



Cyber Security

Christchurch & Dunedin client update 6/7 June 2017 –
abridged version

AUDIT NEW ZEALAND
Mana Arotake Aotearoa



analogy



AUDIT NEW ZEALAND
Mana Arotake Aotearoa

Who is responsible anyway ?

We all are

Resources a plenty

- GCSB – NCSC
- CERT NZ
- NETSAFE
- DPMC –NCPO
- IoD
- MoH - DAB
- DIA – GCIO
- MBIE
- NZ Police
- ISACA
- CSX
- Connect smart

cert.govt.nz/businesses-and-individuals/guides/



IT specialists

Businesses and individuals

About

Guides.

Get practical information and advice on cyber security.

Simple steps to cyber security

Keen to know where to start with cyber security? Learn the basics here.



AUDIT NEW ZEALAND

Mana Arotake Aotearoa

connectsmart.govt.nz



Protect yourself online

newzealand.govt.nz

Search the website



[About](#)

[Events](#)

[Homes & Schools](#)

[Businesses](#)

[Alerts/News](#)

[Partners](#)

[Resources](#)

[CERT NZ](#)

Business User?

Learn more about four simple steps that will help protect your business online...



[Find out more »](#)



How Cyber Smart are you?

Take our 10 question multi-choice quiz to learn more about cyber security

[Take the quiz! »](#)

[About](#)

[More about cyber security](#)

AUDIT NEW ZEALAND

Mana Arotake Aotearoa

iod.org.nz/Governance-Resources/

[Governance Resources](#) / [Publications](#) / [Practice guides](#) / [Cyber-Risk Practice Guide](#)

Cyber-Risk Practice Guide

Put cybersecurity on the agenda before it becomes the agenda. This guide provides boards with five useful principles to help them understand and monitor cyber-risk, develop strategies for seeking assurance, and oversee management. It also poses critical questions directors have a duty to ask.

[Getting on board with diversity](#)

[Conflicts of Interest Practice Guide](#)

Cyber-Risk Practice Guide

[Board Meetings Practice Guide](#)

[Farming Directorships](#)

Share on: [Twitter](#) [Facebook](#) [LinkedIn](#) [Google+](#)



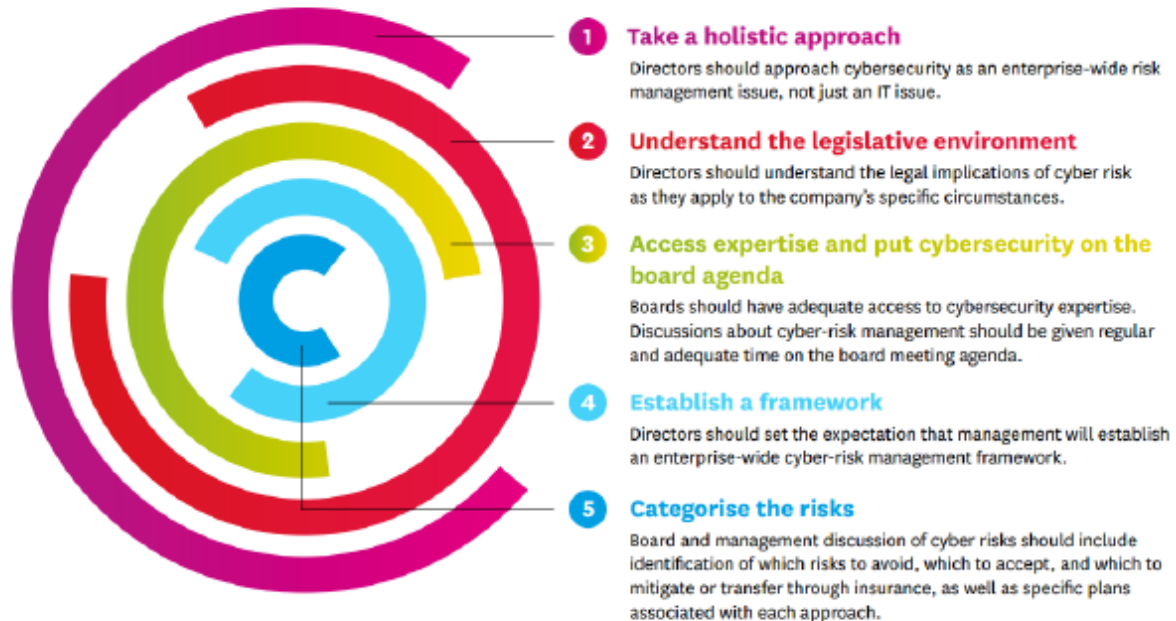
[Download Practice Guide](#) ↓

Director Development
Digital Essentials



Five core principles

There are five core principles for boards in their oversight of cyber risks.



