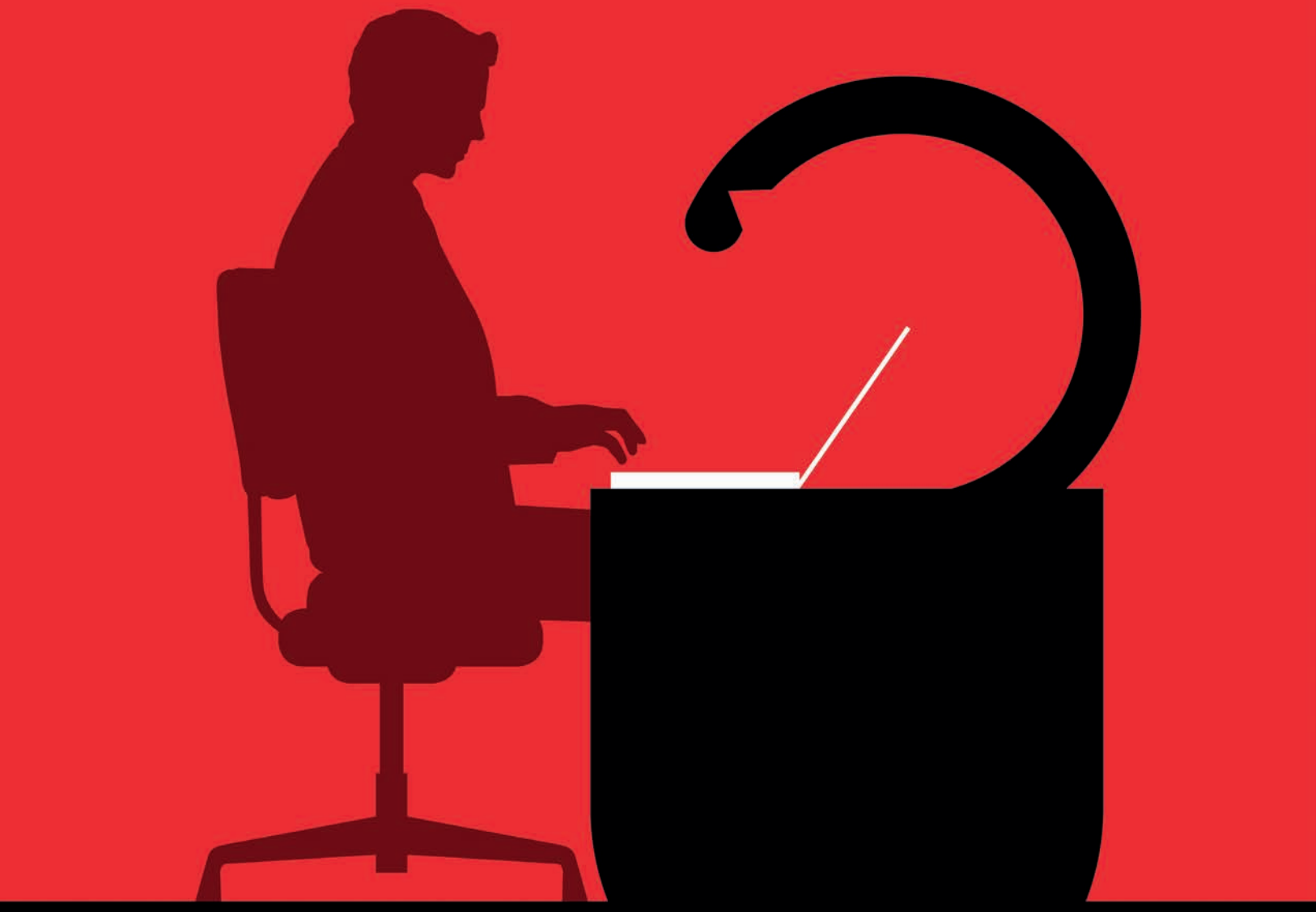

THIS IS **NOT** A DRILL

Cybercrimes may once have been on the periphery of corporates' risk management frameworks. Now they are viewed more as a racing certainty. Christian Doherty takes a look at mounting evidence that cybersecurity needs to be central to treasurers' thinking

One of the difficulties around trying to home in on cybercrime and the techniques used to con companies, banks and individuals out of money is the fact that whatever is eventually uncovered will instantly be out of date.

Just as the furore over the Ashley Madison hack that saw the personal details of 32 million users of the Canadian dating site leaked into the public domain in a blackmail scam had died down, came growing evidence that the cybercrime threat is growing and becoming something of a constant.

