New Zealand's Digital Strategy 2.0

Smarter through Digital

Background (1)

- In 2005 New Zealand released its Digital Strategy as a response to developments in information technology and communications;
- Its vision was for New Zealand to become a world leader in using information and communication technology to realise its economic, social, environmental, and cultural goals, to the benefit of all its people;
- Its three enablers were connection, content and confidence;

Background (2)

- The confidence enabler included actions aimed at promoting a more reliable and secure telecommunications and Internet environment;
- These actions included:
  - a National Computer Security Education Campaign undertaken by Netsafe (a non-profit educational and support organisation);
  - Ongoing support for the work of Netsafe;
  - The passing of anti-spam legislation;
  - The development of an e-crime strategy.

Background (3)

- Digital Strategy 2.0 is an opportunity to assess New Zealand's progress and reset its digital goals for the next 5 years;
- It is currently being finalised following a lengthy consultation process and is due for release in August 2008;

New Zealand's Cybersecurity Framework (1)

- Cybercrime laws prohibit unauthorised access, damage and interference to computer systems and data held on computer systems;
- The Unsolicited Electronic Messages Act 2007 prohibits the sending of commercial spam;
- New Zealand's Centre for Critical Infrastructure Protection (CCIP), supported by the Government Communications Security Bureau, provides advice and support to protect New Zealand's critical infrastructure from cyber threats;

New Zealand's Cybersecurity Framework (2)

- The New Zealand Police E-Crime Lab provides IT forensic services to support police investigations and prosecutions;
- New Zealand's Department of Internal Affairs enforces the anti-spam legislation, and its Censorship Compliance Unit enforces New Zealand's censorship laws, including the sending and publication of illegal material over the Internet;

New Zealand's Cybersecurity Framework (3)

- The Privacy Act 1993 and Codes of Practice issued under the Privacy Act, including the Telecommunications Information Privacy Code 2003, impose requirements on the collection and storing of personal information;
- The Security in Government Sector manual imposes requirements on government organisations to promote the effective security of Government information;

New Zealand's Cybersecurity Framework (4)

- The Officials Committee for the Review of Internet Security (OCRIS) is a high level Government inter-departmental committee responsible for overseeing New Zealand's cybersecurity policy;
- Netsafe is a non-profit organisation which is both publicly and privately funded to provide Internet security and safety education and support services.

A Strategic Consideration and Analysis (1)

- In 2006 the Ministry of Economic Development released a Discussion Paper entitled “A Strategic Consideration of ICT Security and Confidence in New Zealand”;
- The purpose of the paper was to take a strategic look at ICT security and safety issues in New Zealand and seek feedback in order to assess key gaps and priorities;

