Security check

Whether it's because a door is left open, passwords become known to all or there's insufficient protection from external threats, it's easy for data to go walkabout. Guy Clapperton explains everything you need to consider to keep your PC and your documents secure

This article is being typed on a laptop computer – what can I tell you, the sun's out. My work will travel wirelessly to the router that's connected to the internet, which will then transmit it to the publisher. At this stage it will bounce around editing, page design and subbing staff's systems then off to the printing process. That's about five points at which the copy is in transit and could be intercepted or altered. Meanwhile any of these computers through which it has travelled could be vulnerable to a virus attack.

It may sound alarmist but the threats out there are real enough. Many home users and small offices believe that having the latest version of Windows installed on their system means there's no need to worry about such matters. Windows XP is certainly more secure than its predecessor but its built-in firewall only has two simple settings – on and off – and there's no dedicated antivirus software.

It's also far too easy to erroneously assume that all IT security problems are attributable to, or can be overcome by, technology. If this reflects your attitude, think again. Can you account, for example, for everyone who has walked into your premises over the last fortnight? Maybe you keep a guest book for the fire regulations so you can do just that. Now, can you say exactly what they may or may not have seen on monitor screens while they were passing by? And could they have picked up a laptop from a desk if they'd had a mind to?

Thankfully, most times out of a hundred you'll be worrying about nothing when you consider matters like the above. Over the next few pages we'll help you shorten the odds even further.

Rescue me

Inevitably there will be cases where things go wrong and data appears to be lost. First, consider how many of the files were actually critical. Okay, so you've lost a spreadsheet or three that you archived seven years ago – then again, the Inland Revenue can't touch you after six years have elapsed. And if you've backed up adequately there shouldn't be much of a problem.

Hiring a data recovery company needn't cost a fortune. Kroll Ontrack's EasyRecovery Lite service retrieves 25 files per recovery in up to five storage devices and will set you back a princely £49.99. Larger companies facing data loss will pay £95 for an initial investigation into what can and can't be recovered. A plan can then be formulated from the results.

It's worth bearing in mind that data can be recovered in more than one format. DocumentSOS' managing director Georgina Thorburn cites a case in which a writer working from home had a fire and thought his backups (which had melted) were his last hope of recovering his script. In fact the paper copies, although smoke damaged, were readable enough when cleaned up. The majority of damage from fires is in fact smoke damage, she confirms, so don't get too tied to the PC as the be-all and end-all.

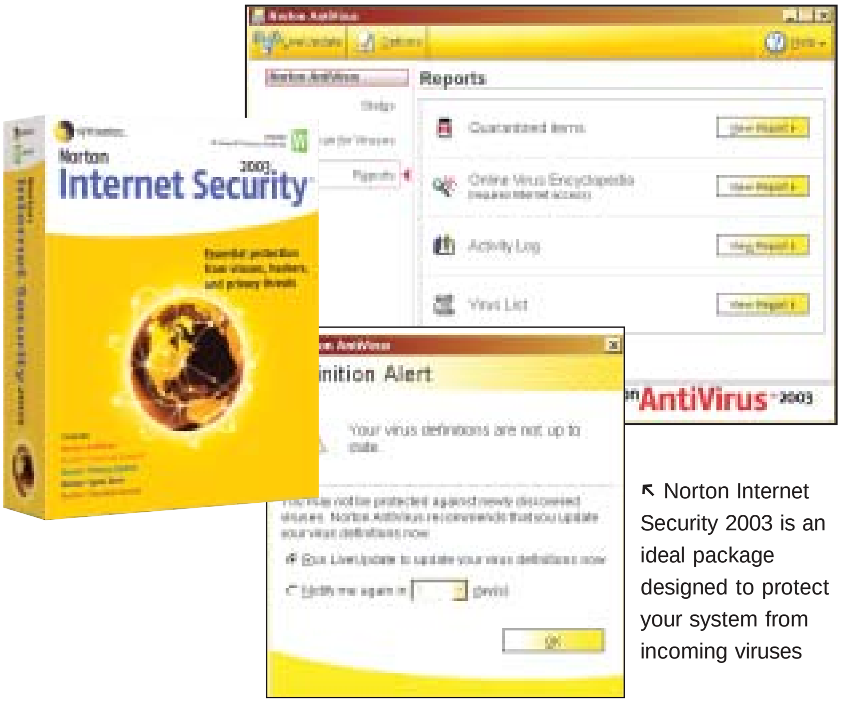
The majority of damage from fires is in fact smoke damage so don't get too tied to the PC as the be-all and end-all

Planning for the worst

London First is a business membership organisation supported by over 300 of the capital's major firms. In its article, *Expecting the Unexpected,* home secretary David Blunkett stated that "Business continuity and planning is just as important for small companies as it is for large corporations." You wouldn't know it to look at the figures.

