Chief Information Officer Group

CIOG: External Drivers of Technological Change

Social and Environmental Impacts on Defence ICT

Mr Greg Farr – CIO Defence   21 September 2011

"Lead the integrated design, cost effective delivery and sustained operation of the Defence Information Environment to support business and military operations."

- Support to Military Operations

- Run the Defence Information Environment

- ICT Reform

  – Optimise investment through sourcing

  – Deliver agreed priority solutions - applications & infrastructure

  – Develop the next generation of capabilities

  – Optimise investment through common enterprise services

  – Improve stakeholder engagement

- Other Groups' Reform with ICT Components

- Support to Minister

- Defence Capability Plan and Green Book activities

CIOG manages:

- A diverse and complex information environment, spanning :
  - Restricted, Secret and Top Secret security classifications
  - data, voice and video
  - fixed and deployed instances
  - domestic and coalition interfaces
- 8 satellite constellations
- three primary data centres, 200+ server rooms
- Four mainframe computers
- 10,000 servers, including Windows, UNIX, AIX, Solaris (virtual and physical)
- over 3000 applications
- over 150,000 desktop computers
- $1.3 billion spend in Defence ICT per year

How does CIOG

  • meet its mandate,

  • within a secure environment,

  • reducing its carbon footprint,

  • complying with whole-of-government policies and

still remain an attractive employment prospect to the next generation of IT professionals?

Australian Government
Department of Defence
Chief Information Officer Group

Mr Greg Farr – CIO Defence

As **Canberra's single largest power consumer**, government and society expect Defence to measurably contribute to ICT environmental issues.

To achieve this, CIOG will:

- Incorporate sustainability and resource efficiency considerations in contracts and operations.

- Improve the management of Defence environmental data through ICT solutions.

- Foster the implementation of Government policies for sustainable procurement, including whole-of-life environmental, energy, water and waste considerations.

- Consider environmentally preferable products and services where feasible and apply whole-of-life cost assessments consistent with Commonwealth policies.

- Where security allows, require that Defence suppliers take responsibility for the reuse, recycling and environmentally sound end of life disposal of their products.

- Operate Defence ICT systems to maximise energy efficiency.

- Where security allows, reuse and recycle used computer equipment in accord with Government ICT Sustainability policies and plans.

Australian Government
Department of Defence
Chief Information Officer Group

Minimising Resource Use

- Printer Rationalisation
- Carbon/Energy Conscious Procurement
- Recycling/reuse of desktop infrastructure

- Automatic desktop shut down overnight is saving Defence $5 million per annum.

- Developing a Single Desktop across multiple security domains - replacing three desktop devices with one.

- Centralised Processing Project – reducing the number of servers and maximising processor utilisation.

- Data Centre Consolidation – transitioning over 200 server rooms to fewer, greener facilities.

- Investigating lighter weight technologies:
  - virtualisation,
  - mobile technologies,
  - cloud computing

www.defence.gov.au/cio

ICT Remediation Program

- Addressing long-term underinvestment and inefficiencies in infrastructure

- Update and replace infrastructure outside effective life

- Hardware replacement cycles offer CIOG opportunities to continuously improve efficiency and reduce our carbon footprint

