

Data Security Corporate Counsel Forum



Kemp Little LLP
22 January 2009





Upcoming Events

Kemp Little, in association with PLC, is hosting a series of breakfast and evening forums for senior corporate counsel to address **key business challenges** for in-house legal teams in 2009 as identified by recent research by PLC.

Data security – laptops left on trains, discs lost in the post and lists found in litter – safeguarding your business against security breaches

- 19 February 2009 (*evening panel forum*)



Upcoming Events

SaaS, FLOSS, SOA and GPL - cheaper software and alphabet soup: securing the benefits and avoiding the pitfalls

- 4 March 2009 (*breakfast CCF*)
- 18 March 2009 (*evening panel forum*)

The devil in the detail of BPO - managing risk and improving return as deals become smaller, shorter, cheaper and universal

- 1 April 2009 (*breakfast CCF*)
- 18 April 2009 (*evening panel forum*)

HR Restructuring – negotiating the minefield and how to get it right

- 15 May 2009 (*evening panel forum*)
- 3 June 2009 (*breakfast CCF*)

Today's agenda

- Housekeeping
- **Dealing with personal data security breaches**
Calum Murray, Kemp Little LLP.
- **Ensuring Data Security – Is your data safe?**
Paul Young, KPMG Advisory
Tom Hopkinson, KPMG Forensic
- Short coffee break
- Q&A

Dealing with personal data security breaches ('PDSB')



PDSB: legal context

- Article 17(1) – data controllers ('DC') to:
*'...implement **appropriate technical and organizational measures** to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing'*
- Seventh data protection principle ("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'*
(paragraph 7, Part I, Schedule 1, Data Protection Act 1998 ('DPA')).
- ICO – onus on DC to ensure compliance with Seventh Principle for any processing of personal data it undertakes (and rest of DPA!)
- how to take *'**appropriate technical and organisational measures**'* ?
- standard DPA terms apply

PDSB: appropriate measures

- ‘*appropriateness*’ of security measures - on a case-by-case basis

- ICO suggests;

- DC adopt a ‘risk-based approach’ to ‘*appropriateness*’ –

“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”.

(see paragraph 9, Part II, Schedule 1, DPA)

- approach to be consistent and continual
 - use ‘*privacy enhancing techniques*’
 - management & organisational = technical

PDSB: appropriate technical measures

- *‘privacy enhancing techniques’*

- ICO

- standards - ISO standards 27001 and 27002

- encryption -

“all portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information”.

- remember ‘continual’ approach
 - and if not...



PDSB: appropriate organisational measures

- processes, polices and supportive training and practices:
 - **processes** – both physical and virtual
 - **policies** - for all aspects of system use and data content lifecycle
 - **staff** - selection, education and update training
 - **practices** – standard implementation
- **contractual** considerations
 - OGC and lessons there
 - third party processors
 - the ‘model’ clauses

PDSB: discovering a PDSB

- post initial reaction (!&*?#!) ...have you got a **policy**?
- ICO – 4 key elements:
 - containment and recovery
 - assessment and risk
 - evaluation and response
 - notification of breaches
- who's on the **team**?
- **chronology** of considerations



PDSB – reacting to a PDSB

- **assessment and risk** –
 - nature of the data and what's happened to it
 - was the data protected and what could a recipient get from it
 - what is the extent of the breach and what harm could follow
- **evaluation and response** –
 - what were causes of the breach
 - how did you respond - did your processes work
 - how can this be improved

PDSB – notifying of a PDSB

- current **legal** position – c.f US
- public sector, regulated or contractually bound?
- ICO’s best practice: serious breaches to be notified and overriding consideration is potential harm to individuals
- ICO creates presumptions to report:
 - “*where there is significant actual or potential harm as a result of the breach, whether because of the volume of data, its sensitivity or a combination of the two”*
 - “*where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm”*
 - “*where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial harm”*
- so... potential harm x volume of data x sensitivity of data?
- ...but still **voluntary**

PDSB – deciding whether to notify

- ICO Good Practice Note:

“Informing people and organisations that you have experienced a data security breach... is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.”

- assuming not obliged to - why?

- maintaining public confidence in data sharing v. operating a transparent business operation

PDSB – decided to notify

- things to get right when notifying
 - **content of notification** - detail, security, response
 - **medium of notification** – communicate effectively
 - **audience of notification** – proportionality, tone
 - **related support to notification** – guidance, assistance, other support
- who do you have to tell v. who are you choosing to tell?
- other interested parties
- media?

