Cyber Security

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

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

AUDIT NEW ZEALAND

Mana Arotake Aotearoa

analogy

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/

certnz

IT specialists | Businesses and individuals | About

Guides.

Get practical information and advice on cyber security.

Simple steps to cyber security

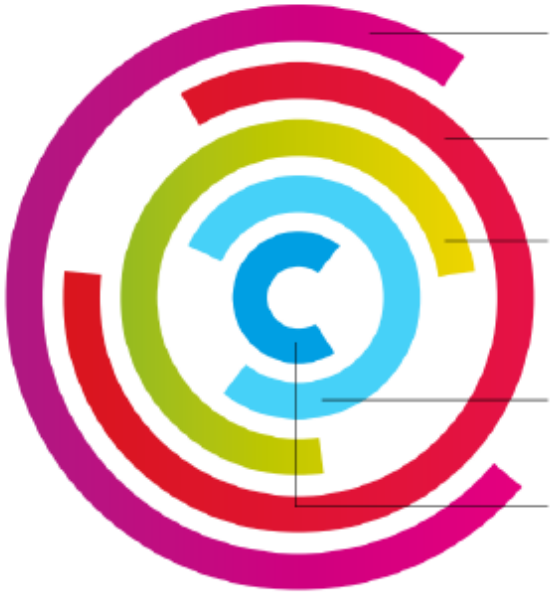
Keen to know where to start with cyber security? Learn the basics here.

connectsmart.govt.nz

iod.org.nz/Governance-Resources/

Five core principles

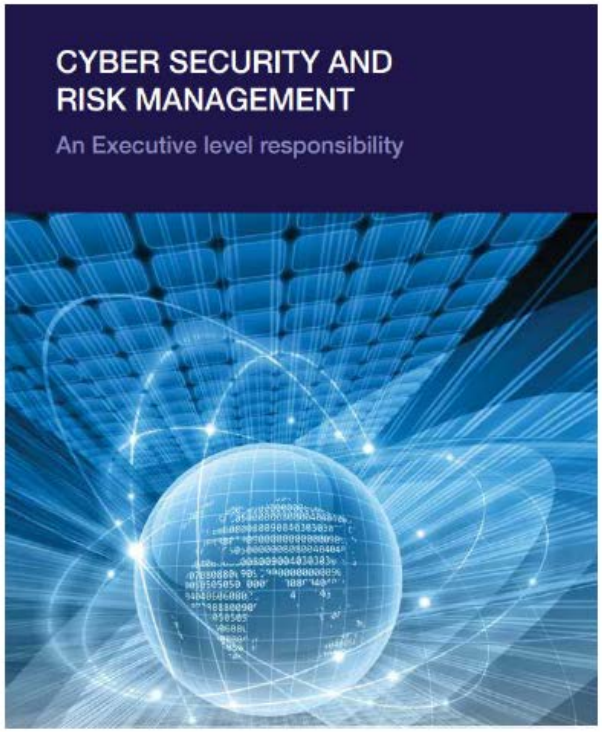
There are five core principles for boards in their oversight of cyber risks.



1. **Take a holistic approach**
   Directors should approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. **Understand the legislative environment**
   Directors should understand the legal implications of cyber risk as they apply to the company's specific circumstances.
3. **Access expertise and put cybersecurity on the board agenda**
   Boards should have adequate access to cybersecurity expertise. Discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
4. **Establish a framework**
   Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework.
5. **Categorise the risks**
   Board and management discussion of cyber risks should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

ncsc.govt.nz/about-us/

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.