A recent Deloitte & Touche survey said that nine out of 10 large businesses had a disaster contingency plan. According to the London Chamber of Commerce, that figure shrinks to 20 percent when you look at small to medium-sized London firms. Gartner Group estimates 40 percent of such enterprises would stay shut if they had a security breach.

This wouldn't be so bad if such problems were easily overcome. However, US research argues against this cosy thought. According to the National Archives & Records Administration in Washington, 93 percent of businesses that suffer more than 10 days of system downtime will file for bankruptcy within a year. Why would this be any different in the UK?



Your virus definitions are not up to date.

You may not be protected against newly discovered viruses. Norton AntiVirus recommends that you update your virus definitions now.

● Run LiveUpdate to update your virus definitions now

○ Notify me again in [ ] day(s)

↖ Norton Internet Security 2003 is an ideal package designed to protect your system from incoming viruses

Risk of infection

Nervous? Good. An appreciation of the problem is a useful first step to curing it. The difficulty is to decide which of the various security issues you should address first. Purchasing some antivirus software is a given. Keep it up to date and your system should be more or less virus-proof as, thankfully, the major antivirus players work proactively together.

Graham Cluley, senior technology consultant at Sophos, argues: "By blocking potentially dangerous executable code, not only will known viruses be stopped but new viruses will be prevented from reaching company desktops. Many viruses arrive as an attachment with a double extension such as nastyoldvirus.jpg.vbs. As well as blocking files with double extensions a list of disallowed file types can be created."

So which antivirus package should you opt for? Sophos works in the background and is light on memory, but requires confidence in installation. Norton AntiVirus

Safety in the home

The integrity of data is paramount in any setting but there is one place in which it is simple to overlook the risks – for people who work at home. The risk of physical damage will be greater simply because you're in an unregulated environment. No, of course home workers aren't exempt from health and safety regs but in practice there's little chance of them being enforced.

Some of the risks that apply in offices won't be relevant in the home. Switching monitors off or using a password-protected screensaver is unlikely to be a useful strategy when your cat is more likely to stumble across the data than your competitor. On the other hand, disabling the keyboard so that your three-year-old daughter can't send the information to Teletubbyland will be more of an issue for the home user, as will the usually neglected uninterruptible power supply.

Backing up remains a vital activity whether in a corporate or domestic environment. The other main difference is in insurance. Not only do home workers or their employer need to insure equipment, they need to tell their mortgage company/landlord and domestic insurers they're working from home. They will almost certainly have signed an agreement not to do so and will need to agree a waiver so that any domestic claims they may have to make later are not invalidated.

scans all your incoming emails for viruses and the current 2003 version does this much faster than its predecessor, while McAfee is also popular with the home user market.

Keeping tabs

Antivirus software is one of the more basic means of protecting data but it's not sufficient on its own. Indeed, many preventative measures have more to do with the physical reality of owning a PC than with anything particularly technical.

Not leaving laptops lying around is a start. In April 01 the Ministry of Defence got into a security flap when an absent-minded employee left his company notebook in the back seat of a taxi. This isn't a unique case, either – during five years up to January 02, the MoD lost 600 laptops through the forgetfulness of staff.

Firms such as Targus and Kensington offer combination locks while password protection and encryption programs can ensure your documents can't be opened by anyone else.

As well as keeping tabs on your portable PC while out and about, you need to be sure no one is checking out your expensive kit while it's in the office or your study either. Keep it out of sight. Bought a snazzy 17in TFT screen for your home system? Fine, but if it's positioned in your living room's front window then put a screen around it to mask it from passers-by. Home PC owners' property is more at risk from casual opportunists than anything else.

Password protection is one of the simplest ways of controlling access to your PC and any network it may be connected to. Choose wisely, combining characters and numerals and avoiding words that are easy to guess such as names of partners, household pets or football teams. Don't make your password a matter of public knowledge and don't leave your logon details handily displayed on a scrap of paper on your desk.

