PC SECURITY

These days, security is on many of our minds. The all-but universal nature of the internet gives hackers and viruses free rein, while the sheer number of computers around can't fail to attract the attention of the more light-fingered members of our society. David Bedford looks at how to tighten up your security

ILLUSTRATION: AILEEN O'DONNELL

Computer security is now big news. The media regularly carries stories of new viruses and their impact on businesses worldwide. But although email viruses are the most hyped aspect of computer security, the threat of a virus attack is just the tip of the iceberg.

Computer networks are hacked to gain access to commercially-sensitive information. Computers are stolen along with the valuable data stored on them. Natural disasters also take their toll – companies suffer losses due to fires, storms and floods; even lightning strikes to the power or phonelines cause damage and disruption. And, since 11 September, terrorist attacks, too, must be taken seriously.

Needless to say, when disaster strikes there's a price to be paid. And when data and productivity loss are taken into account, the cost can be very high indeed. Clearly no company can afford to be complacent about PC security, but preventative measures can be expensive. This undoubtedly deters many people from addressing the issue. However, our increasingly networked home and working methods can leave us particularly vulnerable and businesses, it seems clear, cannot afford not to take protection measures seriously.

Here, we delve into the subject of computer security and recommend practical measures – many of which cost very little – organisations and individuals can take to secure their systems and ensure it remains business as usual.

What's the problem?

Why is computer security such an issue? How costly can security breaches be to an organisation? Quantifying the cost of a typical incident isn't easy. Companies that have been the target of a virus attack, or had their servers hacked, are notoriously reluctant to admit it. Independent surveys are few and far between, but the facts and figures that are available paint a very bleak picture.

The most recent report on IT security, compiled by the National Computing Centre, showed that 44 percent of companies had suffered a security breach during 1998 and that the average cost of those incidents was £7,140. Of large organisations with over 500 employees, the percentage admitting to an incident rose to 60 percent and the average cost was over £20,000.

Even more worrying is a report by Safetynet which suggested that, after a major incident involving the loss or destruction of computer equipment, 80 percent of companies never reopen.

It's not only businesses that are at risk. The Home Office's latest British Crime Survey, reporting on crimes during 1999, also makes depressing reading. The survey shows that 4.3 percent of all households in the UK suffered a break-in and that PCs represented the only growth area in domestic burglaries. Computer equipment is now the fourth most commonly stolen item after cash, video recorders and audio equipment – that makes it one place ahead of TVs. The financial cost to a home computer user will be far less, of course, but the inconvenience caused is still considerable.

Extra security

When the cost can be so high, it's hardly surprising that some companies take security threats very seriously. For example, business communications services specialist Extra provides what it claims is the ultimate in physical and technological security for its clients. Servers are housed in a former Bank of England bullion vault with 14 feet thick granite and reinforced steel walls, sealed against water with pumps for use in the case of localised flooding.

Over 60 CCTV cameras monitor and log movements, there's an independent electricity substation and three autostart diesel generators to prevent downtime during power cuts. Cabinets are cooled by underfloor refrigeration and there's remote environmental monitoring with automatic fire suppressors. Access to the vault is restricted to authorised staff by the use of swipe cards.

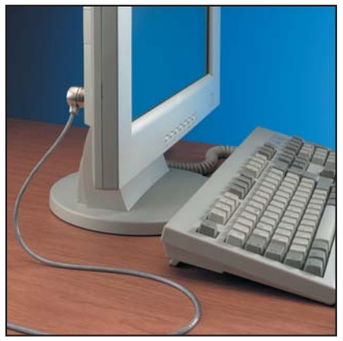
Virtually safe?

It's obvious that physical risks such as fire, flood, accidental damage, power cuts, theft and sabotage are potentially very damaging. But what of remote risks such as those imposed by viruses and hackers? Without some further facts and figures, it's difficult to know which threats are the most serious and, accordingly, where you should concentrate your defences.

