UNDER ATTACK

Small firms are increasingly finding themselves the targets of cyber-criminals, who see them as easy and unsuspecting targets. It's time to take the online threat more seriously, says ***Jo Faragher***

WE'VE ALL READ ABOUT security breaches at household names such as the one that hit TalkTalk last year, or the incident at extramarital affair site Ashley Madison, where a hacking group leaked users' details online and threatened to expose their identities to their unsuspecting spouses. But small companies are potentially more at risk of attack. According to the Government's information security breaches survey published in 2015, 74 per cent of small firms have already endured some form of data breach – and that proportion is only likely to increase.

Complacency is a significant problem. "Smaller companies can be at higher risk than others precisely because they think they won't be hit, and cyber-criminals know this," says Rob Daniels, Head of Portfolio and Commercial Strategy at BT Security. Furthermore, because they focus on growing their business or acquiring new clients, most

Hair today, gone tomorrow

A hairdressing chain in Glasgow received a shock last October when it was targeted by hackers. Ken Main, owner of Ellen Conlin Hair and Beauty, was forced to pay a €1,000 (about £780) ransom after he was locked out of the company database. The chain was a victim of 'ransomware' – a virus that prevents or limits access to the user's system and forces victims to pay a ransom to get access and/or data back.

Although clients' data was not compromised, Main faced losing business owing to the salon system breakdown. After paying up, the firm was given a code to unlock the data, but much of it had been corrupted and was unusable.

Illustration: John Devolle

small businesses will not have a dedicated IT Manager. Often the business owner is the one in charge of choosing, managing and updating technology systems.

The motives behind targeting large corporations seem obvious, but where does the attraction lie with smaller companies? There are two key areas of interest: data and access to other, potentially more lucrative, companies in your supply chain. “Lots of people say to me ‘my data’s not valuable’,” says Colin Tankard, Managing Director of cybersecurity firm and FSB member Digital Pathways. “But although you might not have anything sensitive in your system, a hack into your machine could lead the criminal to 10 of your contacts, and they could then attack 10 of each of their contacts, leading to a wide-scale phishing campaign.”

Tricks of the trade

One of the biggest threats to small businesses is social engineering, where hackers manipulate individuals to do something they normally wouldn’t, such as handing over a password or downloading a virus into the network. A common current scam uses an email that arrives in your inbox, asking for an invoice to be paid. The attachment contains malware which, once downloaded, can access information on the person’s computer.

Other tactics include creating pop-up notifications, seemingly from the office printer or requesting someone clicks on a link to update their anti-virus software, when in fact these links open dangerous holes in a company network or introduce malicious code.

“A good rule of thumb is: if anything appears to be both unexpected and urgent, then staff should be cautious,” says Jamie Randall, who runs consulting company The Friendly Nerd. “Get them to verify it through another source, for example, a phone number. Train staff to be data-focused.”

Open access

Small businesses can also be at risk because they are some of the biggest adopters of mobile and cloud technologies. Rather than spend thousands on IT infrastructure, they use browser-based applications such as Google Docs or Dropbox, and often access documents using mobile phones or tablets.

“This increases the potential ‘attack surface’ of small businesses,” says Mr Daniels. “Downloading a copy of something to a mobile device can make that information vulnerable.” Using public wi-fi networks, for example, in a coffee shop, also increases risk. If employees want to access company data or systems while on the move, they should use a dongle or virtual private network, experts advise.

However, the financial investment involved in bringing in security experts and updating systems puts many firms off. So ‘security as a service’ packages – where you can pay for a range of features such as password management, automatic back-up or device protection – are becoming more affordable and popular. “There’s a misconception among small businesses that if they pay for IT support or services then security is part of that package, but that’s not necessarily the case,” says Marlon Johnson, Managing Director of FSB member JMS Secure Data.

Get the basics right

The Government’s Cyber Essentials scheme, backed by FSB, is now mandatory to win central Government – and some other public sector – contracts. It focuses on five key areas of security control:

- **Malware protection** Preventing or minimising the risk of employees downloading viruses that could corrupt your systems
- **Access control** Encouraging employees to create strong passwords and vary them between systems
- **Firewalls** Investing in a robust firewall and making sure there are no leaks
- **Secure configuration** Ensuring that systems are configured in the most secure way for the needs of the organisation
- **Patch management** Big business software providers such as Microsoft and Oracle release regular patches and security updates – it’s crucial to keep these up to date

Most cybersecurity companies offer a free vulnerability check, so you can see where your systems are most at risk. “Resilience begins with a proper understanding of the assets of the business and the vulnerabilities it has,” says Mike Cherry, Policy Director at FSB. “It has to become a core activity of business, like getting customers and dealing with finance. Businesses should be planning ahead to ensure their resilience in the face of cyber-threats.”

In fact, protecting your business against such attacks is no longer just a ‘nice to have’. Many Government contracts now require some certification that your systems and networks are protected (see box, left), while breaches of data protection legislation can result in hefty fines. “It’s only a matter of time before public companies will need to make a security statement in their annual report,” says Kelvin Jones, Managing Director of Accelero Digital, a software development and cybersecurity training company.

Finally, don’t ignore the potential threat from inside. A survey in 2012 by Ping Identify suggested that 48 per cent of employees would sell their password for less than £5, and more than one-third had shared their corporate log-in with someone else. Fortunately, though, awareness is improving. “We’re seeing more stories about hacks in the newspapers, so they are becoming more aware,” says Mr Daniels.

JO FARAGHER is a freelance business journalist