# CONSTANT VIGILANCE

CYBERSECURITY BREACHES AND CYBERCRIME ARE A GROWING PROBLEM FOR TREASURERS. BUT IF YOU WANT TO EXPLOIT TECHNOLOGY DEVELOPMENTS, YOU ALSO NEED TO PROTECT AGAINST THEM. LESLEY MEALL REPORTS

You are being watched. You are being targeted. You need to be careful. Your name, job title, colleagues and contacts have been collected from social media. Details of your customers and suppliers have been sourced, verified, sifted and prioritised. You are now a pawn in a cybercrime scam. You may be on the brink of your very own personal or professional cybersecurity nightmare.

Over the past year or so, cybersecurity breaches and cybercrime threats have rarely been out of the headlines – and their magnitude, sophistication and success seem to be on the increase. Notable incidents include:

- Leoni AG, Europe's largest manufacturer of electrical cables, and its loss of €40m in what was widely reported as an 'email scam';
- Theft of money from the personal accounts of 20,000 customers of Tesco Bank in what it describes as a "systematic, sophisticated attack";
- Use of an employee login to hack into systems at Three Mobile and steal the personal data of its customers; and
- Use of the SWIFT credentials of Bangladesh Central Bank employees in fraudulent money transfers amounting to an estimated $81m.

Clearly, bank infrastructure and corporate payment systems are popular targets – and a worry for corporate treasurers. When you are responsible for managing and controlling your group's cash, initiating and approving treasury, vendor and employee payments (and protecting the related personal and financial data), you have a crucial role to play in protecting those assets from cyberthreats.

## Raise your game

It makes sense for treasurers to take a more proactive role in the development of the processes and people skills that will help to reduce the risk that cybercrime may have a negative impact on their areas of responsibility. However, when treasurers do become involved in broader company-wide and cross-functional discussions around cybersecurity, they will need some knowledge of the main cyberthreats.

Acquiring this can be a stretch. There is lots of public-domain information and guidance out there (perhaps too much). Inconveniently, it tends to be either too general or too focused on technology. In 2014, the ACT worked with government and other professional bodies to create specific guidance, and you can find *Cyber-Security in Corporate Finance* at www.treasurers.org/node/9799

At www.treasurers.org/cybersecurity you will find a recording of an ACT webinar from 2015. In this, ACT specialists and an external banking security specialist (from RBS) discuss key cybersecurity threats facing the public and private sectors – and offer some practical hints and tips on what treasurers can do to minimise the potential for associated disruption, fraud and reputational damage.

SHUTTERSTOCK

## Reality check

Yet in PwC's recent research report *The 'virtual reality' of treasury*, only 19% of treasurers list security as a critical concern. Sebastian di Paola, global corporate treasury leader at PwC, suggests that treasurers should be "collaborating more with the business, shared services and banks and raising their game in IT security and financial risk management".

On the face of it, raising your game in IT security may seem challenging. Although the consumerisation of digital technologies has made many aspects of IT seem less complex and mysterious,

"Many of us think we have a good handle on different types of security risks, but the reality may be a little different"

cybersecurity has become more so. Threats such as phishing, ransomware, spoofing and whaling can make cybersecurity (and crime) appear more impenetrable than a firewall.

Even less opaque terms such as 'hacker' and 'email scam' can obfuscate or enlighten. "Many of us probably think we have a pretty good handle on the different types of security risks that can threaten our business. But the reality may be a little different," says Ian Kilpatrick, cybersecurity vice president at Nuvias Group. Treasurers may need to read between the lines in IT security as cleverly as they can in finance.

## Between the lines

Let's consider the widely reported 'email scam' at the German company Leoni AG. A company statement confirmed that it became "the victim of fraudulent activity with the help of falsified documents and... the use of electronic communications channels". It put the "outflow of liquidity totalling around €40m" into perspective, by noting that its liquidity situation was not "adversely affected in any material way".

Treasurers know what a slippery customer materiality can be. So can phrases such as 'falsified documents' and 'electronic communications channels'. Apparently, the perpetrators spoofed emails to appear like official payment requests from Leoni in Germany, then sent them to a finance exec at just one of Leoni's four Romanian factories: the only one with the authority to make money transfers.

Perpetrators of email scams do not only target companies in a position to lose millions. The treasurer at a mid-sized non-profit has also been targeted; to conceal his identity, we'll pretend he's female and call him Claudia. "I'm proactive about IT security," she says. "Even before the scam, I had initiated a dialogue with the IT manager, to tighten up procedures to protect my login and payment credentials."

Unfortunately, this didn't prevent a fraudster's email prompting a change to the bank details of a regular supplier, which led to two electronic transfers (amounting to £20,000). "Accounts payable accepted the email as genuine. The FD signed the TT [treasury transaction] forms, then I authorised the supplier payments. Twice," she says. "Now any request to change customer or supplier bank details is verified."

## Socially engineered

The frauds in Romania and the UK were both enabled by technology (spoofed emails), and made easier by technology (electronic payments can be liquidated more quickly and easily than cheques). However, only the victims and criminal investigators have any chance of establishing whether identification of the weak points in their internal policies and processes owed more to technology or to people.

Either way, in both cases, the frauds were successful because, at the final stage of the process, the victims' employees were either directly or indirectly 'socially engineered' into willingly handing over company money, because they believed that they were engaged in legitimate transactions. In their defence, there are some 'very good reasons' why they were so easy to manipulate.

> "An organisation that has bulletproof doors and windows won't necessarily be able to protect against someone who can walk in as if they were a trusted individual"

Jayan Perera, an associate director in cyber consulting at Control Risks, says: "An organisation that has bulletproof doors and windows won't necessarily be able to protect against someone who can walk in as if they were a trusted individual." As he observes, social engineering attacks and other more advanced attacks are easily by-passing the reinforced perimeter walls we have spent years erecting.

## Mixed blessings

These frauds and the false sense of security that may be created by strong perimeter defences (such as the firewalls and other tools we rely on to keep out the baddies), raise some interesting issues for treasurers. They also highlight why it may be easier than it at first seems, to follow di Paola's advice to "raise your game in IT security" – without becoming an expert on it.

Many of the steps that need to be taken to protect the software and systems (and data) that impact on treasury (and how effectively it can manage cash and liquidity and financial risk) cannot be addressed only with cybersecurity technology. To be successful, they also require organisations to devote resources to the development of appropriate processes and people skills.

Treasury has a vital role in raising awareness and developing guidance for others in the financial supply chain; but collaboration will be key. PwC's research found that just one third of people involved in treasury processes report in to the treasurer. So di Paola suggests that "treasury should be seen very much as a process rather than a department".

## Plan for action

More detailed guidance for those involved in treasury processes is available in *Cyber Fraud – the Impact on Treasury* (www.bellin.com/resources/whitepapers), which was written by Royston Da Costa, group assistant treasurer at Wolseley. He says: "My hope is that treasurers will read it and if they have not already done so, conduct a full review of their key treasury processes including payments."

As cybersecurity is a fast-moving area, threat monitory must be an ongoing process. During 2016, 'whaling' emerged as a major social-engineering threat; using the names of legitimate senior executives and (spoofed) email addresses to dupe employees into wiring criminals sensitive documents or money. This year is likely to bring more of the same – plus some new cybersecurity nightmares.

This article first appeared in the March 2017 issue of *The Treasurer.*

**Lesley Meall** is a freelance journalist specialising in technology and finance