Why Isn't Security Easier for SMEs and Consumers?

Roger Clarke

Xamax Consultancy, Canberra

Visiting Professor in Computer Science, ANU
and in Cyberspace Law & Policy, UNSW

UNSW CSE
14 August 2014

http://www.rogerclarke.com/EC/SSACS-13 {.html, .ppt}

Why Isn't Security Easier for SMEs and Consumers?

Agenda

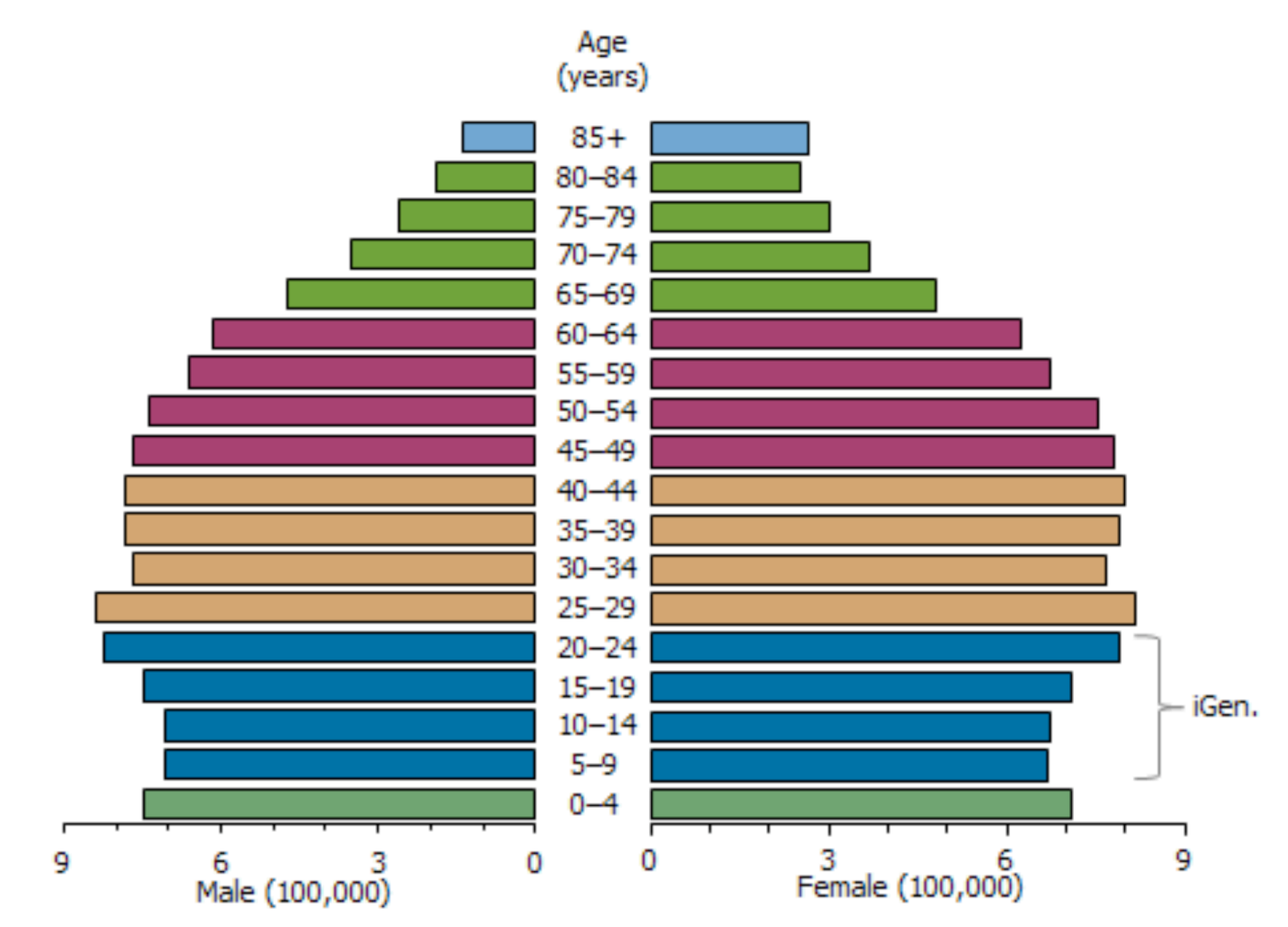
- Security Literacy
- Security Market Failure
- Simple Baseline Security for Organisations
- Security for Consumers is Even Harder
- How to Make Security Much Easier
- How to Make It Happen

