Building a human FIREWALL

Cyber crime is on the up, with SMEs increasingly the target. Stuart Brown, founder of IT support company Cambridge Helpdesk, has some chilling stories to tell

LEGEND has it that a vampire can only enter a home if the inhabitant invites them in. Cyber-criminals generally rely on their victim making the same mistake. Crime has changed. Fraud has replaced burglary and car theft as the most common offence. In January, the annual national crime survey revealed 3.6 million fraud and two million computer misuse offences. These figures are widely believed to be the tip of the iceberg.

The crimes themselves have also evolved. Today's cyber-criminals aren't satisfied with outwitting systems to cause annoyance or embarrassment. They want money, and they know just how to extract it from SMEs. As businesses increasingly beef up their technical protection – from mail

continued on page 52

Stuart Brown

continued from page 51

filtering to anti-virus software – the hackers have turned their attention to the new weak link: staff. Employees have become their route to ransom.

Ransomware

2017 is being dubbed the 'Year of Ransomware', a form of malware enabling cyber-criminals to remotely lock down files on a computer or other connected device, such as a server. The afflicted business needs an encryption key to unlock the files, which the criminal offers for a fee.

The handover is the equivalent of a midnight meeting in a deserted area, except that it happens online, and the business pays with Bitcoins rather than a holdall of bundled notes.

These criminals are just as menacing as one would expect, employing scare tactics such as threatening to post its data online if a business refuses to pay. One particularly nasty variant, dubbed Popcorn Time, waives payments from its victims if they infect a few friends.

Attackers no longer need to be tech-savvy since ransomware is even available in kit form. For criminals, it has literally never been easier to get into business.

Ransomware has been built to evade common protection systems. It's the user who opens the door to it, usually by clicking on a link. The business's system thinks the user wants to encrypt files – a regular and valid occurrence for many – and allows it. The trouble is, it's the hacker who's encrypting the data, not the employee.

While the sum demanded can be relatively modest (often between £500 and £1,500 for a typical SME, but rising (and sometimes much more), there's no guarantee the attackers will release the data on payment, with one US security company finding that 20 per cent paid in vain. Even if the key works, criminals may attack again, forcing the owner to pay repeatedly. Often the biggest financial cost to a company is not in fact the ransom, but business down-time.

In our experience, even when a company has daily offline back-ups in place from which to salvage files, they face 48 hours of lost business, in addition to the costs of the IT work.

While back-ups are the crucial back-stop for SMEs, staff are the first line of defence. We advise businesses to educate employees, and to ensure anyone who suspects they've clicked where they shouldn't has the confidence to own up promptly. Time can make all the difference between a problem limited to a single computer and a total takedown of the business – just as one company we helped discovered when a staff member's Friday afternoon click let in ransomware that spent all weekend encrypting absolutely everything, undiscovered until Monday morning.

Spear phishing

Cyber-criminals have been sending emails purporting to be from someone else for several years, in an attempt to get users to reveal confidential information. Easy to spot in the early days, messages are becoming more sophisticated. It is not uncommon to see emails that appear genuine thanks to spoof email addresses and legitimate-looking logos and signatures.

A recent development is the more targeted 'spear phishing'. The criminal combines social engineering – the act of building a profile of a person based on publicly-available personal or professional details – with spoofing techniques.

A staff member, often someone relatively junior, receives an email that appears to be from a senior colleague. The detail can be spookily accurate, for example mentioning a conference that the alleged sender is attending and has publicly checked into on social media.

Often the email will require an innocuous first response, which provides the criminal with useful clues about company language and culture. Then comes the inevitable ask for a money transfer, or a request to open a file.

The criminals prey on junior staff or recent hires, both less likely to question the authority of the alleged sender, but even senior staff are not immune.

The Met Police's *Little Book Of Cyber Scams* includes the example of a small HR company that was hoodwinked out of £30,000 when the finance director received an email that appeared to be from the CEO, made a transfer and even confirmed the authenticity of the transaction to the bank. The funds could not be recovered.

The human firewall

Most people who fall for these schemes are not stupid – they're human, busy and lulled into a false sense of security. Staff and business owners alike need to recognise the new reality. Their IT team, whether in-house or outsourced, can do much to protect them. Email filtering alone blocks around 20,000 undesirable emails per quarter for a typical 10-person company. But it only takes one to get through, and ransomware, phishing and social engineering are designed to trick users into circumventing the technical protection IT staff put in place.

Several companies, like such as *knowbe4.com* or *layer8ltd.co.uk* will send a test phishing email to a business, to see how many employees will click on something they shouldn't. It's a good way to start to review business vulnerability to human factors, and a first step towards a more resilient workforce. The knocking vampire can't enter if the intended victim ignores it.

It’s never been easier to get into business.

So here are three key steps to keep the cyber criminals out

O **Offline back-ups.** Backing-up business data offline frequently provides a ‘get out of jail free’ card against ransomware. It’s crucial. Companies wanting to keep costs down should prioritise their files to back up the most vital.

U **Understanding.** There are lots of user-friendly materials to help businesses educate their staff about the risks, and the importance of swift action when they suspect a problem. Visit the website below for a list of resources, and for simple steps you can take.

T **Ten seconds.** Encourage staff to take a moment to think before they click a link, to question whether a sender is legitimate, and to check whether a message is real. The criminals rely on habitual, automatic, unthinking behaviour.

For more tips visit *cambridgehelpdesk.com*