Data protection at the source: how to look after your practice

WHETHER A VETERINARY PRACTICE MANAGES ITS IT AND DATA and information security – and back-ups – in-house, or has outsourced it all to the cloud, a basic truth is this: ironically, improvements in anti-virus software – provided the software is regularly updated – mean that 99% of the time, staff are not exposed to viruses and as a result are taken by surprise when receiving a malicious attachment.

Viruses and associated ransomware are as insidious and tenacious as ever, though, and there is no lack of attempts by their perpetrators to send them, but good gatekeeping can keep the majority at bay.

And then there are Distributed Denial of Service (DDoS) attacks, which can cause mayhem to websites and computer networks. More about those later.

Gatekeeping is not only about technology. It also involves human behaviour which, if undisciplined, can result in a potentially dangerous virus infection or, in the case of ransomware, the complete shutdown of a computer unless a ransom is paid.

To explain that differently, staff shouldn’t get too comfortable with their online activities and thereby take security for granted. In order to protect themselves to a greater extent, practices need to remain vigilant and train their people not to open unknown e-mails or visit suspicious – “phishing” – websites.

The latter can have as serious a consequence as opening a malicious attachment because the sites can download malware and other threats, or take you to a web page that, for example, looks like your bank’s home page but isn’t. By logging in to what you believe to be your account, through giving your log-in details, you are at risk of 1D theft as well as financial loss. The same applies to fake PayPal and similar websites.

Individuals working for a practice can be tricked by a phishing website, thereby putting themselves or the practice at risk.

Making regular data back-ups is essential

Let’s not forget the vital role that data back-ups play in good gatekeeping. Back-ups are not only useful in the event of a hard disk crash or theft of computers, or damage caused by fire or flood.

In all those cases they can enable rapid business continuity through data/information restoration. They also come in handy where ransomware demands are made, by enabling the demand to be ignored because the most recent back-up can be put on to another computer.

Back-ups are most effective when a disciplined regime of making them is followed. Real-time back-ups are ideal, but not always practical, especially in a small organisation. Making frequent back-ups, however, is viable but does depend on a level of discipline or selecting automated, scheduled, back-ups.

Bear in mind that any back-ups made locally, i.e. not online but in the office, whether on NAS (Network Attached Storage) devices or even USB drives, do need to be stored safely off-site until being used again. Many smaller organisations don’t do that, adding to the risks they face from data breaches or loss.

Practices can also suffer loss of data through theft of office-based data back-ups, computers, tablets or smartphones. Insecure coding on a practice’s website or software applications can result in websites being hacked into and customer information stolen.

Therefore, practice owners should ensure that website and any software developers they use meet minimum but acceptable standards at least.

They should also be aware of the risk posed to data from the practice of using locum vets and freelance staff, whose own computing and smart phone devices might be exposed to information and data loss for a variety of reasons including theft.

Another threat is bad practice, ranging from allowing friends or associates to use the devices to relying on inadequate or out-of-date anti-virus and anti-malware tools, visiting

continued overleaf
phishing websites and using wi-fi hotspots. Even “secure” hotspots pose security threats.

Safeguarding sensitive data is high on the agenda of any business – or should be! – but we’re all only human and mistakes are made through familiarly breeding errors if not contempt.

**Hosted desktops**

To reduce all risks posed by cybercrime, human error, bad practice, out-of-date anti-virus and spyware software, and theft (or fire), the practice owner has an alternative to the DIY approach, useful though that can be, especially for the smaller practice: the hosted desktops element of cloud computing. Where hosted desktops are deployed, all data and information processing is carried out in a secure data centre rather than an in-house server or individual desktop, laptop or tablet. Back-ups are therefore also made in the data centre, by the hosted desktops provider.

If the provider is ISO 27001 certified, practices can be sure that every action taken in the centre complies with the international gold standard in information security management.

ISO 27001 accreditation means that back-up regimes are strictly adhered to, allowing business continuity to be optimised should it ever be required. Secure storage of back-ups is no problem.

A second secure data centre ensures that in the unlikely event of the primary centre being affected by a “disaster”, the service offered by the hosted desktops provider continues.

Hosted desktops – or Desktop as a Service (DaaS) – can also relieve a practice of all concerns about purchase and support of IT. And crucially, with cloud computing being device-independent, hosted desktops cannot pose a security threat. That is, staff can work on their own devices without compromising the practice’s security policies because they are only using the devices as hardware to access their work.

