Corporate Negligence?

Dr. Andy Jones MBE
Research Group Leader,
Security Research Centre

The experiment

- This research looked at the level and type of information that can be, and is being, given away by organisations when they dispose of equipment that they no longer require.
- This type of research has been carried out before – but not on this scale in the UK and not in conjunction with another country.

The experiment

- The University of Glamorgan in conjunction with Edith Cowan University in Perth, Australia, obtained a number of hard disks for computers that had been released for resale on the second hand market.
- At the time of receipt, the source of these disks was not known.
- The disks were analysed to determine whether any information remained that may have been of value.

The research

- The university of Glamorgan was provided with 105 hard disks that had been obtained from a variety of sources.
- Edith Cowan University obtained a number of computer systems and hard disks from public auctions in the Perth area.
- The disks were analysed, using commonly available tools and techniques to determine whether any information of interest remained on them. The types of tools that were used were the tools available in the Windows and Linux operating systems and hex editors.

What we found - UK

- On the disks analysed in the UK:
  - Of 105 disks obtained, 13 were unreadable and had either been tampered with or had failed in some other way.
  - 16 disks were totally blank and no data could be recovered from them.
  - 52 disks contained sufficient information for the organisation that they had come from to be identified.
  - 49 disks contained sufficient information for individuals to be identified.

What we found – UK (Cont)

- 47 disks contained information on personnel and of a personal nature.
- 18 disks contained financial information on the organisation from which they had originated.
- 7 disks contained information on the network structure of the organisation from which they had originated.
- 4 disk contained information that might be considered as illicit.

What we found - Australia

- Of the first 11 disks that were analysed in Australia:
  - Ten of them had documents that could be recovered without the use of any techniques other than mounting the drive or unformatting it.
    - Two disks could be identified as having come from a manufacturing company.
    - Five disks could be identified as having come from a corporate organisation.
    - Two disks could be identified as having come from a home user.
    - One disk could be identified as having come from a Water Utility.
  - The eleventh disk, which contained no data, could be identified as having come from a telecommunications company as a result of it still bearing an asset tag for the organisation.

BT

The Business Implications

- Potential exposure to Industrial Espionage
  - The quantity and type of information that was available from three of the business organisations would leave them vulnerable to an industrial espionage attack.
- Fraud
  - The information available from the service industry organisation and one academic institute was sufficient to allow for the potential for fraud.
- Identity Theft
  - A number of the corporate, academic and home PCs contained sufficient information to enable Identity theft.
- Breaking the Law
  - In the case of the disks that could be identified to commercial and academic organisations, they had, apparently failed to meet their legal obligations.

BT

The Business Implications (2)

- Non Compliance with Legislation.
  - A large number of the disks from the business and academic sector contained details of individuals that those organisations have a responsibility to protect under the Data Protection Act, as highlighted by this extract from the DPA:

    - **2.**—(1) A data controller shall, as respects personal data kept by him, comply with the following provisions:
      - (*a*) the data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly,
      - (*b*) the data shall be accurate and, where necessary, kept up to date.
      - (*c*) the data—
        - (i) shall be kept only for one or more specified and lawful purposes,
        - (ii) shall not be used or disclosed in any manner incompatible with that purpose or those purposes,
        - (iii) shall be adequate, relevant and not excessive in relation to that purpose or those purposes, and
        - (iv) shall not be kept for longer than is necessary for that purpose or those purposes,
      - (*d*) appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.
    - (2) A data processor shall, as respects personal data processed by him, comply with *paragraph (d)* of *subsection (1)* of this section.

The Business Implications (3)

"Except as otherwise provided in this subchapter, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 6803 of this title"

Excerpt from Gramm-Leach-Bliley Act

The Business Implications (4)

- Companies that carry out business in the USA have to comply with the requirements of the Sarbanes Oxley legislation.
- In the UK if the company is operating in the financial sector it is answerable to the FSA for the way in which it operates. The disposal of disks that contained data that may include that relating to customers would be certain to ensure disapproval and scrutiny from this body.
- In addition to this, for a company operating in the financial sector, there are requirements under Turnbull.
- Finally, for the organisation operating in the financial sector there are the requirements that are mandated in the Basel II Accord.

The Implications for the individual

- Identity Theft
  - A number of the corporate, academic and home PCs contained sufficient information to enable Identity Theft.
- Blackmail
  - At least two of the systems contained information that would expose identifiable individuals to potential blackmail.

Conclusions

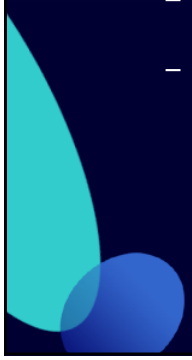
- The number of disks that contained information and the level of information that they contained indicate that the systems in place for the disposal of computers is failing in a large number of cases.
- The potential implication of this failure could be catastrophic for both individuals and organisations if it were to be exploited.
- The disks that were subsequently identified as having been cleaned by the recycling company contained no information whatsoever that could be recovered.
- The number of disks that contained 'illicit' information was far lower than anecdotal reports would have indicated.

Reaction

- Subsequent to the research, the organisations that had been identified were approached to try and determine what had gone wrong.
- Reactions varied considerably.
- Best case from a commercial organisation
- Worst case
- Academic organisation reaction
- Press coverage

Future Work

- There is a considerable amount of additional research that still has to be undertaken. This will include:
  - Search for Recoverable Passwords
  - Analysis of types of security software in use and level of usage.
  - Analysis of disks for additional detail on organisations and individuals



Thank you