BY
Paraic Nolan

The Invisible Enemy - Cybercrime

Paraic Nolan of Big Red Cloud looks at the growing threat to business posed by cybercrime and some of the steps which can be taken to prevent it.

Paraic is the Chief Technology Officer at Big Red Book and Big Red Cloud. Having graduated from UCC with a Bachelor of Commerce he qualified as a Chartered Accountant in 1990. Paraic has worked with many accounting and enterprise resource planning software products as a senior technical consultant and product manager including Take Five and SAP Business One.

Cybercrime is a serious issue for Irish businesses and it's about to get a lot more serious. New European regulations which come into force in Ireland in under two years' time will expose firms of all sizes, no matter how small, to onerous fines of up to 4% of their turnover for even the slightest breach of their data.

The quite innocuous sounding General Data Protection Regulation (GDPR) is intended to strengthen and unify data protection for individuals within the European Union. However, it will require any organisation which holds personal data on individuals – accounting firms, corner shops, golf clubs – to report any data breach to the Data Protection Commissioner. Failure to do so can result in fines of up to €20 million.

If this sounds frightening, then the statistics surrounding cybersecurity and related crime in Ireland and globally are downright scary. According to the most recent economic crime research carried out by PwC more than one in three Irish organisations (34%) experienced such crime within the last two years, up from a quarter (26%) two years ago. And some 44% of these organisations were victims of cybercrime.

The research also found that cyberattacks experienced by Irish organisations have almost doubled in frequency since 2012. The cost of these attacks is considerable with nearly one in five (18%) of those affected incurring losses of between €92,000 and €4.6 million as a result.

The global statistics are even more stark with the European Commission estimating global financial losses due to cybercrime at €350 billion a year currently and rising to €1.9 trillion by 2019. Furthermore, the Commission believes that cybercrime has already led to the loss of 150,000 jobs across the EU.

Vulnerability

The excessive vulnerability of Irish individuals and businesses to cybercrime was further highlighted at a seminar hosted in Dublin in July by Irish firm Cyber Risk International. This vulnerability was attributed to slack security at even the most basic level by a 2015 Eurobarometer Report by the European Commission.

In the survey carried out in March of 2015, 57% of Irish people admitted to opening emails from people they don't know; just 26% of Irish internet users said they regularly changed their passwords; while 75% use the same password across different sites and online services.

Some 9% of Irish internet users reported being victims of identity theft, 10% said they had been a victim of bank card or other online banking fraud, and 7% had fallen prey to ransomware and had to pay criminals in order to restore access to their own device or data.

Threats

Indeed, such is the growing prevalence of this last form of cybercrime that many companies are now recording the ransoms paid as a business expense in their accounts. This form of cybercrime generally works by the criminal fooling the computer into downloading crypto-locker software from a seemingly legitimate website.

Once the software is downloaded it automatically runs and seeks out data files on the user's computer and encrypts them. A message is then displayed telling the user to pay a ransom in bitcoin to obtain the decryption key. Many firms believe they have no choice but to pay the ransom such is the value of the data and the potential consequences for the business of not being able to access the information.

This usually happens due to the simplest and indeed most understandable of errors. A phishing email which is sufficiently convincing leads a user to a site which invites them to download a software update. It's literally all over in seconds.

Another growing form of cybercrime is the denial of service attack. At its most simple this involves clogging up an organisation's email servers with spam or taking down their website through a mass log-in activity. This can be hugely harmful to a business and can cause enormous reputational damage. One of the key problems here is how easy it has become for almost any individual or organisation to mount such an attack. For as little as €100 an individual with a grudge or other motivation can pay for such an attack from one of many organisations based in jurisdictions where they feel safe from the reach of authorities.

Straightforward hacking is the third main area of cybercrime. Hackers gain access to a network and then gain access to valuable data either for fraud purposes or to sell on to rival organisations. And no company or organisation, no matter how large or how well protected they believe themselves to be, is immune from such an attack.

A case in point is the giant American retail chain Target. Hackers gained access to the network not through the company's website or its online sales channel or even through the workstation of one of its employees, they came in through the air conditioning system. That might sound like something out of an old episode of Mission Impossible but it is true. The company had installed a new "smart" air conditioning system which was connected to the company's network – the problem was that the system wasn't protected from outside attack.

The hackers used this classic "back door" to enter the system but once in they didn't act immediately. They waited more than six months until one of the busiest shopping weekends of the year and then stole vast amounts of credit card and other data.

This reflects other data on cybercrime which indicates it takes an average of more than 100 days before hackers are discovered on a network. This is particularly worrying for Irish organisations in light of the requirements under the GDPR to report any security breaches without undue delay.

The issue for accountants

Cybercrime presents a number of challenges for accountants. Those in industry have a responsibility to protect their organisations from economic crime generally and cybercrime in particular while accountants in practice must protect their clients as well as their own firms.

The good news is that cybersecurity needn't cost a fortune. The first port of call for many firms and accountancy practices should be their internet service or web hosting provider. They can provide a variety of security solutions to meet the needs of organisations of almost any size.

There is also a large number of specialist cybersecurity providers who can deliver solutions designed to meet specific needs – again without necessarily entailing excessive cost.

However, there is one thing that all the experts in the field are agreed on – the best defences do not rely on hardware or software, they depend on people. Training staff in areas such as threat awareness and response is the first and most important step in improving cybersecurity. This greatly reduces the risk of employees opening spam, responding to phishing emails or accidently downloading malware.

For larger firms, the designation of one individual with overall responsibility for cybersecurity is a must. Too often, in the wake of a cyberattack, it is found that everyone thought that security was someone else's job but nobody actually knew whose. Having one manager to coordinate efforts in this critical area will help ensure your firm remains up to date with the latest threats and that your systems and protective measures keep pace.

Finally, beware of unsolicited approaches from "experts". A particular scam reported at the Cyber Risk International seminar involves a company receiving a call or email from a self-proclaimed cybersecurity expert who is apologising for inadvertently compromising that company's network in the normal course of their work. They verify their claim by showing that they possess some crucial data from the company. The sting at the end of this is that the expert ends offering to work remotely for the company for thousands of euro per month to protect it from other security breaches.

This is the classic blend of old-fashioned con and modern technology which is increasingly coming to characterise cybercrime. It therefore benefits us all to retain that healthy sense of scepticism with which we approach business dealings generally when it comes to technology related issues.

For a more comprehensive overview of cybersecurity and the measures required to protect your practice, download the *Cybersecurity Ireland 2016 Report* at www.bigredcloud.com/safepractice.