Business Administration

Issue 11

March 1995

ACTION

1. Read Stop Press.
2. File Stop Press together with other material (and remove outdated material) in accordance with enclosed Filing Instructions.

LOOSELEAF UPDATE

Industrial espionage

The problem

11081 Industrial espionage is defined as the unauthorised acquisition of commercial or intellectual information for the purpose of financial, political or personal reward.

Most organisations have information they do not want competitors or the public to know about. If it were to be acquired, the company could suffer disadvantage or embarrassment, affecting its market position and profitability.

The information generally at risk includes:

- Documents - letters, memos, data, formulae, contracts
- Discussions - meetings, management discussions, telephone calls, etc.
- Plans - drawings or blueprints, etc.
- Machinery - prototypes, special processes, etc.
- Products - materials, qualities, etc.

The type of information sought after in the first two items above, will relate to:

- Business development and marketing plans
- Clients
- Employee relations and negotiations
- Tendering
- Investment
- Take-over initiatives

Who may be involved

Intruders

11082 Unauthorised persons who may break into premises, during or outside business hours, to observe, remove or copy documents, machinery, plant, processes or prototypes. They may also introduce audio surveillance devices to target areas.

Visitors

11083 Outside persons, e.g. contractors, who are allowed on the premises during normal working hours and whose presence may normally be accepted by the staff, do have the opportunity to gain information by theft, copying, observing or overhearing. They may also instal listening devices. Such persons could include contract engineers, electricians, vending machine operators etc.

Business visitors

11084 Many business visitors will be acquainted with competitors and, because of their understanding of the business, will be able to recognise the value of information discussed, overheard, or observed by them. This information could be passed on to such competitors for some advantage or even innocently in subsequent conversations.

Cleaners

11085 Cleaners have the run of the premises, usually when there are no staff present, with no constraints over what they see. For a suitable reward, they may remove information or even instal listening devices to sensitive areas. They may even admit a third party.

Employees

11086 Employees often have complete access to the premises and any information contained therein. They can pass information out to third parties for reward, with ease. The reason for this disloyalty can be because:

- they are in financial difficulties
- they are coerced or threatened
- they have a perceived grudge against the company
- they are seeking to gain favour with new employers
- they are greedy

Often, employees are a valuable source of information. Many seekers of company knowledge will find out where employees go drinking after work and will observe and listen to the usually loud, private discussions that go on. One such person admitted to the Author that if he wanted to know what was going on in a particular company, he just visited two or three 'watering holes' in the City.

Another problem with employees, particularly management, is that if they hand in their resignation, they can spend some time before leaving in acquiring as much information as possible.

The answer

11087 The most fundamental need is for the company to recognise the value of its information to outsiders and the consequences of its loss. Employers must make the employees recognise the seriousness of the potential, since it could affect their own job security.

Access during working hours

11088 No unauthorised persons should be allowed in the premises. This means that all access doors should either be secured or monitored at all times during the working day. Employees must be encouraged to challenge any unrecognised person and to report their presence to management. Motivation could be that their own property may be at risk.

All visitors must establish their credentials by reporting to security or reception. Details of the visit must be recorded and the required host must be called to confirm the validity of the visitor. Once accepted, the visitor should always be escorted until he leaves the premises.

Ideally, all accepted visitors should be issued with clip-on identity cards (adhesive labels do tend to come off), which must be collected on their departure. Colour coded cards can be provided, limiting the visitor to specific areas only. This will help staff identify those whose presence is not authorised.

Where possible, meeting rooms should be available to deal with the visitors and they should be located as near reception as possible to preclude the need for the visitor to pass through work areas. Doors to the meeting room should be shut to reduce the possibility of the visitor overhearing discussions or telephone conversations going on nearby.

Internal doors to sensitive areas should be fitted with access control devices allowing only authorised staff into such areas.

When the visitor leaves he must take with him all his property, especially his briefcase (which may contain recording devices to pick up subsequent discussions in the room).

Access at the end of the working day

11089 This period can be extremely vulnerable. Exit routes, particularly via the reception, are usually unmanned and doors are unsecured to allow egress of the employees. At such times, it is relatively easy to enter the premises unobserved and hide in toilets or other unlocked closets until the staff have left.

On many sites, security guards are required to carry out closing procedures, locking doors and windows and even setting the anti-theft alarm systems. However, this activity often occurs a few hours after the closing

time, to allow late workers to vacate the premises. Even when cleaners attend the premises at the end of the working day, doors are often left unsecured and are not locked until the cleaners have finished.

