Volume 1, Issue 3

Quarter 3 2016

Risk Management Newsletter

Risk Management Tips

In previous editions we have focused on education around cybercrime and Data Protection Legislation. This quarter we take a more in-depth look at risk management tips that every business can implement to reduce the likelihood of cyber incidents and to lessen their impact if they do occur.

The importance of good risk management

A number of our clients have made us aware of cyber crime incidents over the past 12-18 months. The average loss from these incidents has been just over €30,000. It is not an amount that most companies can just put down to experience and move on from. And this is just the loss itself; it does not take into account related costs such as lost hours in trying to recover the monies, business interruption, repairing and improving systems, reputational damage and carrying out employee training.

Many people expect us, as insurance brokers, to go straight for an insurance solution for our clients. However insurance should only be the fail-safe if risk management fails. We believe that for clients to get the best cover and premiums they should be in a position to show insurers how good their risk management is around cyber security. This has benefits outside of insurance. For example, larger firms looking to sub-contract works want to know that their data is protected or their systems are not at risk of being breached by passing on responsibility to your firm.

Many of the cyber crime incidents we are seeing are broadly similar—an invoice is received and paid for and it comes to light in time that the request for payment was fraudulent. Almost inevitably the monies are immediately sent overseas and lost in a series of international bank transfers. There are variations in the methods — some attacks are simply emails to a number of firms attaching supplier invoices. Most are much more targeted and sophisticated — we came across a cybercrime incident recently where the criminals had clearly monitored email conversations over a period of time. When they sent their invoice through, purporting to be a supplier, the language in it was reminiscent of how the supplier would have emailed their contact — including a comment about the latest Man Utd match. There was no cause for suspicion on behalf of the accounts department.

€30,400
Average cyber crime loss to our clients from notified cyber crime incidents since 2015.
This figure does not include any additional costs such as lost business time, system repair and damage to reputation

Risk management doesn't have to be a significant burden

However, almost every one of the cyber crime incidents we have seen could have been avoided by one simple step—dual verification. It doesn't cost much to implement; just the time taken to educate employees and the cost of a phone call. We go through exactly what this entails in the following pages. In the last issue we spoke of the need for a culture change among organisations. With an additional step to how bank transfers are made many of the cyber crime incidents that our clients have experienced could have been thwarted. There are other measures that can reduce other common 'cyber' exposures – we hope you find this guide useful.

We have prepared a two-page cyber security risk management document overleaf —it is suitable for printing. We encourage you to share these tips with your colleagues both internally and outside of your organisation to help spread awareness.

Risk Management Newsletter

The below is based around Datalogix's *"5 Ways Small & Medium Sized Businesses can protect themselves from Cyber Attacks"* article in our Q1 issue. It is worth revisiting and expanding on in order to increase awareness of how to protect your business from these incidents.

Cyber security is becoming very much more 'mainstream' in the peoples minds. It features high up on the news, victims regularly share horror stories on radio talk shows and it makes great copy for newspapers. Yet much of the reason for it's huge success is because companies are slow to implement simple risk management steps.

1 - Understand the evolving risks.

This is one of the first and most difficult steps to implement around cyber security as cyber crime continues to evolve. No organisation is too small to be the victim of cyber crime (in fact criminals see smaller firms as a soft target due to resourcing issues). It is almost impossible to keep abreast of every possible scam, however by reading up on the risk through subscriptions such as this one you are giving yourself a better chance. There is a booming IT-security industry which offers consultations and products to better protect firms of all sizes.

EXAMPLE: "CEO fraud" is on the rise on the continent, however we spoke with a Munster-based organisation that experienced it at first hand recently — and narrowly avoided on losing out on €65,000 in the process. Criminals purport to be the head of an organisation and pressurise employees into transferring funds. They often demand that someone in their finance function makes an urgent payment to a third party and advise that it is a highly confidential transaction. They also say that the third party will be in touch and inevitably a phone call comes through from that individual checking if funds have been transferred yet. The whole situation is designed to be quite stressful—order from on high, time pressure, a chaser phone call — and it often results in the employee transferring the funds without thinking rationally about the request. It is over before they know it. Updating awareness of this type of incident greatly reduces the likelihood of your firm becoming a victim.