In October this year, the UK's National Crime Agency announced it was investigating the theft of more than £20m from bank accounts by hackers using malware known as Dridex. That came on a day when even a cursory glance at any newspaper website brought more evidence of cause for concern: Russian hackers design USB stick that can 'fry contents of any laptop'; well-known YouTubers, including W2S and NepentheZ, targeted by criminals who gained access to their EA accounts to steal thousands of pounds worth of in-game currency; TalkTalk's huge loss of customer data last month only adds to the growing list of successful cyberattacks. The list goes on.

The growing tide of cybercrime

These are not isolated incidents. Some of the most salient points from recent UK government cybersecurity research, carried out by audit firm PwC, show how widespread cybercrime now is. In the past year, 90% of large businesses and 74% of smaller firms have experienced some kind of breach.

The survey also revealed that there were up to 5.1 million incidents of online fraud involving 3.8 million victims in the 12 months to September 2015. Just over half involved some initial financial loss to the victims and more than 62% were compensated in full.

IMAGE SOURCE

Amid this growing tide of cybercrime, the need to protect assets is especially pressing for treasurers, given that they are on the front line of operations at the nexus of banking and payments. But the changing nature of cybercrime is muddying the waters of just who in the business is responsible for designing the right anti-fraud framework.

"The treasurer has to be worried about the security of the company's assets – whether cash or similar – and their vulnerability to external threat," says Peter Matza, engagement director at the ACT.

"But the treasurer must be realistic and recognise that, while he can influence some aspects of corporate life, he may not be able to influence them all. For example, 'what are my payment processes' needs care; 'what does the company sell on its website' can't be a treasury responsibility," he says.

The mounting sophistication of hackers' systems

Given the increased dependence of many companies on technology, it isn't surprising that the efforts of cybercriminals have become increasingly sophisticated. Certainly, the world has moved on from hackers simply targeting bank accounts or credit card details. Some of the recent, high-profile cases have illustrated the changing nature of cyberattacks.

Theft of cash via hacked bank accounts is giving way to a bigger, longer game. Chris van Dijl has worked as a corporate treasurer and now runs consultant company Cugavadi, which helps businesses improve their security measures. He has seen the shift from theft to extortion attempts.

"We've seen examples of where you had cybercriminals saying to their victims: 'We've broken your security. We've got something of value to you'," he explains. "And 'We'll put a service attack on so you can't operate as a business on the website that's really important to you'. Once they've done that, they will start to try and have a discussion with you that involves ransom and extortion." This happened in the Ashley Madison case, where no funds were stolen, simply user data, which was then used as a weapon for extorting cash from the site's owners.

Van Dijl spends a lot of his time working with clients on assessing the threats they face and designing frameworks to combat them. This usually focuses on good housekeeping rules: "We try to look at things like the use of authorised counterparties, for instance, so that each counterparty will have to comply with set parameters as per a counterparty risk policy document," he says. "The use of a different counterparty could actually be a breach of a covenant in loan documentation."

Beyond that, Van Dijl's best practice wish list for clients to protect treasury from cybercriminals includes: implementing approved strategies for managing payments; error prevention through constant updating and improvement; robust treasury audit; and the segregation of duties – under which dealing, recording, confirmation and settlement are all split to prevent internal fraud and potential compromise from external sources.

Treasurers should not forget that theft of data can now be as damaging as theft of cash. Credit card details are obviously extremely valuable, but any customer data falling into the wrong hands can cause huge reputational damage; would you do business with a company that failed to protect your details?

Beyond the enormous potential for blackmail and extortion, the possible repercussions from regulators are also considerable – the European Commission rules on data breaches will change next year. Currently, businesses are liable for a fine of up to £500,000 for

Amid this growing tide of cybercrime, the need to protect assets is especially pressing for treasurers, given that they are on the front line of operations at the nexus of banking and payments

