Management of a data breach.

Mick Gorrill

Assistant Commissioner,

23rd October 2009.

▶ 7.25m claimants ▶ 15.5m children ▶ 2.25m partners and carers

NORTH NEWS AND PICTURES

Police search offices at the HMRC Child Benefits Agency office in Washington, Tyne & Wear, from where two CDs containing confidential records went missing

25 million exposed to risk of ID fraud

- **Police are investigating the theft of a laptop from a Royal Navy officer which had held the personal details of 600,000 people. Police said the laptop was taken from a vehicle which had been parked in the Edgbaston area of Birmingham.**
- **It contains data including passport numbers, National Insurance numbers and bank details.**
- **They relate to people who had expressed an interest in, or joined, the Royal Navy, Royal Marines and the RAF.**

HMRC Data Loss.

- The two major institutional deficiencies were:
- Information security simply wasn't a management priority AND
- HMRC had an organisational design which did not clearly focus on management accountability.
- Poynter report June 2008.

Management of a Data Breach.

- In most cases where there is poor security there is also excessive information and poor retention –
- In the security breaches reported to the ICO there is little evidence of privacy impact assessments and or risk assessment.

Sector	Disclosed in Error	Lost Data/ Hardware	Lost in Transit	Non-secure Disposal	Stolen Data/ Hardware	Technical/Procedural Failure	Other	Grand Total
Central Gov	17	25	10		9	5		66
Local Gov	24	16	5	1	27	8		81
NHS	18	57	11	10	85	11	6	198
Other	3	1	1		4	2	1	12
Other Public	29	20	10	2	21	6	4	92
Private	56	35	10	6	66	18	6	197
Third Sector	6	10	1		12	4		33
Grand Total	153	164	48	19	224	54	17	679

Management of a Data Breach.

- All self reported security breaches are fast tracked to the Regulatory Action Division.
- Allocated to an enforcement unit case worker.
- ICO action depends on seriousness of breach,

Management of a Data Breach.

- Many breaches are dealt with informally,
- Advice given or sometimes a strongly worded letter,
- May also suggest DP Audit,
- Around 5% of the breaches have led to regulatory action,

Management of a Data Breach.

- Most common form is a formal agreement
- Or
- Formal undertaking –
- Normally signed by CEO or senior manager –
- ICO follow up after specified period.

Regulatory Action.

- The ICO has taken regulatory action against the following organisations in the public and private sector since November 2007,
- 22 NHS Trusts,
- 8 Private sector organisations,
- 3 Central Government Departments.

Management of a Data Breach.

- Types of breaches:
- Unencrypted portable media devices containing personal information lost or stolen,
- Electronic transfer,
- Disposal of old hardware – hard drives,
- Poor policing data processor contracts-
- Storage and disposal of back up tapes.

Security Breaches

C. Chris Slane

Management of a Data Breach.

Paper files also cause problems;

Examples:

- Hospital relocation,
- Filing cabinets sold on containing paper records (300 probation files in a cabinet on the back of a lorry),
- All avoidable with a little care.

Management of a Data Breach.

- In general, policies and procedures are reasonable but not well known by staff,
- Many breaches are avoidable and are often a result of poor management processes.

Management of a data breach.

- Considerations are:
- Distress and or damage to data subject,
- Type of data –
- Circumstances of breach – avoidable?
- Policies and procedures?
- Evidence of risk assessment?
- Avoidable – poor culture?

Management of a Data Breach.

- Risk Assessment;
- Has the nature of the data, i.e. sensitive been taken into account?
- Is all data treated the same – recognition of higher likelihood of distress – medical records, bank account details, social service records?

Management of a Data Breach.

- Breach Management Plan.
- Containment and recovery.
- Assessment of ongoing risk.
- Notification of breach.
- Evaluation and response.

Management of a data breach.

- Previous breach?
- Appropriateness of regulatory action.
- Possible outcomes:
- Advice re policies and procedures,
- Requirement to sign a formal undertaking as an alternative to enforcement action,
- Enforcement Notice.

Mitigating Risk.

- Breach management plan.
- Privacy Impact Assessment.
- Internal DP Compliance Audit,
- ICO Compliance Audit,
- Personal Information Promise.

Audit and Inspection

- Consent based
- Government “spot checks”
- Constructive process
- ICO and external resources
- Wider powers

Monetary Penalties.

- Possibility of a penalty should act as an encouragement towards compliance
- Or a deterrent against non compliance.
- The penalty must be sufficiently meaningful to act both as a sanction to punish wrongdoing but again a deterrent to that data controller and other data controllers.

Monetary Penalties.

- Before the Commissioner exercises his discretionary power to impose a monetary penalty – has to be satisfied that:
- There has been a serious contravention of S4(4) by the data controller,
- The contravention likely to cause substantial damage or substantial distress,
- The contravention was deliberate
- or

Monetary Penalties.

- The data controller knew or ought to have known that there was a risk that the contravention would occur and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention.

Management of a Data Breach.

- Any Questions?

Information Commissioner's Office

www.ico.gov.uk