



## 20 TIPS FOR...

# ...WATERTIGHT SECURITY

→ attacks – especially the trend for ‘blended’ threats where one or more tactic is combined – companies need a blended solution to combat this.”

### Use the internet to stay up to speed

What goes out of your company can be as dangerous as what comes in. Sending viruses or other damaging or offensive material can spoil your company's reputation and cause technical or financial damage to other companies.

Simon Heron, a director at internet security specialist Network Box ([www.network-box.com](http://www.network-box.com)), advises you to make use of free online information in order to help manage this on a limited budget. For example, you can avoid getting caught out by hoaxes by visiting [www.vmyths.com](http://www.vmyths.com) before emailing your friends and customers and propagating the hoax.

And for up-to-date news on the latest risks and viruses, check out [www.cert.org](http://www.cert.org). The information on the site is quite technical, but it can help inform you of what's around.

### Protect your company at network level

Doing so means your server will stop any potential threats before they reach people's desks. Julian Bogajski, UK commercial director at Sybari Software ([www.sybari.com](http://www.sybari.com)), points out that this approach means you can avoid the embarrassment of pornographic images reaching the end user, or spam being sent to all of your company's listed contacts internally and externally. It also lowers the risk of PC downtime.



**“Make your back-up routine part of everyday IT housekeeping. Stick a sign on the monitor, tie knots in a hankie... just don't forget!”**

GAVIN SMITH DATAFORT

For Ken Whalley, IT manager at the British Safety Council (BSC) ([www.britishsafetycouncil.co.uk](http://www.britishsafetycouncil.co.uk)), it is vital to protect the network. As at so many organisations, BSC staff use email daily. “This form of communication is extremely important to us and we cannot tolerate viruses, worms or other malicious codes bringing our networks down,” says Whalley. In 2002, the BSC adopted an anti-virus solution that uses a number of leading scan engine technologies in one product. “It eliminates potential threats almost immediately,” says Whalley. “Even during the recent attack of up to 500 worms per day such as Mydoom, none of them managed to get through.”

### Test your back-ups

“The biggest risk most SMEs take is assuming their data is backed up and secure,” says Milan Vjestica, managing director of IT security company Cyber Protect ([www.cyberprotect.co.uk](http://www.cyberprotect.co.uk)). “On average, 50 per cent of back-ups don't work, making regular testing one of the most important procedures for any company.” Vjestica cites the sobering

example of one of his customers who had installed broadband but failed to install a firewall. “The company installed anti-virus software, albeit wrongly, which it assumed would defend the network against the majority of viruses. Back-up was a haphazard procedure, which was performed irregularly when the owners remembered to do it. Inevitably, a virus got into the network, creating massive loss of data.” The owners had assumed their data was backed up, yet it had not been performed for over three weeks and even then it hadn't been completed successfully.

“The company had to pay out massive overtime costs in an attempt to get back to normal,” recalls Vjestica, “but it still suffered further financial losses when a number of clients decided to terminate their contracts, as well as very tired and demotivated staff.”

### Develop a routine

The founder of aptly-named security specialist Datafort ([www.datafort.co.uk](http://www.datafort.co.uk)), Gavin Smith, says hardware and software don't have all the answers to watertight security. “Humans are fallible, we forget things, especially important things like initiating a back-up, changing tapes and taking back-ups home,” he says. “Make your back-up routine part of everyday IT housekeeping. Stick a sign on the monitor, tie knots in a hankie... just don't forget!”

### Use automatic updates for anti-virus protection

Sophisticated, email-aware viruses can spread within minutes. This makes it imperative that your software is updated often. An automatic process will remove the worry and conduct the updates without fail. Angus Dawe, joint managing director of Unique Distribution ([www.uniquedist.co.uk](http://www.uniquedist.co.uk)), is a fan. “It would have been an impossible task for us to update our anti-virus manually and [automatic updates] saved us a lot of money in IT administrators' salaries,” he says. “Partner confidence in us is crucial to our business, so it is reassuring to know we are protected against the more cunning of worms that avoid detection at the email gateway.”





If you'd like us to look more closely at the security systems on the market, send an email to [comment@iwks.com](mailto:comment@iwks.com)

## Be strict about passwords

Most businesses have password protection on their PCs, but IBM's ThinkVantage specialist Adrian Horne ([www.pc.ibm.com](http://www.pc.ibm.com)) advises firms not to be too cocky. Just because they use passwords doesn't mean they are safe. "Without a strict password policy, staff will default to using simple passwords such as spouses' names or other easily remembered words," he says. "Passwords should be a combination of numbers and letters, making up words that are not related to the user. These complex passwords should be changed regularly."

Many companies allow staff who have resigned to leave before their passwords have been disabled, while keeping new employees waiting for their access details. "The only way to solve both these potential security breaches is to make sure that the issuing and withdrawal of passwords is respected as one of the most important tasks in administering the computer infrastructure," says Thorne.

