Legal aspects of information security

23 May 2013
Ross McKean
Agenda

• What could it cost me?
• What is the enforcement risk?
• What are my legal obligations?
• How secure is secure?
• Supply chain and cloud risks
What could it cost me?

£450-850k average cost to large organisation of worst security breach

£35-65k average cost to small business of worst security breach

Information Security

Breaches Survey

PwC 2013

"Just a darn minute! Yesterday you said X equals two!"
What is the enforcement risk?

**ICO monetary penalties: the triggers**
- serious contravention of DP principles
- likely to cause substantial damage or distress
- deliberate or reckless (and failed to take reasonable steps to prevent the risk)

  = monetary penalty

**ICO’s seriousness rating:**
- “serious”: £40,000 - £100,000
- “very serious”: £100,000 - £250,000
- “most serious”: £250,000 - £500,000

**Some stats**
- Security related ICO fines since 2010: 32 (out of 35 fines)
- Average ICO fine since 2010: **£90 k**
- Highest ICO fine: **£325,000** Brighton and Sussex University Hospitals NHS Trust
- FSA fines for data breaches: e.g. Zurich insurance **£2.2m** (2010); Norwich Union **£1.26m** (2007); HSBC **£3m** (2009)
The changing legal landscape

Maximum UK penalty for DP breaches now: £500,000

Maximum penalty under the draft General Data Protection Regulation:

£2% of global turnover

“The supervisory authority shall impose a fine
up to 1 000 000 EUR or
in case of an enterprise up to 2 %
of its annual worldwide turnover”
Article 79 GDPR
What are my legal obligations?

Data Protection Act 1998, Seventh Principle

- *Appropriate* technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. *(Schedule 1, Part 1)*

What’s “appropriate”?

- Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to -
  
  - A) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
  
  - B) the nature of the data to be protected.

Plus specific requirements relating to processors / supply chain. *(Sch 1 Part 2)*

+ Sector specific rules
How secure is secure?

ICO guidance

• A practical guide to IT security – June 2012
• ICO’s “our approach to encryption”
• Guidance on cloud computing – October 2012
• Guidance on BYOD - February 2013

BIS/ CESG/ GCHQ

• 10 steps to cyber security - October 2012

Technical standards

• ISO 27001
Supply chain and cloud

• Increasingly extended, complex, international supply chains
• Controller remains liable – and only as “secure” as the weakest link
• Brighton NHS fine arose from failure by contractor to wipe data from PCs

Key watch out points
• Assess your risk and know your supply chain – kick the tyres
• Assess supplier’s security: 7th Principle
• Where is the data actually held? 8th Principle
• Is it actually deleted?
• Can you audit the above? Third party audit?
Contact details

For more information please contact:

Ross McKean
+44 20 7067 3378
ross.mckean@olswang.com