XAMAX Consultancy Pty Ltd

Security Literacy Among .au Organisations

	SecLit	**SecIllit**
LBEs	6,000	–
GAs	6,000	–
MBEs	25,000	50,000
SMEs	50,000	700,000
µEs	10,000	250,000
	100,000	**1,000,000**

XAMAX Consultancy Pty Ltd



http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/2071.0main+features952012-2013

http://www.rogerclarke.com/II/iGen.html

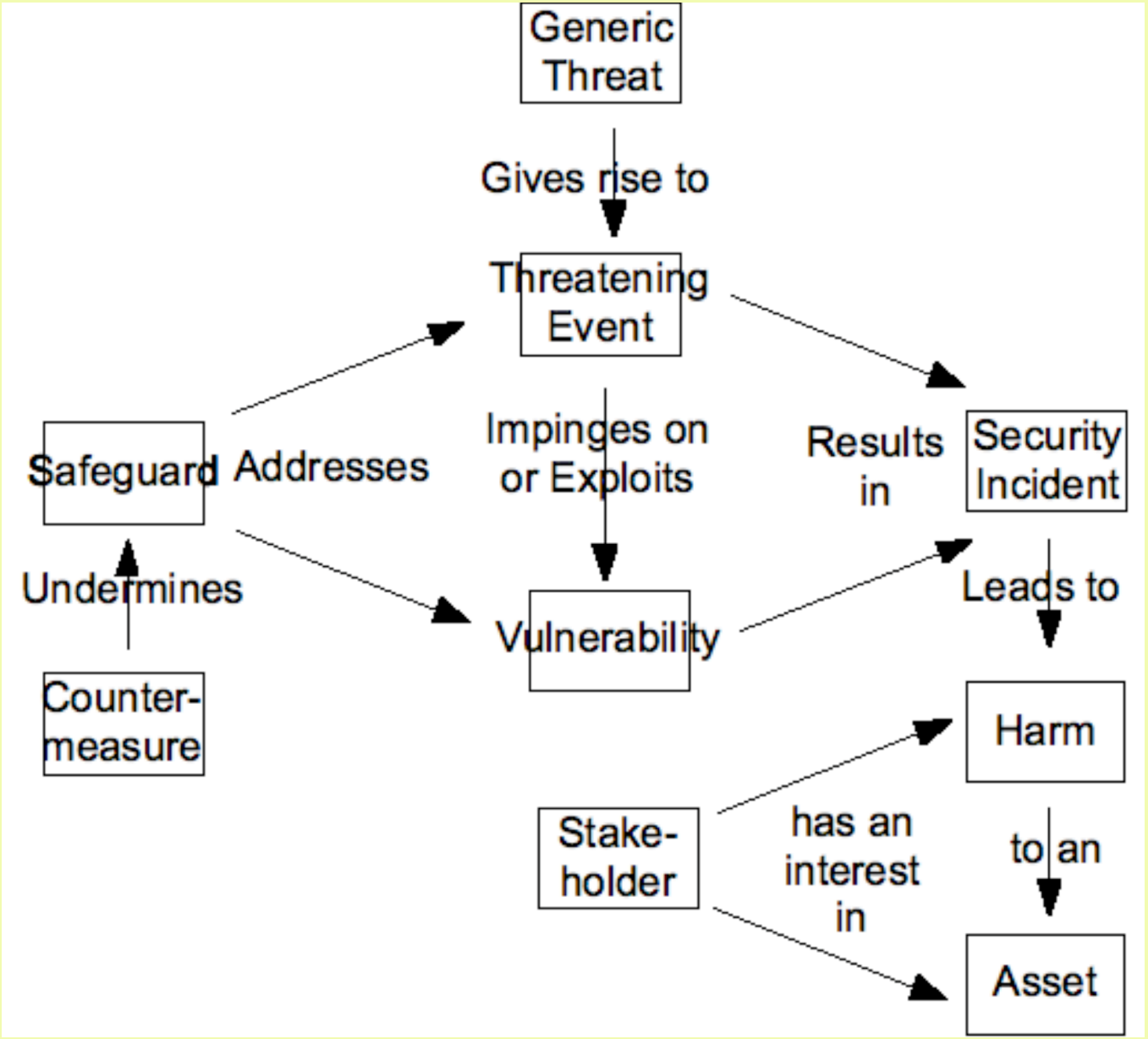
http://www.smh.com.au/action/printArticle?id=5630200

