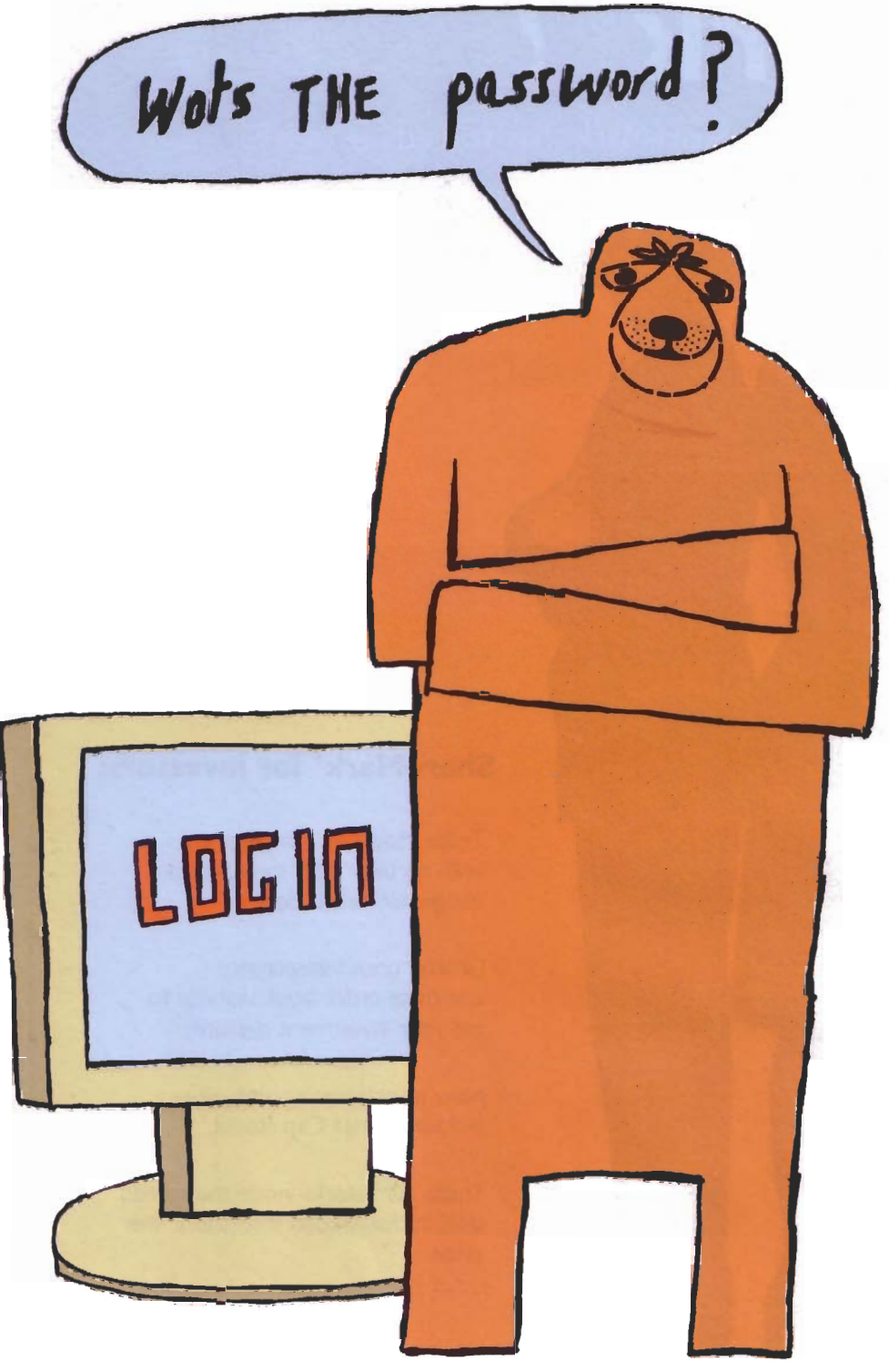


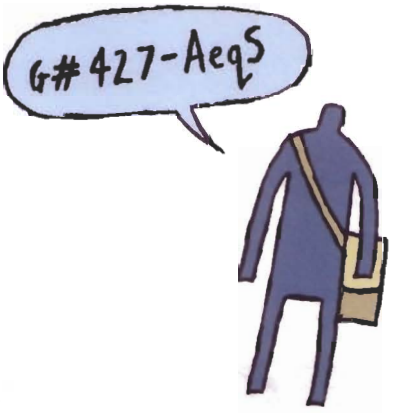
A piecemeal approach to security doesn't work. In the second of a two-part series, *Matthew Stibbe* looks at how to deal with this issue strategically.

Like the physical security in your office, your information security systems are only as good as the weakest element. You can have a great alarm and deadlocks on the doors, but it doesn't mean a thing if you leave the windows open every night.

Creating and revisiting a good security plan is the right way to get security done. It lets you prioritise key tasks, assess risks and co-ordinate the work. There are four stages to creating and using a good security plan:

Audit.. Consider the assets you are trying to protect, both tangible (e.g. computers) and intangible (e.g. reputation and privacy). Consider the risks. Evaluate the state of your current security. The result should be a prioritised list of risks, sorted by the likelihood of the threat and the pain it would cause if the worst happened. This is also the time to assess your own level of competence and knowledge and the resources you have to implement the plan.

Plan. The point of the plan is to identify tasks that will improve security, tackling the highest priorities first. For each risk, consider how to transfer, avoid, mitigate or (worst case) live with it. For example, if the threat is virus attacks, you can mitigate this with staff training, avoid it with up-to-date anti-virus software, transfer it by outsourcing e-mail security or live with it by, for example, restricting people's access to e-mail. The plan should include a project team responsible for implementation and name the senior manager directly responsible for security. Like all good plans, there should be a timeline, appropriate signoffs, a budget and a framework for ensuring compliance.



ADD MUSCLE TO YOUR NETWORK

Execute. Communicate with staff. Train where necessary. Carry out the plan. Test it and get feedback from users about any problems. Modify if required.

Monitor and repeat. Threats evolve and companies change, so once the plan has been executed don't just put it on the shelf, monitor compliance: make sure new computers are properly secured, train new staff, continually update virus checking software. Schedule a date for a re-run of the whole process.

