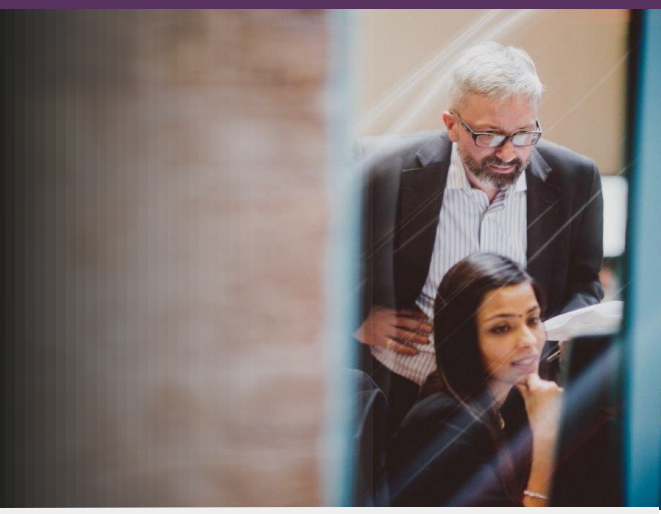
RIAA Barker Gillette

*Always Available*

# How vulnerable is your business to hackers?



October 2017

**Do you know what a DDOS attack is? Are you more vulnerable than the Greeks to Trojan attacks, or do you have enough Bitcoins stuck down the back of your virtual sofa to pay off a hijacker? Hackers are getting smarter, more ruthless, and more determined every day. And they're not just focusing their efforts on the big corporations any more.**

A recent poll carried out by Barclaycard, found that out of 500 SMEs asked, 44% were worried about the effects of a cybercrime attack or data breach, compared to 34% who were more worried about Brexit as a major impact on their future. It seems that the back-door hackers have more of a hold over our concerns than the Brussels bureaucrats. The result is that last year, UK SMEs spent £2.9 billion on cyber security. That's an average of £1,600 per business, with 34% of small businesses concerned about managing and preventing threats and breaches. While consumers may be more cyber-savvy, it seems that businesses still have some catching up to do.

The average cyber-attack will cost an SME around £3,000, and the FSB found that, on average, small businesses in the UK are the victims of around four attacks every two years.

## GDPR – cyber security is your responsibility

As well as damaging your business (and your reputation), a cyber-attack could leave you open to accusations of failing to protect personal data, especially if you hold client or customer information digitally (such as credit card details). With the new General Data Protection Regulations (GDPR) now coming into force, you have a duty of care to protect your clients' personal information. If your firewalls and anti-virus software allow an attack to get through and as a result directly impact your clients and customers (such as their personal details being stolen), then you could end up in court. That data includes not just financial details, but names, addresses, telephone numbers, in fact, anything that could identify your customers.

From 25 May 2018, it's up to you to take care of your customers' data. You will also be required to report any attack to the relevant supervisory authority within 72 hours of becoming aware of a breach, and prove that you have taken all reasonable precautions to stop an attack.

## How to beat the hackers

Ideally have professional IT advice, but having a robust firewall and up-to-date anti-virus software is a good start, making it more difficult for hackers to get into your system. To keep your business and your information secure you should:

- **Update your system**: the most recent attacks have been against the now-aged Windows XP operating system. While it's a good, solid operating system, it's vulnerable to attacks and is now no longer supported by Windows. Thus, XP is not being 'patched' (including security updates). 'Byte' the bullet and upgrade.
- **Build a better firewall**: firewalls and anti-virus software should provide you with a good line of defence. Make sure you choose one that is designed to cover networks, rather than just single outlets. Buying a home firewall and then asking it to protect your multi-user office system is asking for trouble.
- **Train your staff**: it is worth having a designated Cyber Security officer if you're a medium sized business and get them trained in the latest techniques for Threat Analysis, mobile and static security, and even Ethical Hacking. But it's also well worth training all your staff on how to recognise phishing emails, the dangers of

clicking on unrecognised email attachments, and online security protocol.

- **Back up regularly**: that means every week, not every year. If you have a recent back-up point then you're less likely to lose all that essential information, even if a hijacker locks you out.

### Can you hold your internet service provider/software provider responsible for a cyber-attack?

If you're thinking of bringing a juicy case against Microsoft for allowing a worm to wiggle its way through your firewall and into your computer, think again. You've signed a licence agreement with a software provider, which puts the onus back on you to ensure you allow regular updates and patches to be uploaded onto your operating system. Your internet service provider is also pretty much out of the loop as far as legal action goes, as attacks are usually so widespread that no provider is immune.

So, the best course of action is ensuring you do everything you can to protect yourself, your business, and your data.

**Veronica Hartley**
**020 7299 6922**
**veronica.hartley@riaabg.com**
**www.riaabarkergillette.com**