Network administrators encourage staff to vary their passwords periodically, but NEC Security's Carl Gohringer suggests enforcing a change of logon code every 30 days can have a negative effect as forgotten passwords will quickly become a drain on administrative resources. NEC is pushing biometric authentication instead and has a long tradition in this area, providing fingerprint-recognition services to the FBI. However, unless you're a large corporation or have particularly sensitive data, you probably won't need to implement such stringent measures.

Your data may not be a matter of national security but it does pay to ensure

In April 01 the Ministry of Defence got into a security flap when one absent-minded employee left his company notebook in the back seat of a taxi. This isn't a unique case, either – during five years up to January 02, the MoD lost 600 laptops through the forgetfulness of staff

Tedious as it may be, there's no excuse for not backing up. If you don't have a dedicated backup server, products such as BT's Datasure and Netstore's Online Backup allow you to do it online. Having stored your documents, take the backup media outside the office so that even if the building burns your data doesn't

safety measures are in place and that your files are regularly backed up. Then make sure the backups work. "It is always a surprise to me how few companies test their backup copies and equipment," says Bryan Mills, executive director of IT infrastructure group ServiceTec.

Tedious as it may be, there's no excuse for not backing up. If you don't have a dedicated backup server, products such as BT's Datasure and Netstore's Online Backup allow you to do it online. Having stored your documents, take the backup media outside the office so that even if the building burns your data doesn't. Fireproof safes aren't as protective as you may think; unless they are heatproof as well, backup media will warp and rapidly become useless.

When nature attacks

So what about plagues, nuclear wars and pestilence or, more likely, faulty air conditioning which can happily knacker a computer if it's positioned straight underneath it.

Physical location has a lot to do with potential damage. Take the IBM executive who left his laptop in his car parked outside the office only to find that, following a freak storm, the car had flooded. He'd sensibly put his laptop under his raincoat to throw thieves off the scent, but drying out the PC had no effect.

Despite this, recovery specialist Ontrack was able to restore the data. "No one can predict a natural disaster," says Ontrack's Todd Johnson, "but in the majority of cases what nature does we can undo. Flood victims with water-logged computers should not panic at the apparent damage nor attempt to dry it out themselves, but send the equipment to a data recovery specialist as soon as possible."

Data recovery companies may not be necessary for every environmental mishap, however, and there are inexpensive precautions you can take. Every home worker who has mission-critical work and deadlines should have a spare keyboard to hand just in case – spilling coffee or tea over the keys will cheerfully put you out of action for a few weeks or more depending on the repairs.

Building security shouldn't be overlooked either. If you're in your own office ensure that the burglar alarms are fitted properly and up to date then ask your insurer for a discount – you might well get one. If you have the resources, hire a security guard but be warned: this can advertise to potential thieves that you have something worth stealing.

If you're moving into serviced offices find out how often the building has been burgled. Some offices are targeted just because it's assumed a new business will have up-to-date equipment. Lockable cages for PCs are available inexpensively through many high street computer stores and you might also want to consider storing hard drives and backups in a secure server room.

Power struggles

Power is another important consideration – and not just if you have a full-blown power cut. PowerWare's managing director Mark Derbyshire says 84 percent of its customers nationwide have experienced power interruptions. This could cause serious harm to your computer network

Top 10 security tips

1 A bad workman blames his tools **The risks to which your computer is exposed are as likely to be human and managerial as technical. Check the positioning of computers and ensure that laptops aren't left where they shouldn't be.**

2 Strangers not welcome **Your antivirus software should operate across all networks your PC is connected to and it should be constantly updated – preferably daily.**

3 Data overload **It's that age-old rule: back up your information, methodically and regularly.**

4 In need of restoration **Practice restoring your important data from backups – they can go wrong!**

5 Good riddance **If your disks are removable then do just that – remove drives and put them in safes when you're not using them.**

6 Choose your friends carefully **Don't overlook burglar alarms and security guards, but watch for the reputations of serviced offices. There was a spate of burglaries in a serviced South London office in the early 1990s just weeks after a group of seemingly unprofessional decorators had been working in the building.**

7 If your name's not down, you're not comin' in **Ensure your system has firewall facilities of some kind – whether it's an inexpensive software package or a more sophisticated hardware-based product.**

8 Service charge **If the worst does happen and you lose precious information then shop around for a data recovery company – services start at around £50. For more on data security, visit www.ukonlineforbusiness.gov.uk/informationsecurity.**

9 Are you being served? **Encrypt emails coming in and out of your company's server and ensure that PDA data is password-controlled.**

10 Show them who's boss **Stress the importance to your staff of all the security procedures and routines that are in place. If need be, hold seminars to reinforce the point.**

so it's best to purchase an uninterruptible power supply or surge protector (which cost around £100).