[HOME](#)[ABOUT US](#)[NEWSROOM](#)[INCIDENTS](#)[RESOURCES](#)[TICSA](#)

ABOUT THE NATIONAL CYBER SECURITY CENTRE

The New Zealand National Cyber Security Centre (NCSC) provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.



ABOUT NCSC

The New Zealand National Cyber Security Centre provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.

The Centre is a key element of the NZ Cyber Security Strategy released in December 2015. This strategy recognises that as the use of the internet in New Zealand increases, so too does our vulnerability to cyber threats.

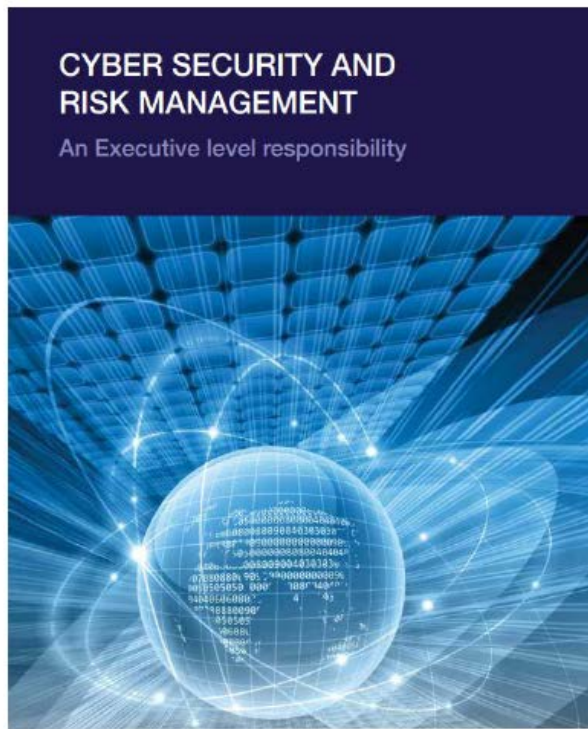
Countering these threats is a shared responsibility, and the government will work in partnership with industry, non-government entities and academia to improve New Zealand's cyber security. The role of the NCSC is to protect government systems and information, to plan for and respond to cyber incidents, and to work with providers of critical

ABOUT THIS SITE

This site is the primary publication medium for official information relating to the National Cyber Security Centre (NCSC).

All facts, figures, statements, publications and advisories made available through this site are accurate at the time of publishing.

NCSC guide



Cyberspace poses risks as well as opportunities

Cyber security risks are a constantly evolving threat to an organisation's ability to achieve its objectives and deliver its core functions.

Security failings in today's information-driven economy can result in significant long term expense to the affected organisations and substantially damage consumer trust and brand reputation. Sensitive customer information, intellectual property, and even the control of key machinery are increasingly at risk from cyber attack. The targeting of electronic assets has the potential to make a material impact on the entire organisation and possibly its partners.

The topic of cyber security needs to move from being in the domain of the IT professional to that of the Executive and Board, where its consideration and mitigation can be commensurate with the risk posed. The traditional approach to thinking about cyber security in terms of building bigger walls (firewalls and antivirus software) - while still necessary - is no longer sufficient. A holistic approach to cyber security risk management - across the organisation, its network, supply chains and the larger ecosystem - is required.

This document provides key questions to guide leadership discussions about cyber security risk management for your organisation. They are intended to be non-prescriptive, as organisational context will vary.

This publication incorporates work originally researched, drafted and published by our international partners (Australian Defence Signals Directorate, Her Majesty's Government of UK (Crown Copyright), US-CERT). It has been reproduced with permission and any changes have been made at the discretion of the NCSC. As this publication notes, even well-defended organisations may experience a cyber incident at some point. This publication controls, and does not, offer any insurance against such incidents. Organisations are urged to seek professional advice in addressing the risks identified here. This publication is not intended to be a substitute for that.