**DDoS attacks**

Recent research by security company Imperva concluded that the UK is now the second most targeted country after the US when it comes to DDoS attacks, which are designed to bring websites down and make computer networks unworkable. The number of attacks was up 200% in the past year, according to the firm, with some being directed by former workers disgruntled at their employers.

They paid as little as a few pounds sterling to buy an attack by a DDoS provider, highlighting the dangers that can come from within.

The smaller a practice, the less likely it is to have the resources to combat, or at least be prepared for, a DDoS attack. However, if its computer network has been outsourced to the cloud, the cloud services provider should have the capability to stop an attack or make it as brief and ineffectual as possible.

**High-level security**

Hosted desktops enable practices of 10 or more staff to benefit from high-level cyber security tools previously only affordable by large organisations. The tools include robust firewalls, enterprise quality anti-virus tools and web filtering, optional encryption of sent e-mails and management of all the access devices. They are affordable because the costs are shared with other customers of the hosted desktop provider. Also shared is the cost of high-end, enterprise-grade software applications.

Other tools in the provider’s arsenal control and enforce acceptable use policies, block access to inappropriate websites and any other sites a practice owner or manager wants to exclude from accessing, and generally reduce misuse of the internet by any individual working for a practice – the owner and any partners included.

Dual-factor authentication, or 2FA, is an option offered by some providers. It helps prevent unauthorised access to information and data by enforcing the identification of individuals through a combination of user name, password and information known only to them.

2FA that uses SMS has now been declared insecure by the National Institute of Standards and Technology (NIST), ensuring there will be an impact at some point for users of the 2FA that is utilised by Gmail, Apple, etc.

**Summary**

Veterinary practices can go it alone with cyber security, data back-ups and business continuity. Risks posed by using locums and freelance staff can be countered in part through a combination of good practice and basic tools a practice can use itself; if its IT hasn’t been outsourced.

Good gatekeeping will reduce cybercrime risks for the practice that wants to go it alone, but the upsides won’t be able to compare to what the cloud-based hosted desktops alternative provides, including deploying its arsenal of tools to combat DDoS attacks and hacking.

To learn more, see workplacelive.com.

---

**Arranging a residential mortgage – a guide for vets**

REGULATION IN THE FINANCE WORLD is ever-increasing and this can make obtaining a mortgage a challenging, stressful and time-consuming process.

With the uncertainty following Brexit looming, there is the added question of just how long the UK’s interest rates will remain low. With these factors in mind, it’s always advisable to seek professional, bespoke and qualified advice before hopping onto or even up the property ladder.

The key to getting a competitive deal on a mortgage – and that means the cheapest – is being armed with as much information as possible. Here are some key points that might help you along the way...

I’ve recently qualified and am working in my first year after training – do I need to provide a mortgage lender with a minimum of two years’ accounts? Generally speaking this is true if you are self-employed. However, as a qualified vet it is possible to arrange a mortgage in advance of actually starting to work, as long as you can provide suitable supporting confirmations. With as little as a 10% deposit, lending can be based on your new proposed salary or self-employed income, at very competitive rates.

What happens if there’s a variation between my accounts and HMRC SA302s? Regular mortgage underwriting will likely take issue if your accounts and SA302s do not match. This may be due to taking advantage of tax breaks set by the Chancellor – for example 100% deductions for capital allowances. However, lending can be agreed on the pre-destruction figures with suitable explanations.

I’m trading as a limited company – will this affect my level of borrowing? The majority of lenders will lend against an average of your latest two years’ salary and dividends. However, in some cases it may be more beneficial to lend against your latest year’s if this is higher.

Alternatively, if your salary and dividends do not present very favourably, you may still be able to achieve increased borrowing by lending against your most recent year’s “Share of Net Profit”, after corporation tax and adding in your salary.

How many times my income can I borrow? You may well have heard that 4x is the general multiplier the majority of lenders go by. In actual fact, nowadays the majority of lenders will use affordability calculations to work out levels of borrowing. These take into account a detailed breakdown of your cost of living and existing commitments.

So, depending on your status and credit score, a lender’s affordability calculations could equate to between 4 to 5.5x income, although your individual circumstances could mean it’s actually less.

Will I get a mortgage if I’m joining a practice as a partner but haven’t started yet? Of course. Mortgage lending can be

---

**Julie-Ann Hawkins** is a CeMap-qualified mortgage adviser and director at FTA Mortgages Ltd, who specialises in advising on and arranging bespoke mortgages for healthcare professionals. See http://www.ftaninance.co.uk/mortgages/ for more information.