



FRAUD and INFORMATION THEFT

Protect yourself and your company from info thieves.

BY JANE SMITH

Identity hi-jacking and personal identity fraud is rife in the UK.

Over 70,000 cases for 2003.

How can we protect ourselves and the companies we work for?

Fraud and information theft is on the increase and there is substantial evidence to support the need for us to protect ourselves as individuals and to protect the businesses we work for. This, and recent revisions to the Data Protection Act provide a sure sign that the demand for related office products such as shredding machines and screen filters is set to see a boom.

However, it also seems that sales are being held back through lack of education and an attitude of 'it won't happen to me'. But as you will see, the likelihood of identity fraud or identity hi-jacking affecting you or somebody you know is growing all the time and is a reality.

Craig Boulter, Sales Director for the Office Technology Division of HSM UK shared their information with us to show just how big the problem is getting. Bin raiding arrived from the USA around four years ago and is active and growing in the UK. It is not only the small, lone fraudster rummaging through household bins pretending they've

dropped their keys, the practise is now being adopted by more organised gangs targeting businesses.

From an individual's point of view there are 4 main areas of identity fraud:

0a) Application Fraud –

where the victims details are used to obtain credit

b) Account Takeover –

where the fraudster convinces the bank that they are you

c) Wholesale Assumption Fraud –

where the fraudster gathers enough information to virtually duplicate your identity

d) Internet Fraud – where your name and card details are captured and then used without your knowledge

Emma Crelin, Marketing Manager for Fellowes also shared some information with us gathered from some research carried out by them and credit reference agency Experian late last year. This showed that the estimated cost of information theft in the UK was a staggering £1.34 million and that the number of cases had risen from 27,720 in 2001 to over 70,000 estimated for 2003.

IT IS estimated that, globally, corporation secrets valued at \$250 billion are stolen each year as a result of indiscreet business practices.

Shred that

In terms of sales opportunities the message has to be 'every household should have one' – a shredder machine that is. And today there are many small, personal and home office models available on the high street. Suppliers such as HSM, Rexel, Fellowes and GBC all have a range of entry-level machines designed for home/personal use. We spoke to Elke Hahmann, Marketing Executive for GBC who told us, "We too see big growth in the home market and we have recently revamped our range to reflect this."

Boulter at HSM says, "It's education that will really get the growth accelerating. It's really important to explain to customers the risks they run if they don't shred their documents. Many people just don't think it could happen to them and that applies to businesses too."

So, turning attention to the commercial sector both HSM and Fellowes were able to share some pretty scary statistics with us. Company identity hi-jacking, as it is known, is on the increase too and the potential monies involved are high. This in turn seems to be attracting more sophisticated and organised perpetrators.

Wasted time

The scary thing, though, is that some companies are just not thinking it through when it comes to disposing of their waste paper documents.

The London Borough of Camden and Experian were assessing the extent to which bin raiding could influence information theft and fraud. They analysed the contents of 327 domestic households and 71 company's waste. They found that:

45% had discarded company letterheads

25% of documents contained a Director's signature

44% had thrown away whole invoices

20% had thrown away company bank details

>> p. 10



In these cases no attempt had been made to shred or destroy any of this data.

Any of this information could potentially lead to fraud. And when it is written down in black and white it is blatantly obvious. So why don't all companies shred their documentation before disposal?

This is where you come in. Talk to your customers about their document disposal procedures. Are they using best practice and does all their staff understand the potential dangers in not shredding sensitive information.

TALK to your customers about their document disposal procedures. Are they using best practice and does all their staff understand the potential dangers in not shredding sensitive information.

Data copy

Added to the issues of identity hijacking there is also the subject of data protection. The Data Protection Act (1998) covers the collection, storage and use of all personal data

“It’s education that will really get the growth accelerating. It’s really important to explain to customers the risks they run if they don’t shred their documents. Many people just don’t think it could happen to them and that applies to businesses too.” CRAIG BOULTER, HSM

Take the time to 'gen up' on the machines available. You need to guide your customer in terms of the capacity the machine is capable of and the level of security required. From small desk-side machines, through to huge heavy duty, departmental destroyers and from simple strip cut machines to the new 'Level 6' or 'Extreme' cross cut machines where the particles are minute – giving the choice of spaghetti or confetti – there are now machines to suit every need. There are even shredders built to destroy multi-media (floppy disks and CDs etc).

in the UK. 'Personal data' relates to a living individual who can be identified from the stored data, or from other information that is in the possession of – or is likely to come into the possession of – the data controller. This also includes any expression of opinion about the individual. The Act states: 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.' The Act goes on to give further guidance on matters that should be taken into

account in deciding whether security measures are appropriate. To be honest it is mostly common sense.

Consequently, when applied to business, companies need to be very careful about who can see what data and how that data is stored, managed and disposed of. It is especially important to consider measures of confidentiality and security in situations where the general public are involved or where employees are working remotely with any sensitive data.

Corporate data is also covered by the Act. It is estimated that, globally, corporation secrets valued at \$250 billion are stolen each year as a result of indiscreet business practices.

Screen savers

We've talked a lot about the safe disposal of documentation but it is also the security of the data that must be considered. A very obvious product opportunity here are privacy screen filters. Available from a number of manufacturers including 3M, Fellowes and Acco, we were able to talk briefly to Phil Jones, Market Development Manager, 3M Computer Filters.

'Without doubt there is a major opportunity for privacy screen filters in all sorts of environments but particularly where there is a lot of people moving around and/or where the general public are close to the computers for example in doctors surgeries, hospitals or job centres.

But the other really important area to consider is people working on the move – in planes, trains and cafes – a laptop privacy filter will ensure computer secrets do not get into the wrong hands.'

'Privacy Filters restrict the viewing angle so that only the person seated directly in front of the monitor sees the information displayed'.

Jones also shared with us a number of considerations to help evaluate whether or not a company is complying with the Data Protection Act. Can your customers provide satisfactory answers to the following? It could be that these questions will help in understanding your customers' needs.

- >> How many of your staff have personal information on their PCs?
- >> Are your CCTV monitors on display in reception or other public areas?
- >> What appropriate safeguards are in place to ensure unauthorised members of staff and visitors to the office cannot see personal data when they pass by PCs and CCTV monitors?
- >> Do the monitors have privacy filters?
- >> Who in the organisation is your Data Controller and are they aware of these issues?

For more information about The Data Protection Act (1998) visit www.informationcommissioner.gov.uk