ICT.govt.nz Contact us 

[Governance and Leadership](#) [Strategy and Action Plan](#) [ICT System Assurance](#) [Guidance and Resources](#) [Products and Services](#) [Programmes and Initiatives](#) [News and Updates](#)

Governance and Leadership

[Home](#) » [Governance and Leadership](#) » [The GCIO Team](#)

The GCIO Team

Providing ICT Functional Leadership

The GCIO Team

Government Chief Technology Officer

Government Chief Privacy Officer

System Transformation

Relationship Management

The Government Chief Information Officer is supported by a team of people across the Department of Internal Affairs, and you can find out what they do and how to contact them in this section.

Agencies across government also contribute to, and in some cases lead, development of the work programme.

If in doubt, contact the Relationship Management team or email gcio@dia.govt.nz

netsafe.org.nz/advice/business/

[ABOUT US](#) [REPORT](#) [OUR WORK](#) [CONTRIBUTE](#) [CONTACT US](#)



[Report Online Incidents](#)

[Online Bullying & Harassment](#) [Scams](#) [Security](#) [Parenting](#) **[Business](#)** [Educators](#) [Young People](#)

POSTS IN CATEGORY

BUSINESS



[BUSINESS](#) [HOW TO](#) [SECURITY](#)

**PREVENTING RANSOMWARE
ATTACKS**



[BUSINESS](#) [SCAMS](#)

**'SOCIAL ENGINEERING'
DEMYSTIFIED**

KEEP UP WITH NETSAFE

Subscribe to our mailing list

* indicates required

Email Address *

First Name

Last Name

AUDIT NEW ZEALAND

Mana Arotake Aotearoa



Search

HOME	ABOUT DPMC	CABINET OFFICE	GOVERNMENT HOUSE	NATIONAL SECURITY AND INTELLIGENCE	MINISTRY OF CIVIL DEFENCE & EMERGENCY MANAGEMENT	POLICY ADVISORY GROUP	GREATER CHRISTCHURCH GROUP	CONTACT US	
------	------------	----------------	------------------	------------------------------------	--	-----------------------	----------------------------	------------	--

IN THIS SECTION

- » NZ Intelligence and Security Bill 2016
- » New Zealand Intelligence Community
- » National Security
- » National Security governance structure
- » New Zealand's National Security System during a crisis
- » **DPMC's Security and Intelligence Group**
 - » National Assessments Bureau
 - » **National Cyber Policy Office**
- » National Exercise Programme

CONTACT DETAILS:

National Cyber Policy Office
Pipitea House
1-15 Pipitea Street
Thorndon
WELLINGTON
Phone: (04) 819-8200
Email: contact form

NATIONAL SECURITY AND INTELLIGENCE » DPMC's Security and Intelligence Group » National Cyber Policy Office

NATIONAL CYBER POLICY OFFICE

The National Cyber Policy Office (NCPO) was established in 2012. NCPO leads the development of cyber security policy advice and provides advice to the government on investing in cyber security activities, including the CERT (Computer Emergency Response Team). The Director of the NCPO is Paul Ash.

NCPO formally reports to the Minister for Communications on cyber security policy matters, in consultation with the Prime Minister, as the Minister for National Security and Intelligence, and other Ministers as appropriate.

A refreshed New Zealand Cyber Security Strategy, accompanying Action Plan, and a National Plan to Address Cybercrime, were released on 10 December 2015 and replace New Zealand's 2011 Cyber Security Strategy.

This new Strategy signals the Government's commitment to ensuring New Zealand is secure, resilient and prosperous online. The Strategy has four principles:

- partnerships are essential
- economic growth is enabled
- national security is upheld
- human rights are protected online.

The Strategy has four intersecting goals.



business.govt.nz/news/webinar-keeping-your-small-business-safe-online/

Search



business.govt.nz

Webinar: Keeping your small business safe online

More than half of New Zealand businesses experience security attacks at least once a year. But many feel they don't have the right tools and policies to protect themselves.

Help is at hand. Here are tips and resources recommended by our panel of experts to protect your business from scams and hack attacks.

[Ifraud](#)
[eek](#)

Experts from the private sector and government agencies offered tips and advice in a web seminar hosted by business.govt.nz and the Ministry of Business, Innovation and Employment's digital economy team.

