

INFORMATION SECURITY – PUBLIC CONFIDENCE ENDANGERED?

Lord Toby Harris

tobyharris

Monday 15th September

ENISA - FORTH: Network and
Information Security

INFORMATION SECURITY – THE POOR RELATION

- Information security – the poor relation of technology
- Information security – the poor relation of security
- Why has this happened?
 - Emotional issues
 - Cultural issues
 - Financial issues
 - Cynicism

WHY IDENTITY AND SECURITY MATTER

- Advent of broadband and new communications technology
- Convenience and changing expectations
- E-commerce
- E-government and efficiency
- Critical national infrastructure

AND WHY ARE PEOPLE STARTING TO WORRY?

- Identity theft, e-crime, phishing etc
- Corporate data loss, hacking and vulnerability
- Government data loss and state-sponsored attacks (terrorist attacks to come?)
- And no-one is accepting responsibility

 - Personal
 - Corporate
 - Government

WHERE DOES THE THREAT COME FROM?

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

WHAT ARE THE RISKS

- DDoS attacks, malware, email spam, phishing, identity theft etc
- Compromising of personal safety
- Scale difficult to determine but increasing and perception of risk rising even faster
- “e-crime” not separately recorded: “fraud is fraud, child abuse is child abuse”

WHAT PUTS PEOPLE AT RISK

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

Made worse by products behaving badly

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
- In 2006/7, admitted system compromises:
 - 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
- In 2008: “not in the public interest”

HOW BIG A RISK TO THE CNI?

- Republic of Estonia – cyber-attack May 2007
- Cyber spying biggest security threat – 3rd Annual Virtual Criminology Report (input from NATO, FBI, SOCA etc)
- Cyber disruption in Georgia – July/August 2008
- Cabinet Office National Risk Register – August 2008

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

LORDS SELECT COMMITTEE ON PERSONAL INTERNET SECURITY

- 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

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?

MIS-SELLING ID CARDS

- 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

SO WHY SHOULD THE GOVERNMENT ACT?

- 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 CAN GOVERNMENT DO?

- 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

MAKING GOVERNMENT ACTION EFFECTIVE

- 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

THE RESPONSIBILITY OF THE CORPORATE SECTOR

- For the private sector operating part of the CNI brings with it certain responsibilities:
 - Prescribe standards for the design/operation of the CNI
 - Monitor those standards and require compliance
 - Locate responsibility for recovery planning and providing legal authority
- Generally sharing the responsibility equitably:
 - Equipment manufacturers and suppliers
 - Software manufacturers
 - Service suppliers
 - End-users

A STRONGER LEGAL FRAMEWORK?

- Strengthening Data Protection Act & Computer Misuse Act
- A new Data Breach Notification Law
- An IT Sarbanes-Oxley?
- Proper system of recording security breaches and e-crime
- Higher priority to tackling high-tech cyber-crime
- Exacerbation by computer?
- Building international cooperation

A SIMPLE MESSAGE FOR ALL

- 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

LORD TOBY HARRIS

Toby Harris Associates
26 York Street
London W1U 6PZ

toby.harris@blueyonder.co.uk