Volume 2, Issue 2

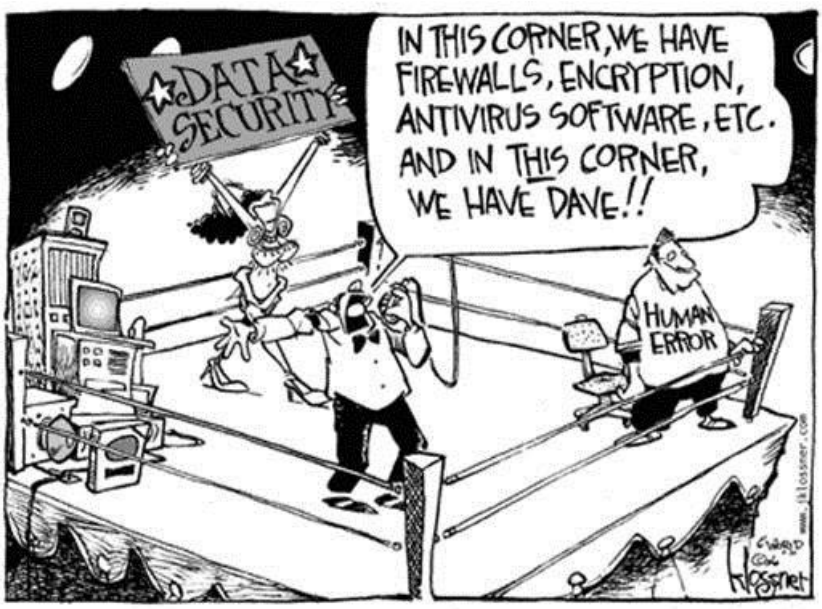
Quarter 2 2017

Risk Management Newsletter

Reducing Human Error

The best IT systems and controls can be let down by simple mistakes. As such, increasing awareness of cyber security exposures is critical; staff training should be carried out with follow up reminders to reinforce the message. With that in mind, never let it be said that we don't bring solutions to our readers!

To err is human...



Humans make mistakes. A hotel client of ours doesn't simply accept email instructions to transfer money to suppliers; instead they contact the third party over the phone to ensure the instruction came from them (dual verification). However, a senior member of staff received an urgent request to transfer €100,000 to a new account just as he was heading into an important meeting. In an error of judgement the process was ignored and the transaction approved. The email turned out to be fraudulent, and the client became yet another victim of cyber crime.

We also spoke with a principle who had ingrained risk management in his staff via training. Yet a well drafted email with an inviting attachment caught one of his employees off guard - they opened it without thinking and the firms systems were locked down by Ransomware. The firm lost a whole day of trading as they restored their IT systems from their backups.

...but how to forgive the swine?

Apologies for the awful pun. By way of seeking forgiveness, we have included on the following pages risk management tips that individuals can take to try and reduce the likelihood of being caught out by cyber crime. See how many you and your business are already implementing.

Don't forget, we include some recent examples of cyber incidents at the end of the newsletter.

Risk Management Newsletter

Your company may already have excellent security procedures, but these can be undone by poor staff behaviour. We consider some steps you and your employees can take to help reduce the chance of cyber incidents occurring.

Companies can take several steps to improve their cyber security. For example keeping anti virus and software up-to-date, installing firewalls, regularly backing up data and testing to make sure these backups can work if called upon. Refer to our Risk Management Tips newsletter from last year for more information - it's available here: http://www.olearyinsurances.ie/articles-and-newsletters. Below are some simple steps that individuals in your company can take to do their bit. Ask yourself how many of these are you already using and where can you improve?

Anti-virus on mobile phones / tablets

These are a no-brainer for PCs and laptops, yet they are also widely available - for free - for mobile phones and personal tablets. The software can only try and keep on top of viruses as they evolve, so they are not going to catch everything, but they do serve as a useful starting point for protecting against known viruses.

Attachments

Do not open anything you were not expecting. Vigilance and constant reminders are key. An email with an attachment accompanied by some very short text is a red flag - e.g. "please review these documents". Forward screenshots of suspicious looking emails around your office and warn staff not to open them - it helps reinforce the message.

If an email is suspicious but you're still not sure, and you feel you have to open it - do so from your mobile phone. That way, even if it is malicious, your phone should be the only piece of technology affected - much cheaper than repairing your IT systems.

Pick up the phone

A common feature of most of our newsletters, with good reason - if all of our clients carried this out they would have avoided most if not all cyber crime incidents we have seen. If a client or supplier emails through new / amended bank details, pick up the phone to ensure the instruction is genuine. Make sure to call your normal contact, not the number on the email. Anyone dealing with transfer of monies should be carrying this out.

Personal email

If an employee's personal email account has been hacked and if they are logged on to their work computer, then your company's cyber security measures could be rendered useless. Employees should be discouraged from logging in to personal accounts on workstations such as PC's or laptops. This can be difficult to implement, so explaining the rationale for this measure could be beneficial.

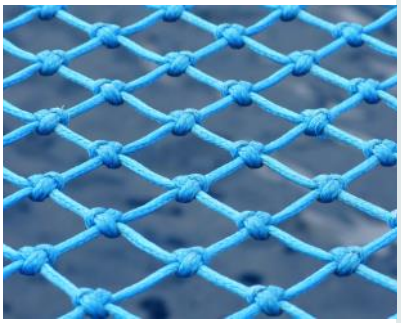
Passwords

Everybody knows that they *should* change passwords regularly, but how many actually do so? There are apps that are designed to securely store your passwords , but what if these get hacked (as happened to LastPass)? Setting up a password-protected spreadsheet on your computer containing your various logons and passwords helps - all you then need to remember is one key password, which can be changed regularly. But what if that spreadsheet is accessed somehow?