"The escalating use of household computers and their peripherals is unleashing demands for increased power," says Derbyshire. Electrical demand, spurred largely by the high-tech market, is reportedly projected to increase 17 percent by 2010.

Derbyshire warns that: "Unless the energy industry injects sufficient investment in its infrastructure it will struggle to match the nation's demands. Common power problems such as spikes, surges, brownouts and outages may become regular occurrences."

A surge protector or UPS therefore sounds like a necessity, rather than a wise precaution.

→ The Pulsar Ellipse UPS range keeps your PC running for a short time when the primary power source is lost

↘ The Powerware 5115 contains a battery that kicks in when the device senses a loss of power

→ Trend Micro's Gatelock offers a built-in virus checker as well as firewall facilities

Sophisticated software

You might not be able to prevent power fluctuations but you can do plenty to secure your files from prying eyes. For example, Samsung's X10 notebook range has built-in fingerprint recognition technology called AuthenTec, while NEC offers not only fingerprint-based biometric products but iris scanners and smartcards too.

It's likely to be a while before the home user protection becomes that sophisticated but you can easily protect your data with a firewall. This software sits between your computer and the internet, keeping intruders away from your network while allowing your staff and/or family in.

Firewalls start at the very budget end – ZoneLabs' ZoneAlarm is free to download (grab a copy from www.zonelabs.com or this month's cover disc). One step up is the inexpensive Norton Firewall, which works well but needs configuring everytime you want a fresh application to reach out to the internet.

Hardware firewall systems are even more sophisticated and don't require as much configuration as you'd imagine. The Draytek Vigor2600x, for example, acts as a network router as well as a firewall and an ADSL adapter, while Trend Micro's Gatelock offers a built-in virus checker in addition to a firewall.

Larger companies should talk to an independent installer and administrator to pinpoint a suitable firewall system. For firms that use up to 10 PCs, though, off-the-shelf products should provide enough security. To assess your vulnerability go to http://grc.com and try Shields Up. Alternatively, access it from this month's cover disc. This free software quickly checks the security of your computer's connection to the internet.

And don't worry if you only have Windows XP's built-in firewall. It's a good start but, as Kevin Foster, strategic director of security tester NTA Monitor, says: "Given the widespread use of Microsoft products, the pace of attacks exploiting such holes would be frightening. Contrast this with firewall products that have less lines of code – typically a few hundred thousand at most – which can be more thoroughly checked resulting in reduced scope for discovering flaws."

Going mobile

If much of your work is conducted outside the office then you need a different security approach. Although there are plenty of handheld PCs that can manage wireless communications, few models offer firewalls to keep miscreants rifling through them.

But, says Utimaco Safeware's Jackie Groves, "Sensitive business information needs to be protected as it is accessed and transferred beyond the firewall. Without giving thought to the security of the actual mobile devices themselves, organisations may find their private data falling into the wrong hands."

Strong authentication such as passwords and virtual private networks will ensure the only person capable of accessing a mobile device's data is its authorised user. "Increasingly, employees are putting the company at risk from a security breach without even realising it," says Groves.

"Mobile working has added flexibility and convenience to working life. But in order to do their jobs, employees are often hooking up their own wireless devices, such as PDAs and laptops, to the corporate network. Unsecured and not covered by the corporate security policy, the unwitting use of rogue devices by company staff opens up yet another backdoor to the organisation's infrastructure."

There are simple, non-technical rules that mobile employees should follow as well. If a laptop has a removable hard disk then take it out when it's not in use. And keep the notebook itself out of sight.

Use your head

Whether you're office-based, work on the road or from home, taking regular backups and installing up-to-date antivirus software as well as a firewall will protect your system from unplanned attacks and ne'er-do-wells. Just don't forget to use your commonsense when positioning and storing IT equipment. ■

Check out this month's Technofile on page 66 which takes an in-depth look at antivirus and firewall packages