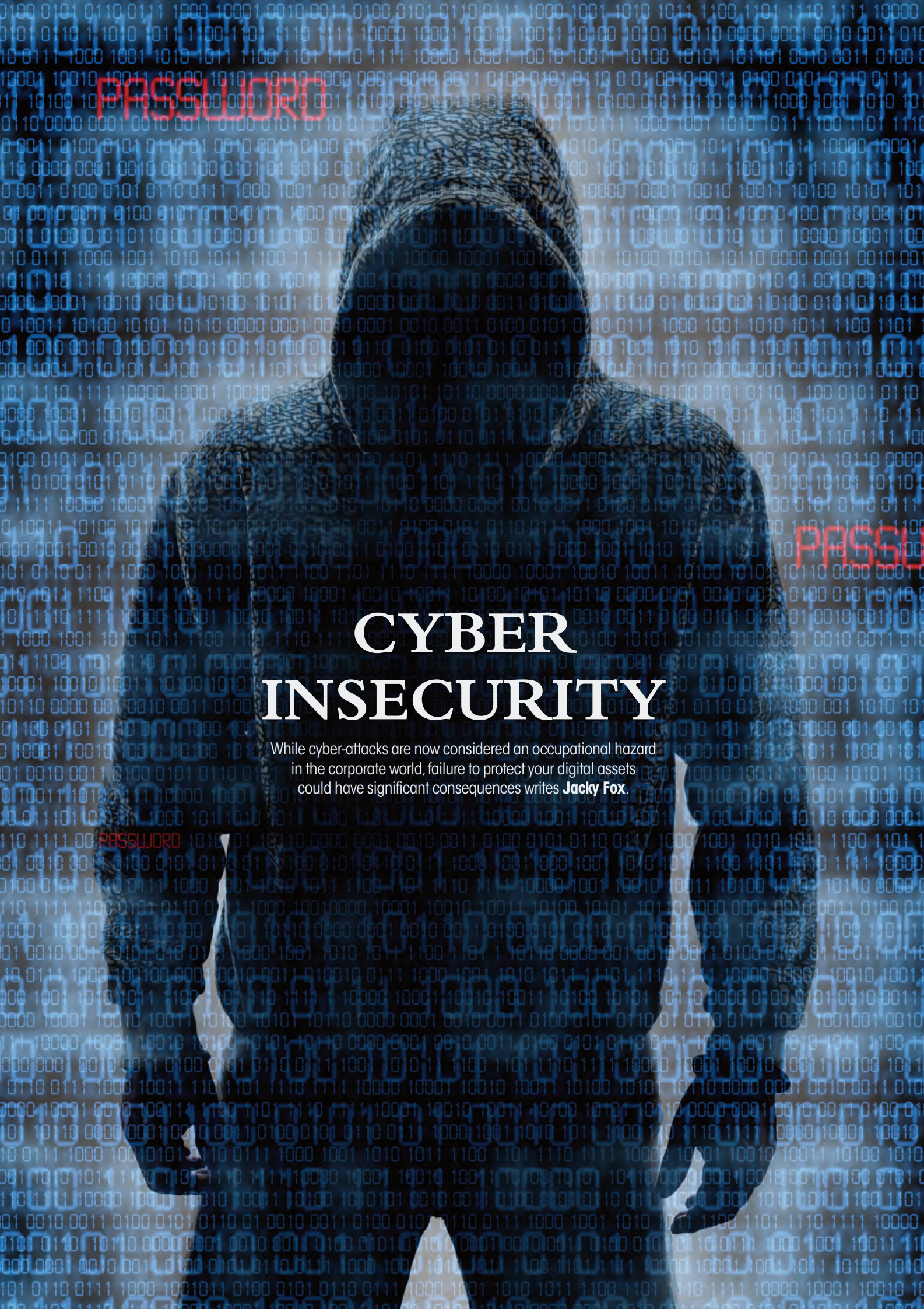

CYBER INSECURITY

While cyber-attacks are now considered an occupational hazard in the corporate world, failure to protect your digital assets could have significant consequences writes **Jacky Fox**.

With organisations now hacked on a frequent basis, some might believe that there is no real way to avoid being the next target. Deterring a determined hacker can be almost impossible but if you identify your most important cyber assets, understand how and why they might be vulnerable, and put some advanced planning in place, you will give your business a fighting chance of surviving a serious cyber-attack.

