Volume 5, Issue 4

Quarter 4 2020

Risk Management Newsletter

Taking stock

In our final newsletter of 2020 we go into more detail on some of the key cyber security issues that we have seen throughout the year. This includes ransomware, data breach and cyber crime updates. As usual we include examples of what we have seen across our client base.

Ransomware on the rise

When we first started this newsletter back in 2015 ransomware demands were typically fairly low. We had clients who had been locked out of their systems by criminals and who had no choice but to pay the ransom, with payments of €1,000-3,000 being made. Criminals wanted to make the ransom seem affordable against the cost of setting up files from scratch or incurring costs of IT security experts.

We had seen a trend towards larger ransom requests of €8-15,000 in recent years. However we read with interest a report by US firm Coverware that the average Ransomware payment by companies to criminals is now $111,605 (€94,800)! This is due to a number of high payments as larger firms were forced to pay such ransoms — the median payment is still $44,000 (€37,000). Coverware found that SME's are most likely to be targeted, particularly services firms, although in truth all sectors have experienced such incident which is also our own experience. At the end of the day if you use email, your business is at risk.

CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

O'Leary Insurances are please to have renewed our membership with **Cyber Ireland** for another year. Cyber Ireland is the national cyber security cluster which brings together industry, academia and government. The aim is to enhance our national standing and to position Ireland as a world class cyber security practices, solutions and investment hub.

In August we contributed to the Cyber Ireland's newsletter with a blog piece aimed at busting myths related to Cyber Insurance. The link to that piece is here.

In this issue:

Hidden costs of a Data Breach— IT system repair

There are several potential hidden costs to a data breach. Below we go through an actual example of IT system repair after a seemingly minor incident.

The background

The company became aware that incoming emails of one employee were being forwarded to a hacker. Upon investigation this had been happening for a period of about 14 months. They immediately engaged an IT security consultant to investigate.

The issue was confined to a data breach involving a small number of individuals, all of whom were informed. The Data Protection Commissioner (DPC) was also immediately advised. At the time of writing there has been no punishment from the DPC, and no monetary loss from Cyber Crime.

Locating the source of the breach

The insured engaged IT Security Consultants to investigate and remediate. They found that an employee clicked on a malicious link sent by a phishing email. Clicking this link gave the criminals access to the employees email inbox. They set it up so that all emails received were also forwarded to their email address. The employee in question mainly dealt with sensitive correspondence from clients, so the criminals would have had unrestricted access to this information.

IT system repair

The consultants enacted an upgrade of the IT systems, along with installing Multi-Factor Authentication on email accounts. They also carried out training for all staff, in order to raise awareness and prevent re-occurrence of the incident.

The cost

The company in question has a small number of employees and the number of individuals affected by the breach was low. There was no 'fallout' in terms of punitive measures from the Data Protection Commissioner or claims from those affected.

Yet, the cost for the work carried out by the IT Security Consultants was over €10,000. That is fairly typical in our experience for relatively minor incidents. The company in question was able to avail of their Cyber Insurance policy, which covered the cost after payment of the policy excess. It should be noted that the IT security firm used was the company's choice as they were familiar with their IT systems — the insurer was happy with this.

Cyber Crime—in every crisis there is an opportunity

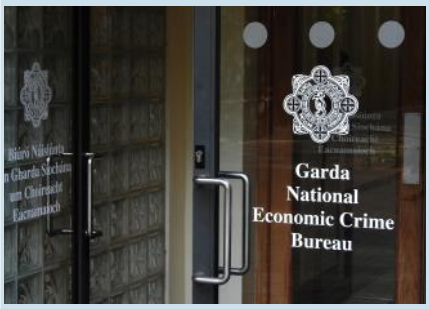
Our July issue included warning from a senior Garda regarding the prevalence of Cyber Crime in Ireland. In August both Interpol and the Gardaí reiterated this message to the general public.

Interpol warned of an "alarming" rate of cyber crime during the Covid-19 pandemic, with criminals using tactics such as impersonating health authorities or government advice in phishing emails. Their release stated that there was a marked increase in ransomware attacks from early April, when more people started working from home.

> *"With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption"* — Interpol

The agency had an expectation that further increases in activity would continue, speculating that *"the potential for increased financial benefit will see cybercriminals continue to ramp up their activities and develop more advanced and sophisticated modi operandi."*

Within a week the Garda Síochána issued a warning related to Invoice Redirect Fraud. It followed on from a Bank of Ireland commercial customer losing €2.1m to cyber criminals.



> *"The Dublin based business was making a payment to a UK based business when they received an email purporting to be from this UK business asking them to send the payment to a new bank account number. The Irish business did their due diligence and contacted the number supplied in the email and the person who answered the phone confirmed that all was correct. The money was then sent to the new bank account which transpired to be in Hong Kong. It is now known that the phone number contained in the email was also incorrect and the business was actually talking to the fraudster."*

Regular readers will know that the mistake here was to rely on the phone number within the email. Instead they should have used the number they have on file for this business, to verify the bank details.

Thankfully the Garda National Economic Crime Bureau was promptly advised and the funds have been frozen in a bank account in Hong Kong. Unfortunately not all victims of Cyber Crime are so lucky.

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.

Hotel — IT security costs — May

We referenced this loss in our last newsletter. The amount lost to cyber crime was over €90,000, however thankfully most has since been recovered. Over €5,000 will not be is lost and the same amount is owed in IT security costs. The claim in question is being dealt with by a Cyber Insurance policy.

Financial services—Cyber Crime—February

Our client was unaware that they had been hacked, with the hackers using their email account to authorise a transfer of around €800,000. The company were speaking with their bank by phone when the bank raised that they were ready to make the transfer, at which stage the fraud was discovered.

Solicitor—Data Breach & Cyber Crime—September

The company in question were hacked. Their bank prevented a €100,000 transfer to criminals. Upon investigation it transpired that potentially sensitive data had been compromised during the hack. Investigations are ongoing.

f 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	Joanna O'Donnell	091 454 031	jodonnell@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.