Volume 1, Issue 1

Quarter 1 2016

Risk Management Newsletter

Cyber Crime Edition

Welcome to the first edition of our Cyber Newsletter

Here we bring together information on cyber security and privacy legislation, without the use of confusing jargon. In this issue, we focus on the growing problem of cyber crime.

Introduction : The Rise of Cybercrime

As Ireland's largest independent insurance broker, we have an unrivalled overview of what is happening to Irish companies of all sizes and across a range of industries. Below are **real-life, Irish examples** from our own clients.

Retailer

Our client pays their overseas supplier monthly by electronic transfer. They received an email from their 'supplier' chasing for payment. The client replied confirming that the payment had been sent, again the supplier advised it was not received. After discussion they agreed to resend the payment to a new bank account. It was subsequently discovered—after the transfer—that the email from the supplier chasing payment was not from them at all. Thus far the monies—a five figure sum - have not been recoverable.

We have also seen similar incidents with multiple **solicitor** clients suffering 5-figure losses. Anyone with significant amount of client funds are high value targets—accountants, fund managers, insurance brokers and estate agents would also fall into this category.

CYBER CRIME

involves criminals—be they individuals or, as is quite common nowadays, syndicates—extorting money from innocent individuals or companies. They have a multitude of ways of doing this and are becoming more sophisticated all the time. Globally cybercrime is now on a par with, and quickly passing out, the illegal international drugs trade. In the UK, cybercrime is now officially the most common criminal offence. Think about that. Clever criminals don't rob houses anymore; from the comfort of their own homes, they trick people out

Accountant

A sole trader accountant received what appeared to be an authentic invoice. Upon opening a link his system was encrypted (locked down). His business was shut out for 3 days while an IT security company resolved the issue. In that time he almost missed a VAT return for a client. On top of the lost productivity, the whole ordeal cost him a considerable sum of money to get back up and running.

The methods being deployed by criminals are becoming so sophisticated that it is becoming difficult to establish whether correspondence is legitimate or fraudulent. On the next page you will find risk management tips from an IT expert.

O'Leary Insurances were delighted to take part in one of Ireland's most popular podcast's for professionals, The Firm, on the topic of Cyber Crime. To listen please click on this link.

About The Firm Podcast - Leading Irish Law Firm, Clarke Jeffers Solicitors interview experts in various areas of law and discuss key topics with a view to providing practical and useful legal information to individuals, companies and advisors alike. Presented in a user friendly, uncomplicated and sometimes light hearted manner. "The Firm" provides practical legal information, hints and tips accessible while on the move and regardless of location.

Risk Management Newsletter

It's not just large companies experiencing cyber crime; the SME sector is targeted by criminals due to the perception that these companies have fewer resources to devote to IT security. We spoke with **Der Cremen, Operations Director of IT specialist Datalogix** to discuss risk management.

5 Ways Small & Medium Sized Businesses can protect themselves from Cyber Attacks

Cyber attacks. We're all hearing about them; we read about them daily and many of us have experienced them. Every day, they become a starker reality for all businesses and organizations – no matter the industry or size. While government, business leaders, and the media have been saying that cyber-attacks are no longer a question of *if,* but *when,* the clamour isn't enough to minimize the harsh effects of these threats. Unfortunately for most, companies won't know they've been hacked until it's too late.

1. Understand the evolving risks.

Cybersecurity preparedness starts with having a complete understanding of the internal and external vulnerabilities that can affect any business, how hackers can gain entry including their different methods and motives, and how to identify points of weakness. Learn the different types of cyber fraud schemes and common threats – everything from phishing and spoofing scams, social engineering, malware, systems hacking, pharming, and everything in between.

2. Develop a security policy that is ingrained into corporate culture.

Defining protocols to abide by is critical, but in order to be effective, the policy must permeate throughout every process, every decision, and the whole mentality of the organization – squarely embedded into its overall business strategy and how each employee operates. After all, your employees are the gatekeepers of your company's information, making them the first line of defence against corporate account takeover. Educate your employees about the warning signs, safe practices, and responses to a suspected takeover. Make sure they use complex, unique passwords and maintain a "clean desk environment" where personal and confidential information aren't exposed.

3. Pick up the phone.

Verify financial requests and confirm details by phone instead of relying on email to initiate or complete any financial transaction – whether you are dealing with your bank, vendors, clients, or employees. Use a two-step verification process to add another layer of security to approving outgoing funds – it will help protect you from a loss.

4. Keep your software up to date.

Don't delay updating your anti-virus software or other security applications. Up to date software will help you guard against the latest threats and keep your infrastructure secure.

5. Have an incident response plan and practice it.

Just like a fire drill, having a plan of action for responding to a cyber incident is crucial. Even more important, it should be practiced so that all your employees know exactly what to do in the event of a breach.

