Volume 5, Issue 3

Quarter 3 2020

Risk Management Newsletter

State of the Nation

In this edition of our newsletter, we examine trends being seen across Ireland with respect to GDPR and also hear what the Gardaí are experiencing relating to cyber crime. Our clients have also experienced a marked increase in Cyber Crime attacks in recent weeks—we include details on the last page.

GDPR update

In February German privacy regulators criticised Ireland's Data Protection Commissioner (DPC), Helen Dixon, for being slow to make decisions regarding fines. However, the Irish DPC, Helen Dixon, has always been clear that she wants any fines to be as watertight as possible, in order to mitigate against potential appeals.

Ikea's Cookie Consent not OK

We have all become used to pop-up messages about 'cookies' on websites. Their importance was highlighted recently when Spain's Data Protection Authority fined IKEA €10,000 due to installing cookies without receiving consent.

And in May we had our first Irish GDPR fine, against Tusla. The child and state agency were fined €75,000 with respect to three individual complaints. One complaint related to Tusla accidentally disclosing the contact and location data of a mother and child victim to an alleged abuser.

There are also other potential fines in the pipeline including one against Twitter; we expect to be looking at these in more detail in the not-too-distant future.

WhatsApp and employee use

We attended an interesting seminar in February, see pages 2-3. One interesting point raised by Deirdre Crowley of Matheson related to employees using WhatsApp, for example using group chat to swap shifts. It was noted how such groups can quickly shift towards inappropriate content, over which an employer has little control. However, UK legal advice is that the employer as Data Controller is legally responsible for such chats, which implies a need for strict company procedures.

In this issue:

State of the Nation

Detective Chief Superintendent Patrick Lordan of the Garda National Economic Crime Bureau (Financial Intelligence Unit) provided fascinating insights into what his unit have been seeing regarding GDPR and Cyber Crime. He was speaking at a seminar organised by Matheson & Nathans Trust.

Cyber Crime

Supt. Lordan firstly distinguished between cyber crime (denial of service attacks, data theft) and cyber *enabled* crime - another name for business email compromise. His unit dealt with over €10m of losses from the latter over the previous 12 months.

Irish businesses have become more aware of risk management in recent years (e.g. carrying out dual verification for bank details), but cyber criminals are continually changing their tactics to defraud companies. Below is one example discussed in the seminar:

- ⇒ Cyber criminals hack Company A's systems
- ⇒ They identify third parties that are due to transfer money to Company A, such as Company B.
- ⇒ The criminals call Company B advising they need to update their bank account details.
- ⇒ The suspecting employee hangs up the phone. They email Company A to tell them what happened. This is exactly what the cyber criminal wants to happen.
- ⇒ The criminal replies to the employee in Company B, pretending to be Company A, and reassuring the employee that it was a legitimate request. They would be able to use the same type of tone that the relevant employee would use, having monitored their emails.

In one such loss criminals waited three months for the largest possible invoice and when they struck they cost the company in question nearly €500,000. (We recently spoke with a company that came within seconds of losing even more than this). The average loss the Gardaí have seen is around €35,000.

One method suggested to reduce the likelihood of such losses is to avail of the IBAN checker. It's free and will tell you the location of the bank. If you are being asked to transfer funds to a client in Galway and their bank account is being updated to Cork, or overseas, it raises a flag.

Supt. Lordan suggested that categorising some of the incidents he has seen as a 'hack' might be overstating it — sometimes it's simply a matter of guessing weak passwords to gain access to a company's systems. It all comes back to robust security procedures and employee training.

State of the Nation continued
Data Breaches and GDPR

"Organised criminal gangs are coming knocking on your door...and they will succeed."

That was the stark warning from Supt. Lordan to Irish businesses about the data they hold. Even the most basic **data breach** is valuable to criminals — it is "quite easy" to open a bank account with just a name, an email, an address and a forged identity document.

A huge area of security failure is where robust corporate IT systems are let down by poor security and training. For example, is the heating / lighting contractor calling into your office known to you? Rogue or disenchanted employees who steal data for financial gain or due to a grudge are also a huge issue here in Ireland.

Another example given was of a heavily pregnant lady entering a business with a USB of her 'baby scan'. This was a simple technique designed to prey on people's good nature— as soon as the USB was connected it had circumvented much of the IT security measures and infected the company's computer system with malware. Would your employees know to say no?

Regarding **GDPR**, while data protection fines tend to grab the headlines, companies need to be aware of potential costs related to an investigation by the Data Protection Commissioner (DPC). There are examples of companies being told to cease certain activities while investigations are ongoing.

The Gardaí recommend it is much easier to handle a breach when the relevant bank(s) are notified. In one example this led to the DPC & Gardaí being notified within 24 hours and disrupted the criminals who had stolen the data.

Tips to prevent data breaches:

- ✓ Regular employee training and communications to reinforce the message
- ✓ Do not allow USBs access for any member of staff (test USBs on a PC not connected to the network if you have to use them)
- ✓ Update passwords regularly
- ✓ Have a data breach response plan — this is critical for when a breach does happen. And have it printed off and easily accessible in case systems are down!

Cyber security "needs pure education...you need all of your employees working with you" - Supt. Lordan

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.

In our last issue we flagged how 'working from home' may cause increased opportunities for Cyber Criminals. Unfortunately that has proven true for at least two of our clients in recent weeks. It is possible to insure against the losses outlined below, as both of these clients did.

Solicitor— Cyber Crime — April

In April a solicitor client lost a six-figure sum to cyber criminals. The firm were defrauded by fake signatures sent over email—it appears their client's email was hacked and taken over by the criminals. While around half of the funds were eventually recovered, the remainder had to be claimed under the firms Cyber Insurance policy.

Hotel — Cyber Crime — May

In a similar incident to the above, a hotel has lost a large five figure sum. The Financial Controller was tricked into transferring the funds. At this stage we don't have detail on who was hacked and we await confirmation of what, if any, funds can be recovered by the banks involved.

If you wish to discuss further with us please contact any of the below.

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	Maria Murphy	091 778 677	MMurphy@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 and fifty 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.