Sheffield Hallam University

Once more unto the breach...

Dealing with Personal Data Security Breaches

Helen Williamson
Information Governance Officer

Sheffield Hallam University

Aims of the session

What are we going to look at?

- What is a data security breach?
- Why do breaches need managing?
- What are the risks?

- Our experiences - how Sheffield Hallam University has managed breaches and lessons learnt

Sheffield Hallam University

Why does data security matter?

Data Protection Act requirements

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.

The 7th Data Protection Principle

Sheffield Hallam University

ICO Corporate Plan

Published 25 March 2014

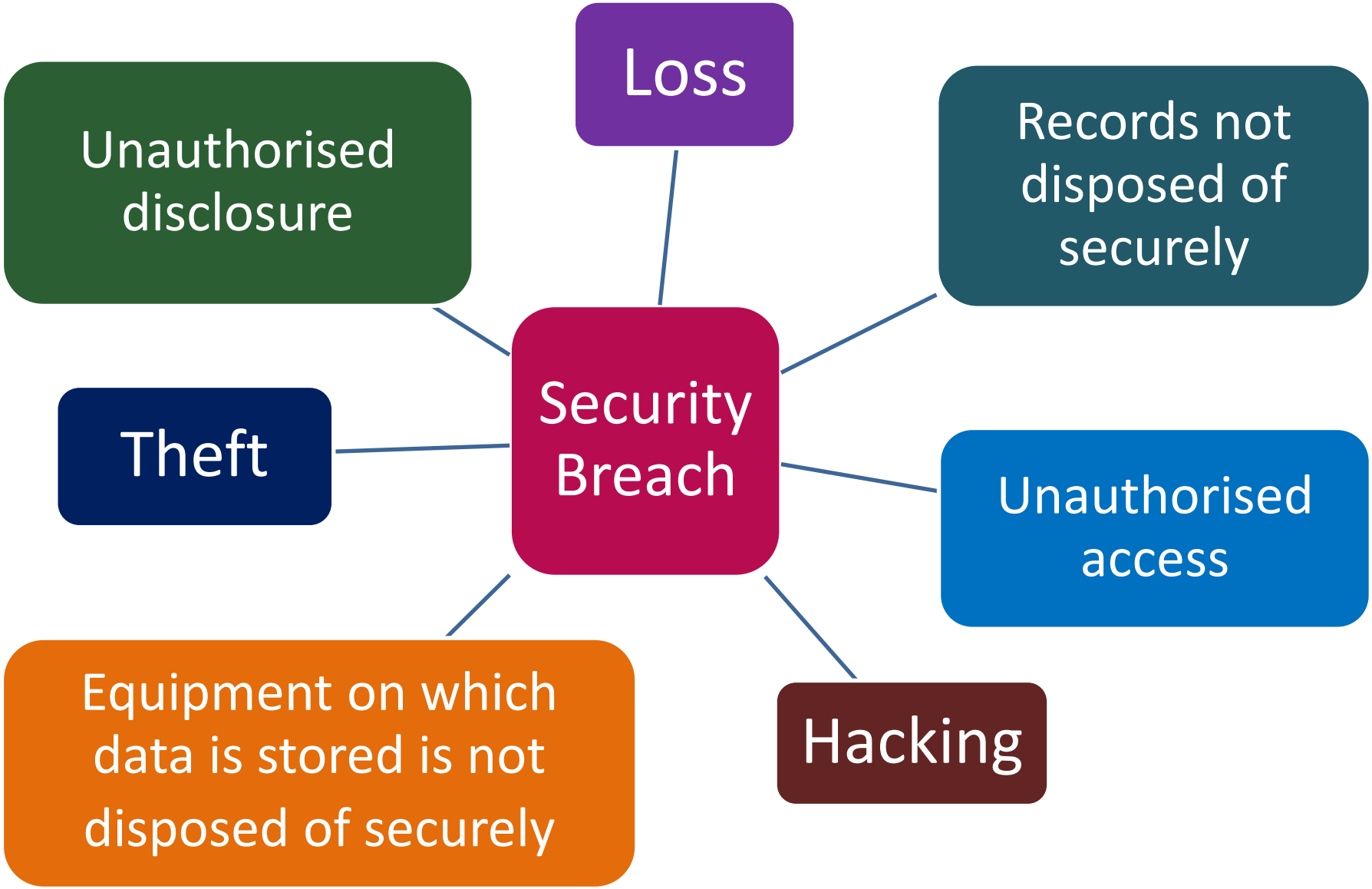
The plan confirms that we will be adopting a fresh approach to handling people's data protection concerns, with cases brought to our office being increasingly used to identify broader data protection problems and improve organisations' current practices.