DataLogiX
IT Solution Specialists

are an IT specialist solutions company providing services to all business sectors from SMEs to multi-national organisations. With a combined experience of over 40 years in the IT industry they specialise in the design, implementation and support of IT solutions for our clients. With vast experience and extensive knowledge of the IT industry combined with strategic technology partnerships, they provide the services clients need to improve their overall business efficiency and effectiveness.

P: 021 4357905¦ E: Info@datalogix.ie ¦ W: http://www.datalogix.ie/

Risk Management Newsletter

What rights do customers have when money is fraudulently taken from them by criminals? Who has responsibility for the funds—is it the bank, the credit card issuer or the customer themselves? We asked **Gary Matthews of Gary Matthews Solicitors to discuss.**

With the advent of technological innovation and, more specifically and recently, the internet, there has been a growing need for and development of electronic fund transfer (EFT) payment systems. EFT's are regarded as the third age of payment. It is increasingly recognised that large-scale technology is a two-edged sword: on the one hand, it has the potential for creating new opportunities and solutions to current problems, however, on the other hand, left unattended, it may create new problems.

> *"The customer may nevertheless be liable...where the customer's negligence enabled a sophisticated 'electronic thief' or 'pirate' to obtain information"*

A credit card holder is liable for all transactions that have taken place before notification of a loss if they have acted with extreme negligence. Although no piece of Irish legislation specifically contains a definition of the concept of 'extreme negligence', this leads one to rely on case-law to provide principles and examples of extreme negligence. In relation to EFT it determines that, for instance, a holder acts extremely negligently when they record their personal code in any easily recognisable form, in particular on the electronic payment instrument or on any item that they keep or carry with the instrument and also when they do not notify the issuer without undue delay after becoming aware of the loss or theft of the instrument.

Customer's Liability for Unauthorised Consumer-Activated Fund Transfer: In principle a customer is not liable in the absence of a proper authentication of the security agreed upon with the bank. The customer may nevertheless be liable in the absence of such proper authentication where the customer's negligence enabled a sophisticated 'electronic thief' or 'pirate' to obtain information that facilitated the bypassing of the security procedure in the initiation of the unauthorised payment order. However, where the unauthorised payment order has been properly authenticated, in the absence of fault by the bank, there may be no common law grounds to fasten liability on the bank; the customer is bound by the properly authenticated payment order regardless of whether or not he has been negligent.

Nevertheless, the customer's negligence may become relevant in situations where the bank has been negligent too. In fact, in addition to the degree of adequacy or reasonableness of the security procedures implemented by the bank, namely the standard of care the bank is required to meet, the question of the relevance of the customer's negligence, where the bank was negligent too, remains unclear. Thus, even where the unauthorised payment order has been properly authenticated, where both the customer and the bank were at fault, a question arises as to how the loss is to be apportioned. The question is whether the loss is to be apportioned between the bank and the customer according to their respective degree of fault, whether the loss is nevertheless allocated to one of the parties, or whether an elusive search for the party primarily responsible for the proximate or immediate cause to the loss should be launched. Neither legislation nor case law has provided a definitive answer to this; instead each case will turn on its own set of facts.

GaryMatthews SOLICITORS

This is an edited excerpt from Gary Matthews Solicitors' article on *"Electronic Fund Transfer Payments—The Allocation of Liability for Misappropriated or Mistaken payment"*. The full article can be viewed by clicking here.

P: 01 903 6250 ¦ E: info@gary.ie ¦ W: www.gary.ie

THANK YOU FOR READING

Cyber Insurance - why should you consider it?

The environment we operate in has changed significantly in recent years. We have a reliance on technology, and a duty to protect our clients' data. EU legislation is changing with formal punishments to be meted out for non-compliance with regulations from 2018.

Cyber Insurance is the safety net if your risk management measures fail, it can remove a lot of this risk off your company's balance sheet.

How much does it cost and how can I get a quote?

Pricing starts in the hundreds of Euros and is dependent on firm size and nature of your activities. To obtain a quote is very straightforward, for most firms all that we require is some very basic information. Please speak with your contact in O'Leary Insurances or else contact Brian O'Mara (021 453 6860 or 083 842 4087 / email—bomara@oli.ie), to discuss further.

Why O'Leary Insurances?

You need peace of mind that your insurance policy will protect your firm in the event of a claim being made. No one size fits all. We have carried out an extensive review of the market and are able to tailor solutions to your needs. There are many "Cyber" insurance products available; these range from policies which offer basic cover for malicious hacks, to the most comprehensive products which:

- get to the root of the problem—be it accidental or malicious - and prevent it from getting any worse
- cover the cost of the loss as soon as it has been established
- cover the cost of notifying clients and employees
- deal with subsequent claims or regulatory actions.

About O'Leary Insurances

Insurance Brokers & Consultants, Est. 1961

From an initial complement of three staff in 1961, Archie O'Leary, now Chairman of O'Leary Insurances, has successfully overseen the growth and development of 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.