Regulating for Information Security

Professor Ian Walden
Institute of Computer and Communications Law
Centre for Commercial Law Studies, Queen Mary, University of London
Introductory remarks

- Legal frameworks
- Regulatory controls
  - Behavioural obligations
    - e.g. breach notification
  - Regulatory institutions
- Protecting critical national infrastructure
- Facilitating authentication & data integrity
- Controlling cryptography
Legal frameworks

- e.g. African Union Convention on ‘Confidence and Security in Cyberspace’ (draft)
  - Electronic commerce
    - Validity & enforceability; transparency requirements & contractual obligations
  - Security
    - Evidential rules, electronic signatures & certification schemes
  - Data Protection
    - Security obligations
  - Cybercrime
    - Substantive & procedural law
Institutional response

• Supervisory authorities
  – Independent, oversight (incl. audit rights) & enforcement
    • e.g. Data protection, NIS, Trust services……

• Computer Security Incident Response Teams (CSIRTs)
  – CERT Co-ordination Centre
    • From Carnegie Mellon University (1988) to more than 84 nations
    • Reactive & proactive services

• Warning, Advice & Reporting Points (WARPs)
  – Community-based
    • Filtered warnings, advice brokering & trusted sharing
Critical National Infrastructure

• Dual nature of the Internet
  – As source of threat & protected subject matter
    • e.g. US, *The National Strategy to Secure Cyberspace* (2003): “the healthy functioning of cyberspace is essential to our economy and our national security”

• Protecting infrastructure
  – e.g. UK: Civil Contingencies Act 2004, Category 2 Responders, s. 22: ‘public electronic communication networks’
  – e.g. Australia: Telecommunications and Other Legislation Amendment (Protection of Submarine Cables and Other Measures) Act 2005, No. 104

• Protecting data
  – e.g. South Africa: Electronic Communications and Transactions Act 2002
    • Chapter IX: ‘Protection of Critical Databases’
      – “Minister may prescribe minimum standards or prohibitions in respect of..”
eSignatures....

• Digital signatures, PKI & certification services
  – e.g. EU Directive ‘electronic signatures’ (1999) to Regulation on ‘electronic identification and trust services’ (2014)

• Legal recognition

• Regulatory schemes
  – Qualification
    • Mutual recognition & interoperability
    • Liability
Controlling cryptography

• Cryptographic systems/software as a dual-use good
  – Authorisation schemes

• OECD Guidelines for Cryptography Policy (1997)
  – 8 principles
    • Trust in & choice of cryptographic methods
      – e.g. NSA & the Dual EC DRBG standard!
    • Protection of privacy & lawful access

• Wassenaar Arrangement
  – 41 parties (incl. most EU states, US, Russia, Japan)
    • 2013 Reforms: ‘Advanced Persistent Threat Software and related equipment (offensive cyber tools)’
Concluding remarks

• Cybersecurity & the rule of law
  – Legal certainty

• Confidence, trust & security
  – Shifting liability & risk
    • e.g. Consumer protection rules

• Cost & impact of regulation
  – For the market & for the state
    • e.g. digital signatures & PKI