It is possible to insure against certain computer risks, such as virus attacks, (see www.insuranc-e.com, for instance), although policies will insist on the same kinds of protection that common sense demands. Since insurance can often take weeks or months to pay out after a major incident and many companies go bust after a serious loss – even with insurance – it should be considered a last line of defence not a front line.

Last month, I looked at firewalls, viruses and software updates. There are four other important security techniques that you need to implement as a priority.

Strong passwords. Because most companies rely exclusively on passwords to authenticate users, it is very important that users pick passwords that are not easily guessed. This is not a technical solution, but a policy and training issue. Strong passwords:

- Have at least seven characters
- Do not contain the user's name, company name or a complete dictionary word
- Are not variations of previous password
- Contain a mix of upper and lower case letters, numbers and punctuation marks
- Are changed regularly
- Are kept secret and not given out to strangers (even with a plausible story)

Microsoft Windows XP™ and Microsoft Small Business Server 2003 have systems that can enforce a given password policy and lock users out who fail to comply. They can also log off automatically if unused for a given amount of time so that computers are not left open when people are away from their desks.

WI-FI WORRIES

Wireless networks, sometimes called 802.11 or Wi-Fi, are really useful. Laptops and PDAs can connect to company systems and the Internet without physical cabling. This makes it especially useful for small companies where office layouts and locations change frequently.

There is a downside: by default they are very insecure. For instance, I walked around Soho and Mayfair with a wireless-enabled PDA and found three open networks in under an hour. I could have used them to mooch off their Internet connections, send spam e-mail or try to hack into their computers. I didn't need to go into any buildings to do this at all. A more scientific survey in the City found that 25 percent of the wireless networks there were not secure.

