

THE SECRETARY AND SECURITY

Alexander Baron investigates security in the office. It's not just a matter of locking the odd door.

A couple of weeks ago I was in Holborn on business and walked past the headquarters of British Gas. Remembering I had my gas bill in my pocket I walked up to the reception desk and asked the uniformed security man where the local showroom was located. He told me the nearest was in Islington, but if I wanted to pay by cheque, I could do so here. Then, letting me through the turnstile, he directed me to the security office at the rear of the building. Once inside, I had the free run of this large, office complex; I was carrying a case which could have contained anything, and no-one gave me a second look, even though I passed at least half a dozen uniformed "security" officers in the few minutes I was there. I left through the front entrance with a wave from the gent who had let me in.

"Even if you work in a small, friendly office, sadly people still take liberties – and things that don't belong to them."



Watch out, watch out

The methods some professional thieves and con-men use are ingenious, to say the least. One man walked into a supermarket and set up his own check-out. Another approached a woman in the restaurant of a major store and, addressing her by name, announced in a loud voice that an irregularity had been found with the credit card purchase she had made a few minutes earlier. Assuming him to be a floor manager, the embarrassed shopper handed over her card for him to check, and that was

Tips for Top Security

- Don't leave anything of value lying about.
- Today's thief dresses just like the next person – don't trust anyone.
- Mark all portable office equipment.
- When you leave the office, make sure all doors and windows are locked.
- Depending on the type of trade you work in, be aware of the possible breaches of security – don't leave anything to chance.
- Always shred any confidential items before putting them in the bin.
- Be wary of the tall dark stranger who seems more keen on your company than you!

the last she saw of either of them. Other scams include dressing up as security officers, officials or putting on a white coat and walking out of an electrical shop with a microwave oven under each arm.

"Don't trust anyone, and don't leave anything of value lying about, not even for five minutes."

The stereotyped burglar is readily identifiable in mask and striped jersey, carrying a bag marked SWAG. The *real* burglar who breaks into your house is just as likely to wear a three-piece suit, or the one who robs your

A few weeks before this I had visited the offices of a well known pressure group, staffed by paid workers and volunteers. On the wall was pinned a notice expressing regret that from now on the petty cash was being kept under lock and key because an anonymous individual had been helping himself to small sums of money.

The above anecdotes illustrate two things. One: even if you work in a building where everyone carries ID cards and where there is much visible security, any Tom, Dick or Harry can still walk in off the street and walk out unchallenged, possibly with a bagful of expensive equipment. Two: even if you work in a small, friendly office where



office could be smartly dressed in rain-coat, scarf and high heels; no-one will give her a second glance, and no-one will suspect that the handbag she's carrying is yours.

The moral is: Don't trust anyone, and don't leave anything of value lying about, not overnight, not during the lunch hour, not for five minutes. Challenge strangers if you are the least bit suspicious. Even people who have a bona fide reason for being in your office may help themselves to something on the way out. Offices, store cupboards, etc, when not in use, should be kept locked and ideally the key should be kept under the control of one person; others should be granted access only if and when they need it and a record should be kept.

Office theft

Equipment that is light and portable should never be left lying about. Here, one thinks immediately of calculators, adding machines and, of course, telephones. Such equipment should also be marked. Any crime prevention officer will advise you how to do this - simply



ring up any main police station during office hours. The police also have a number of leaflets on crime prevention; ask for the one called *Mark It To Keep It*. They will also be able to supply you with "marked property" stickers.

No figures are available, but it is a safe bet that thieves and burglars who "work" offices steal equipment to sell rather than to use. If equipment is known to be marked the potential thief will think twice before stealing it. It becomes more difficult to dispose of, and, in the event of its being recovered, easy to return to its rightful owner. All police forces collect veritable Aladdin's caves of untraceable stolen property which they auction off periodically. The cost of marking property is negligible, as is the time and effort involved. Not only that, it should be tax deductible and you may be able to negotiate reduced insurance premiums. Contact your insurer for further details.