Below are some other resources mentioned during the MBIE web seminar:

Recommended online resources

Organisation	Includes information about:
CERT NZ — national cyber security response team	<ul style="list-style-type: none">• Reporting cyber security problems• Online security advice for businesses
Digital Journey's Cyber Security Tool	<ul style="list-style-type: none">• Online assessment of your business's cyber security — and what

[Related content](#)

[Home](#) » [Advice](#) » [Email and Internet safety](#) » [Electronic crime – what it is and how to report it](#)

[Advice](#)

[Email and Internet safety](#)

Electronic crime – what it is and how to report it

[About malware](#)

[Online child safety](#)

[About online identity theft](#)

[About Internet scams, spam and fraud](#)

Electronic crime – what it is and how to report it

Electronic crime, also known as e-crime or cybercrime, refers to criminal activity that involves the Internet, a computer or other electronic devices.

Some e-crime relates specifically to computers, such as distributing damaging electronic viruses or launching a denial-of-service attack which causes a computer system to deny service to any authorised user.

Other examples include fraud, harassment, copyright breaches and making, possessing or distributing objectionable material such as child pornography.

On this site are some common forms of e-crime that you may encounter and advice on what to do to protect yourself against them.

- [Malware](#)
- [Internet scams and fraud](#)
- [Online child safety](#)
- [Online identity theft](#)

On this page

- [Mobile phone usage](#)
- [Reporting electronic crime](#)
- [How to protect yourself and your family from e-crime](#)

Related information

[NetSafe - The Orb website](#)

[Keep your children safe](#)

Frequently asked questions

Home →

What You Need To Know

Protective Security Requirements – an overview

The Protective Security Requirements (PSR) outlines the Government's expectations for managing personnel, physical and information security. The PSR will better help you manage business risks and assure continuity of service delivery. The PSR clearly sets out what agencies must and should consider to ensure they are managing security effectively.

Implementing the PSR will enable agencies to assure the Government and the public they have appropriate and effective measures in place to protect New Zealand's people, information and assets.

The PSR is organised into a four-tier, hierarchical structure.

Tier one – the Government's directive on the security of government business.

Tier two – the core policies and mandatory requirements agencies must implement to ensure a consistent and controlled security environment throughout the public sector.

[Directive on the Security of Government Business](#) →

[Introduction and Overview to the PSR](#) →

[Strategic Security Objectives, Core Policies and the Mandatory Requirements for Agencies](#) →

[Glossary](#) →

gcsb.govt.nz/publications/the-nz-information-security-manual



GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

[About us](#) [Our work](#) [NCSC](#) [Working for us](#) [Publications](#) [Contact](#)

[Home](#) / [Publications](#) / [NZ Information Security Manual \(NZISM\)](#)

NZ Information Security Manual (NZISM)

Introduction

Safe, secure and functional information systems are vital for the successful operation of all government organisations. These systems underpin public confidence, support privacy and security and are fundamental to the effective, efficient and safe conduct of public and government business.

The consequences of a security lapse can be significant, regardless of where in an organisation it occurs or how severe it is. These consequences can damage an organisation's reputation, undermine public confidence and cause significant damage to information systems. The damage can be intensified where a single system is used by multiple agencies.

Governance, assurance and risk

IN THIS SECTION

[Annual reports](#)

[Chief Executive expenses](#)

[News](#)

[NZ Information Security Manual](#)

PUBLICATIONS



The screenshot shows the website for the National Health IT Board, specifically the page for the Health Information Standards Organisation (HISO). The page features a navigation menu, a search bar, and a main content area with a sidebar on the left and a news section on the right.

NATIONAL HEALTH IT BOARD

ConnectedHealth
My information. Better care.

About this site Accessibility

Type your search query here Search

About us Health IT Programme Who we work with Our programmes Patient portals Standards News & events

Home / Who we work with / HISO

Who we work with

- National Information Clinical Leadership Group
- Consumer Panel
- Telehealth Forum
- HIGEAG
- HISO**
 - About HISO
 - Committee members
 - Publications
 - Terms of reference
- Health IT Cluster
- Sector Architects Group

Health Information Standards Organisation (HISO)

The Health Information Standards Organisation (HISO) supports and promotes the development and adoption of fit-for-purpose health information standards for the New Zealand health system.

The Health Information Standards Organisation (HISO) supports and promotes the development and adoption of fit-for-purpose health information standards for the New Zealand health system.