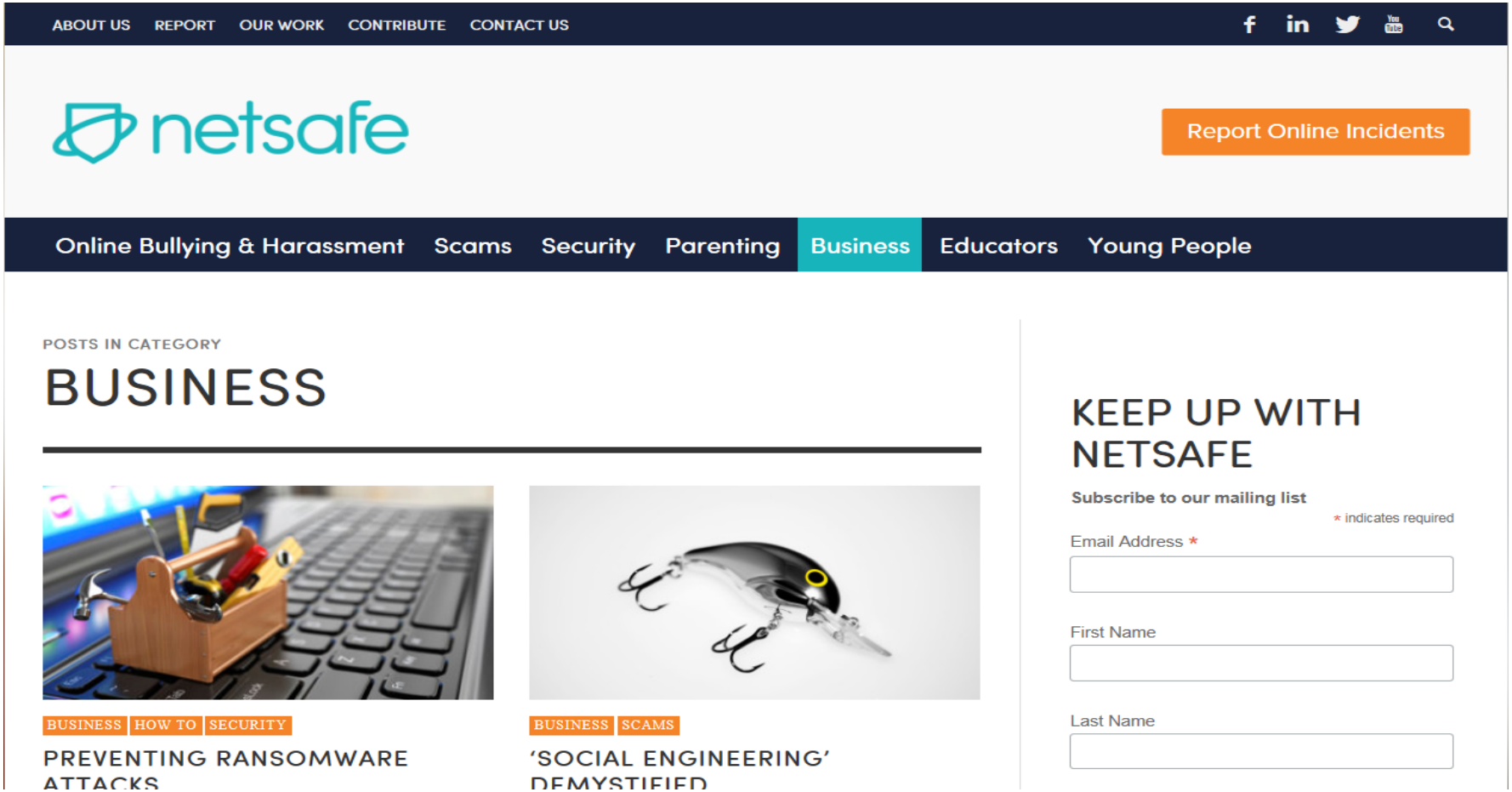
The topic of cyber security needs to move from being in the domain of the IT professional to that of the Executive and Board, where its consideration and mitigation can be commensurate with the risk posed. The traditional approach to thinking about cyber security in terms of building bigger walls (firewalls and anti-virus 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.

ict.govt.nz


ICT.govt.nz
Contact us
Search
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
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/



dpmc.govt.nz/ncpo

Search

DEPARTMENT *of the* PRIME MINISTER *and* CABINET

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.