Sheffield Hallam University

What is a Data Security Breach?

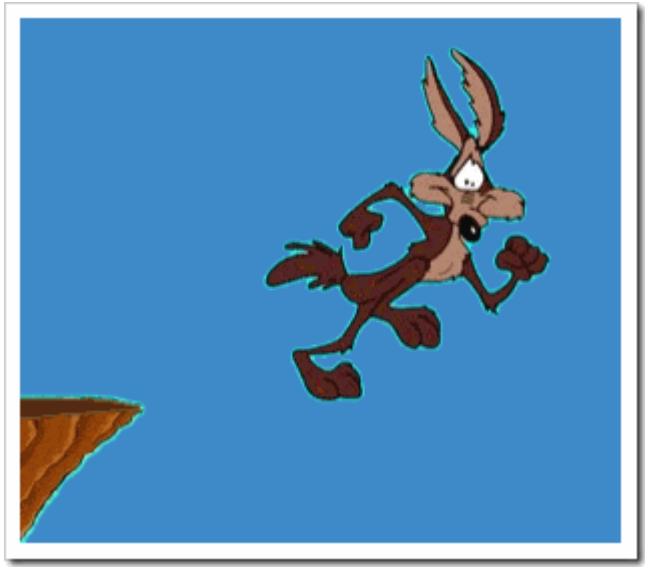
an event or series of events leading to the unintentional or unauthorised disclosure of information which compromises the security, confidentiality or integrity of data

Sheffield Hallam University



Sheffield Hallam University

Near Misses and Close Calls



i.e. the point just before the point of no return

helps to identify risk areas and to manage those risks before breach incidents occur

Sheffield Hallam University

Possible consequences and actions

- Damage and distress to data subjects
- Complaints from data subjects
- Investigation and enforcement action by Information Commissioner
- Reputational damage and negative press coverage
- Monetary penalties or fines
- Staff disciplinary issue
- Criminal offences
- Loss of trust amongst stakeholders
- Civil action: Compensation and legal fees

Sheffield Hallam University

The Fine is Right !

Sheffield Hallam University

What is the maximum ICO fine for a breach of the DPA?

A. £10,000
B. £50,000
C. £100,000
D. £500,000
E. £1,000,000

Sheffield Hallam University

How much is the highest fine issued so far?

A. £175,000
B. £225,000
C. £275,000
D. £325,000
E. £424,000

Sheffield Hallam University

Which security incident resulted in the highest fine?

A. Theft of a bag containing papers relating to a child sex abuse victim
B. 3000 patient records found on second hand computer bought on online auction site
C. NMC loses 3 DVDs of student fitness to practice case inc. details of vulnerable child
D. Sony website hacked compromising the details of millions of customers inc. passwords and payment card details.
E. Bank of Scotland repeatedly faxed customer details to wrong recipients

Sheffield Hallam University

A Question of Data Security

What happens next?

Sheffield Hallam University

New member of staff uses hybrid copier/scanner/fax machine in open plan office

A. Presses fax instead of scan and sends documents to last number dialled
B. Scans it but sends it to a shared drive which is accessible to 50 other staff
C. Presses copy instead of scan, leaves machine running and returns to find copies gone
D. Collects copies from printer and also picks up someone else's documents which all go in same envelope to external third party

Sheffield Hallam University

Member of staff's IT account hacked

A. Member of staff used work email for personal banking and responded to phishing email.
B. Student complainant saw login on post it note on her desk during appointment
C. Gave out login details to PA on bus unaware that a fellow passenger recognised login as SHU
D. Family member added key logger to machine

Sheffield Hallam University

External assessor takes application forms away from panel meeting

A. Reads papers on train and fellow passengers shoulder surfs
B. Leaves papers in station toilets and returns to find that they have disappeared
C. Sees that applicant is sister of pop star and sells information to press
D. Realises one of the applicants is a neighbour and posts information on Facebook

Sheffield Hallam University

Data Security Breach Management Procedure

Our procedure and experiences

- Short procedure devised in 2009 in line with ICO guidance and following series of high profile data losses, e.g. HMRC child benefit records
- Feedback from auditors and experience led to review in 2011/12
- Revised procedure issued in 2012.