2 - Staff training

A company can implement the best security systems available, but all of this can be to no avail if employees are not educated on what to look out for. Cyber security is a relatively new concern for companies and staff training is a critical element—for both employees and senior management. With many of the incidents we come across it is easy to blame human error, however some scams are so sophisticated that they give uneducated employees little chance — education is key. Regular updating of passwords, clean desk environments, having clear and defined company policy around security - these should all be part of the company culture.

EXAMPLE: many individuals receive phishing emails through to their work inbox. A common example would be trying to entice someone to open an attachment or click on a link infected with malware. These have moved on quite a bit from the days of long-lost Nigerian relatives getting in touch to the stage where it can now be difficult to ascertain if an email is genuinely from a service provider. Employees and management should be educated on what to look out for and to quarantine an email if in doubt.

A useful tip from Datalogix is to open an email on a mobile phone if you are not sure of it's authenticity - in the event it is an infected message, a new phone tends to be less expensive than a new server.

3 - Dual verification (pick up the phone!)

This sounds a lot more complicated than it is. Simply put it entails verifying a request is genuine by using a different channel. For instance, when you login to a restricted part of your online banking the bank sends a code to your phone.

EXAMPLE: your accounts department makes regular payment to a supplier and you have been making transfers to their account for some time. They contact you by email requesting you to update their account details as they have changed bank. This is where it is important to pick up the phone to verify that the request is genuine. Do not to trust a phone number on the email— this could easily be fraudulent. Instead, ring the number you have always used for that supplier.

Start implementing this measure for all new bank accounts provided to your company. Dual verification greatly reduces the likelihood of falling for such a scam and would have saved our clients hundreds of thousands of Euros over the past twelve months. Your clients and suppliers shouldn't mind - you are trying to protect their money!

4 - Keep your software up-to-date

Anti-virus software and firewalls will not make you impervious to cyber attacks. Well-resourced institutions including many banks, the Pentagon and the CIA have been hacked. However, over to Der Cremen from Datalogix—*"not having up-to-date software is like leaving your front door open."* There are additional products available to reinforce your company's Cyber security for companies with budgets of all sizes, do the research and find the right one for your budget.

EXAMPLE: we've had clients who have had their IT systems locked down for a number of days due to employees going onto unsafe websites and their systems requiring repair.

Another example we have come across is criminals hacking phone systems by guessing a mailbox password and making premium calls to Slovenia - it was likely that a default password was never changed on the handset.

5 - Have an incident response plan and practice it.

Cyber attacks don't obey the rules of normal business hours. Who would be alerted if your systems were taken down over the weekend or at 2am on a Tuesday morning? Is there a documented plan in place? And has it been rehearsed? Some of our clients have greatly reduced the extent of cyber incidents because of how effective their incident response plans were.

EXAMPLE: we placed a cyber insurance policy for a client on Tuesday afternoon. At 2am on Wednesday morning their system alerted them of a breach and they immediately enacted an emergency response. They were back up and running from backups later that day with just a few hours of business lost.

A large client in the technological sector had a significant incident on a Friday where their system became infected by malware. They immediately enacted their recovery plan by contacting the Chief Technology Officer. He scrambled his team of 15 IT professionals and they worked on over a weekend - the system was back up and running for Monday morning.

Risk Management Newsletter

The below are a sample of matters advised to us from firms of all sizes across a range of industries. We share updates on our LinkedIn and Twitter pages to educate our clients, feel free to subscribe:

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

Risk transfer is the final step in a comprehensive risk management programme; it is a safety net in the event of your cyber security procedures failing. The most cost-effective way to do this is by purchasing a Cyber Insurance policy.

O'Leary Insurances specialise in placing bespoke Cyber and IT insurance for clients across a number of industries, including:

- **charities**
- **data processors**
- **healthcare**
- **legal firms**
- **construction**
- **financial services**
- **IT / tech**

The average premium our client's pay for a comprehensive tailored Cyber policy is just over €1,500. For most firms, a proposal form should take no more than 5 minutes to complete.

If you wish to discuss further please contact us.

For new clients please contact Brian O'Mara — bomara@oli.ie or 021 453 6860.

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 or risk management advice.

Thank you for reading.