PDSB – responses to notification

- ICO: assessment of breach and adequacy of response
 - no further action or investigation
 - outcomes of investigation –
 - no further action
 - imposition of requirements
 - instigation of formal enforcement action
 - enforcement outcomes and reputational influence
 - additional powers of ICO
- Other parties:
 - contractual counterparties
 - affected data subjects
- is change coming?

Useful URLs

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L281/31)

http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

- Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

- Data Protection Act 1998 - ICO Legal Guidance

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

- ICO Good Practice Note Guidance on data security breach management

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf

- ICO Good Practice Note Guidance on notification of data security breaches

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf



FORENSIC

Ensuring Data Security – Is your data safe?

Breakfast seminar – Kemp Little LLP
Thursday, January 22, 2009

ADVISORY



Agenda

- Background
- Implications
- Three pillars of information risk
- Five deadly sins
- Five top tips
- Questions

Data (in)security is high profile

“Data on more than 6,000 prisoners lost”

Source: Telegraph.co.uk 9/1/08

“Leak shows law firm's view of clients”

Source: Timesonline 22/09/05

A million bank customers' details sold on eBay for £35

Source: Telegraph.co.uk 26/08/08

“Facebook generation' too lax with data, warns information watchdog”

Source: Timesonline 29/10/08

“We are living in an age where protecting your information has never been so important”

UK Information Commissioner's Office

“We may take enforcement action if firms fail to encrypt customer data take offsite”

UK Financial Services Authority

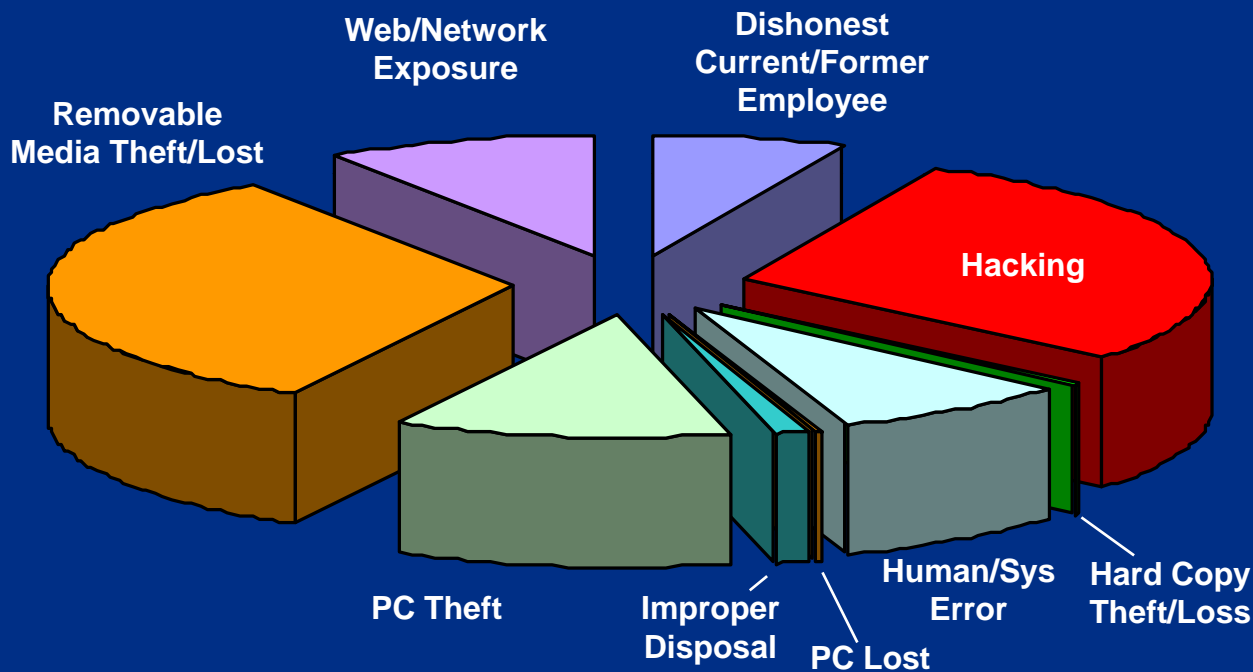
Implications for companies

- You have access to highly valuable, proprietary information
- 95+ of all business records exist only in electronic format
- Your clients expect data security; it is a competitive advantage
- Do you have a business model that leads to a loss of control, i.e. outsourcing, off-shoring etc?
- The way we work has changed (i.e. mobile access etc)
- ...and so has your organisational culture (i.e. “Y” generation)

Reputation – what would be the effect on your business if your firm became known as one that loses data?

Key incidents / threats

People affected vs. type of breach:



Threat actors:

Opponents on cases

Disgruntled employees

- Accidental loss

Competitors

- Seeking competitive intelligence

Organised Crime

- Patterns from Eastern Europe

Foreign Intelligence Services

- Politically / Economic motivated

Source: Data Loss Barometer, KPMG 2008. Excludes figures for three major incidents.

