Volume 5, Issue 1 | Quarter 1 2020

Risk Management Newsletter

Identity theft - a growing threat

Happy New Year from all at O'Leary Insurances, and welcome to our first Risk Management Newsletter of 2020. Thank you for continuing to read our content - a special thanks to those hardy souls that have been with us for five years now!

We start the year as we mean to go on, with original content on an emerging area of risk to Irish companies.

Over the past 12 months a number of our clients have received solicitors letters claiming that the company in question had been hacked, and as a result their customers has been defrauded out of money. Even more worrying is that there can be merit to these allegations.

On the following pages we go through a live example of such an incident, where the sums involved are eye-watering.

We have also gathered suggestions from industry experts on how best to prevent this happening to your business. To do so we look at the problem from a Cyber security perspective, as well as considering how best to protect your company from a legal perspective.

This is an important topic so it is the sole focus of this quarter's newsletter.

In this issue:

If there is anything you would like us to look at in future newsletters please let us know - cyber@oli.ie.

Identity theft and cyber crime

What happens when your client loses their own money, but your company is accused of being at fault?

This is recommended reading if clients, suppliers or third parties transfer money to your business. It is in direct response to a new type of exposure that has affected a number of our clients.

The story behind the loss

In May of last year, a solicitors' firm was hacked. The hackers perused their emails and sent 'chaser' emails to anyone owing the firm money.

> *"Email has all the trappings of how we "speak" virtually to our contacts, from introductions ("Dear valued customer"), to signoffs ("Best wishes, Dave"). That's a goldmine for any attacker who wants a foolproof way of impersonating someone and copy your style and email writing tone. From a business point of view, an email account will have contact details for clients and colleagues ready to hand…the attacker is no longer just impersonating you – as far as the email proves, they are you. And you, as the victim might not even realise you've been compromised right away."* - **Brian Honan,**

The firm included a disclaimer under their email signatures stating that they will never send their bank account details by email. The hackers simply removed the disclaimer from these emails, while simultaneously attaching their own bank account details. These emails looked legitimate to clients of the firm as they came from their email address.
Two clients fell for the fraud and transferred money to the criminals. The total amount lost was well over €300,000 - none of which has been recovered. Other clients have experienced similar losses, we have seen separate claims for between €6,000 and €49,000.

This loss would not have happened were the firm not hacked - Proximate Cause is the legal term. In each instance, once it had been established that the firm was hacked and not their client, the individuals looked to take a claim against them.

The conundrum

Accounts departments in most companies know to carry out verification procedures when transferring monies to new accounts, such as picking up the phone to the person you deal with normally to ensure an email is genuine (dual verification). However the average person on the street will not carry out these procedures.

While having an email disclaimer is a positive step, it relies on your clients paying attention. You can put it in **bold**, **red**, or even electric pink - if it's not on the next email they receive from someone pretending to be you, there's a good chance it will be forgotten about.

There is a Cyber Security adage which classifies two types of companies - those that have been hacked, and those that don't yet know they have been hacked. So if we accept that there is a good chance that you can be hacked, but also that your clients are a soft target, how is a company to protect itself? You cannot simply stop taking money from customers or suppliers!

The Cyber security solutions

Prevention is better than cure, so the first step is for a company to review it's own security levels. Brian Honan is one of Europe's foremost Infosec experts. He points out that email security settings can often be lacking.

"In my experience, many companies just use cloud-based email with default settings.

Instead, they should tailor the level of security to their risk. The potential impact from true business email compromise is so damaging that there is a strong argument for making companies focus attention on protecting their email above all other systems. There are plenty of security controls to help do this, from two-factor authentication to data loss prevention, and security awareness training. An attacker only has to get lucky once, as the old security saying goes. And if one finds their way in, you might as well switch off the lights on your way out."

Education is also important - *"attackers are adept at exploiting our natural curiosity, desire to be helpful, love of a good bargain, and even our time constraints to persuade us to click"* according to Honan.

