ADAM BERNSTEIN

Don't bury your head in the cyber sand

● Hacking, online security breaches, phishing, cloning, theft by staff – call it what you will, computer security is a real problem that's becoming not only more acute, but something that affects all businesses.

ADAM BERNSTEIN is a writer with years of experience running a small business

OXFORD-BASED POPHAM Hairdressing found itself in a nasty position. A small two-salon firm, it suffered at the hands of a cyber attacker who infected and locked down the firm's eight computers and demanded a payment of £5,000 per computer. Popham didn't/couldn't pay and the attacker made good on his or her threat. Some data was recovered, but not before much disruption and cost, which the firm estimates as in the region of £8,000.

At the other end of the spectrum, 2011 saw Sony's PlayStation network hacked, compromising the personal details of up to 70,000,000 customers and resulting in the network shutting down for several weeks. The costs to Sony were around US$171m.

> **One way to limit the risk of breach is to simply not collect and store information beyond what is absolutely necessary, because whatever you do collect has to be protected.**

The veterinary world also isn't immune. In June 2012, Elm Veterinary Group manager Della Barbour was sent to prison for two years eight months for stealing £290,000 and covering up the theft by altering the firm's Sage computer software system.

In the US, the East End Veterinary Emergency and Specialty Center website was hacked by someone who claimed to be with the Islamic Electronic Army. The hacker posted text urging readers to convert to Islam.

Statistically speaking

And the problems are only set to increase. The Government's 2013 Information Security Breaches Survey showed 87 per cent (up 11 per cent on the year) of small firms experienced a breach of some kind while 93 per cent of large firms had been targeted. In some cases, the damage caused by the intrusion cost more than £1m, but for small firms the average cost ranged from £35,000 to £65,000.

Interestingly, 36 per cent of the worst security breaches were caused by inadvertent human error while 57 per cent of small businesses suffered staff-related security breaches. Yet despite the risk, a Home Office report, *Crime against businesses: Detailed findings from the 2012 Commercial Victimisation Survey*, says the average amount spent on IT security per year by businesses was only £200.

Protect your practice

When it comes to protecting a business, the first thing to realise is users can never be totally safe. The best they can do is minimise the risk of attack; users should never be so naïve as to think they are invulnerable.

The next step is to understand exactly what is at risk – that is your data and IT equipment. Just think of what you hold and use – employee and client information, payroll data, banking credentials, pricing and performance information and so on. In terms of equipment, think of the computers, web-connected printers, your telephony systems and broadband and data backup systems.

It's important to realise the threats are not just external (as in career criminals), they can be competitors or former and current employees. And remember a cyber-attack doesn't necessarily mean attack by a gang armed with banks of computers; it can boil down to an employee who abuses a computer system for his or her own benefit. By way of example, a small family run publishing house in Sussex suffered a £210,000 loss perpetrated by its bookkeeper with access to the accounts system. But other forms of attack include the blatant theft of equipment – laptops, smartphones and memory sticks, remotely conducted attacks on your systems, and attacks on systems belonging to other firms linked to you – including cloud storage.

Plan for an attack

Before any steps can be taken to reduce the risks, you need to assess the state of your practice in terms of your present security measures.

You need to detail your records, where they're stored and how they're protected, what equipment you use and which companies provide critical services to the firm. Are there alternatives in case of disaster?

How well are members of staff briefed on security? Are they lax when choosing passwords? Are they aware of how important it is to not discuss sensitive information with third parties? Do you change passwords when members of staff leave?

Are you really as IT literate as you think you are? No matter how good your knowledge might be, there will be someone out there who knows more than you. For this reason, it's important to have the backup of a good IT support company you can trust to implement good IT security for your systems.

Putting a new regime in place

Controlling access to your network is the first line of defence. This means turning on the firewalls on your computers and the network devices you employ. At the same time, take care of your wireless networks by enabling the strongest encryption the network allows, engaging MAC (media access control) address filtering and turning off the SSID (service set identifier) broadcasting. In simple terms, the encryption is akin to a lock on your front door; the MAC address can be likened to an approved guest list, and the SSID is the name the device broadcasts to other network devices to identify it.

Next you need good anti-virus software on all computers. As one unnamed Oxfordshire NHS surgery found, once a virus is loaded on to one networked computer, it can quickly propagate around the whole network, causing pandemonium. Computers should also be locked down to allow acceptable sites and no more and, at the same time, ensure all computers are regularly updated to take account of issued software patches.

Another part of the solution is to also educate employees (via policies) as to what they can and cannot do with a computer and the best practices of data security (and passwords). Also consider anyone who works off site and the devices he or she utilises. The National Cyber Security Alliance in the US (www.staysafeonline.org) has materials and information on employee education that may help. The advice on email is to be careful on what is opened and the links that may be offered. The best phishing scams replicate legitimate organisations and seek information that can be used to log in to accounts without the need to hack.

Also, don't let web browsers store passwords – enter them each time manually – and also look for "https" in the web address of any financial organisation you are logging into to demonstrate site safety.

Secure the equipment. This means logging all the equipment the practice possesses, the software (and licences) utilised and, most importantly, the passwords for individuals and administrators. All passwords need to be changed regularly and whenever, for example, someone leaves. Also restrict the use of recordable media such as CD/DVD disks, USB memory sticks and external hard drives. This not only makes it that much harder for anyone to take data off the premises, but also reduces the risk of data being lost.

IMAGE: SXC/Andrej Troha.

Monitor everything. There's precious little point in setting up control systems for your IT if you don't monitor what's going on. So collect activity logs and make sure you have the ability to find unauthorised usage. At the most basic of levels, broadband routers can easily be set to automatically report, via email, any third party attempts at intrusion. By extension, manage user rights for systems and control access to sensitive equipment and data. You need to ensure computers don't have administrator rights that will allow users (or hackers) to easily change system settings or load unauthorised software.

Many people don't fully appreciate that any third parties they engage can introduce risk. If, for example, you plan to store information off site and online (the cloud) you need to ensure the third party is reputable and reliable. Allied to this, if online systems allow employees access to sensitive information, two-factor (think two signature) authentication should be sought.

Only collect and store data you need. The Data Protection Act 1998 already makes this quite clear, but in simple terms, one way to limit the risk of breach is to simply not collect and store information beyond what is absolutely necessary, because whatever you do collect has to be protected.

Lastly, and most importantly, create a disaster recovery plan and test it. Don't wait until it's too late.

What can go wrong?

Clearly, the risk of burying your head in the sand is grave. While some firms may be lucky enough to never be the victim of an attack, the consequences of being selected cannot be ignored. Apart from the financial loss and the chaos following an intrusion, the public vilification and loss in client confidence that firms face following an attack must surely be a call to action. In July 2013, kitchenware firm Lakeland was forced to publicly admit its passwords system has been hacked and that customer accounts could be at risk. Don't put yourself in the same situation.