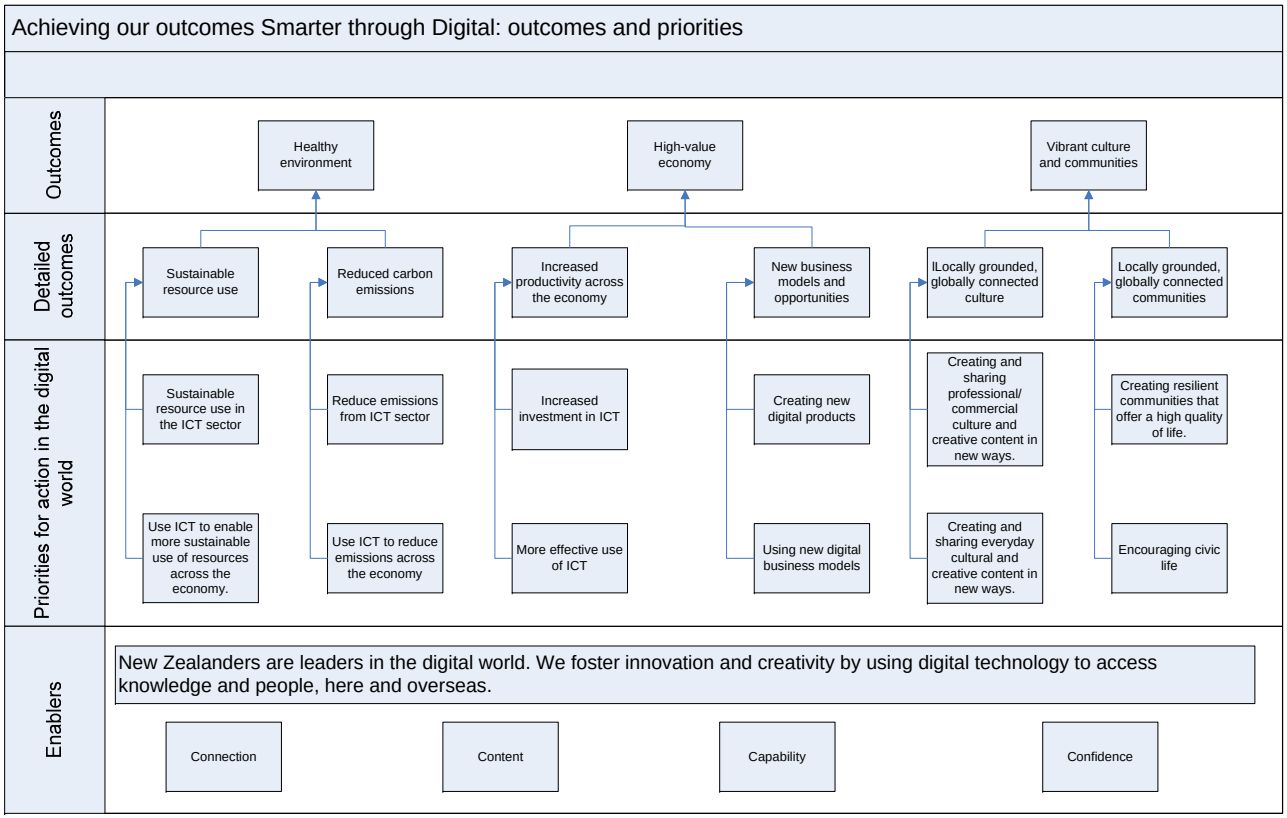
A Strategic Consideration and Analysis (2)

- Guidance was obtained from the OECD work on information security which promoted a global vision for ICT security of developing and promoting a culture of security amongst all participants and established nine guiding principles;
- Key gaps and priorities identified for New Zealand were:
  - The need for improvement in New Zealand's threat prevention, detection and response capability for critical infrastructure and business networks, with the possible need for a New Zealand CERT;

A Strategic Consideration and Analysis (3)

  - The need for more comprehensive education and awareness-raising for business and households on ICT security and safety risks and protections;
  - The need for more effective collaboration between Government, business and community groups to bring about improved ICT security outcomes.
- The feedback from the discussion paper has contributed to the work on Digital Strategy 2.0.

Digital Strategy 2.0 (1)



Digital Strategy 2.0 (2)

- Digital Strategy 2.0 is more focused on achieving outcomes, particularly a healthy environment, a high-value economy and vibrant culture and communities;
- It sets new goals for each of the four enablers (connection, content, capability and confidence);
- The new goal for confidence is to “ensure secure and trusted digital networks, and universal understanding of online safety and privacy issues”;

Digital Strategy 2.0 (3)

- The four priorities for action for "Confidence" are:
  - Ensure the security of ICT infrastructure and networks;
  - Enhance the security of digital information;
  - Ensure universal awareness of online safety, security and privacy issues;
  - Enforce cyber-crime law.

Digital Strategy 2.0 (4)

- Key actions to help achieve these priorities are:
  - Better resourcing for CCIP to provide a full 24/7 cyber-threat prevention, detection and response service for Government and critical infrastructure;
  - Scoping the establishment of a general CERT for New Zealand;
  - Undertaking a review of identity management across Government (i-govt);
  - Continued support for Netsafe for education and awareness-raising;
  - Implementing an initiative to promote international cross-border cooperation amongst privacy enforcement authorities;
  - Implementation of the New Zealand E-Crime Strategy, including the establishment of a National Cyber Crime Centre.