The 1998 Business Information Security Survey (the latest statistics available) identifies the four main risks as power failure, LAN (local area network) failure, viruses and theft. However, the average cost of each type of incident varies. Theft stands out head and shoulders above the rest with an average cost of £17,557 per burglary. It would be wrong to ignore the other risks – and we will look at other security threats in this article – but from these statistics it's clear that theft is where the major part of your efforts should be expended.

Many thefts can be prevented by taking simple precautions – such as thinking about where you locate your PCs. Don't place computers against a downstairs window from where a burglar could steal your equipment without even entering the building. If your office is partially based at ground or lower level, easily accessible, fully-opening windows are an obvious exit route for thieves making off with your valuable equipment.

If you're a home user, don't place your PC near an upstairs window, either. This just advertises the fact that you have a computer and, since half of UK households still don't own a PC, it makes your home an attractive target.



While keeping items of value out of sight is the least expensive security measure, it's also worth spending a few pounds on ensuring opportunists thieves are discouraged. Simple antitheft products that announce their presence can be very effective, although the cheaper models provide protection only against the more casual burglar.

An inexpensive yet obvious option is to mark your electrical equipment. There's no harm in including both visible and invisible ownership details. In addition to making the equipment less attractive to a would-be thief, the presence of an indelible identification means that any stolen equipment recovered by the police will be returned to its rightful owner. Stationery companies, office equipment suppliers and PC vendors all sell this type of product.

Security cases that physically lock your computer to a desk make it far harder for the system to be moved. Some of the better enclosures can withstand a sustained attack – say, five minutes – with a hammer, jemmy and chisel, so it's advisable not to help thieves by storing such tools in an office.

Protection against data theft can be equally simple. Don't leave floppy disks or CDs on your desk, especially if members of the public are allowed into your office. And then there's the question of passwords. They are only effective if used properly. Many people select a password that is easy to remember, but this also means it's simple for someone else to guess. Choose a long and convoluted password and certainly don't opt for your name, your partner's name, your phone number or the like. Having picked an obscure word, don't display it on a Post-It sticker around your desk space.

Finally, make sure your data is adequately and frequently backed up. This means that, if the worst happens, you still have a hard copy of your work. Setting up and implementing an automated backup routine is simple, as you'll see from the *Protect your PC* workshop on page 156 of this issue.

• Equipment marking Retainagroup: 020 7823 6868; www.retainagroup.com.
• Locks and security cases Boxx Security: 01494 440 000. C&P Security Systems: 0500 549 114; www.cpss.com. Secure PC: 020 8744 3993; www.securepc.co.uk.

As you go beyond the first level of protection, prevention becomes expensive. This shouldn't deter you, though, since these costs will be negligible compared to the costs associated with a major catastrophe. The Gartner Group recently forecast that half of all small companies would be hacked by 2003. European firms spent €3.4bn on security products and services in 1999, while the cost of PC theft is running at €625m a year.

You could try fitting internal PC alarms, which plug into an expansion slot and are triggered if anyone tries to open the case or move it while the power's off. Another product is WebDetect, a piece of software that tracks down stolen PCs by tracing phone numbers from the IP address if it is connected to the internet after the theft. Cleverly, WebDetect will continue to protect a PC even if the hard disk is reformatted.

The data residing on your hard drive is far more valuable than the PC itself. Consider using removable hard disks and locking them away in a safe each night. Alternatively, set up a regime in which data is stored on a central server rather than locally on each desktop. It's then an easy matter of locking that server away in a secure room.