HISO works with health provider and shared services organisations, clinical and consumer groups, software vendors and industry bodies, the academic community, the wider government sector and other standards development organisations. HISO links with the international standards community through the International Health Terminology Standards

HISO news

- HISO 10023:2015 Project for the Integration of Mental Health Data (PRIMHD)
30 July 2015
- HISO 10052:2015 Ambulance Care Summary Standard
28 May 2015
- HISO 10029:2015 Health Information Security Framework
09 December 2015

Related pages

- Approved standards
- Endorsed standards

ISACA
Trust in, and value from, information systems

Support Shopping Cart Join ISACA Sign In ENGLISH

ISACA My ISACA Site Content SEARCH Advanced Search

ABOUT MEMBERSHIP CERTIFICATION EDUCATION COBIT KNOWLEDGE & INSIGHTS JOURNAL BOOKSTORE

CSX CYBERSECURITY NEXUS Insights and resources for the cybersecurity professional from ISACA LEARN MORE >

ISACA > About ISACA share f t in g+ m

About ISACA

As an independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. Previously known as the **Information Systems Audit and Control Association**, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.

- ▶ ISACA Acquires CMMI Institute
- ▶ Bylaws and Articles of Incorporation
- ▶ Annual Report
- ▶ Annual General Meeting
- ▶ History
- ▶ What We Offer & Whom We Serve
- ▶ @ISACA Newsletter
- ▶ Licensing and Promotion
- ▶ Press Room
- ▶ Volunteering
- ▶ IT Governance Institute
- ▶ Contact Us
- ▶ Advocacy

History

ISACA was incorporated in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the growing field of auditing controls for computer systems. Today, ISACA serves 140,000 professionals in 180 countries.

More >>

View ISACA Fact Sheet

What We Offer & Whom We Serve

ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide. The COBIT framework and the CISA, CISM, CGEIT and CRISC certifications are ISACA brands respected and used by these professionals for the benefit of their enterprises.

More >>

Quick Links

I want to...	My Bookmarks	Saved Searches
• Access press releases and fact sheets		
• Learn about ISACA		
• Learn about licensing and promotion		
• Subscribe to @ISACA		
• View ISACA boards and committees		
• Visit the IT Governance Institute		

https://cybersecurity.isaca.org/csx-nexus

The screenshot shows the top navigation bar of the CSX website. On the left is the CSX logo with the text 'CYBERSECURITY NEXUS' below it. To the right are links for 'ENTERPRISE TRAINING', 'SHARE', 'SEARCH', and 'LOGIN'. A 'MENU' button is located in the top right corner. Below the navigation bar, the breadcrumb 'Home > Program Overview' is visible. The main heading is 'CYBERSECURITY NEXUS™ (CSX)'. Below the heading is a descriptive paragraph: 'CSX is designed to help fortify and advance the industry by educating, training and certifying a stronger, more skilled workforce that can keep organizations and their information secure- now and in the future'. The background of this section features a blurred image of computer code.

BUILDING A STRONGER CYBER SECURITY WORKFORCE

CSX will help you gain the knowledge and skills to get the job done and give you the guidance to keep your career moving in the right direction. Our holistic program is designed to help you no matter where you are in your career, and serves as a premier, one-stop source for all things cyber security.

DISCOVER CSX

VIDEOS

NEWSROOM



AUDIT NEW ZEALAND

Mana Arotake Aotearoa

Understand the risks...

- Legal liability
- Third party risk (credit card details etc)
- Intellectual property
- Reputation
- Client details / data
- Financial risk
- Interruption of service
- Non-fulfilment
- Remediation costs

and then manage them

- Treat or minimise
 - Managed security services
 - In-house capability
 - Education
- Transfer
 - Insurance
- Accept
 - Understand what your accepting
 - Business continuity planning

What else

- The basics make a big difference
- Keep improving
 - Measures work best if you and your team remain current
- Educate others
 - Push for improvement internally and externally
 - Your security is linked to that of others