5 SIMPLE STEPS TOWARDS TIGHTENING UP YOUR DEFENCES

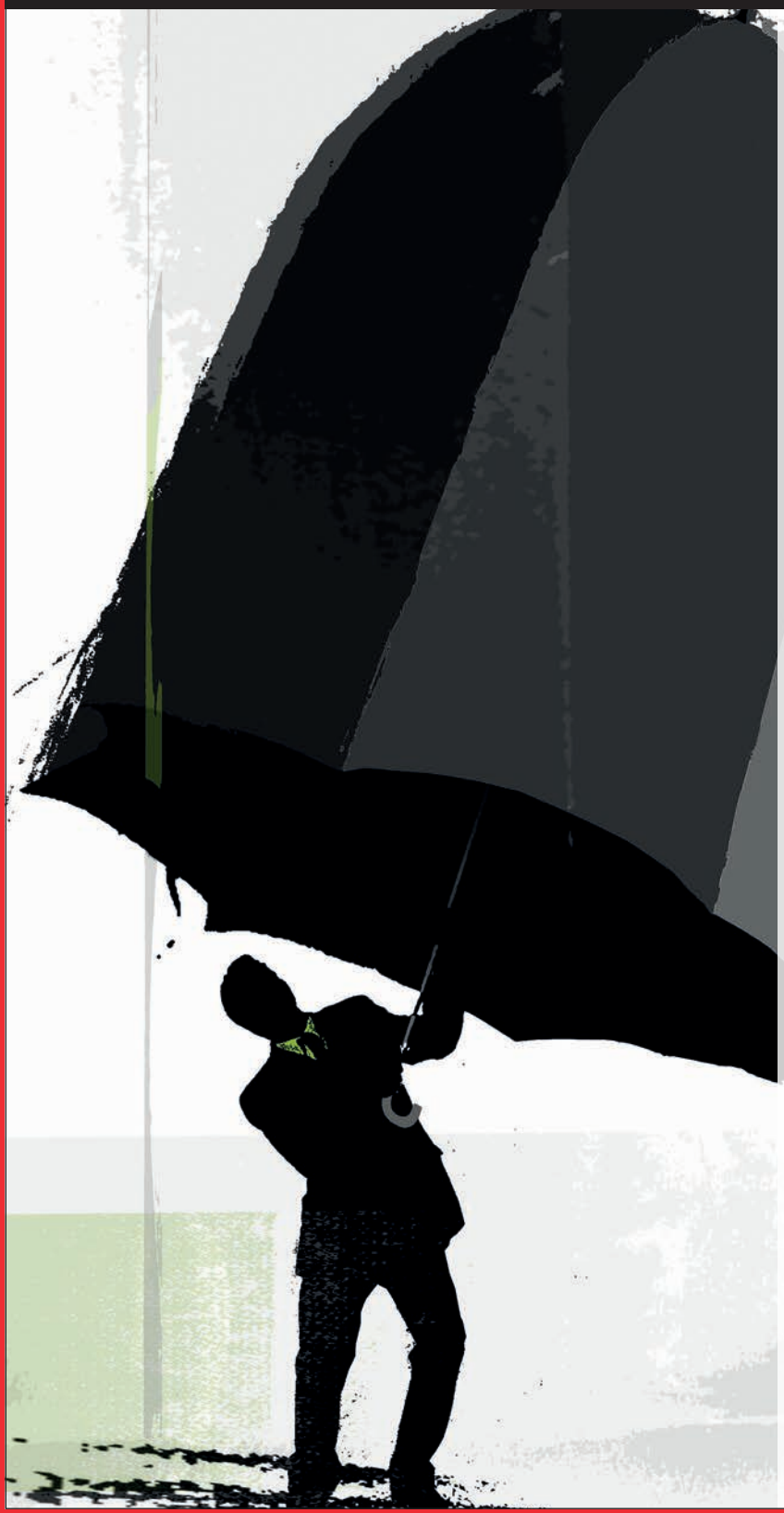

IMAGE SOURCE

1 Use secure memory sticks

The USB has become a ubiquitous part of office life and is a convenient way of transporting data. They are also exceptionally good at carrying malware and viruses designed to disable systems and generally wreak havoc. To counter this, a new generation of protected USBs is becoming available. USB sticks with built-in keypads can help to block unauthorised use.

2 Consider using a VPN

Virtual private networks (VPNs) can offer a vital tool in protecting businesses that need to communicate between different hubs over the open internet. By using a VPN, the business can create what amounts to a safe channel between two points (say, head office and a branch in the network), protecting data that passes through it, safe from any prying eyes (or malicious ones). The fact that a VPN is relatively easy to install adds to its attraction.

3 Always use double-factor authentication

Double or two-step authentification is a common-sense, no-frills effective way of ensuring unauthorised individuals don't gain access to devices or systems containing sensitive information. It requires authorised managers to use two different methods of identification to access sensitive applications – a password and digital signature, for example. There is a growing range of authentification tools in the market – Apple, for instance, is pushing its biometrics solution Touch ID, which uses thumbprint technology to block unauthorised access to mobiles and tablets.

4 Consider testing your defences

Engaging the services of a security consultant to test the strength of your cyber defences can be a useful way of exposing vulnerabilities quickly and quietly. The growth of 'ethical hacking' services in recent years has mirrored the rise in cybercrime. This is a valuable exercise – several large banks have submitted themselves to so-called cyber war game exercises recently, and the Bank of England has made no secret of its exercises and efforts in this area.