Security Literacy Among .au Entities

	SecLit	**SecIllit**
LBEs	6,000	–
GAs	6,000	–
MBEs	25,000	50,000
SMEs	50,000	700,000
µEs	10,000	250,000
	100,000	**1,000,000**
People	100,000	**18,000,000**

XAMAX Consultancy Pty Ltd

The Conventional Security Model



XAMAX Consultancy Pty Ltd

http://www.rogerclarke.com/EC/SSACS-13.html#App1

The Conventional Security Model

- Threatening events impinge on vulnerabilities, resulting in harm to assets
- Safeguards protect against threatening events, vulnerabilities and harm
- Security is a condition in which harm is in part prevented and in part mitigated, because threats and vulnerabilities are countered by safeguards
- **Avoid, prevent, minimise or cope with harm, by balancing safeguards' predictable financial costs and other disbenefits against security incidents' less predictable financial costs, and other disbenefits and contingent risks**

XAMAX Consultancy Pty Ltd

The Challenges

- Security is **Not Designed In** to devices, systems software or network infrastructure – it's always an add-on / retro-fit
- **Diverse Technical Contexts**, at hardware and OS levels, overlaid by multiple apps
- **Closed Technical Contexts**
- Categories of **Threats** are legion, and change continually
- Categories of **Vulnerabilities** are legion, and proliferate

The Challenges

- Security is **Not Designed In** to devices, systems software or network infrastructure – it's always an add-on / retro-fit
- **Diverse Technical Contexts**, at hardware and OS levels, overlaid by multiple apps
- **Closed Technical Contexts**
- Categories of **Threats** are legion, and change continually
- Categories of **Vulnerabilities** are legion, and proliferate

- Diverse **Contexts of Use**
- **High value is placed on Convenience** (which is experienced continually)
- **Low value is placed on Security** (experienced rarely)
- **Hedonism** undermines considered, reflective and responsible attitudes
- Security Features involve **Intrusiveness** into work and play & require understanding and concentration

Market Failure

- Those Challenges are costly to address
- Business enterprises only invest if:
  - it's a cost of being in the game; or
  - it makes money
- SecLits assess risk dispassionately;
  but SecIllits judge risk spontaneously
- SecIllit Customers don't value security,
  and certainly not enough to pay for it
- Market mechanisms won't solve the problem
- **The Security Gap won't be addressed without Market Intervention**

XAMAX Consultancy Pty Ltd

Research Method

- Identify possible Interventions
- Search for evidence of the extent to which these Interventions are being used, and being effective:
  - The Privacy Commissioner's Guide
  - 'Absolute-Minimum' Security Safeguards
  - Regulators and Industry Associations
  - Profile-Based Security Guides
  - Security Product Suppliers
- Identify the Impediments

A Possible Intervention

IPP 4 (1989-2014)
NPP 4 (2001-2014)
APP 11 (2014-)

A Possible Intervention

IPP 4 (1989-2014)	Info Privacy Principles (public sector)
NPP 4 (2001-2014)	Nat'l Privacy Principles (private sector)
APP 11 (2014-)	**Aust Privacy Principles (both sectors)**

- Obligations exist to take such steps as are reasonable in the circumstances to protect [personal data] from:
  - misuse, interference, loss
  - unauthorised access, modification, disclosure

XAMAX Consultancy Pty Ltd

http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/sch1.html#_Toc382303250

A Possible Intervention

- In April 2013 and July 2014, the PC'er updated the 2001 **'Guide to Info Security'**
- Did it:
  - Declare a minimum set of safeguards?
  - Express them in an updateable Appendix?
  - Permit alternatives, based on an accessible risk assessment report?

