The office cleaner wanders around the IT department emptying bins into a black plastic sack. He bends below each desk to look for stray sandwich wrappers and plastic cups. Whilst he's under the desk, it is a matter of seconds for him to attach a hardware key logger between keyboard and system unit. These small key loggers are effectively invisible on the back of the computer, and record every keystroke the IT folk make for the next week. They will capture user names and passwords, as well as every e-mail and browser entry. Often this will include credit card information from Internet shopping, home address details, bank account details – in fact whatever the individual typed into the computer during that week.

Of course there are plenty of similar opportunities throughout the organisation – the CEO's secretary's PC for instance, or the Finance Director's. It's just like bugging with virtually no risk and far bigger rewards according to Peter Wood, Chief of Operations at First Base Technologies. Most organisations are vulnerable to this type of attack and will never know that it has taken place. The truth is that no-one conduct proper staff vetting, and they certainly don't check the cleaner's credentials!

Industrial espionage and organised crime are a real threat, but most surveys show that the more significant risk is from inside the organisation. An employee can often see far more corporate information on the head office network than anyone realises. If hacking is defined as attempting to gain unauthorised access to sensitive information, then most organisations have significant number of hackers on their staff. Disgruntled employees (and ex-employees) present a very serious threat to business through access to critical data and personal information. Suppose an employee, with just a little Internet research, discovers how to read everyone's e-mails or even send mails as if they were the CEO.

Today, access to information is almost always controlled by a password. Users, even technical experts and senior staff, frequently use incredibly easy-to-guess words, such as 'password,' 'holiday,' or even their own name. The use of trivial passwords to secure "service accounts" – highly privileged accounts used by backup programs, network control software and anti-virus tools – is so common that gaining control of an entire network frequently takes take no more than a few minutes.

Organisations make very dangerous assumptions about the security of data on their networks. No-one considers, or more importantly tests, who might be able to view or steal mergers and acquisitions data, business plans, payroll information or BACS payments. On a typical corporate Windows network, anyone with an administrator account can see or copy anything. Putting information on a network server is not the same as locking it in your desk drawer.

In the words of Fox Mulder, 'trust no-one.' If someone steals your password, it is a significant step towards stealing your identity. It won't just impact your employer but your personal life too. In fact it could easily leave you with a reputation for enjoying child pornography, a large credit card bill and an even larger overdraft.

First•Base Technologies · Town Hall Chambers · High Street · Shoreham · West Sussex · BN43 5DD · UK
Tel: +44 (0)1273 45 45 25 Fax: +44 (0)1273 45 45 26 info@firstbase.co.uk