The motivation for – and the severity of – cybercrime varies hugely, depending on the type of criminal involved and the nature of their target. A state-sponsored hack is likely to be completely different from that of a common thief or a 'script kiddie'. It is nevertheless important to protect your cyber assets in direct proportion to what makes them attractive, to whom, and the impact that losing them might have on your business.

Spending time identifying why someone might want to hack your firm is a worthwhile investment. If you work in finance, your job description alone suggests that you have access to funds and makes you an attractive target for cybercriminals. The more common reasons include access to, or theft of, sensitive data such as intellectual property or credit card or bank account details; access to one of your business associates; the transfer of cash; free use of your firm's facilities; disruption of your day-to-day business; and embarrassing an organisation and discouraging clients from using its services.

An external person can gain unauthorised access to a system in many ways. The most common methods are exploiting a known vulnerability and the introduction of malware – or some combination of the two.

THREE STAGES OF HACKING

Hacking can be easy and in general, there are three main stages involved – footprinting, enumeration, and exploitation. A hacker goes through a similar process to a house burglar; they survey the property and neighbourhood, test the property to see if there are any obvious points of entry, and then attempt to break in. It is worth mentioning at this point that attacking a system without the permission of the owner is illegal.

Footprinting involves gathering information about a target, often from afar. Methods include sourcing publicly available information about an organisation such as location, names of employees in key areas, press reports about new ventures or products, accessible websites, email address formats, domain names, and IP address ranges; or possibly analysing publicly available documents or emails to determine the software used to generate the files.

> "IF YOU WORK IN FINANCE, YOUR JOB DESCRIPTION ALONE SUGGESTS THAT YOU HAVE ACCESS TO FUNDS AND MAKES YOU AN ATTRACTIVE TARGET."

The enumeration or scanning stage uses the information gathered from the footprint. For example, by running specially designed scanning tools against an identified webserver you can typically find out the name and version number of software running on it. These scanning tools are publicly available and can inform you of known vulnerabilities with specific configurations. The good news is that these tools can be very noisy as, unless a hacker makes an effort to hide their activities, it is easy to see that your systems are being scanned – provided you monitor them.

If known vulnerabilities are identified, this information – coupled with other information gathered at the footprinting stage – can be used to exploit or enter the system. Once inside, the hacker then tries to move around from system to system and potentially leave a back door open for future re-entry. Depending on the hacker's motivation, they may target specific data for theft or destruction, use your system resources, attempt to steal passwords or credit card details, or simply sell system access to another party.

MEANS OF ACCESS

A huge variety of cyber scams and attacks can be inflicted on an organisation. Some of the more disruptive and damaging events include banking trojans, ransomware, distributed denial of service (DDoS), and fund diversion using social engineering.

At some stage during an attack, a hacker may attempt to install malware on the target's system. Clicking on links in emails from unknown or atypical sources, for example, remains a successful method of malware introduction into many organisations despite regular warnings.

There are two main approaches to email phishing: send out large volumes of emails or spam and you can be guaranteed that someone will click on the link, or create a crafted spear-phishing email for an individual or organisation that will entice them to read it. After all, people who work in finance will typically open an invoice, HR will open a CV, marketing will read a press cutting and so on.

It is a lesser-known fact that your system can become infected with a 'drive-by' attack. Simply visiting a webpage can introduce malware into your system, and you don't have to open, click on, or download anything to get infected. It is therefore important to block or discourage users from visiting unapproved websites. This technique can be used to target individuals or organisations by infecting 'watering holes' or websites a user or group would likely visit.

In terms of malware designed to collect banking credentials or encrypt data for a ransom fee, several variants of banking trojans are in circulation with some more sophisticated than others. Hackers typically install a form of key logger on the system to

> "IF YOU DON'T HAVE A GOOD FILE BACK-UP STRATEGY IN PLACE, YOU COULD BE IN REAL TROUBLE."

record keystrokes with the aim of capturing banking credentials. Once captured and received by the hacker, the credentials can be used to transfer funds from your account. Online banking systems usually incorporate some form of two-factor authentication, requiring a user to supply something they know – typically a password – with something they have, such as a certificate or fob, in order to access their account. Two-factor authentication generally provides additional assurance of identity, but social engineering techniques or use of the victim's own system to gain access to certificates have been used to complete fund transfers despite these additional layers of security.

