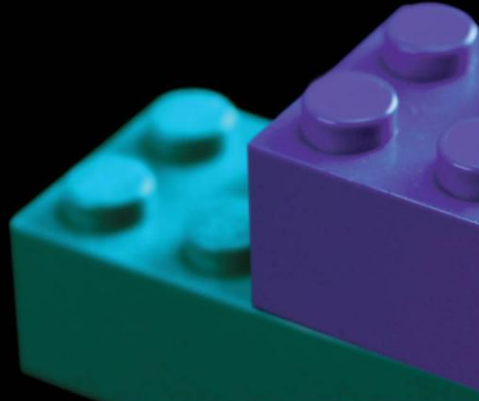


Data protection and breach notification experiences

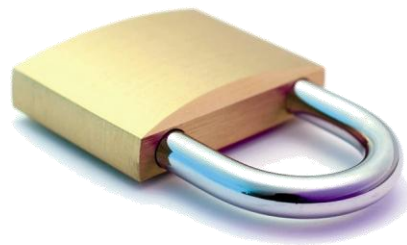
Stewart Room

February 2010



Breach Disclosure

Building a new legal framework for data security



New legal framework for data security

- Third cycle of legal development, since 2003
- Creation of the “regulatory bear market”
- Trajectory of the law is to more disputes and litigation

Components of the new legal framework

- Legislation
- Government policy
- Regulatory guidance
- Rules for best practice
- Enforcement actions
- Case law
- Private law arrangements

Issues, ideas and philosophies in breach notification

- Political interest
- Protection of personal information
- Bites on unprotected information
- Transparency mechanism
- Early warning system
- Do no harm principle
- Adjusting power

The forthcoming EU regime (1)

- Dir 2002/58/EC amendment cycle from November 2007 to October 2009
- Providers of publicly available electronic communications services
- Access control mechanisms
- Description of terrors
- Security policy
- Best practice recommendations
- Breach disclosure

The forthcoming EU regime (2)

- Personal data breaches
- Notifying without undue delay
- Standardisation of form and content
- Technical implementing measures
- Guidelines on disclosure
- Auditing
- Inventory of breaches
- Sanctions

The current UK regime

- ICO guidelines, March 2008
- FSA Handbook
- Data Handling Review
- Operation of standards for best practice, eg 27001
- Private law arrangements within PCI DSS
- Freedom of Information
- Law of confidence & HRA
- Litigation disclosure

Preparing for the new environment

- Systems v. operational regulation
- Security policy
- Contract initiation
- Project initiation
- Worker adequacy
- Third party assurance
- Culture

For further information

- Data Security Law and Practice
- stewart.room@ffw.com