



Handling the “Toxic Liability”

(quote from David Smith, Deputy ICO)

Andrew Cormack
Chief Regulatory Adviser, JANET(UK)
Andrew.Cormack@ja.net



And the answers are?

According to O'Donnell...

- Clear Responsibilities
 - Information Risk Owner, Asset Owners, Data Users
- Universal Training
 - Annual, for everyone
- Increased Scrutiny, with sanctions
- Appropriate Technologies, for when those fail
 - Encryption, pen.testing, secure networks, etc.
- Look how these would help HMRC...

LGA: “people, places, processes, procedures”



What About Us?

- Similar scale databases (10-100K ppl)
- Plus sensitive/commercial data
- O'Donnell may not apply yet
- But DPA Principle 7 already does:
 - “Appropriate technical and organisational measures shall be taken...”
 - Does O'Donnell set the standard?



How to Address This?

- What are our strengths?
- What can we do together?
- What tools do we need for the job?



References

- O'Donnell Review

http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

- LGA: Data Handling Guidelines

<http://www.idea.gov.uk/idk/core/page.do?pageId=9040133>