XAMAX Consultancy Pty Ltd

But No Intervention At All

- In April 2013, **OAIC** updated its 2001 **'Guide to Info Security'**
- Did it:
  - Declare a minimum set of safeguards?
  - Express them in an updateable Appendix?
  - Permit alternatives based on an accessible risk assessment report?

- **No**
- OAIC has, twice, spurned the opportunity
- The document features:
  - 34 x 'appropriate'
  - 74 x 'reasonable'
  - some 'steps and strategies which may be reasonable to take'
  - no minimum requirements

XAMAX Consultancy Pty Ltd

http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-information-security

Absolute-Minimum InfoSec Safeguards

1. Physical Safeguards
2. Access Control
3. Malware Detection and Eradication
4. Patching Procedures
5. Firewalls
6. Incident Management Processes
7. Logging
8. Backup and Recovery
9. Training
10. Responsibility

Absolute-Minimum InfoSec Safeguards

2. **ACCESS CONTROL**, including:

- user-accounts allocated to individuals for their, & only their, personal use
- privileges limited to only the software, functions and data that are required for that person's work
- tight control over super-user accounts, to reduce the opportunity for abuse of access privileges

3. **MALWARE DETECTION AND ERADICATION**
   (Malware is used here as a generic, encompassing viruses, worms, spyware, bots, rootkits, etc. – http://rogerclarke.com/II/RCMal.html)
   - on all inbound traffic; and
   - periodically on all storage devices

4. **PATCHING PROCEDURES**
   To ensure the frequent application of all security-relevant updates and patches to all systems software and application software

Absolute-Minimum InfoSec Safeguards

- That set relates to
  the era of IT Departments and desktops
- For the Mobile / Wireless / Untethered Age?
  - BYOD Policies?
  - Mobile Device Management /
    Mobile Application Management
    (MDM/MAM) Tools?
  - ?

XAMAX Consultancy Pty Ltd

Absolute-Minimum InfoSec Safeguards
A Less *Ad Hoc* Approach

- Stratify into Market Segments
- For each Market Segment:
  - Conduct a generic Risk Assessment
  - Establish a generic Risk Management Strategy
  - Articulate Strategy into a Management Plan

? Segment by sector and segment

? 'Carefree' / 'Normal Business' / 'Exposed'

XAMAX Consultancy Pty Ltd

Tentative Stratification of Security Safeguards

- Baseline Security Features
  Low Security / High Convenience
  http://www.rogerclarke.com/EC/SSACS-13.html#App2
- Additional Security Features
  Medium Security / Medium Convenience
  http://www.rogerclarke.com/EC/SSACS-13.html#App3
- Further Secure Features
  High Security / Low Convenience
  http://www.rogerclarke.com/EC/SSACS-13.html#App4

Consumers – Some Extra Problems

- Risks are very difficult to understand
- Safeguards are very difficult to understand, to find, to install, to configure, to maintain, to trust

- Consumer Devices are designed to be insecure
- To avoid designed-in vulnerabilities, consumers have to forego some of 'the Internet experience'
- Some basic transactions, even payments, rely on consumer devices being insecure

- **SME solutions need to be scaled for Consumers**

Server Control of Consumer Devices

- Java Applets
- ActiveX 'Controls'
- 'Asynchronous JavaScript and XML' (AJAX)
- Drive-by Downloads
- HTML5
- Mobile Apps