Three pillars of information risk

1. Confidentiality

- Information is not disclosed to unauthorised individuals, entities or processes
- The need to keep information secret

2. Integrity

- Safeguarding the accuracy and completeness of information
- The need to place trust in the information

3. Availability

- The information is accessible and usable upon demand by an authorised individual, entity or process
- The need to access information at the right time in the right place



Five deadly sins

1. Do not use Yahoo / Gmail / Hotmail for work
2. Do not do work on your home computer
3. Do not rely solely on your IT team to make security decisions
4. Do not carry confidential information on an insecure device
5. Do not publish your life on the web (incl. Facebook etc)



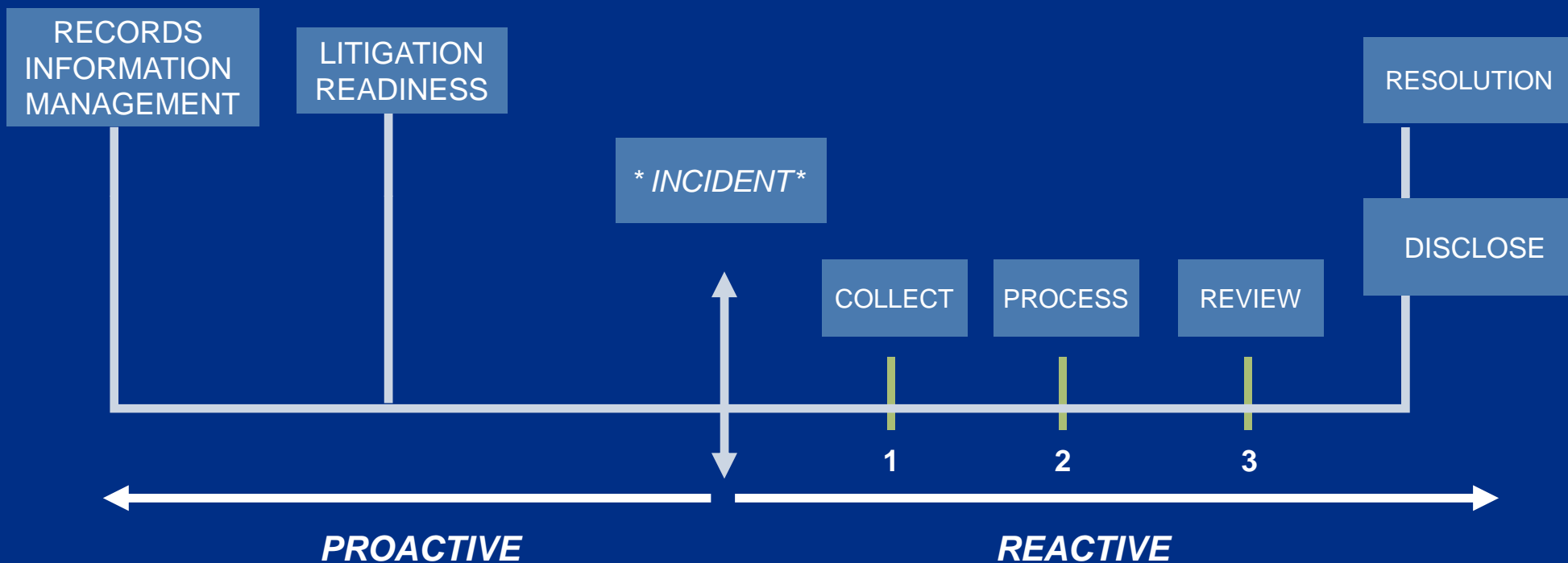
Five top tips

1. Treat client data as Gold - know where it is, how it is stored, who has access to it
2. Promote a culture of security amongst all staff, *led from the top*, and rigorously control the use of personal devices
3. Take IT security responsibility for your business decisions
4. Vet your staff
5. Have a clear plan on what you should do if you lose data

Of those data security breaches caused by company insiders, **37%** are **malicious**

Source: Compuware, 2008 Survey

E-discovery



Five questions for your IT department

1. Is my laptop data encrypted?
2. Do you dispose of our old IT equipment securely?
3. Is our firm's anti-virus up to date?
4. Do you provide secure data backup for me?
5. Can I send client data securely using our email?

Q&A, contacts



Tom Hopkinson

Tel: +44 20 7694 5304

tom.hopkinson@kpmg.co.uk



Paul Young

Tel: +44 7876 034 115

paul.young@kpmg.co.uk