

PRIVACY BREACH CHECK LIST

► FIRST 24 HOURS...

Identify someone who can coordinate a response

Gather information

- ? Has the data really been misplaced or has it been stolen? Might it be still in the premises, or easily retrievable?
- ? What information is involved? Is it very sensitive personal information?
- ? How many people are affected?
- ? What other organisations are involved?
- ? What are the risks that could arise as a result of the breach? Will people suffer major consequences as a result of the breach?
- ? How quickly might people be affected by the breach?
- ? Is the matter likely to be of great media interest?
- ? If there is to be public discussion, identify a company spokesperson who can speak with authority and if necessary, continue to do so right through the crisis whether resolved immediately or over a lengthy period of time?
- ? What regulatory authorities might be involved?

Work out immediate response

- ? What immediate steps do we need to take to prevent any further breaches? E.g. shut down website or coordinate with other organisations involved
- ? What immediate steps do we need to take to prevent or minimise harm to individuals from the breach e.g. in relation to credit reporting monitoring,
- ? What do we need to do to ensure that no evidence is destroyed if the matter is likely to be reported to the police?
- ? Do we need to make the breach public immediately? (Is it likely to be leaked? Is it urgent that consumers know straight away? Will the brand be best maintained by telling people straight away?)
- ? Whom do we need to inform internally and what will we tell them?

► FIRST WEEK...

Further investigation and steps to retrieve information if possible

Prepare and implement an issues management strategy

- ? What if any regulators will we inform?
- ? Do we need to inform the stock exchange?
- ? Is it important that we tell the consumers affected? If so what?
- ? Will we tell the police? Is it a criminal matter?
- ? Is it a public interest matter that we should tell the media about? If so what?
- ? What key message do we want the public to know?
- ! If there is to be public discussion, identify a company spokesperson who can speak with authority and if necessary, continue to do so right through the crisis whether resolved immediately or over a lengthy period of time
- ? How much do we tell staff internally and who do we tell?

Prepare a written outline of what has happened and keep track of who contributed information to the outline. Include a list of all staff involved and who discovered the problem

Take any short term remedial steps necessary to deal with breach and prevent further breaches

► LONG TERM PREVENTION...

After first week if problem not fixed

- ! Prepare a long term issues management strategy
- ? What steps can be taken to recover data in the longer term?
- ? When should we halt steps to recover if the issue is not resolved?

Policies and procedures

- ? Do we fully understand the "lifecycle flow" of information in our organisation's system?
- ! Review security policies and procedures and amend to strengthen security procedures
- ! Review risk management procedures and ensure these are adequate

Technology

- ! Review computer systems and ensure technology is adequate to prevent this and other breaches
- ! Find out who your regional high tech crime officer is – they may be willing to meet you and suggest how to tighten security

Training

- ! Ensure members of staff are aware of and trained in such procedures

Audit

- ! Have regular internal and external audit processes to ensure policies and procedures are adequate, up-to-date and implemented