Remember, whenever you leave the office unoccupied, always make sure it is locked. All ground floor and accessible windows should be fitted with window locks, and a burglar alarm should be clearly visible on the outside wall.

"If equipment is known to be marked, the potential thief will think twice before stealing it."

like other equipment, this should be kept under lock and key except for a reasonable quantity for day-to-day requirements.

Likewise, the odd phone call on company telephones in company time is taken for granted. However, with the introduction of callstream numbers, many companies saw their phone bills rocket. The proposed itemising of phone bills appears to be going too far; no-one likes being spied on, but it is possible now to buy call blockers which can be used to prevent certain calls being made. Callstream numbers cost 38p per minute, international calls more than twice that, so installing one of these can pay for itself in a very short time.

Some companies even go so far as to log the number of photocopies made, but this is taking office security to extremes; there is no evidence that this facility has ever been significantly abused, and there exists a thriving subculture of office poetry and humour, thanks largely to the Xerox machine.



Petty practice

Petty pilfering is an accepted practice and is regarded by most staff and management as a "perk" of the job. The anthropologist Gerald Mars even wrote a book about it called *Cheats At Work*. Not even the most Draconian employer will object to his staff taking home the odd biro or notepad, but stationery is, of course, expensive, so,

Industrial espionage

Sounds thrilling, doesn't it? But stealing industrial secrets is far removed from the realm of James Bond. Recently a gentleman from a company that specialises in "bugging", "debugging" and surveillance appeared on London's LBC Radio, and some of the things he revealed were most interesting. Surveillance and bugging equipment is readily available to the general public. There are several shops in London that stock it, and the columns of certain publications advertise a wide range of such devices, like those from a low-budget thriller. Sweeping for tape recorders or transmitting fountain pens is hardly likely to become part of your office routine, but the very fact that such devices exist proves that someone must be up to no good.

Personal Security

If you have credit cards, a new holder called 'Cardsafe' has just come onto the market. The brainchild of engineer Peter Briggs, it is a miniature safe which holds up to six cards and fits comfortably in the pocket. It has a combination lock which, if tampered with, exudes a sticky, corrosive dye, rendering its contents useless. Available from £14.99, one major insurance company is so impressed that it is offering CardSafe holders a special discount on credit card insurance.



If your company is involved in the plastics industry (for example) it may spend millions of pounds developing a new material; drug companies make enormous investments in research. Then someone comes along and steals or photographs the development files. This can and does result in millions of pounds and many years of research being wasted. But it is not just processes and technological developments that are targeted by industrial spies.

Even something as mundane as a customer mailing list falling into the wrong hands may lose a company tens of thousands of pounds-worth of business.

When this sort of thing happens, even if foul play can be proved, there is little or nothing a company can do. Stealing secrets may be immoral, but unless a burglary or some overt act has been committed, it isn't illegal (there are some exceptions to this). And even if the spy is prosecuted, the company probably has no redress for lost profits.

"Some companies even go as far as to log the number of photocopies made."

Those of you who work in the financial sector will already realise how easy it is to transfer thousands or even millions of pounds in a few seconds, electronically. If the wrong person has access to classified informa-

tion a company can very easily be taken to the cleaners, even to the extent of bankruptcy.

Disks and discussion

Much information nowadays is kept on disks, which are so unobtrusive that it might be weeks before you realise a particular one is missing. And, of course, disks, like other documents, don't need to be copied - it's the information they carry that's important, not the disks themselves. From disks to dustbins! One security consultant claimed that just by rummaging through waste paper baskets he was able to procure information that could be damaging to a company if it were to fall into the wrong hands, a competitor say. So make sure that any confidential documents you dispose of are first put through a shredder.

Finally, be careful what you say, especially if you work in the financial sector. Is that tall, dark stranger you met in the wine bar yesterday lunchtime trying to get his name in your little black book, or is he instead more interested in the contents of your Filofax?