It is important that the number of egress points from the building, at the end of the day, are restricted. The doors used should be fitted with automatic closers and the locks should be self-latching, so that they cannot be opened from without. To make sure that the door closes properly, a localised audible alarm can be fitted, which will indicate if the door is not secured.

Ideally, the reception area should be manned until all staff have departed to make sure that unauthorised persons do not enter. If the site has manned security, a CCTV camera can be installed in the reception area, or other exit points, to be monitored by a guard.

Access outside working hours

11090 The standard perimeter and premises protection described in previous sections should be applied. Additional alarm protection should be fitted to the 'sensitive' areas.

All sensitive information should be filed and locked away in cabinets, cupboards or safes. The cabinets should not bear labels indicating the contents, since this does help the criminal. Authorised users of the cabinets will know the location of files without having to refer to the written labels on the front.

Files themselves, within the cabinets, can be coded rather than having individual labels. Again this will cause any outsider to spend more time in seeking information and increases the chance of their being observed. Whilst management may pass down instructions about the securing of sensitive information, disciplines do tend to erode and regular, after hours checks should be made, by management, to identify any breaches.

It is essential that keys to locked cabinets etc., are not left around. Criminals will know the usual hiding places of such keys and they can be used to open the facilities. It can be argued that the storage units can be forced open, but at least the company will know it has been compromised and can initiate a damage limitation exercise.

Any windows allowing observation of processes or special machinery should be opaque.

External rubbish containers can be a valuable source of information, discarded printouts, scratch pads, letters and even typewriter ripbons can yield a great deal to the trained eye. Any sensitive documentation should either be shredded or incinerated.

Employees

11091 The recruitment, selection and vetting of staff is most important (see 11226 below), particularly for those who are to be employed in areas considered sensitive.

A contract of employment should contain a requirement that any employees and officers leaving the company should observe its confidentiality and should not disclose information relating to the company to other persons. (See CONTRACTS at 4078 and Schedules A and B.)

Management personnel leaving the company should be required to vacate the premises immediately, to limit the amount of information taken. Of course, they may have been active in gathering such information or property before making their departure known and in such cases, management should check for missing files etc.

In high risk situations, new employees can be subjected to psychometric testing to determine their adequacy for the position and give a reasonably clear picture of the integrity of the individual.

The most vulnerable individuals within the organisation in terms of supplying information to outsiders, are those suffering financial stress. This can be brought about by alcohol or substance abuse, gambling, marital difficulties etc. Line managers should observe their departments for personality changes, usually associated with stress, and if noted should report them to senior management. Counselling of the individual and offers of help can prove most cost effective and will usually increase the sense of loyalty of the employee.

If an employee is discovered passing confidential information out to others, disciplinary action must be taken. Remember, if he has been caught, he may well have been involved in previous instances, and is likely to continue his activity with even greater care. If a person is suspected of passing on information, he should be carefully monitored and even investigated to confirm the suspicion.

Staff need to be made aware of the potential of the problem and should be encouraged to report any suspicious approaches.

The majority of staff will be departmentalised, being involved in just one part of the operation. Efforts should be made to limit their activity to their area only and restrict their movements. They should not be able to simply wander into other areas. The easiest way of preventing such unauthorised access is by management dictums, but these are not always observed and it may be necessary to create physical restrictions, such as access control (see 11186 below), to keep them out.

Internal documents should be graded to identify their sensitivity and their issue should be on a need to know basis. Highly sensitive documents should be numbered and photocopying should be prohibited.

Contractors

11092 Contractors **will** often work for a number of companies, some of whom may be in competition. It is essential that the company carefully selects and checks references on contractors applying for work, finding out if possible who their other clients are.

Contractors should only attend a company by appointment. The names of their representatives should be supplied and identities should be checked before any passes are issued. They should be escorted to their place of work and when their job is done, should be escorted out. They must not be allowed to wander around the premises.

Many organisations have vending machines and contracts with the suppliers to clean and refill the machines on a regular and frequent basis. Often the service engineers will become recognised as an integral part of the company and their presence will be readily accepted by the staff. Indeed, they may even become friendly with the employees and may even ask questions relating to the business.

Such familiarity must be avoided and departmental managers should note the potential problem. Certainly, the engineers should not be allowed to wander into offices or indeed any places not involved in their work.

Cleaners

11093 If a contract cleaning service is used, the same checks should apply as with any other contractor. Attention should also be paid to the way the contractor recruits the cleaning staff and the frequency of personnel change.