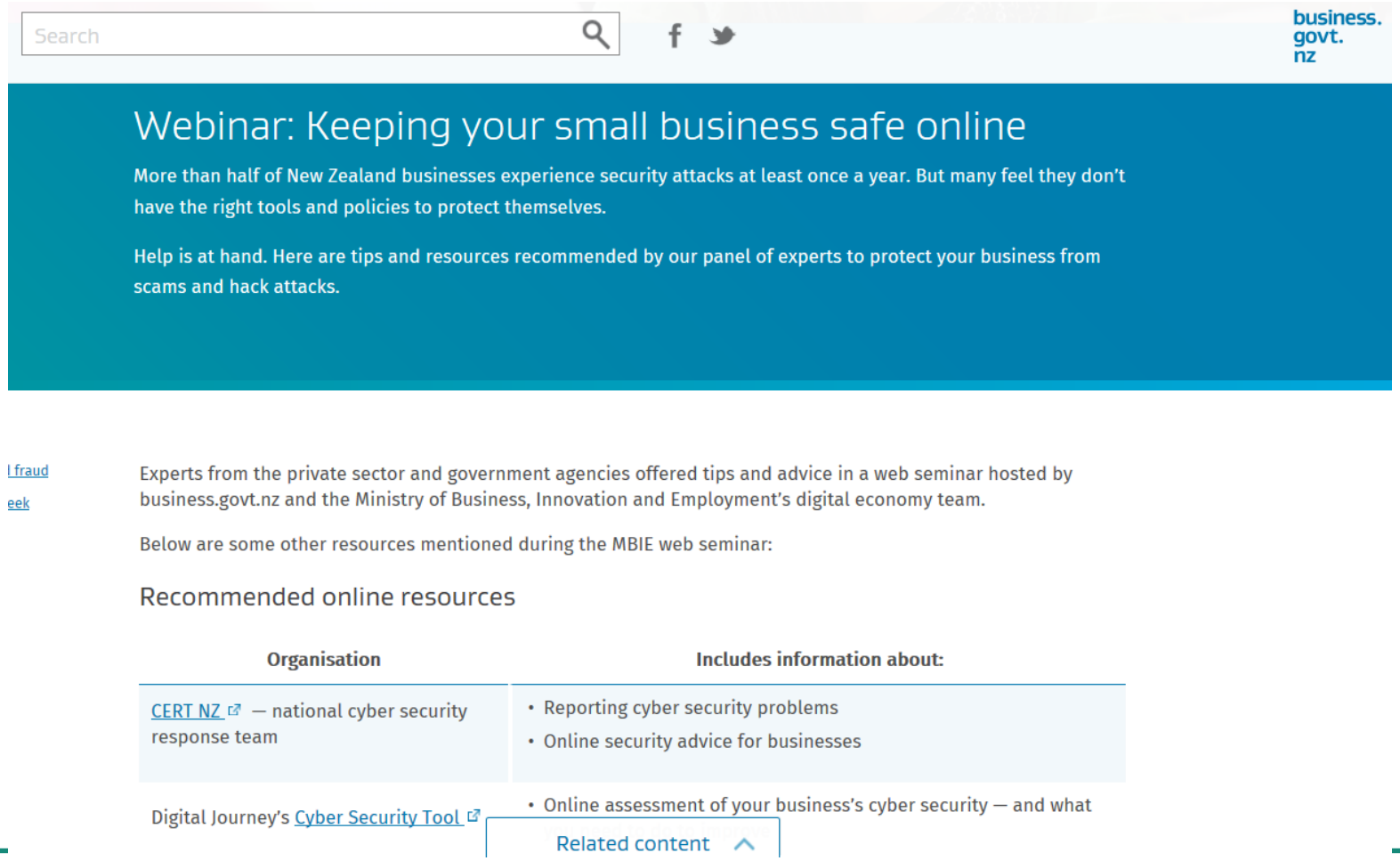
This new Strategy signals the Government's commitment to ensuring New Zealand is secure, resilient and prosperous online. The Strategy has four principles:

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

The Strategy has four intersecting goals.