A NASTY RANSOM ATTACK

A particularly nasty crypto ransom attack is now in circulation globally with malware targeting an organisation via a phishing email. If the user clicks on the link within the email, the victim's system will reach out to a command and control server that downloads and runs the crypto malware. When activated, the malware encrypts data files on the infected system and any external or network drives the system is mapped onto.

Users typically become aware of the attack when they attempt to access a file and receive a message stating that the data has been encrypted and decryption keys will only be provided upon payment of a ransom. Payment is typically requested in bitcoin, an online currency that is much more difficult to track than traditional bank transfers or credit card payments. Sadly, if you don't have a good file back-up strategy in place you could be in real trouble – particularly if your back-ups are held on a mapped drive and also become encrypted.

DENIAL OF SERVICE ATTACKS

Denial of service (DOS) attacks occur when a web service is overwhelmed by spurious traffic and becomes unable to service normal, legitimate requests. An attacker does not need to use their own infrastructure to carry out these attacks as DoS services can typically be hired for less than $100 for 24 hours. There has been a rise in DoS attempts where an initial short attack is followed by a ransom email demanding a fee to avoid a more damaging attack at a later date. Again, the payment is typically requested in bitcoin.

Several Irish organisations have also been exposed to a scam to in recent months involving a series of spoof emails, invoices, letters or calls requesting that funds be transferred to an illegitimate bank account. This scam is often preceded by a request to change the payment account details for a legitimate supplier and can involve emails that seemingly come from 'the boss' instructing payment. Finance departments should be vigilant where account details have been recently changed, or if payment requests are made out of sequence or for unusually large amounts.

So, how can you avoid being the next victim of cybercrime? Implementing the following suggestions will help minimise the risk to your organisation:

- Install anti-malware software and keep it up-to-date;
- Don't click on email links from unknown or atypical sources;
- Use complex passwords or passphrases, keep them safe and don't use the same password on multiple systems;
- Encrypt vital data and safeguard the decryption keys;
- Check your systems for known vulnerabilities;
- Operate good software update management practices;
- Monitor system usage and payments;
- Avoid visiting suspect websites;
- Use two-factor authentication for sensitive transactions;
- Keep good back-ups of your important data; and
- Train your system users in safe online practices.

Jacky Fox is Digital Forensic and Cyber Security Lead at Deloitte.

IRISH BUSINESSES EXPOSED TO LEGAL RISK

Less than one third of businesses in Ireland are prepared to deal with a cyber-attack with a significant majority not fulfilling basic legal requirements, according to A&L Goodbody's *2015 Cyber Risk Study*. This haphazard approach leaves firms open to possible litigation and fines, not to mention the potential loss of intellectual property and commercially sensitive information.

Basic legal obligations not being fulfilled by businesses include: not having written cyber-security policies in place (65 per cent); not providing training to employees on what to do in the event of an attack (59 per cent); and not allocating responsibility to any one employee or team to deal with an attack (49 per cent).

Highlighting the need for companies to deal with cyber-security issues from the top down, the survey also found that one in four company boards have not been briefed on their organisation's legal obligations and the mechanisms that are in place, if any, to deal with a cyber-attack. Less than one third of companies surveyed said they were fully prepared to deal with an attack and, when prompted, cited a lack of awareness of their company's legal obligations as their biggest challenge. The survey also found that half of companies surveyed stored their data with a third party off-site and – within this group – 44 per cent admitted to not knowing their supplier's cyber-security attack policy.

According to John Whelan, Partner and Head of A&L Goodbody's International Technology Practice, "As cyber risk becomes more sophisticated, and more prevalent, businesses are exposed to increasing risk to their reputation and bottom line," he said. "Boards and senior management must have policies in place to protect their business should a cyber incident occur. An important part of this is ensuring that basic legal requirements are met, and the survey shows that while many businesses are aware of their exposure they are not fully prepared for it."

Mr Whelan added: that, in addition to the operational and business risk, there is material legal risk with consequences in terms of possible legal and regulatory action, and potential harm the company's market reputation.