Apple - Siri



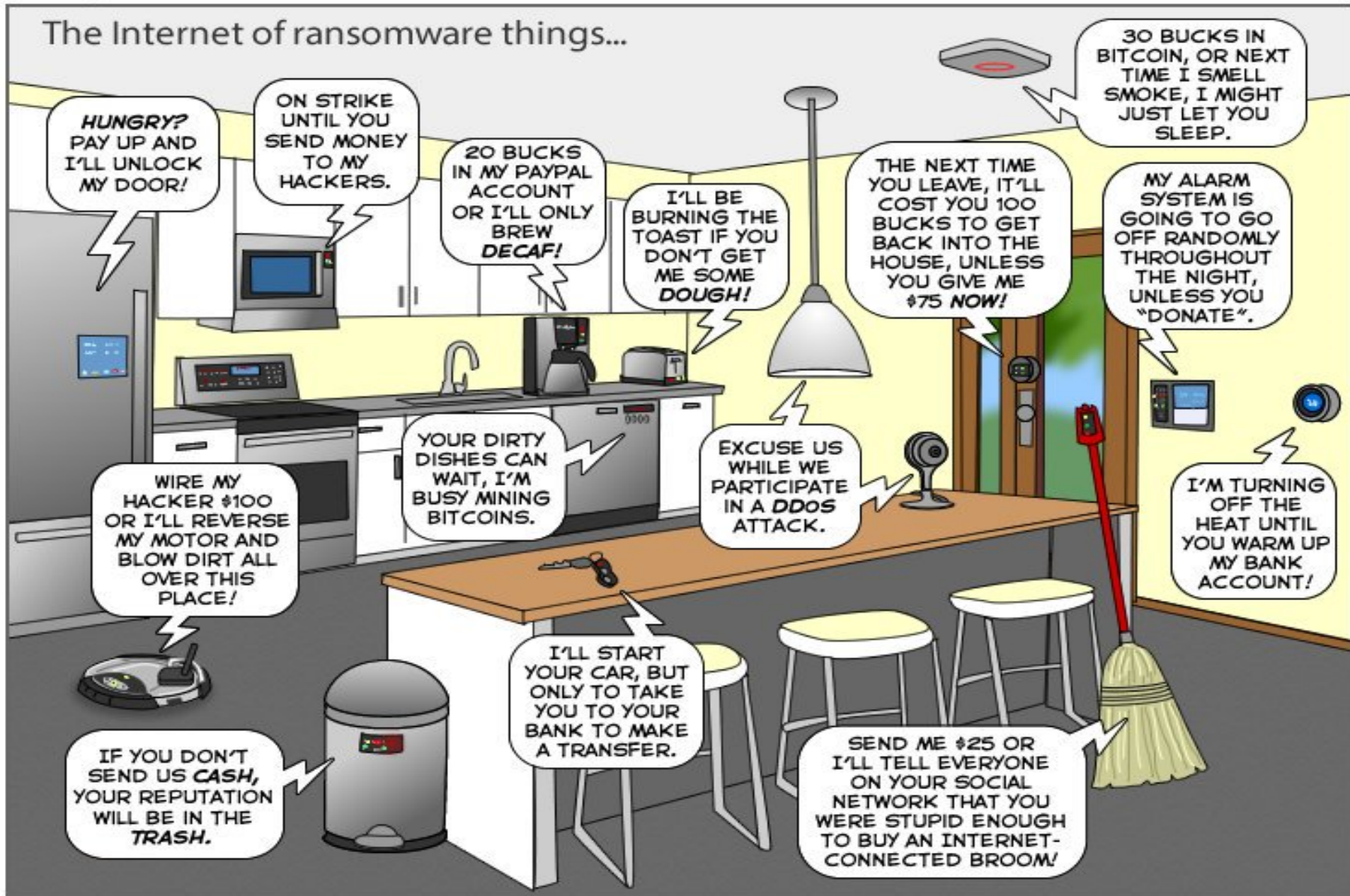
A toaster



IoT toaster



The Internet of ransomware things...



Information systems audit team



Manage security services - scope

- Policy
- Education
- Add/remove/change users
- Password settings
- Unique ids
- Remote access
- Firewalls, intrusion detection
- Periodic user reviews
- Super user
- Domain access
- Events & logs – monitoring
- Detect & protect from malware
- Physical security

Next steps

Take action today

Do not wait until it is too late

Get cyber on your agenda before it becomes the agenda

Educate yourself

Educate your family

Educate your staff & peers

[Do not click that link](#)

Questions?

Alan Clifford – Director, ISAA

Alan.Clifford@auditnz.govt.nz

021 453 351

Many thanks – and good luck