



20 TIPS FOR WATERTIGHT SECURITY

BY NICOLA SMITH

If your system goes down for more than 10 days, your business has a 93 per cent chance of going bankrupt within a year*. After reading that, you might want to put system security at the top of your to-do list. We asked the UK's leading IT experts for advice

Assess how secure
your business is



"A good starting point for any SME is to conduct an 'automated' vulnerability assessment of their IT environment," says Colin Bradley, senior consultant for Dimension Data (www.didata.com). "Such an audit provides you with a relatively low-cost view of your company's security posture and key requirements." Risk audits are often free, such as the online resource found at www.surfcontrol.com/go/erauk.

*US National Archives & Records Administration



SECURITY TIPS

Install a firewall

Jeremy Penston, security manager at PIPEX Communications (www.gxn.net), goes one step further, and believes firewalls are the best place for SMEs to start. "[Firewalls protect] against hackers getting into a network and corrupting or deleting the systems' contents or, even worse, using the network to turn on others," he says.

David Hayward agrees. He is the managing director of MMI Automotive (www.mmi-automotive.com), which specialises in computer systems for the manufacturing industry. "With the threats that lurk on the internet, we realised that if we didn't take security seriously and install proper security measures, not only could we lose important, confidential data but also our reputation could be at stake," he says. "We don't have a huge IT budget but the firewall we have is a cost-effective solution that stops hackers from attacking our networks; exactly what we need."

Make sure your supplier knows their stuff

"Ignorance of the law is no defence," warns Neale Stidolph, sales director at IT support company ATM Technology Management (www.atm.ltd.uk). "If you are going to use some form of outsourcing for your IT security needs, ensure you pick a company that has solid demonstrable and broad-ranging credentials in the field of information security. Being able to sell and install a firewall is not good enough."

Stidolph recommends you demand knowledge of the ruling bodies and legislation, such as the Data Protection Act, and the obligations these place on your company. "This is one thing that cannot be outsourced, so it is critical that the third party understands this and can help the company put in place management and control structures to satisfy this need."

Be specific about your email addresses

If you use your own domain name, make sure your hosting company does not use 'catch-all forwarding' (such as email sent to anything@yourdomain.com), advises Steve

Masters, communications manager of MK Secure Solutions (www.mailkey.com). "By accepting email only to specific addresses you have set up, you will greatly reduce the amount of spam you receive." Masters applied this theory to his domains and saw a 70 per cent fall in spam.

Take data off-site

A service provider may be able to do this for you cheaply by providing co-location. Thomas Howard, founder of Qube Networks (www.qube-networks.co.uk), says co-location makes sense, enhancing business continuity "and creating wealth for the business through added functionality and performance enhancements" while also providing greater stability. "It is surprising the amount of SMEs I come across that aren't aware of the less costly alternatives available to them," Howard adds.

Stephen Mayhew, IT manager at nationwide property firm Donaldsons (www.donaldsons.co.uk), has seen the benefits. Donaldsons' customer base is ever expanding, generating mountains of computer data every day. Before the company took its data off-site, members of staff in its eight offices backed up the data on to tape, and had to change their back-up tapes every day so that the back-up could run over night. "This was an administrative hassle, heightened by the fact that we do not have IT support staff at every location," says Mayhew, "to say nothing of the fact that tape is known to degrade over time – it is not a reliable medium."

Educate employees

Nick Ray, chief executive of security specialist Prevx (www.prevx.com), recommends giving staff some basic education about the risks of cyber attacks and how they can be reduced – "for example, not opening email attachments from unknown sources," he says.

MK Secure Solutions's Masters takes this issue seriously. "Never assume an email is from the person it appears to be from," he says. "Identity theft is becoming more common, especially among virus writers, who make viruses appear to come



CHECKLIST

THE FOUR MINIMUM REQUIREMENTS FOR A SECURE BUSINESS

- A firewall.** This is an electronic barrier that sits on a network server and protects the PCs hidden behind. It serves as a defence against external threats by screening all incoming information. It is essential for protecting your business against hackers and destructive computer programmes.
- Anti-virus software.** Viruses can enter a PC or a network from disks or via the internet and email. There are a number of vendors offering anti-virus solutions, which should be used to automatically check every file and disk that comes into your business.
- Updates.** It is no good having the latest software if you don't keep it up to date with the manufacturer's freely available patches. Visit the manufacturer's website and apply patches as soon as they are available.
- Data back-up.** Whether you do it in-house or outsource this responsibility, make sure your critical data is backed up on a daily or weekly basis.

from people you know. The biggest cause of virus proliferation is careless people, not poor IT security."

Encrypt your company's email

There are several encryption solutions available, such as products that use a secure server appliance situated within the sender's firewall. Emails are composed as normal and simply tagged to be sent by recorded delivery. Recipients then receive a notification email telling them they have new mail ready for collection and inviting the entry of a previously agreed password.

Often cheaper than other solutions, such products can be used without the need to install and maintain new software at either the sender or recipient's end. "Any business that values security should look at their email," says Gordon Olson, chairman of security and management firm Meticulus Solutions (www.meticulus.com).

Don't overlook any single area of security

Atchison Frazer, VP, marketing at security vendor ServGate (www.servgate.com), believes SMEs with budget constraints and without full-time IT staff can avoid overlooking a critical part by using an all-in-one security appliance. He advises companies to consider a product that provides: virus, spam and URL filtering; a firewall; and VPN (virtual private network), web caching and intrusion detection – all in a single unit. "This enables companies to significantly reduce the time, cost and difficulty of managing their IT security," he says. "And with increasing sophistication of



"Pick a company that has solid credentials in the field of IT security. Being able to sell and install a firewall isn't good enough"

NEALE STIDOLPH ATM TECHNOLOGY MANAGEMENT