

Guide to managing staff securely

Protection against the threat of the 'insider'.

The UK's Security Service MI5 recently released guidelines for companies to protect themselves against external threats from 'insiders', whether criminal, terrorist or espionage, or from competitors seeking a business advantage.

This could be a permanent or temporary member of staff, contract or agency, who abuses or exploits access to your premises for a variety of reasons including personal gain, boredom, revenge or sympathy with some external cause. Alternatively a vulnerable member of staff could be forced to cooperate with terrorists or criminals through fear, because they are being coerced or blackmailed, says the Home Office.

Whatever the motivation an 'insider' can cause your company a great deal of damage.

Quite a bit of this advice is just common sense and recommends good recruitment and employment practices, but personnel security can bring up a lot of difficult and sensitive issues. Procedures to help prevent staff crime, spying, acts of sabotage and so on, can be seen as intrusive and bitterly resented, plus employees can feel as if their basic rights are being infringed.

The Home Office says that whatever the circumstances, it is important to ensure that any measures taken are proportionate to the perceived risks and that staff should understand these and be prepared to accept any measures taken to reduce risks.

Good practice

- Establish the bona fides of potential employees. Ask the individual to provide full name, date of birth and address, with supporting official documents such as passport or driving licence. Ask to see a recent utility bill confirming the given address. Accept only original documents – no copies.
- Take up references from school, college, universities and previous employers and check that they are genuine. Request proof of academic qualifications (again, insist on original documents).
- Ask for details of unspent convictions, where allowed under

the Rehabilitation of Offenders Act, 1974. Individuals in England and Wales will soon be able to obtain statements, known as 'basic disclosures' from the Criminal Records Bureau (CRB).

- Where relevant, seek proof of the right to work in the UK.
- Remind applicants that supplying false information, or failing to disclose material information may be grounds for dismissal.

Encourage your staff to be alert to anything unusual in an employee's behaviour or attitudes and to voice their concerns. Reassure them that all such information will be handled sensitively and confidentially. Any action taken must, of course, be in accordance with employment law and other legislation.

Operate a security awareness programme to remind staff of potential threats, both internal and external, and of their role in countering them.

Operate a 'need to know' policy where possible, minimising access to confidential locations, assets or information only to those staff who need it.

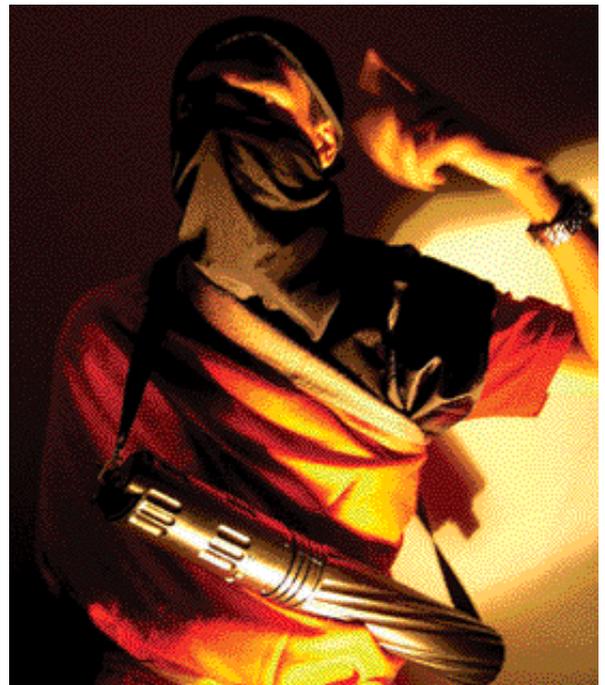
Consider physical access controls to particularly sensitive areas, or random searching on entry and exit of such areas. This is a very intrusive course of action, however, and staff need to fully appreciate the reasons behind it.

Contractors and agency staff

The use of contractors and agency staff for a range of services (IT support, catering, cleaning, security guarding, consultancy etc) can create new vulnerabilities and expose business to greater 'insider' threat. A contractor may have no direct access to sensitive information, but they may be able to plant a listening or other device in your building which could cause equal damage.

Some agencies are very careful in their staff selections. Others, however, are less rigorous and open to exploitation by terrorists and their sympathisers, or by others who wish to damage an organisation.

- Make it a contractual obligation



Don't leave your company vulnerable to attack

that contractors should validate the identities of their staff.

- Conduct regular monitoring of your contractor's compliance with the contract.
- Establish that the contractor is part of a recognised professional organisation, responsible for accrediting standards in that industry.
- Ensure that procedures are in place for you to confirm that the individual sent by the contractor or agency is the person who actually turns up. (Ask for a photo of the individual together with name in advance of their arrival; also ask for a photo ID from the individual that can be checked on entry.)
- Provide passes to contract staff which must be worn at all times and make sure they are all handed back once the work has been finished.
- Agree a procedure for substituting contract staff with temporary replacements, when the usual contract staff are away or sick and consider whether the replacement's duties or access need to be restricted.
- Supervise contract staff at all times.
- Nominate a permanent member of staff to be responsible in personnel terms for contract staff, so potential problems can be identified and addressed early.

www.mi5.gov.uk

Who's listening to your business secrets?