5 Look into government schemes

The HMG Cyber Essentials Scheme sponsored by the UK government sets out to help smaller businesses understand the threats they face and the steps they can take to protect themselves. Described as basic cyber hygiene, the scheme has developed into an assurance framework for businesses in need of greater protection. See: www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf

a data breach. However, under the new rules, that could change to anything from 2% to 4% of global revenue.

Alongside data breaches sits the rise in so-called spear phishing. A recent incidence of this was particularly worrying, given the simplicity of the attack: US firm Ubiquiti Networks reported that it had been the victim of a scam that saw $46m pilfered from its bank accounts by cyber thieves. The attack was devastatingly simple: fraudsters managed to get the company to wire transfer funds based on a forged email that looked like it came from a senior executive.

This type of scam is different to the volume-driven phishing attacks of the past, where the criminals play the odds. Sending 100,000 emails may turn up a catch; spear phishing, as the name suggests, is based on a patient, targeted and specific approach. Criminals stalk their prey by researching the company, gathering as much information as possible. They find the names of executives, they look into supplier relationships and follow staff on social media.

How to protect your organisation against a cyberattack

The intention is to build a picture of the company in order to design a plausible fraud: thieves may send a mail purportedly from the sales director to the FD asking for authorisation on a payment to a supplier, or a request to click on a link that will lead to a virus or other malware. A less-than-vigilant response – say, a single verification of payment, or lack of awareness of clicking on unsolicited links – can spell disaster.

For Bob Stark, vice president of strategy at treasury security systems vendor Kyriba, combatting these types of attack demands a lot from treasury teams. "What I find treasury has in common with the rest of the organisation is really two things: data security and application security," he says. The first? "That covers making sure that the actual data is encrypted and stored in a safe place. Some IT departments will recommend that data is pushed into the Cloud, or at least off-premise in some way, because they recognise that having it in an internal server room is an unnecessary risk and compromises data security."

The second consideration, according to Stark, is application security, which involves designing adequate controls within the technology tools that they use. "In treasury, that's often [within the] bank and it's going to be treasury management systems; in some cases, it might be trading portals as well."

These technologies need to abide by basic security protocols, such as strong password controls, two-factor authentication, IP filtering and so on.

> "With the right technological tools, treasury is able to monitor bank accounts and potentially identify any abnormal transactions to be followed up promptly, which does potentially increase the chance of recovery of funds"

For Rachael Fisher, group treasurer at manufacturing business Rotork, the twin approach of tackling data and application security is a big part of her anti-fraud strategy. So where does Fisher see her role in protecting the company from the worst of the cybercriminals?

"Since an increasing proportion of cybercrime relates to attempts to obtain cash, our role is central to the fight against cybercrime, working in partnership with other departments – IT for instance," she says, pointing out that treasury is perfectly placed to work with banks to understand the controls they have in place and to obtain best practice recommendations around internal processes.

"Treasury is the team that works with banks if crime attempts happen, to seek to recover the financial losses or provide evidence to support insurance claims," she says. "And, of course, we are often deemed to be responsible for ensuring group procedures are robust enough to prevent fraudulent payments and for communicating with those involved in payment processes to ensure they are aware of current trends in cybercrime and appropriate responses."

Risk management policies and technology

But Fisher points out that treasury teams have to grasp the nettle on this issue and not leave it to the IT function. "With the right technological tools, treasury is able to monitor bank accounts and potentially identify any abnormal transactions to be followed up promptly," she says. "And while you could see this as shutting the stable door after the horse has bolted, prompt follow-up of these does potentially increase the chance of recovery of funds and it could also be regarded as a deterrent for crime being initiated from within."

Stark agrees, but points out that no matter how sophisticated the system may be, the policies that underpin its operation are more important. "Treasurers have to review their policies to ensure that they align with everything from general internal policy to being cognisant of the risks that are out there today; they need to ensure their policy is modern and aligned with what the risk profile is.

"Any risk management approach has to be a combination of reviewing what you have in place: does it meet your objectives? Is it protecting you from the risks you face?" he says. "If the answer is yes, great; you're in good shape. Review of those is absolutely crucial."

No system can replace sensible policy adopted across the organisation, Stark points out. "Technology should be put in place to actually implement and support that policy," he says. "So if you've great policies, but you've dire technology, you're going to be exposed. If you've great technology, but it's not implemented around great policies, then, once again, you have the same problems."

Christian Doherty is a business journalist