INFORMATION SECURITY – NO MORE THE CINDERELLA?

Lord Toby Harris

tobyharris

Wednesday 20th June 2007

FIRST Conference - Seville

THE VIEW FROM THE KITCHEN

- Information security – the Cinderella of technology
- Information security – the Cinderella of security
- Who are the Ugly Sisters and the Wicked Step-mother?
  - Emotional issues
  - Cultural issues
  - Financial issues
  - Cynicism

WHY IDENTITY AND SECURITY MATTER

- Advent of broadband and new communications technology
- Convenience and changing expectations
- Identity theft
- Whose responsibility?
  - Personal
  - Corporate
  - Government
- E-commerce
- E-government and efficiency
- Critical national infrastructure

HOUSE OF LORDS COMMITTEE

- What is the nature of the security threat to private individuals?
- What can and should be done to provide greater computer security to private individuals?
- Who should be responsible for ensuring effective protection from current and emerging threats?
- Is the regulatory framework for internet services adequate?
- How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?
- Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

HOUSE OF LORDS COMMITTEE – 2

- A data breach law for the UK?
- Proper recording of identity theft cases
- Shifting the balance of responsibility
  - Equipment manufacturers
  - Software producers
  - Service providers
- Adequate resourcing of enforcement

WHAT PUTS PEOPLE AT RISK

- Ignorance
- Carelessness
- Unintentional exposure by others
- Technology flaws
- Deliberate criminal acts

Made worse by products behaving badly

A CONSUMERS’ BILL OF RIGHTS

- Don’t give others my data without my permission
- Don’t lose my data
- Don’t abuse my data
- Don’t waste my time
- Can I prove who I am and can you prove who you are?
- Is the information accurate and can it be readily corrected?

HOW TO TURN ID CARDS INTO A PUMPKIN

- Not a significant counter-terrorism tool
- Limited benefits re illegal immigration and border control
- Key message should have been citizen benefit: enabling the individual to establish their identity and entitlement
- Not helped by long history of success in public sector IT projects

BUT WITH A FEW WHITE MICE …

- Government wants to promote e-commerce
- Major agenda on improving efficiency of public services
- Government should ensure that public education and understanding is promoted
- “e-citizenship” in the national curriculum?

AND WHAT BIG TEETH YOU HAVE

- Regulation, regulation, regulation ….. for everything else
- Policing – resources and priorities
- Making the punishment fit the crime
- ….. but Government needs to put its own house in order first with its own systems and the CNI

THE CRITICAL NATIONAL INFRASTRUCTURE AT RISK

- 2000: Love Bug virus shuts down Parliamentary Network
- 2004: Sasser worm hits Coastguard Service
- May 2002 – May 2004: 71 instances of Ministry of Defence systems compromised by malicious programmes
- Republic of Estonia – cyber-attack May 2007

WHO’S EATING MY PORRIDGE TODAY?

Latest year security breaches:

- MoD – 35
- DfID – 10
- DfT and DTI – 9 each
- DCA – 7
- DWP and Home Office – 2 each
- nil reported by HMT, DoH, DEFRA, Cabinet Office, FCO, DfES, DCMS, NIO and DCLG.

IF YOU GO INTO THE WOODS TODAY ……

- Teenage hackers
- Small criminal enterprises
- Organised crime
- Nation states
- International terrorists

WHOSE JOB IS IT TO PROTECT THE CNI?

- CNI systems are essential for national health and well-being
- CNI is in both public and private sectors
- Public sector: is security a KPI?
- Private sector: do commercial interests require same security as national interest?

THE ROLE OF THE CPNI

(CENTRE FOR THE PROTECTION OF THE NATIONAL INFRASTRUCTURE)

- Each element of CNI responsible for own defence
- CPNI is advisory not regulatory
- CPNI facilitates information exchange
- CPNI assesses and advises of threats
- CPNI provides technical support and assistance
- ***BUT*** is that enough?

THE DANGER OF COMPLACENCY

- MI5: Britain “four meals away from anarchy”
- Public sector compliance with security requirements is poor
- Risk for private enterprises is not the same as risk to the country
- Is there a proper disaster recovery plan?

REGULATION vs. VOLUNTARISM

- Does a voluntary approach lead to more cooperation?
- The commercial risk gap
- Why is the approach a voluntary one within Government?
- What drives the recovery plan in the event of disaster?
- Requiring greater responsibility from individuals and from the corporate sector

AN AGENDA FOR LITTLE RED RIDING HOOD - I

- High level political leadership
- “Muscle” within Government:
  - Service delivery requires that the systems underpinning services are secure from attack
  - KPIs within Government to reflect importance of information security and clear lines of responsibility
  - Guidelines for next Spending Round to require that security is built into systems
  - Giving statutory status to CPNI with powers of regulation (and direction) in and outside Government

AN AGENDA FOR LITTLE RED RIDING HOOD – II

- For the private sector operating part of the CNI brings with it certain responsibilities
- Prescribing standards for the design and operation of the CNI
- Monitoring those standards and requiring compliance
- Locating responsibility for recovery planning and providing legal authority

AN AGENDA FOR LITTLE RED RIDING HOOD - III

- Strengthening Data Protection Act
- A new Data Breach Notification Law
- An IT Sarblanes-Oxley?
- Sharing the responsibility equitably:
  - Equipment manufacturers and suppliers
  - Software manufacturers
  - Service suppliers
  - End-users

AN AGENDA FOR LITTLE RED RIDING HOOD - IV

- Proper system of recording security breaches and e-crime
- Higher priority to tackling high-tech cyber-crime
- Exacerbation by computer?
- Strengthen the Computer Misuse Act
- Building international cooperation

ALL FAIRY TALES HAVE A MORAL

- Information security is not an optional extra
- Information security is as important as physical security
- At best reputation and public/business confidence are at risk
- Delivery, delivery, delivery or the bottom line are all vulnerable
- Ultimately survival depends on it

FIRST IS BEST

- F is for Firm Leadership
- I is for investment
- R is for regulation and Enforcement
- S is for a security culture
- T is for Trust in the IT security experts

….. and happily ever after?

LORD TOBY HARRIS

Toby Harris Associates
26 York Street
London W1U 6PZ

toby.harris@blueyonder.co.uk