

## How to lose your Quality data

introduction to IT security

presented by

Gillian RICHARDS, Cyber Security Risk Assessor

The value of sensitive data around us is often underestimated; only when it is lost or stolen is its true worth appreciated. We should look at the data we have and estimate the risks to its loss that come from cyberspace and others.

The risk of loss is associated with Technology, People, Policy and Procedures. The highest risk comes from People.

### ① Concerns

#### Weak passwords

Software to crack passwords can now be downloaded from the internet. A typical weak 8 character password can be cracked in 30 seconds.

It is recommended that

1. pass phrases (first character of each word in a memorable ,personal phrase)
2. one word embedded into another (lose & data -> lodaseta)
3. random letters taken from long words (**personification**)
4. convert characters into look-alike numbers (0=O 4=a 5=s \$=s 8=b)
5. randomly use upper case within a word (eRofIAtn) be used

#### Capturing keystrokes

Keylogging software unwittingly loaded, appearing to be a freebie screensaver from a friend or a pop-up from the internet, can record and transmit every keystroke you make. This in turn can provide criminals with your user names, passwords, and other sensitive data.

Hardware in the form of USB devices which are installed by cleaning staff at night, also capture keystrokes.

#### Phishing

Two classic types of e-mail sent out to millions of e-mail addresses appear as:

1. Banks requesting your confidential information
2. Inland Revenue wanting your bank details to allow an overpayment to be sent to your account. This leads to a spoof website.

Sufficient numbers of people still reply to make it worth the criminals continuing.

#### Trojan software

Pop-ups from the internet asking for sensitive data, concealed as:

1. *Your network connection has been lost, please re-enter username and password.*
2. An invitation to respond to a survey, with the offer of an award.
3. Gadgets sent in the post to plug into a USB port, claiming to be toys, but in reality spyware.

#### Social engineering

Getting information by talking to people, looking over their shoulder, or reading documents on their desk.

Getting friendly with people so they are happy to give you information.

The smoking room is a classic location to listen to people's conversations.

65% of calls to help-desks are about passwords

### **Poor equipment**

Mobile I-phones have no protection. British government no longer use Blackberry phones.

Public WI-FI networks have low security.

### **Poor discipline**

Passwords are frequently kept under the keyboard (tip for auditors!)

20,000 mobile phones are left in London taxis each year

## **② Threats**

### **Industrial Espionage**

It is the culture of some countries, companies and people to save inventing the wheel again by stealing their competitor's process understanding. Monitoring volumes of data flowing across borders gives a clue to threats. Examples were given of China and Russia being falsely accused and old friends like France with high volumes of data crossing to the UK.

Spear fishing, is increasing as criminals target an individual who has specialist knowledge / data.

A single 20Gbyte I-pod can carry ¾million word documents

### **Criminals**

Sensitive data, particularly as a means to carrying out fraud is big business. Criminals earn more from IT fraud than from drugs.

**Hactivists**, Employees with a **grudge**, **Insiders** seeing opportunities to make easy money.

All under estimated as people who can steal sensitive data for their own ends, causing a loss to their employers.

## **③ Safeguarding your data**

IT security

- \* Have time outs on computers to stop unlawful use while user is away from his/her desk.
- \* Use disk encryption
- \* Have a separate, communal computer in the office, for employees to use for personal matters.

User guidance

- \* Train staff as to what data is sensitive and which can be safely circulated

Compliance

- \* Have procedures (based ISO 27001) to control data flow
- \* Audit procedures.

Policy

- \* Most senior managers are motivated to look after data; to loose data does irreparable damage to the businesses image.
- \* Middle managers tend to be more interested in cost aspects than the safety.
- \* Employees are not aware of the issues.

#### ④ Useful websites

- \* Help about protecting yourself on-line is available from a government sponsored website:  
<http://www.getsafeonline.org/>
  
- \* If you receive a phishing e-mail purporting to be from a bank, send it to:  
[http://www.banksafeonline.org.uk/fags/fags\\_6.html](http://www.banksafeonline.org.uk/fags/fags_6.html)  
banks are keen to close down such sites and need our help.
  
- \* Help for those responsible for children is available at:  
<http://www.thinkuknow.org/Default.aspx?AspxAutoDetectCookieSupport=1>  
The latest information on those sites that children like to visit, mobiles and new technology. Find out what's good, what's not and what you can do about it. Most importantly, there's also a place which anyone can use to report if they feel uncomfortable or worried about someone they are chatting to online.

Gillian RICHARDS is a Cyber Security Risk Assessor working in Berkshire, and can be contacted at [gillianrichards3@googlemail.com](mailto:gillianrichards3@googlemail.com)

Notes by Richard KIRBY, Chairman of Thames Valley Branch of the Chartered Quality Institute  
26<sup>th</sup> March 2010