Will O'Brien, Director of PWC's Risk Consulting department, concurs. *"Organisations need to examine their business culture, and their organisational procedures, policies and structures. Many improvements that make the organisation work more efficiently and effectively will also help secure the business against cybercrime."*

Ricky Kelly, co-lead of Ronan Daly Jermyn's Cyber and Data Protection Group, feels that *"it is imperative that companies implement technical mechanisms to prevent and detect compromises as soon as they occur. There are various technologies and services available to assist with this but technical measures alone will not offer 100% protection. They must be supported by various strict and well implemented policies and processes.*

An example of those policies includes a Password Management Policy and Acceptable Use Policies. The Password Management Policy will ensure that the passwords being utilised are sufficiently complex, are regularly replaced and are not used across various other services. Acceptable Use Policies should, amongst others, ensure that good practices are being observed and the security of firm equipment. Criminals are continuously searching for new and imaginative ways of relieving individuals and organisations of their information, assets and funds. It is imperative that companies stay alert and undertake regular monitoring and updating of their systems, processes and policies. When the inevitable happens companies should have a well-rehearsed, clear and accessible incident response protocol in place. Where a successful business email compromise has occurred it is likely to also have resulted in a Personal Data Breach and companies should separately have regard to their obligations under Data Protection laws."

Specific to bank account details, Will O'Brien suggests that companies use more secure communication channels when communicating .

"In situations where it is necessary to use email, a more secure alternative might be to split and forward the account details through two different media channels. This could mean sending the digits for the first half of an IBAN number via email and the latter half by letter, fax, text etc. At this point, the recipient should contact their solicitor to verify the authenticity of both communication media channels used, to verbally confirm both of the following:

- *The account details.*
- *The reason for the transfer.*

The recipient should use the telephone number listed for the solicitor on the Law Society website, or other such number that is personally known to the sender or publicly listed" - **William O'Brien, PWC**

The legal solution

To take this further, we asked what measures a company can take to protect their position, in terms of how they correspond with their clients.

Companies *"should issue detailed engagement letters together with their terms of business at the earliest opportunity. Those engagement letters must be issued by post on the companies headed note paper, be signed, provide the company bank details (if only for receiving payment of its own invoices) and very clearly outline that any request, particularly requests received by email, to change the bank or payment details should be treated as a fraudulent request. It should further set out that, in the event of any such request, the client is required to check with the partner / director of the company (with whom they regularly correspond) by phone before executing any payment. Finally, the company should disclaim any loss incurring as a result of a failure to comply with its terms of business or fraud.*

Where a company is sharing its payment details at any time, other than by its engagement letter and including with clients or third parties, for the purpose of obtaining funds it should again only do so by sending the details on the company's headed note paper and require (in the same document) the recipient, before making any payment, to contact a partner or finance department within the company to reconfirm the details over the phone." - **Ricky Kelly, Ronan Daly Jermyn**

We include a summary of the recommendations on the following page ——————————>

Summary of recommendations

Cyber security

1) Review your security levels
2) Educate staff
3) Examine your business culture, including IT policies and procedures

Electronic fund transfers

1) Consider sending details by two different communication channels
2) Recipient should verify the communications are genuine (dual verification)

Protect the company's position

1) Update engagement letters or contracts with third parties
   i) Include warning about change of details by email being interpreted as a fraudulent request
   ii) Include a disclaimer around losses to third parties who do not comply with your terms

Thank you to our contributors:

Brian Honan, BH Consulting Brian.Honan@bhconsulting.ie
Will O'Brien, PWC will.obrien@pwc.com
Ricky Kelly, Ronan Daly Jermyn ricky.kelly@rdj.ie

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.

Manufacturer

The company received an email which they believed to be from a regular supplier advising to update bank details. They failed to carry out dual verification and lost €75,000 as a result.

Nursing home

The owner was carrying out construction works on a new site. While making a number of payments at one time, they accidentally authorised a fraudulent one to a supplier and lost €60,000. Again, dual verification was not carried out.

Technology

Criminals carried out a distributed denial of service (DDoS) attack which overloaded the company server. It resulted in prolonged downtime and complaints from many of their customers, resulting in loss of clients and reputational damage.

Office	Contact	Phone	Email
Cork	Brian O'Mara	021 453 6860	bomara@oli.ie
Dublin	Robert O'Leary	01 663 0618	roleary@olid.ie
Galway	Angela Rossborough	091 778 677	arossborough@olg.ie
Waterford	Laura Elliot	051 309 130	lelliott@oliw.ie

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 eight 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, building 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.