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

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



AUDIT NEW ZEALAND
Mana Arotake Aotearoa

NZ Police

New Zealand POLICE
Ngā Pirihimana o Aotearoa

About us | Māori and Police | Major events | Jobs

Search

Home | Stolen/Wanted | Missing persons | Advice | News | Contact us

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

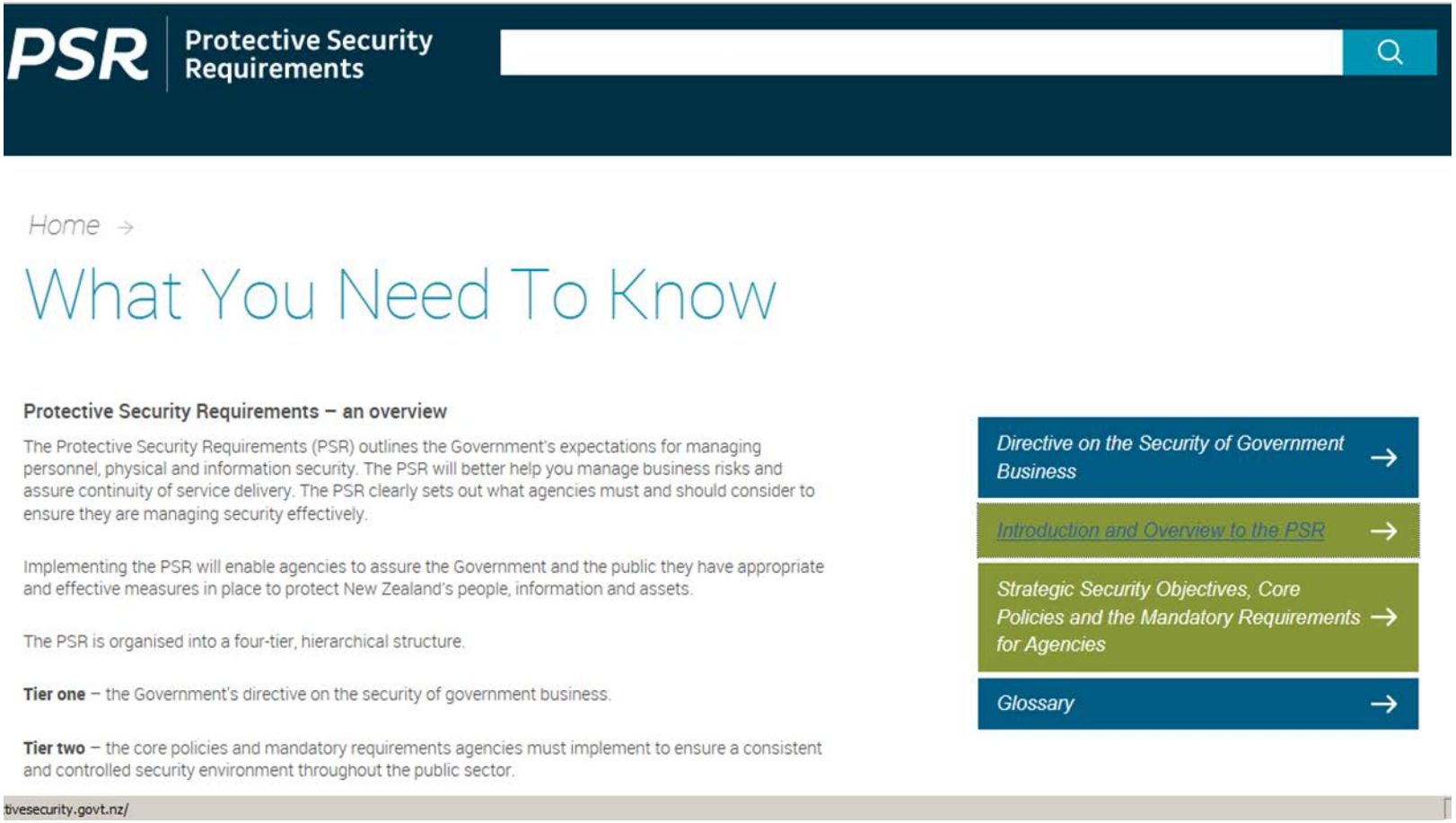
NetSafe - The Orb website