## Invest in an effective anti-spam service

Neil Watson, marketing manager at intY ([www.inty.net](http://www.inty.net)), which provides managed email and internet access, advises SMEs to run anti-spam software. "This will stop email servers from being swamped by unsolicited traffic, and employees from wasting time deleting it."

James White, IT manager at drug and alcohol treatment charity Addaction ([www.addaction.org.uk](http://www.addaction.org.uk)), says anti-spam software is working for his company. "About 85 per cent of spam emails are being stopped," he claims. "For a small organisation like ours, stopping more than 100 emails a day is still a great time-saver. It helps staff be more productive. Because both the anti-spam and the anti-virus systems work at internet level, and quarantine infected email away from our system, bandwidth and storage space are left unaffected."

## Use a virtual private network

Paul Thackeray, UK managing director at SonicWALL ([www.sonicwall.co.uk](http://www.sonicwall.co.uk)), a security seller to SMEs, believes that virtual

private networking – essentially a secure data connection over the internet that costs a fraction of the price for leased line services – aids secure communications between a company's sites, branch offices, home workers and main network.

One VPN convert is Neil Prevett, director of IT and communications at Dorset-based Lester Aldridge Solicitors ([www.lesteraldridge.co.uk](http://www.lesteraldridge.co.uk)). "VPN access has helped us introduce more flexible working practices for staff and save money through greater productivity and lower connection costs," he explains. "The fact that we have placed our public servers on the web is further testimony to our confidence in the improved security measures. We now enjoy the same high levels of security on the network extensions to our branch offices and to our business partners as we have at our head office."

## Adopt verified computer screens

Confidential data is often left open for all to see, even when every conceivable security measure has been put in place. This happens when employees leave their PCs to attend meetings or pop out to lunch without locking their computer screens.

But you don't need new technology for this, says IBM's Horne – you just need a policy to make sure that you and your staff use technology that is already available, such as locking the operating system or using a password-disabled screensaver. "Staff should be educated about the types of environments that are not secure," suggests Thorne. "For instance, in crowded public places confidential information on a notebook can be easily seen by reading over the user's shoulder. This advice is particularly important as wireless hotspots in public places become prevalent."

## Don't let staff download rogue software

This might not be a popular policy to implement. But Bryan Mills, chairman of IT support company ServiceTec ([www.servicetec.com](http://www.servicetec.com)), believes the security threat and cost of unlicensed software is underestimated. "Users often introduce this rogue software by downloading material from the internet. It can slow down their PC, corrupt the network and may be illegal. Although the

## THE PRICE OF SECURITY

Piece of mind could cost less than you think

■ **Risk audit:** Free

■ **Checking the validity of emails and keeping up to date with virus news:** Free (see [www.vmyths.com](http://www.vmyths.com) and [www.cert.org](http://www.cert.org))

■ **Firewall software:** From £1 per user, per month

■ **Anti-virus software:** £3-£4 per user, per month, depending on the level of protection

■ **Anti-virus updates:** Free

■ **Data back-up.** *Floppy disks in-house:* Negligible. *Outsourced solutions:* From £10 per month (to store up to 1Gb of information). A free 30 day trial is available at [www.datafort.co.uk](http://www.datafort.co.uk)

■ **Co-location space:** £100 set-up plus about £20 per month for minimum requirements (typically, 1u rackspace for one server and 5Gb/month data transfer allowance). The monthly costs can increase to over £500 depending on your needs

problem can be reduced by preventing staff downloading their own applications and removing all the local CD drives, in practice this is difficult to police."

Mills advises businesses to create a standard desktop image, showing the same agreed suite of software on each PC. This should be locked so users can't add other applications without authorisation.

## Don't forget physical security

A physical security breach last year prompted PR firm ITPR ([www.itpr.co.uk](http://www.itpr.co.uk)) to rethink its security. "We were burgled at a cost of £20,000 – not insignificant for a 20 staff, £1.4 million turnover business," says the firm's managing director, Ashley Carr. "Insurance covered most of the theft, but it took nearly five days to restore normal business operations, during which we lacked the ability to respond quickly to our clients." Gill Hunt, managing director of virtual meeting place Skillfair ([www.skillfair.co.uk](http://www.skillfair.co.uk)), advises companies not to overlook more obvious security measures. "Check locks, alarms and access to equipment. That includes not letting children into your home office – they can easily load unchecked software and games on to your computer!"

## Publish an internet monitoring policy

It's a good idea to monitor internet usage. But you must make your employees aware of what you're doing or risk breaching their privacy, as pointed out by Ed Macnair, EMEA security product manager at systems and security seller NetIQ ([www.netiq.com](http://www.netiq.com)). "Involve employees in developing and publishing a legally-compliant policy defining appropriate internet use and circulate it at regular intervals," he advises. "Every employee must confirm in writing that they understand this policy." ■



**"The fact that we have placed our public servers on the web is testimony to our confidence"**

NEIL PREVETT LESTER ALDRIDGE SOLICITORS