HTML

- Support for:
  - multi-media streaming
  - open channels as well as sessions
  - geolocation
- **A way to subvert sandboxing**
- **A way to subvert user control, by inverting the Web from pull to push**
- **A way to access local data and devices** (e.g. cameras, microphones), giving rise to "A Pandora's box of tracking in the Internet"

XAMAX Consultancy Pty Ltd

http://www.sophos.com/en-us/medialibrary/PDFs/other/sophosHTML5andsecurity.pdf

The Primary Geolocation Technologies

Technology	Acquirer	Process	Data Quality
Cell Location	Base-Station	Device registers with the base-station 10 times per second	50-100m or several hundred metres
Directional Analysis	Base-Station	Receivers have a known arc and range	Sector within Cell, with errors
Triangulation	Base-Station	Multiple base-stations per Cell enable location within the intersection of their Sectors	Multilateral space within Cell (e.g. a triangle), with errors
Signal Analysis	Base-Station	TDOA (Time Difference of Arrival, aka multi-lateration) RSSI (Received Signal Strength Indicator) AOA (Angle of Arrival)	Small space within Cell, with errors
Proximity to a particular Wifi Router	Any Message Recipient	Commercial services gather and maintain databases of recorded location of Wifi Routers	10m claimed 50-100m measured with errors
GPS	The Device	Device detects satellite signals, Device self-reports its coordinates	7-8m claimed 20-100m measured availability and speed issues, with errors

Mobile Apps

- Will Google and Apple really protect eConsumers against other parties?
- And who will protect eConsumers against Google and Apple?
- Retrofitting of Mobile OS to the Desktop
  Mac OSX ➔ iOS Android / bluetracks

XAMAX Consultancy Pty Ltd

Do we really know NOTHING??

- ASD (2013) 'Information Security Manual' ('**the ISM**') Defence / Australian Signals Directorate, August 2013, at http://www.dsd.gov.au/infosec/ism/index.htm
- ASD (2013) '**Strategies to Mitigate Targeted Cyber Intrusions**' Defence / Australian Signals Directorate, April 2013, at http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- DBCDE (2013a) '**Stay Smart Online –** Business' Dept of Broadband Communications and the Digital Economy, 2013, at http://www.staysmartonline.gov.au/business
- DBCDE (2013b) 'Stay Smart Online – Home Users' Dept of Broadband Communications and the Digital Economy, 2013, at http://www.staysmartonline.gov.au/home_users
- **RACGP** (2013) '**Computer and Information Security Standards**' Royal Australian College of General Practitioners, 2nd Edition, June 2013, at http://www.racgp.org.au/your-practice/standards/ciss/

Possible Security Profiles

- **Low Security / High Convenience**
  'Carefree social media' ... social ephemera, trivia
- **Medium Security / Medium Convenience**
  'Careful social media'
  Enterprise purposes
  Privacy and/or security concerns
- **High Security / Low Convenience**
  Undercover operatives, corporate takeover analysts, researchers handling delicate data, diplomats, ...
  Persons-at-Risk (protected witness, whistle-blower)

XAMAX Consultancy Pty Ltd

Appendix 2: Baseline Security Features
Low Security / High Convenience

User Accounts

- Authentication required for:
  - payment transactions above a low minimum threshold
  - transactions that involve the disclosure of payment-related data
  - communications that contain particular keywords

Internet Traffic Controls

- Controls on consumer-hostile Web features that create serious vulnerabilities, including:
  - cross-site scripting
  - features of and/or exploits using, Flash, Silverlight and similar
  - features of and/or exploits using, scripts, ActiveX controls, Java, JavaScript
  - ads that are objects rather than just images
- Prohibition on outgoing traffic without encryption,
  where it contains authenticators and/or payment-related data
- Firewall installed and configured

Executables Controls

- Malware detection and remediation software, installed, configured, auto-updated, and run:
  - on all incoming files, streams and messages that may contain executables
    (i.e. including office documents that may contain macros)
  - cyclically on all stored files that may contain executables
- Prohibition on auto-invocation of newly-loaded executables, except where the download results from an explicit user request for download and invocation, and the executable has passed malware checks
- Prohibition on remote invocation of both newly-loaded and stored executables, except were the invocation results from an explicit user request for invocation, and the executable has passed malware checks

