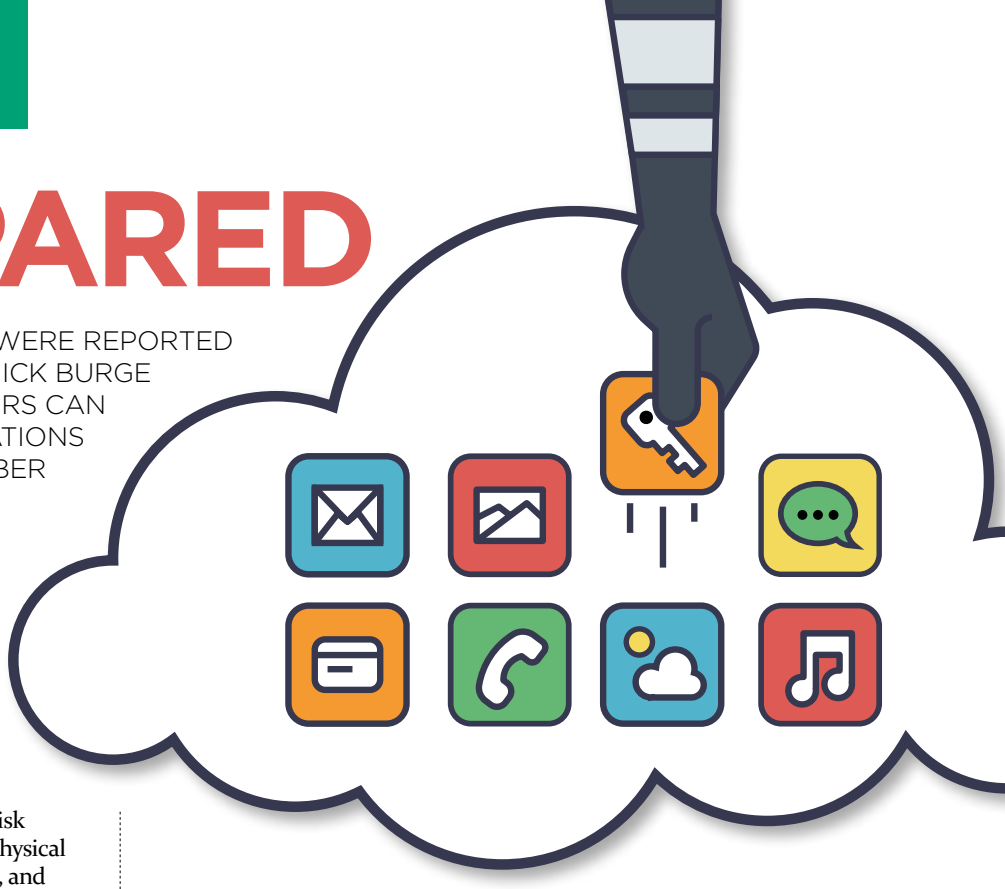
BE PREPARED

LAST YEAR, 2.5 MILLION CYBERCRIMES WERE REPORTED IN THE UK ALONE. GILES TAYLOR AND NICK BURGE EXPLAIN WHAT CORPORATE TREASURERS CAN DO TO HELP PROTECT THEIR ORGANISATIONS AGAINST SUCH ATTACKS, AND WHY CYBER RISK IS NO LONGER JUST AN IT ISSUE



SHUTTERSTOCK

The beauty of digital systems is also their weakness. With most businesses going through a digital transformation, led by the deliverable promise of efficiency and lower costs, it is inevitable that more of their processes and customer interactions will pass through an IT-enabled platform.

Data confidentiality, integrity and availability can all be compromised by a cyberattack. Each has the potential to translate into significant financial losses – not least in the form of fines from regulators. What's more, when the EU's General Data Protection Regulation comes into force in 2018, UK businesses will likely face much stiffer regulatory penalties – with the maximum being 4% of global turnover, considerably higher than the current limit of £500,000.

The consequences of a cyberattack stretch far beyond simple financial impairment for business, however. For example, increasing dependence on technology has seen the rise of IT concentration risk. This means that certain industrial sectors have become reliant upon particular technologies.

An increasing number of businesses in industry sectors, such as media, depend on cloud-computing services as their main revenue-generation platforms. Were any of these platforms to be taken offline, the impact on the sector would be devastating, not just on the industry, but also across ancillary services, and other businesses.

Risk ownership

This creates a challenge for a business trying to understand its own risk profile. Amid all its physical and service suppliers, and connections to the outside world, its successful operation is contingent upon the containment of risk by a third party.

Such risk is considerably more difficult to quantify. It follows that if the risk cannot be appropriately quantified, then it becomes difficult for a board to understand the potential impact of a risk event on the business. How then can a business determine the financial consequences and appropriate liquidity and financial arrangements that might be needed following an attack?

Understanding that a business is more reliant on technology does not require management to be fully cognisant of the technicalities of the interconnected world. However, it does require a full grasp of the fact that connectivity generates certain risks, and that these risks, if manifested, can and do impact the bottom line.

The common assumption that if a company's commercial systems are dispersed across multiple locations means it is safe, is misguided. Current levels of integration and connection give attacks so much more reach.

It is essential for the board to incorporate a response to this new style of risk into company strategy. In meeting this need, it is vital to understand that a cyberattack can often be a discreet affair and that the average time it takes for a commercial breach to come to light is over 200 days. By then, it may be too late.

The threat

There are a number of ways in which a business may be attacked. Key among these (accounting for up to 90% of attacks) are the so-called 'phishing' and 'spear phishing' methods.