Keep your children safe

Frequently asked questions

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

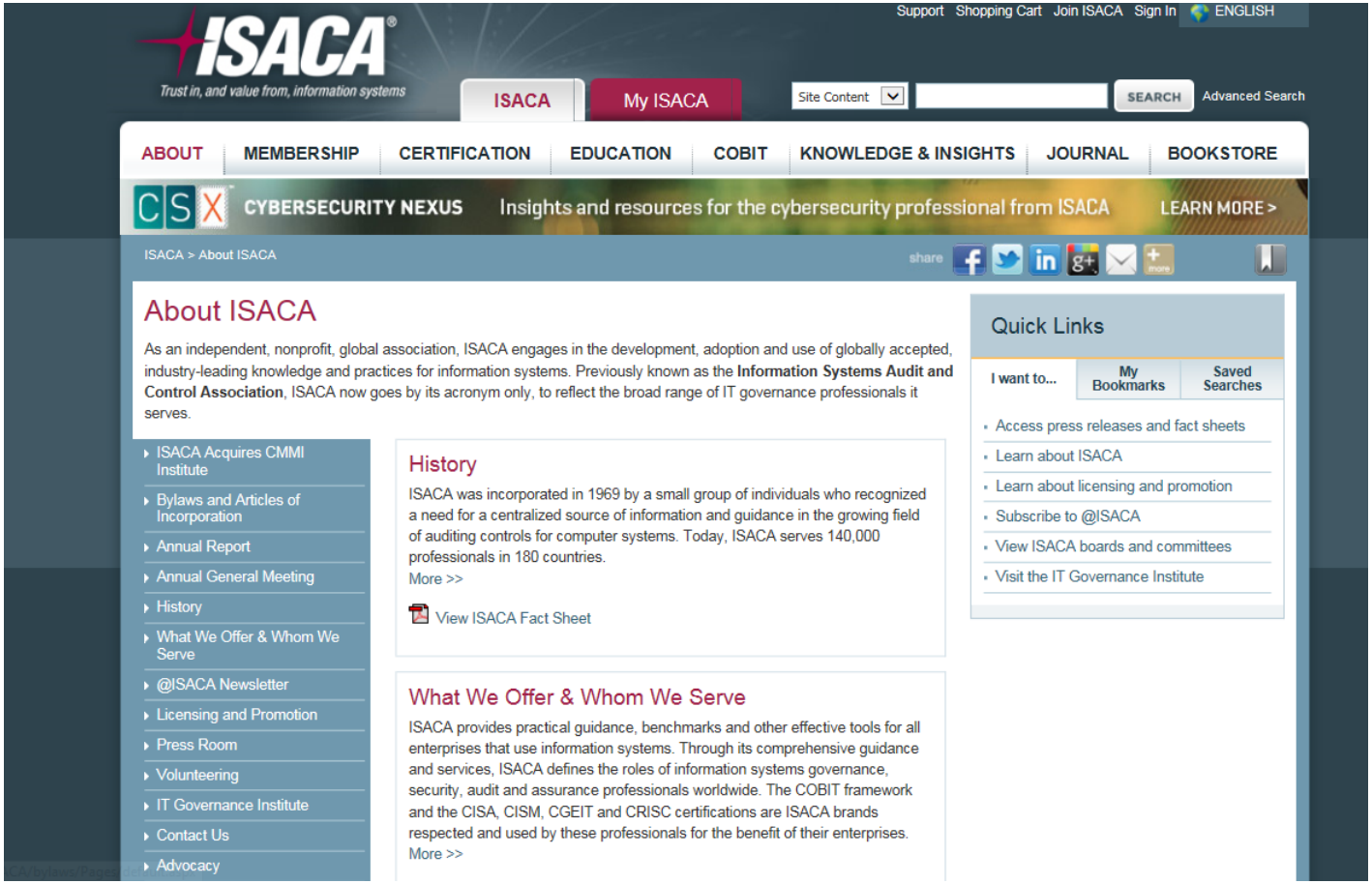
protectivesecurity.govt.nz



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

healthitboard.health.govt.nz

Isaca.org


Support Shopping Cart Join ISACA Sign In ENGLISH
ISACA
Trust in, and value from, information systems
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
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

