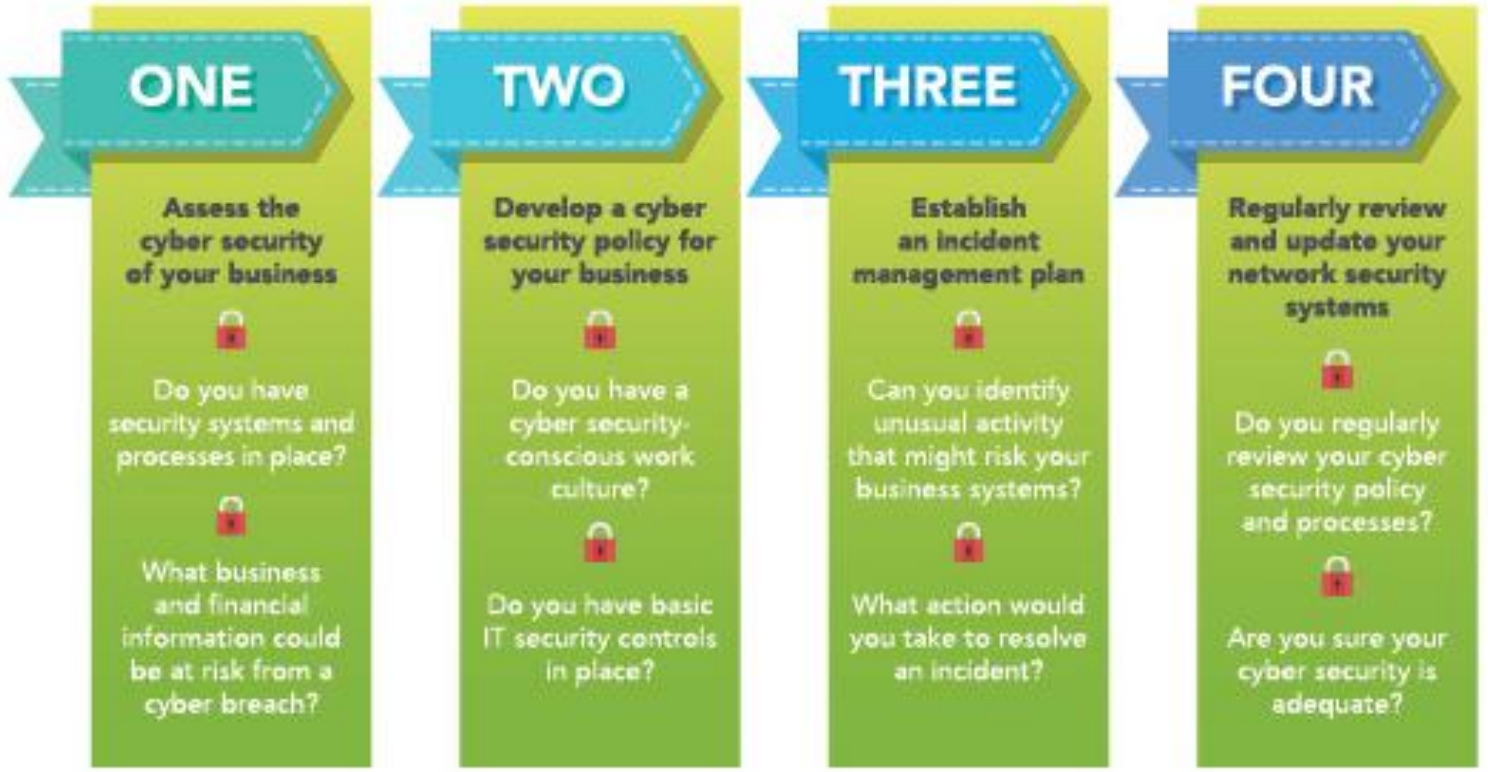
- Connecting the dots from the IT department to the Board

- IoD cyber risk practice guide released this week


- NCSC guidance: “Cyber Security and Risk Management” available at connectsmart.govt.nz

# What can you do when you get back to the office?



# Thank You

www.connectsmart.govt.nz

Twitter: @ConnectSmart NZ

#connectsmart

**Paul Ash**
**Director, National Cyber Policy Office, Department of the Prime Minister & Cabinet**
**Connectsmart@dpmc.govt.nz**

connect SMART
Protect yourself online

newzealand.govt.nz