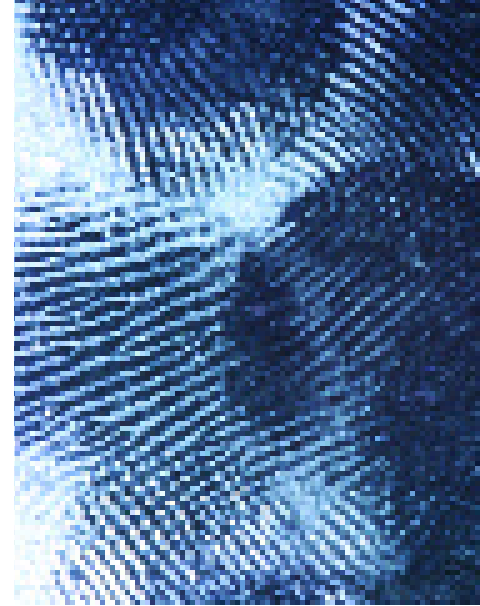


CORPORATE PROTECTION

In the first in a three-part series on corporate protection, we focus on the home and mobile worker. Portable and mini products can do the same jobs as their big brothers.

BY KNEEZ BUKHARI



What you don't know can hurt you. Corporate fraud can cost your company millions, and with more and more employees taking the opportunity to work flexibly, often from home, new scams are evolving all the time to catch the unsuspecting off-guard and steal your identity, your money and anything else available.

Homeworkers and those working on the move need to be aware that the risk of corporate fraud is higher and suitable security measures need to be taken. As Jill Organ, senior category manager, Rexel Business Machines, says, "The workplace today can be anywhere you happen to be, from a hotel room to the kitchen table. The problems of identity theft and corporate fraud are thus more widespread than ever." There are various policies, products and procedures companies can use to protect their investments. Here, we cover just a few of them, and let you know how to highlight the facts to your customers, making sure they understand the potential risks and are informed enough to be able to take the appropriate action. >>



According to credit reporting firm, Experian, there is no single definition of fraud, but some types of credit fraud that occur include:

- **IDENTITY THEFT:**
the unauthorised use of personal identification information to commit fraud or other crimes
- **IDENTITY ASSUMPTION:**
long-term victimisation of identification information
- **FRAUD SPREE:**
unauthorised charges on existing accounts

Credit thieves and fraudsters have numerous ways of gathering personal and corporate information. These can range from looking over your shoulder if you're using a laptop while traveling, stealing credit cards or letters from your mailbox, to rifling through household or company waste for discarded information or hacking into your computer. They could even simply request your personal information via unsolicited emails or telephone calls.

Before the advent of the commercial internet, it would take a great deal of knowledge and skill to assume another's identity. Now, accessing and making use of personal information has never been easier for cyber-criminals. Nearly everyone who uses the internet has experienced an attempt by somebody somewhere to obtain personal identifying information.

Have you ever had an email from someone in Africa or, more

recently, Iraq, claiming to need a secure account through which to send money to the UK? Have you ever received an email from someone claiming to work for your bank, asking you to verify who you are with security information? Have you ever noticed an icon on your desktop for a downloaded programme that you have no knowledge of downloading? Have your customers? From unsolicited mails asking for personal information to the un-requested installation of spyware and worms, those who want your data, will find a way, and it's getting worse. According to the CIFAS, the UK's fraud prevention service, between 1999 and 2003 the number of reported cases of identity and impersonation fraud grew from 20,000 to over 100,000.

There are various routes to your sensitive data and all must be covered. Ask your clients what kind of security measures they currently take and how they think they could potentially be targeted. Then let them know just how easy it would be for someone with intent to get a hold of their personal information and use it to their own benefit. All it takes is one bank statement carelessly tossed away, or one wrong click of your mouse.

Electronic security issues can be solved with devices such as iris or palm recognition systems, which eliminate the need for passwords. There are also numerous programmes available to counteract or block worms and viruses. Computer users should also routinely back up their data, whether in the office or at home. Make sure

“The workplace today can be anywhere you happen to be, from a hotel room to the kitchen table. The problems of identity theft and corporate fraud are thus more widespread than ever.”

**JILL ORGAN,
SENIOR CATEGORY MANAGER,
REXEL BUSINESS MACHINES**

you remind your clients of this, it's amazing how many people are oblivious to this very basic rule. Companies need to be asking their home-workers what security provisions they have in place and alerting them to the risks of data theft.

Phil Jones, market development manager for computer filters at 3M, also highlights the fact that mobile computer users need to comply with The 1998 Data Protection Act (DPA). When computing on planes and trains, in coffee shops, cafés and other public places, it can be almost impossible to ensure your computer secrets do not get into the wrong hands. And if unauthorised people can see sensitive or

confidential information on your screen, you could be breaking the law. Jones suggests that for people computing on the move to comply with the DPA, a Laptop Privacy Filter is a simple, low cost accessory. Privacy filters operate like tiny vertical blinds, effectively restricting the viewing angle, so that only the person seated directly in front of the monitor sees the information displayed. People viewing from either side see a blank, dark screen.