Good news: wireless security is pretty easy to implement. Bad news: there's lots of jargon and implementations vary with manufacturer. So it's time to read the manual (or call tech support). The key points are:

- Don't broadcast the name of the network (known as the SSID).
- Change the SSID to an anonymous, hard-to-guess word.
- Restrict wireless access to normal office hours.
- Restrict access to known and trusted computers (called 'MAC filtering').
- Switch on and use the standard encryption to prevent casual eavesdropping (the Wireless Encryption Protocol or WEP for short).
- Don't let people set up their own uncontrolled wireless networks.

Physical security. If hackers have physical access to your computers, getting at the contents is easy. This means that theft or unauthorised access to an office computer is often easier than hacking through a firewall. So you need to make sure your office security is tight and that employees take proper care of laptops. Computer locks (such as the Kensington Microsaver™), security marking, door and window locks, alarms, asset tagging and special security around server rooms are all important. Don't forget to log computer serial numbers so that stolen equipment can be returned if recovered. Laptops are a special problem. Of five million in the UK, about 100,000 are damaged each year and another 67,000 stolen. So:

- Use a padded but nondescript bag
- Train users to keep laptops in sight at all times
- Keep laptops locked when unattended
- Never leave a laptop in plain sight in a car
- Keep separate copies of data stored on laptops
- Use the encrypted file system in Microsoft Windows XP™ to secure confidential files

Spam filtering. Unsolicited e-mails are unwelcome; often carry viruses and waste users time, whether they are peddling porn, scams or dodgy pills. Getting rid of them before they reach e-mail inboxes is therefore a good idea.

Microsoft Outlook 2003™ includes a built-in spam filter than can eliminate the majority of unwanted e-mails. SpamAssassin™, Brightmail™ and Messagelabs™, among others, sell spam filtering software that works on company servers, rather than individual desktops.

Backup. Keeping regular, up-to-date backups of your data and storing them offsite (as well as testing that the system works from time to time) is the equivalent of an airbag in computer security. It doesn't do anything to improve your driving but if you crash it may save your life.

SMALL BUSINESS SERVER 2003 TO THE RESCUE

Microsoft's new Small Business Server 2003 is the latest version of their server range. Besides all the usual server functionality – web hosting; file, printer, fax and Internet connection sharing; e-mail hub and the new Sharepoint services for use with Microsoft Office – it has a range of features designed to enhance security:

- Centralised access to data so that users only see the data they are meant to see.
- Built-in security firewall
- The Backup Configuration Wizard speeds the creation of an effective backup strategy.
- Built on proven Windows Server 2003 technology for improved reliability and better security.
- Password policies that ensure that all users select strong passwords
- The Premium edition also includes Microsoft's powerful Internet Security and Acceleration Server which pretty much does what it says on the label.

Where next?

Go to www.microsoft.com/security/protect/ for a step-by-step guide to setting up virus protection, software updates and a firewall.

For fortnightly security newsletters, an online quiz and detailed advice, go to www.bcentral.co.uk/security and www.microsoft.com/uk/security

Order a free copy of the British Chamber of Commerce's Guide to IT Security from: www.bcentral.co.uk:80/technology/security

Writing a security plan: www.ukonlineforbusiness.gov.uk/informationsecurity, www.microsoft.com/technet/archive/security/bestprac/bpent/bpentsec.asp and www.ietf.org/rfc/rfc2196.txt

Microsoft certified partners: www.microsoft.com/uk/experts

Backups: www.bcentral.co.uk/technology/buy/hardware/Backup.asp

Microsoft Small Business Server: www.microsoft.com/windowsserver2003/sbs

WiFi security: www.wi-fi.org/OpenSection/secure_the_network_setup

ILLUSTRATION: TIM ELLIS/WWW.DEBUTART.COM