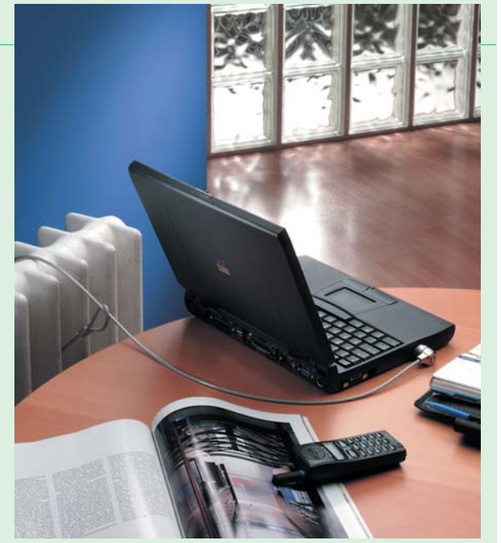
General security issues should not be ignored either. Issues to consider are security guards, door locks, controlling personnel entry via swipe cards and general-purpose burglar alarms. As you make sure all these are up to scratch, don't forget that your beefed up security measures must comply with health and safety legislation (see www.hse.gov.uk).

But danger doesn't only come from malicious attacks. The possibility of fire is an obvious one and the preventative measures – fire extinguishers that work, are full, and which your staff know how to use – are equally obvious.

Less obvious, perhaps, is the issue of lightning strikes to power lines. In addition to causing power cuts, lightning can cause spikes and surges on the mains supply which, in turn, can damage electronic equipment. Power-related threats can be combated by investing in a UPS (uninterruptible power supply). These automatically saves files and performs a controlled backup routine so as little data is lost as possible .

• Health and safety information Health & Safety Executive: 08701 545 500; www.hse.gov.uk.
• Internal PC alarms and security software Secure PC: 020 8744 3993; www.securepc.co.uk. WebDetect: 01633 250 315; www.webdetect.com.
• UPSs American Power Conversion: 0870 845 8520; www.apc.com. Belkin: 01604 678 300; www.belkin.co.uk.

Safety in the home



Much of the advice offered here is designed to help businesses prevent or recover from expensive security breaches. There is some justification for this emphasis – the risks are greater than those to home users, as are the costs of a security breach. Even so, the issue of security shouldn't be ignored by the home user, especially anyone running a business from home. So how much of the information provided here applies to the home PC user?

Domestic protection

Except for issues such as security guards and swipe cards on doors which, quite clearly, only apply to business premises, everything we discuss is relevant to the home user. The only difference is that the cost of an incident will usually be less and the amount spent on prevention will be less as a result.

Ironically, home users have tended to ignore security, believing that these sorts of problems always happen to someone else. However, since PCs are now highly sought after by domestic burglars, basic antitheft precautions – perhaps a cable system and some form of marking – are a must.

Security products such as a UPS (uninterruptible power supply) – a device that prevents PC crashes and data loss in the event of power surges or cuts – and firewalls are no longer the sole domain of the business user. Both of these security devices are easily affordable to those with a more modest budget.

You might not think that hacking is a major problem for the home user and, admittedly, you're not as likely to be attacked as a high-profile company. However, there are always hackers on the lookout for a vulnerable computer and, with the introduction of always-on internet connection services such as ADSL (asymmetric digital subscriber line), the likelihood of an attack is greater than ever.

Kevin Chapman, consumer and small business director of Symantec, says consumers are aware of the threat viruses pose, but there's a misconception that PCs come preloaded with security software. However, the sort of threats that will most affect home users are likely to be viruses transmitted via the internet, and juvenile exposure to inappropriate material. Despite this, Symantec has found that 60 percent of families with children aged up to 15 years would not consider content-filtering software a priority to protect them.

Finally, check your PC equipment is covered by your household contents insurance policy. If you run a business from home your computer may not be covered unless you inform the insurance company of this and, in most cases, pay an additional premium.

Whenever your company's PCs are connected to the internet or to a network they're at risk, because you are providing an open channel enabling remote machines to receive data from and send it to your hard disk. This is how the majority of viral attacks have come to be spread indiscriminately by email, rather than by hackers directly trying to gain malicious access to your company's server.

There are a number of steps you can take to exclude unwanted visitors from your network, of which antivirus software is among the simplest and least expensive solutions. For practical advice on how to keep your data safe from hackers and viral attacks, see *Protect your PC* on page 156.