To safeguard your credit cards, banks recommend changing your personal ID number (PIN) every three months. They also recommend that consumers become a bit more creative when choosing their PINs. When doing so, avoid using information that is easy to figure out, such as phone numbers, birthdates, or a series of consecutive numbers.

Other products that can be recommended or offered by companies include safes and shredders and you need to let your customers know what the best products are for them and their staff. Andrew Cummings, sales and marketing director at Aurora Electronics, says corporate, employee and customer identity fraud arising from the theft of company records and documents is a rapidly growing, serious but largely avoidable crime.

One important aspect which is crucial to the fight against this crime is the destruction of all unwanted business records; paper based waste and electronic storage media. Craig Boulter of HSM, which has carried out some research into the subject of corporate fraud, cloning and identity theft, suggests that in

“Procedures may be in place to protect against electronic theft but physical damage must also be guarded against”.

MARK BROOKES, CHANNEL MANAGER, INDIRECT MARKETS, CHUBB SAFES

the same way that companies often equip home and mobile workers with a laptop computer and other essential equipment, they should also provide them with a document shredder. Says Boulter, “Obviously this can be a small desk size unit such that it does not take up too much space. However, we would suggest that a level three machine or higher and preferably a cross-cut version is specified to ensure security of the shredded materials.”

Tyron Hill, senior European marketing director for Shredders at Fellowes, says when talking about corporate fraud, it could almost sound like only big companies are at risk but the reality is that every type of company, from the biggest one to the one-man SOHO home worker can become a victim of corporate identity theft. For small companies, the best way to protect themselves against ID fraud, says Hill, is to be diligent. Either consider providing staff with suitable shredders, possibly a higher end model for credit cards and CD shredding as well, or insist that all sensitive data, including paper, disks and CDs is returned to the office for shredding. There are a variety of high performance shredders available today that are compact, very portable and will fit into little spaces. Companies need to treat the data that an employee takes or has at home as an equivalent or higher security risk than at their main offices.

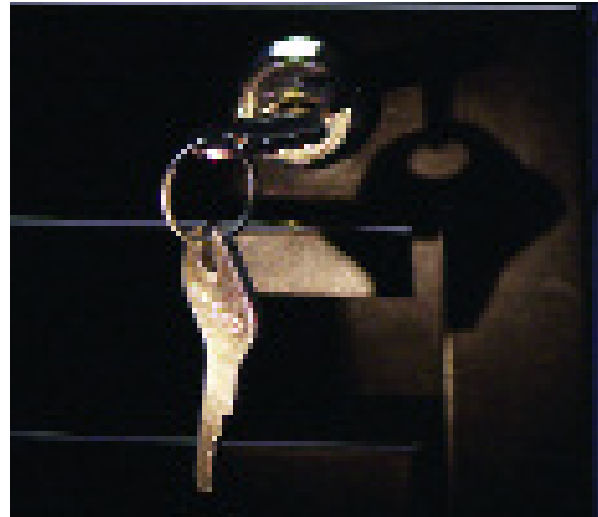
Another good protection measure for the home office is a fire safe or cabinet. Mark Brookes, channel manager, Indirect Markets at Chubb Safes, says this is the last

line of defence against fire and theft. Brookes advises, “Procedures may be in place to protect against electronic theft but physical damage must also be guarded against.”

According to the Association of Burglary Surveyors, one in five companies will suffer a major disaster over a five year period and 80% of these will cease trading after a major fire. Buildings, furniture and computer systems can be replaced if insurers pay out; however these are of no use unless you have the information to re-start. Insurers will need stock records, trading history etc to settle a claim – the longer it takes to receive a pay out the more likely it is that the business will fail. Contracts, drawings, designs, R&D work, employee records, confidential client information etc could all be lost. These may not be critical to the business but would involve high cost to reproduce and may have legal repercussions.

As a salesperson, you need to identify what information is kept by the business, how the information is stored, quantities involved and how important this is to the business (We know it is, but the client has to realise it for themselves!). Ask what if questions to make them understand how much they rely upon it. From these few questions it is possible to formulate a proposal by justifying the cost of a security measure against the cost of a business going under.

The advantages to working from home are obvious, as is the selling potential. People are catching on to this growing phenomenon fast – so, don't get left behind! ■



IF THE KEY FITS...

Chubb has organically grown from a UK based family business into a large multinational company. Today, Chubb extends its knowledge, design and engineering skills for the highest quality products to international markets.

Chubb has considered how best to support people in offices and its conclusion is that there is a requirement for a different range of equipment tailored for this market. To this end, Chubb Safes is bringing to the attention of dealers its new SecureLine range.

Explains sales director Tom Rochford, “The SecureLine range is available at lower price points with discount opportunities and therefore gives appropriate margins for dealers.”

Chubb Safes offers a support network, preferring to train dealers on the product and help incentivise their sales people. Says SecureLine channel manager Mark Brookes, “We're keen to work on a face-to-face and one-to-one basis, as we've found that once a sales person has managed to make one sale then they're off and running. We work hand in hand with them to drive that process forward.”

Spicers already holds most of the products in its main catalogue, the rest are available from the Specials Department. Hanmar Wholesaling also holds much of the range. Chubb Safes is leading with XPD (Officepoint and Officestar) as well as with Dealer Network and Advantia.