Changing your passwords is the only true way of protecting yourself. It ensures that, even if your details are compromised, they are void after a short period of time. Also, don't use the same password on every website - a hack on one potentially gives criminals access to all of your other accounts - they will try! Think of it this way - a hack on a newspaper subscription could give access to your emails using the same password, which could help build up a profile of what pages you subscribe to, maybe even where you bank.

Cyber Insurance - the safety net if all else fails

By Brian O'Mara, O'Leary Insurances



Most of us have had close calls, others will undoubtedly have been caught out.

- opening suspect emails
- somehow downloading a virus
- maybe even losing some money to cyber criminals.

The best case scenario is that a lesson is learned with no financial loss and minimal damage to your systems. However, what if you are not so lucky?

I present on the topic of risk management to companies around Ireland. Yet recently, after returning from annual leave, I was working through my emails. One such message was from a client from whom I was expecting forms. I hovered the mouse over the attachment and came mightily close to opening it - but there was something slightly off in the text of the email, so I paused. I rang the client and was told not to open anything, they had been hacked. Despite all of my training, a lapse of concentration nearly caught me and, by association, my company off guard.

Risk transfer

Since 2015, the average cyber crime loss to our clients has been over €36,000 - we have even come across a small number of six-figure losses. These are not sums of money that many firms can put down to bad luck and move on from. Other clients have, on the face of it, had smaller losses such as their computer systems being down for a day or two. However by the time the IT people have been in and systems are back up and fully operational the costs involved can be significant.

Insurance is the safety net if your security systems fail. It removes uncertainty by taking risk away from a company's balance sheet. Premiums are competitive at the moment with comprehensive coverage available (**including for theft of monies**) due to the number of insurers offering cover. For example, below are come policies we have recently placed for clients:

Industry	Policy limit	Total premium
Accountant	€1,000,000	€1,087
Call Centre	€3,000,000	€4,510
Catering	€250,000	€1,520
Charity	€250,000	€575
Construction	€250,000	€890
Engineer	€250,000	€575
Financial Adviser	€1,000,000	€1,344
Healthcare	€1,000,000	€890
Not for profit	€1,000,000	€1,440
Solicitor	€250,000	€835

Cyber Insurance is a relatively new product and it will continue to evolve as the risk does likewise. It is imperative to use specialist insurance brokers to ensure you are looking at a suitable product. O'Leary Insurances have invested significant time in building up our expertise on the various Cyber Insurance policies available in the market. **We recently negotiated an improved Cyber wording for the majority of our clients including 'any one incident' cover - much broader than the aggregate cover generally available in the Cyber Insurance market.**

We are happy to talk you through whether cyber insurance could be of benefit to your company. For firms that have good risk management procedures it is straightforward to obtain pricing for Cyber Insurance - we can usually provide indicative pricing based on revenue. If you would like to discuss further please contact whomever you deal with within our organisation or you can speak with our team by emailing cyber@oli.ie.

Brian O'Mara specialises in Cyber Insurance. He gained experience overseas placing complex solutions for clients. As well as compiling this newsletter, he regularly presents on the topic of cyber insurance and represents the Small Firms Associations on IBEC's GDPR (Data Protection Regulations) taskforce.

E: bomara@oli.ie T: 021 453 6860

Thank you for reading our newsletter. Below are links to our own social media pages. Follow these to keep abreast of important updates.

LinkedIn: https://goo.gl/u06ncG Twitter: @OLearyInsurance Facebook: https://goo.gl/DILziV

Below are a selection of cyber incidents that we have come across recently. As usual, these are all real-life Irish cases.

Solicitor - Cyber Crime

A rural solicitor usually verifies email bank details over the phone. However, a hacker was able to duplicate a key client's email. The practice let their guard down and accepted the email without following up to verify the instruction was genuine - €40,000 was transferred. The bank caught the transaction in this instance. Interestingly, the Gardaí have seen a number of similar incidents and believe that the perpetrator was based in Ireland - the vast majority of cyber crime incidents are perpetrated by criminals based overseas.

Professional Services - Phishing

A consultant opened a phishing email which affected their own system. However, it also forwarded the email to all of the contacts in that consultant's inbox, many of who in turn opened the attachment as it came from a trusted source.

Various - CEO fraud

This entails someone impersonating a senior member of your staff in order to trick a colleague in to transferring funds to a criminals bank account. We have seen a handful of CEO-fraud incidents in recent months in the communications, construction, health, hospitality and professional services sectors. Some were successful while others were either picked up by good internal procedures, or by luck. The amounts involved ranged from around €30,000 to €50,000

If you wish to discuss further please contact us. For new clients please contact cyber@oli.ie - we have 9 offices around Ireland to respond to your needs.

About O'Leary Insurances

Insurance Brokers & Consultants, Est. 1961

From an initial complement of three staff in 1961, originally founded by Archie O'Leary, O'Leary Insurances has successfully grown & developed into an Insurance Brokerage which specialises in providing a high level of customer service throughout Ireland.

With over two hundred employees now operating from nine locations nationwide, O'Leary Insurances provides a comprehensive insurance broking service to all sectors of the Irish Economy. As part of this insurance broker service, we have consistently maintained our strong emphasis on professionalism and personal attention through all of our products, buildings on our hard-earned reputation for dependability and commitment.

Our highly trained and experienced personnel would be delighted to be of service to you and would welcome the opportunity to discuss both your Personal Insurance and Business Insurance requirements with you. We are confident that our knowledge and expertise can assist you in the management of your insurance needs and can assure you of our very best attention in meeting the challenges of the future.

Disclaimer – as insurance brokers we cannot provide legal advice.

Thank you for reading.