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

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

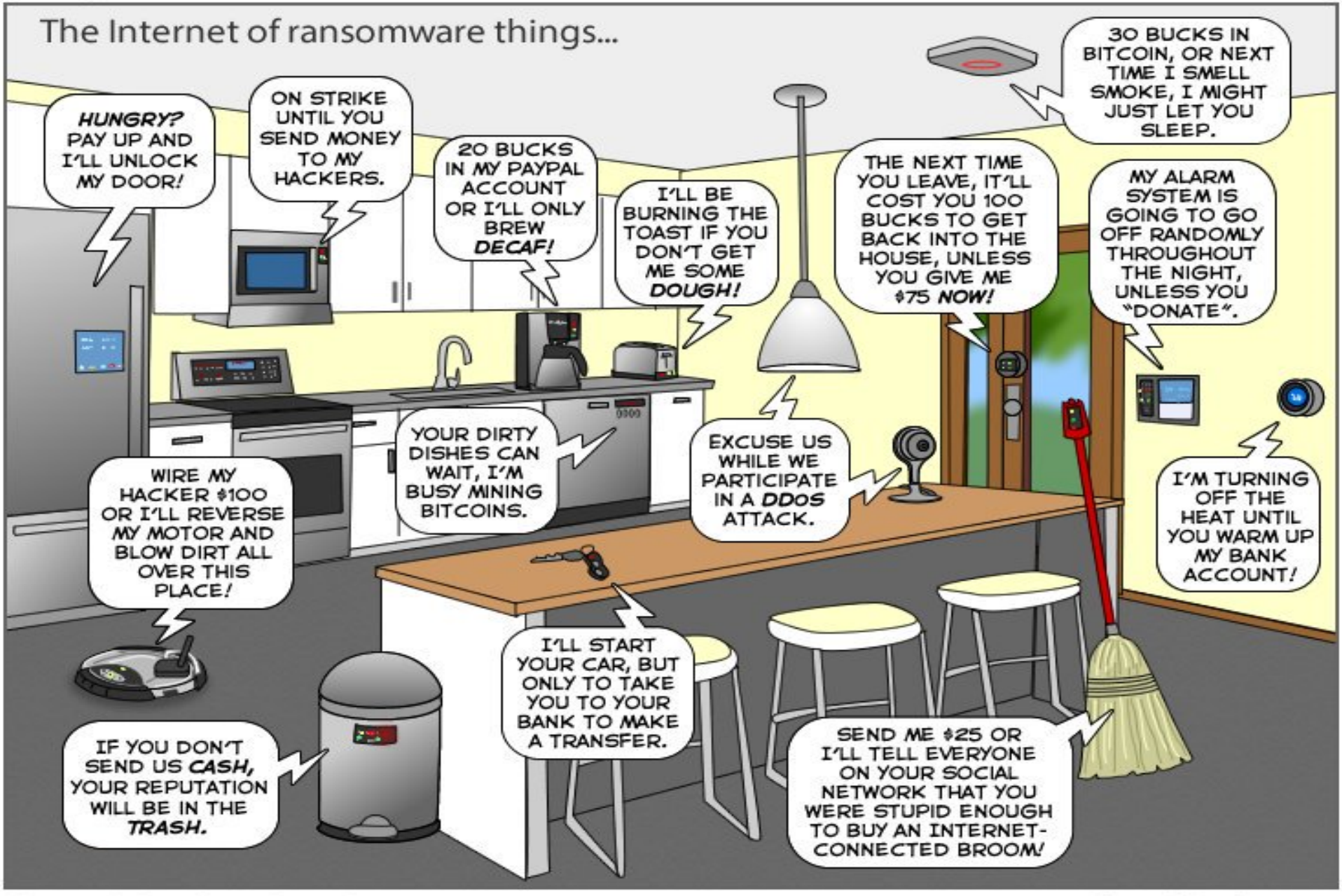
What else

- 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



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