Even if you haven't chosen to share the files on your PC (made them accessible to others on your company network) there are ways for hackers to steal your data or cause damage by deleting or modifying files. Operating systems have been known to have security loopholes and malicious software called Trojans (perhaps received as email attachments) can be used to circumvent Windows' security features.

TOP 10 SECURITY TIPS

1. Common sense **This is the first level of security, and it costs you nothing. Be sensible and think about where you position your desktop PCs. If you regularly work on the road, remember not to leave your laptop on view in a car.**
2. Antitheft products **Think about investing in some antitheft products for your company's PCs – for example, cables, enclosures, markings and possibly an internal alarm.**
3. General building security **Make sure your office's alarm and locks are adequate and, if burglary is especially prevalent in your area, consider a security guard and swipe cards on the doors.**
4. PC security features **Look for models with removable hard disks or, for laptops, a fingerprint scanner or smartcard slot.**
5. Laptop bags **Don't use a holdall which advertises the fact that you're carrying a laptop around – invest in a more secure, backpack-type case instead.**
6. Back up **We can't stress how important it is to regularly back up your vital data. This way, if your PC(s) get stolen or damaged, you won't lose valuable data.**
7. Protection from natural disasters **Make sure you have sufficient fire extinguishers and invest in a UPS (uninterruptible power supply) to protect against power cuts and mains surges.**
8. Web security **Use up-to-date antivirus software and don't open attachments unless you know what they are.**
9. Firewalls **For the small office or the home user, a personal firewall provides protection at a modest cost.**
10. Data recovery services **Prevention is better than cure but, if the worst happens, you may need to call in the professionals.**

Fighting back

To combat attacks, you need to invest in a firewall. A firewall acts as a defensive barrier and sits between your network (or even a single computer) and the internet. Using a variety of rules it analyses incoming traffic, filtering out anything it considers to be malicious.

Traditionally, a firewall is either a standalone hardware unit or a piece of software running on a dual-ported gateway PC – that is, a system with two network connections. These offer a high degree of protection, but can be expensive and are by no means easy to set up. Choosing and installing this type of firewall is a specialist task. If you don't have an inhouse network specialist you should enlist help from a consultant.

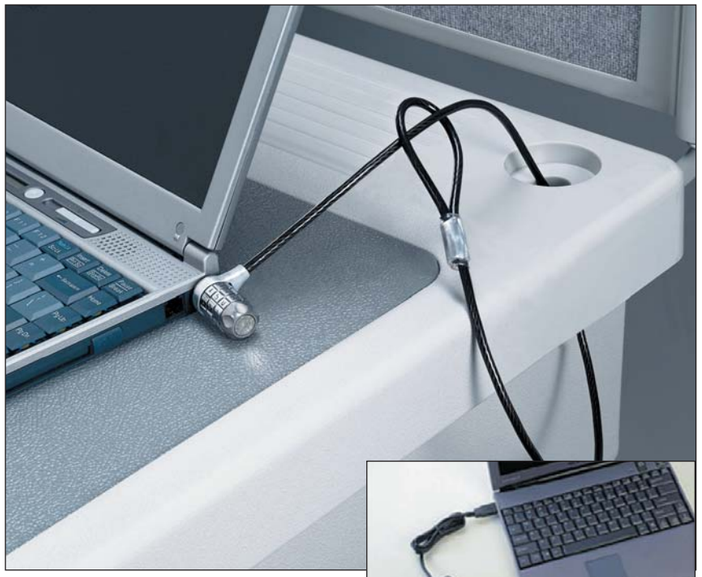
Personal firewalls are becoming popular with home and small business users. A personal firewall simply requires software to be installed on each PC that you want to protect. Personal firewalls are aimed at the ordinary PC user rather than the networking specialist and are much easier to install and set up than a conventional firewall. This makes them a practical proposition not just for PCs on a small business network but also for those with an individual home computers.

• Firewall software McAfee: 01753 827 500; www.mcafee.co.uk. Symantec: 01628 592 222; www.symantec.com. WatchGuard: www.watchguard.com

MOBILE WARRIORS

As soon as a piece of equipment leaves the confines of the home or office, it becomes even more vulnerable to loss, damage of theft. Security should therefore be a major priority for anyone who regularly uses a laptop on the road. And, as with office equipment, a lot comes down to plain common sense.