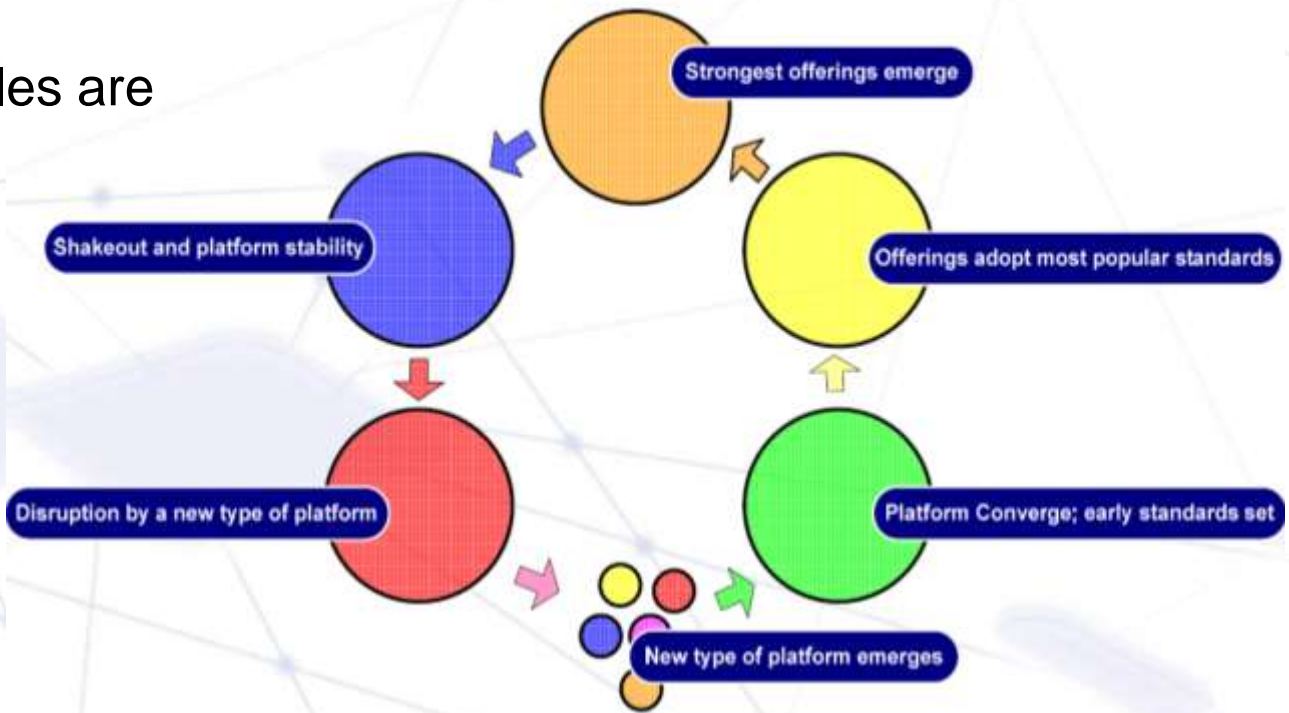**We are seeing profound changes in workforce behaviour and expectations:**

- Generational change: Baby Boomers → X → Y → Z → ?
  - The workforce is populating with individuals who expect flexibility and the ability to influence their workplace
- Individual expectations:
  - Work/life balance
  - Work from home, remote access: DREAMS, Blackberry, BYOC
- Applications Stores
- Individual choice versus corporate control

Evolution or Revolution?

ICT technology lifecycles are rapidly decreasing.

Defence can not afford to follow practices that deliver obsolete solutions due to overlong processes

Strongest offerings emerge

Offerings adopt most popular standards

Shakeout and platform stability

Platform Converge; early standards set

Disruption by a new type of platform

New type of platform emerges

We need new thinking to deliver contemporary, cutting-edge solutions.

Source: http://blogs.zdnet.com/Hinchcliffe

ICT is changing…

Disruptive technologies, often socially derived, are dictating our future environment, providing unique challenges, but frequently suggesting unique solutions.

Think how the internet, Google, Wikipedia, Facebook, Twitter have changed our world and forced us to change the way we operate…

But where would we be without them?

www.defence.gov.au/cio

New Solution Sources

The competition for IT shops comes not from other IT shops but from the likes of iPhones, Google, Facebook etc.

We have a choice in many instances: long and costly development cycles with complex integration or downloading an application from an iPhone for $5.

That's the competition!

We need to think about how we source solutions.

Applications stores…   **In-house development…**

Open source…

Blended solutions…

Traditional sourcing…

Israeli military 'unfriends' soldier after Facebook leak

"The Israeli military cancelled a raid after a soldier posted details of the operation on Facebook. The unnamed soldier revealed the time and place of the raid and details of his unit. He was later court-martialled and sentenced to 10 days in prison."[1]

Risks to Defence from use of social media include security breaches, loss of reputation, loss of intellectual property and code of conduct infringements.

But, **let's not cry wolf** - these risks already exist across many media types and we can't close our eyes to the importance of social media in our modern society.

So how do we address its use by Defence personnel?

Policy? Education? Code of conduct? Personal responsibility?

"If a person makes a sketch, drawing, photograph, picture or painting of any defence installation in Australia or of any part of one and the person has no lawful authority to do so the person is guilty of an offence"

The Defence Act of 1903

Times change, we need to change with them.

1. news.bbc.co.uk/2/hi/8549099.stm

Our Mandate *versus* **our Wish-list**

Personal Choice *versus* **Tightly Controlled User Devices**

Very Early Certainty *versus* **Evolutionary Development**

Agility *versus* **Risk Avoidance**

Every organisation has challenges associated with social and generational change, these challenges are exacerbated by size

Defence is no exception