Designated persons should be made responsible for cleaning sensitive areas and they should lock themselves in whilst working. On leaving the area, the doors should be re-secured.

In extremely high risk situations, a security officer should be in attendance, monitoring the activity and securing the area on completion of the work.

During their occupation of the premises, all external doors should be locked.

If the cleaners notice other persons on the premises, they should immediately report the fact to their supervisor or challenge the person. After all, if the person is there to steal or damage property, they may be held responsible and could lose the contract and their own jobs.

In situations where there is an intruder alarm installation, the supervisor may be required to set the alarm when the duties have been finished. It is essential that he knows the precise setting procedures and in such cases, the system should be connected to a central station, where the setting and unsetting activity is monitored.

Audio surveillance

11094 'Bugging' devices are freely available and are openly displayed in a number of magazines. They are cheap, efficient and reliable, and can be used to pick up discussions and telephone conversations.

There are essentially three *in situ* devices:

- Hardwire - using a concealed microphone in a target area, with direct wire connection to a listening post or recorder in the same building.
- Radio transmitter - using a tiny microphone and transmitter, which can send signals some distance from the site.
- Telephone devices - for tapping into telephone lines or using the receiver as a microphone.

Hardwire devices are rarely used nowadays, since their installation takes some considerable time and, unless professionally done, can be detected with ease.

However, the radio transmitters are easily concealed from view and are disguised to fool even the most practised eye. The devices can be included in electric plugs, power points, ashtrays, and marketing goods such as pens, calculators, clocks etc, which sit on the desks or are carried by key personnel. As indicated, such devices are easily acquired, although the user should have a radio transmission licence (and no illegal user is going to identify himself).

Even a simple device can send a signal several hundred metres and a receiver can be left in a parked car, some distance away, to pick up the signals. Often, a sound activated cassette recorder will be connected to the receiver, switching on when sounds are heard and switching off during silence to conserve the tape.

The most common target areas for the installation of these devices are:

- Boardrooms
- Executive offices
- Meeting rooms
- Management dining rooms
- Executive toilets
- Executive homes

The telephone devices, whereby the receiver is turned into a microphone, can be activated by dialling the target number, and giving a signal which can activate the microphone before the phone rings and stopping the receiver from ringing. The device will then pick up any sound from within the room. Of course, the receiver must have a direct line to the outside, but such a phone can be accessed from anywhere in the world using STD.

Old fashioned switch-gear panels can also be interfered with to pick up conversations of particular extensions.

Wire taps are also used, on office and home lines, to intercept conversations.

11095 It is important to determine if the company has been 'bugged'. There are a number of 'bug' detectors available, but many of these are of questionable value. Even if the detectors are suitable, in the hands of amateurs they are worthless.

If a company determines it could be the target of outside interest, it should call in experts to carry out a scan of the target premises and specific areas. The counter surveillance service must be one of integrity and should have the correct equipment to cover all current methods.

Some of the companies recognised by the Author are:

Godfrey Dykes Consultancy Ltd,
Leecroft, Hill Brow Road, Liss, Hampshire GU33 7PX
Tel: (01730) 892734

Farleigh Projects International Ltd,
Suffolk House, College Road, Croydon, Surrey CR9 **1DR**
Tel: (0181) 688 6799

Control Risks Group Ltd,
83 Victoria Street, London SW1H OHW
Tel: (0171) 222 1552

If an electronic sweep, to detect the presence of devices, has been carried out, it is quintessential that persons are denied the ability to introduce further devices immediately afterwards. It is therefore necessary to have access control disciplines in place so that they can be applied immediately the sweep has been completed. All risk areas should have suitable mechanical or electronic locks fitted so that they can be used to seal the rooms. Keys or cards for operating the locks should not be left where unauthorised persons can gain access to them. Subsequent entry into the areas should be restricted to authorised persons only. Any cleaning of the room should be supervised.

It is possible for authorised business visitors to introduce a device into the areas during meetings and they should not therefore be left alone. Miniature transmitters can be well concealed in a matter of minutes and will not be seen in a subsequent visual search.

Electronic sweeps should take place at least every four months.

In the foregoing text, reference was made to a recording briefcase. These devices are even advertised in the National Press. They consist of a briefcase fitted with a concealed miniature microphone and voice activated recorder. The user will normally be a business visitor and he will 'forget' to take his briefcase away when he leaves the meeting. This will then faithfully record any post-meeting discussions. Later in the day, the visitor will return to collect the briefcase and have recordings of the subsequent discussions.