So, for example, don't leave your laptop in the car or, if you have no option, make sure it's locked in the boot rather than on display on the back seat. If you do have to leave your portable unattended on occasion, get hold of a laptop security cable such as Fellowes' Combination Cable Lock, which has a four-digit resettable combination, much like that used to secure bicycles. These fit into your laptop's security slot and allow you to lock it to an immovable object.



↑→ Notebook data is at even greater risk from theft than that held on a PC. If you're a seasoned business traveller, don't take any risks: invest in a security device, such as a cable lock

Think, too, about what you carry your laptop in. A conventional notebook case certainly looks smart, but it's just advertising the fact that there's an expensive laptop inside. And remember that street crime is a growth area. Although it might not promote the same image, your portable PC would undoubtedly be safer in a holdall or even a scruffy supermarket carrier bag.

Alternatively, you could invest in a backpack-type case, such as those produced by Targus. Quite apart from disguising the fact that you're carrying expensive equipment, it's much harder for a mugger to run off with one of these than to grab something out of your hand.

However much care you take, there's always the possibility of a lapse in concentration – it only takes one slip to do a lot of harm, as one politician found to his cost when he left his laptop in a taxi. To prevent this sort of mishap you could invest in a laptop alarm. There are various types to choose from. Alarms are triggered if someone tries to remove your laptop; others if the notebook becomes separated by more than a few metres from the keyfob on your keyring.

Finally, why not consider security when next purchasing a laptop? Many manufacturers produce high-end models with built-in owner-verification features. Portable PCs are available with fingerprint scanners and/or smartcards for access control. Ultra-portable notebooks with separate hot-swappable drives can be a secure option – just remember to remove the hard drive whenever there's a chance your laptop will be out of sight.

• Backpack portable carriers Targus: 020 8607 7000; www.targus.com/emea.
• Fingerprint scanners and smartcards CI Solutions: 0870 752 3030; www.ci-s.com. Targus: 020 8607 7000; www.targus.com/emea.
• Laptop alarms CI Solutions: 08707 523 030; www.ci-s.com. Targus: 020 8607 7000; www.targus.com/emea.
• Laptop security cables Fellowes: 01302 885 331; www.fellowes.com. Targus: 020 8607 7000; www.targus.com/emea.

DISASTER RECOVERY

Prevention is better than cure and, if you adopt some or all of the measures discussed here, your computing equipment will be less prone to catastrophe. But however many precautions you take, accidents do happen. So what can you do when disaster strikes? And how can you recover with the minimum amount of disruption and cost?

If you haven't backed up your data or it is hopelessly out of date then there's very little you can do – your business will undoubtedly suffer. If, however, you have adopted a regular backup regime, while you'll almost certainly have to duplicate some work but this should be limited to files you've created or edited over the last day or two.

Even if you lose your data and have no backup as a standby, you may not be doomed. In the case of a theft or a serious incident such as a fire, there's no way you'll be able to recover the missing files. But in the case of a viral attack, disk crash or data destruction caused by a hacker, there may be a way out.

Following these sorts of incidents, the data on your disk won't necessarily be lost, even if the file or directory is corrupted and Windows can't find it. There are experts who can recover data from damaged disks, although this sort of service doesn't come particularly cheap.

Data recovery can cost anything up to a couple of thousand pounds, depending on the disk size, the number of files and the degree of damage. Recovering data from large disks on servers costs considerably more. Using a data recovery service is a good last resort, but keeping it secure in the first place is the best solution of all.

• Data recovery services CBL Technology: 0800 028 2069; www.cbltech.co.uk. MJM: 0800 072 3282; www.mjm.co.uk. Ontrack: 00 800 1012 1314; www.ontrack.co.uk. Vogon: 0800 581 263; www.vogon.co.uk. ■