Storage Controls

- Vulnerability detection and notification software, installed, configured, auto-updated, and run cyclically on all stored executables
- Auto-update of selected system software and applications

Settings Controls

- Following each auto-update of system software and applications,
  override of the provider's default settings with the device's default settings
- Prohibition on modifications to settings by software
- Warnings when highly insecure settings are manually selected

Backup

- Auto-backup / mirroring of:
  - configuration settings
  - address-books

XAMAX Consultancy Pty Ltd

Baseline: Low Security / High Convenience

User Accounts

- Authentication required for:
  - payment transactions above a low minimum threshold
  - transactions that involve the disclosure of payment-related data
  - communications that contain particular keywords

Backup

- Auto-backup / mirroring of:
  - configuration settings
  - address-books

Storage Controls

L Vulnerability detection and notification software, installed, configured, auto-updated, and run cyclically on all stored executables

Auto-update of selected system software and applications

Logging of all changes to settings

M + Logging of all changes to software

Protection of logs

H + Logging of all changes to user data

Encrypted data storage

Prohibition on, or at least controls over, publicly-shared files

Frequent, automated date-time synchronisation

Solutions Driven from the Supply-Side?

- **Desktop Virtualisation**, e.g. Citrix
  Service not application, high dependence on server, complete network dependence, network latency
- **Native Solutions** from equipment / OS providers
  High dependence on supplier, supplier-specific, not platform-independent, hostage to the supplier
- **Container Solutions**
  A virtual machine or other segmented area, data sandboxing, access denied to the full set of facilities available on and from the device

XAMAX Consultancy Pty Ltd

http://www.itnews.com.au/Resource/358142,the-true-cost-of-byod.aspx

Formal and 'Soft' Regulatory Options

Table 1: Regulatory Forms and Regulatory Roles

Actors	**Regulation** ('Government')	**Co-Regulation**	**Industry Self-Regulation**	**Self-Regulation** ('Governance')
The State	**Determines What and How**	**Negotiates What and How**	Influences What	Has Limited Influence
Industry Assocn	Influences What and How	**Negotiates What and How**	**Determines What and How**	Influences What and How
Corporations	Contribute to Industry Assocn	Contribute to Industry Assocn	Contribute to Industry Assocn	**Determine What and How**
Other Stakeholders	May or May Not Have Some Influence	May or May Not Have Some Influence	May or May Not Have Some Influence	May or May Not Have Some Influence

Formal and 'Soft' Regulatory Options

- **Formal Regulation**

  Merchantable Goods, Product Liability
  Maybe applicable to 'appliances'?

- **Co-Regulation**

  PC'er Industry Code power has failed
  DBCDE not prepared to be a regulator

- **Industry and Professional Self-Regulation**

  Standards Associations?
  ECMA? CCIA? AIIA??
  ACM? IEEE? SAGE? ISSA? SANS? IFIP?
  ACS?? ISOC-AU?? SAGE-AU?? AISA??

Conclusions

- Because of market failure in info security, Intervention is necessary
- Interventions have been contrived, at the very best, half-heartedly and ineffectively
- It appears that much bigger losses will be needed before any of the players act
- Computer Science is not driving practice

Why Isn't Security Easier for SMEs and Consumers?

Agenda

- Security Literacy
- Security Market Failure
- Simple Baseline Security for Organisations
- Security for Consumers is Even Harder
- How to Make Security Much Easier
- How to Make It Happen

XAMAX Consultancy Pty Ltd

Why Isn't Security Easier for SMEs and Consumers?

Roger Clarke

Xamax Consultancy, Canberra

Visiting Professor in Computer Science, ANU
and in Cyberspace Law & Policy, UNSW

UNSW CSE
14 August 2014

http://www.rogerclarke.com/EC/SSACS-13 {.html, .ppt}