Phishing uses a blanket email to thousands of recipients (often from stolen email addresses) in the hope that some will click on a link. This allows the target system to be compromised in some way, often by uploading malware that sits in the now infected computer to do the attacker's bidding. This may be to steal data or engage the computer with other similarly compromised machines in a distributed denial-of-service (DDoS) attack, effectively overloading and shutting down a system. This was recently experienced by Amazon and Twitter.

Spear phishing will see a criminal seek out information about an individual, often a more senior company representative, through public sources of data (often just using the internet). The information gleaned will be used to personalise the approach such that it is very believable. Once the content is accessed, the system is open to attack; senior employees are often targeted because it gives access to potentially more valuable data, whether that is for purposes of industrial espionage, extracting money or corporate vandalism.

Be aware, too, that ransomware attacks are on the increase. All sizes of company may be targeted, but often it begins with a DDoS attack, followed by a message that threatens further shutting down of systems unless payment is made to the perpetrator (usually in untraceable Bitcoin).

Rising up the cybercriminal agenda is the concept of the crypto-locker. Entry is typically

via spear phishing. Access to systems will enable the attacker to begin encrypting company data, denying legitimate user access. The ransom note is then delivered, usually threatening further attacks of greater magnitude, and often applying an 'unlocking' price of increasing size as time passes.

The victim's response in each case will be a matter of policy, presuming there is one.

Lloyds Bank's work with TheCityUK, a financial and related professional services membership body, and insurance broker and risk adviser Marsh on its May 2016 document, *Cyber and the City: Making the UK financial and professional services sector more resilient to cyber attack*, evidences how too few firms are tackling the cyberthreat in a cohesive way. Only 50% of large UK firms have cyber in their top 10 risks, only 30% have tried to quantify their cyber exposure and only 25% have a cyber-incident response plan. And until policy is framed, breaches will neither cease nor diminish.

The weakest links

Of course, no company is likely to warrant the resources for full protection of every system; the cost will be prohibitive and, in practice, the results will be too restrictive on business processes. In defending an organisation, it is vital to get the basics right for both internal and external assurance.

Governance guidance in the form of Lloyds Bank's 10 key cyber security considerations (see box, above) will help steer business in the right direction. The UK government's *Cyber Essentials* document series also goes some way to preparing the ground.

However it is tackled, the approach is best coordinated through a risk management programme. This must be capable of directing investment to the most important corporate assets: protection of key data is included here, but shielding business-critical systems, such as those for payments, production or logistics, must be part of this plan.

But cybercrime is not just an IT matter: people and processes also sit in the firing line. As a key financial player within a business, the treasurer will be a target. As guardian of banking and payments systems, fraudsters may seek to trick the unwary treasurer into changing or signing off transactions. Emailed last-minute 'urgent' large payment instructions from someone masquerading as the CFO are not unheard of.

Ensuring all personnel – especially senior staff, such as treasurers – are appropriately trained to recognise and deal with a threat is a vital and sometimes final line of defence against significant loss.

More than money

While potentially damaging for a business, fraud is just a part of cybercrime. The loss of systems and data may far exceed the immediate cost of any financially motivated attack. Operational downtime, consequent loss of revenues or other financial impact, reputational damage and loss of trust among customers and shareholders can prove calamitous.

Preparations should focus on ensuring the business can respond financially in the event of a serious attack. This may simply extend to taking out an insurance policy; specialist providers exist in this space. But insurance may not be enough. If an attack is of sufficient magnitude, the lag between attack and settlement of claim may disrupt the working capital position, revenues and even the capital position of the firm. Companies need to estimate the potential financial and liquidity impact of a cyber event. This will include familiarity with the types of attack and thinking through the consequence of a breach on the financial position and factoring this in to modelling the liquidity buffer needed to safeguard the business.

Putting in place and managing the liquidity buffer across the various components of available cash, committed facilities and other forms of liquidity mean that treasurers need to be cognisant of the risk, potential magnitude and duration of various types of cyber breach. This will enable the treasury to play a key role in ensuring resilience.

Action plan

To be truly effective, defence against cybercrime should not be thought of solely in terms of technology. Instead, think of it in terms of an overall business risk management strategy, covering people, processes and systems, and financial resilience.

For companies that are well-prepared, the overall impact of a cyberattack can be significantly reduced.

CYBER RISK: BE PREPARED

The following questions may assist your company in becoming more aware of, and protected against, cyberthreats:

1. Have we identified and understood the company's critical information, assets and services? Where are they stored and who has access to them? Consider suppliers, contractors, etc.
2. Have we considered who might want to attack us, why and what the impact of a successful attack might be?
3. Do we have a risk appetite for different types of cyber events impacting our business?
4. Do we know what vulnerabilities we have and do we have an effective and efficient vulnerability management process?
5. Have we risk assessed how well our critical assets are protected and produced a gap analysis?
6. Do we have a prioritised action plan to enhance our capability to protect our business against cyberattacks?
7. Have we ensured our colleagues (and, if appropriate, our clients) are aware of the cyberthreats, especially the risks associated with social engineering and phishing attacks?
8. How do we know our defences work – have we tested them or sought external assurance?
9. Do we have a plan (is our incident response and disaster recovery prepared) in the event of a successful cyberattack? Have we considered taking out adequate cyber-risk insurance cover?
10. Do we have a process to regularly review our key information, data assets and the cyberthreat to our business?

Finally, if your business is the victim of a cybercrime, you should contact Action Fraud (www.actionfraud.police.uk)

Nick Burge (pictured left) is head of global corporates structural & regulatory solutions; and **Giles Taylor** (pictured right) is head of data and cyber security at Lloyds Bank Commercial Banking

LLOYDS BANK