Sheffield Hallam University

Aims of the Procedure

- provide clarity about who shall do what, why and when at each point once a security breach has been identified;
- ensure that action is properly coordinated
- limit the damage caused by the breach
- identify improvements in data security which will prevent similar breaches in the future
- ensure that there is a proper audit trail of actions and decisions.

Sheffield Hallam University

The Procedure: 6 stages

1
- Discovery
- Reporting

2
- Assemble Data Breach Team

3
- Containment
- Recovery

4
- Notification

5
- Evaluation
- Response

6
- Implementation
- Audit

Sheffield Hallam University

Discovery and Reporting

- Relies on one of our 4000+ staff recognising a data security breach and knowing/remembering who to report it to
- Information Governance Officer takes initial account of breach:
  - which data have been lost or compromised
  - how the data have been lost or compromised
  - when the breach occurred
  - where it occurred.
- Initial breach level (minor or major) – determines who attends breach team

Sheffield Hallam University

Assembling a Data Breach Team

- Drawing on wider pool of expertise and specialisms
- Value in unpicking incident using different perspectives
- Template/checklist for meetings to ensure all aspects covered
- Gives added weight

Sheffield Hallam University

Alignment with other processes

- HR processes - staff disciplinary
- Student and staff complaints
- Internal and external communications
- Fraud response plan
- Major incident plan and business continuity

Sheffield Hallam University

Notification

When and what to communicate to stakeholders

- What is the harm or likely harm to individuals?
- Could notification help individuals to mitigate the risk?
- Is there a danger of "over notifying" which may cause disproportionate enquiries or distress?
- Should the ICO be notified?
- Is there a need to notify other third parties?
- Should the media be informed or is it necessary to prepare a response to possible media enquiries?
- Is there a need for a contact procedure for further information or questions, e.g. a helpline number or web page?
- How urgent is the need to inform individuals or organisations?

Sheffield Hallam University

Responding to the ICO

General points

- Usually required within 3-4 weeks of receiving ICO letter
- Full response – usually only get one opportunity so tell them everything they need to know
- Provide evidence of what has been done
- No need to quote lots of legal jargon at them

Sheffield Hallam University

Case Study - Student Email

The breach

- Member of student administration staff emailed hundreds of students returning from placement year using SHU and personal email addresses.
- Entered all addresses into the "To" field instead of "Bcc" field.
- Effect was to share each email address with all other recipients.
- One student complained to the ICO that we had shared their address

Sheffield Hallam University

Case Study - Student Emails

Putting the Procedure into Action

- Assembled team
- Minuted meeting using template
- Investigation
- Emails to all affected students
- Email apology to the complainant
- Guidance to staff delivered via Communication Plan
- Changes to email set up
- Publicised email auto-forward function to students
- Review Meeting

Sheffield Hallam University

Our response to the ICO

What we included

- Background/context about University and HE
- Data Security Breach Management Procedure
- Action taken
- Notes of meetings
- Copies of emails/notifications/apologies
- Advice issued to staff
- Screen shots of information posted on intranet
- How the issue will be addressed in staff training
- Details of planned review

Sheffield Hallam University

Outcome of ICO's investigation

Key points in the letter from the caseworker

- Compliance unlikely
- 7th Data Protection Principle breached
- The University's data security breach management procedure is "comprehensive"
- No enforcement/regulatory action in this case
- "Thank you for your timely and very thorough investigation of this complaint and your very detailed response to us."

Sheffield Hallam University

Strengths and benefits of Data Breach Management

What we feel works well

- Good procedure:
  - Comprehensive
  - Enables us to deal with broad range of incidents
  - Integrates with other procedures

- Team
- Enlisting help from internal communications team for emergency communications
- Thorough response to ICO with evidence of actions
- Template for meetings

Sheffield Hallam University

Lessons Learnt and Future Challenges

- Further improvement of awareness of the procedure and the need to report incidents and near misses
- Staff anxiety about procedure and meetings – fears about potential consequences
- Difficulty in assembling senior staff quickly
- Small incidents with no wider consequences dealt with by email and signed off by Chair
- Better communication of lessons learnt across the University