Volume 6, Issue 2

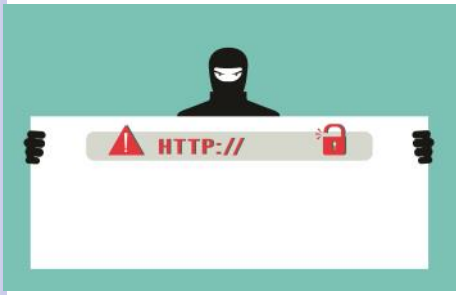
Risk Management Newsletter April 2021

It has been a busy three months since our last issue. In this issue we include examples of websites being duplicated, a piece on threat monitoring and also some explanation regarding Ransomware, along with the usual examples of what we have seen amongst our client base nationwide in recent months.

Corporate Identity Theft

In January we were contacted by a client whose website had been duplicated by Cyber Criminals. Their website had experienced unexpected sharp increase in site visits from overseas. It transpired that cyber criminals had copied over whole sections of the website, even going so far as to replicate some employee profiles onto their new site. The only change was a new firm name and contact number.

In this issue:



One potential aim of Corporate Identity Theft such as this is to trick unsuspecting third parties into dealing with fraudsters, and ultimately to pay money to them for a service that they have no intention of providing. When contacted by this fake company, members of the public may check out their website to ascertain if they are genuine—the idea is that a professional looking site implies authenticity.

Thankfully the company became aware of this and the website was taken down. We received a good tip from the Cyber Insurer who was looking after the incident, as outlined below:

RISK PREVENTION TIP:

To reduce the likelihood of Corporate Identity Theft of your website, speak with your website provider about inserting code within the site which prevents users from copying and pasting text from the site. This simple step may encourage criminals to go after an easier target elsewhere.

Food for thought

UCD fined under GDPR

UCD were fined €70,000 under GDPR in December. This related to a small number of log-in details related to email accounts being posted online. To make matters worse, it took UCD 13 days to notify the Data Protection Commissioner (DPC) of the breach after they became aware.

Under GDPR, the DPC and those affected must be notified without undue delay but not later than 72 hours. The college also had to undergo a "programme of action" as stipulated, which no doubt would have added to the overall cost of this incident.

Separately, Queens University Belfast advised that they had come under Cyber attack in March— as yet they have advised of no data breach.

LinkedIn Upgrade

This quarter we are highlighting the great work of Liam Lynch, of L2 Cyber Security Solutions.

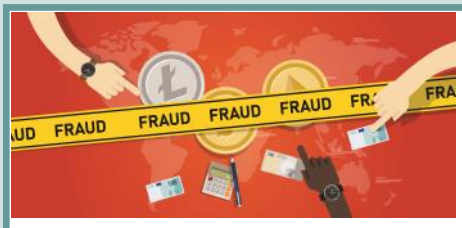
Liam specialises in Cyber Security and Data Protection Training and Consulting. He rather generously uploads concise and easy-to-understand 'Weekend Wisdom' videos every Friday, featuring a fairly spectacular Tipperary backdrop.

Recent topics have included how innocent people become Money Mules for cyber criminals, an explanation of Typosquatting and why NOT to change passwords regularly (more to follow on that in Q3!).

We encourage people to keep abreast of Cyber Security updates, and this is a great place to start.

Liam's LinkedIn is: *Liam Lynch | LinkedIn*

All of the previous videos are available on https://www.L2CyberSecurity.com/blog



Cryptocurrency Con

Gardaí advised in March that a Corkonian was conned out of **€30,000** by cyber criminals. Sergeant Brian Mc Sweeney explained further:

"The injured party was contacted about an investment opportunity involving cryptocurrency. The scammers offered the person a chance to invest, with a promise of a high return. The injured party gave bank details for the deposit of the profits from the investment. As a result, the details were used to withdraw over €30,000 from the account."

Gardaí figures show that investment fraud increased by 120% in the past year, but the figure is likely higher—many such instances go underreported due to embarrassment.

Threat Monitoring—the new first line of defence

We have seen first hand in recent months the benefit of Threat Monitoring for our clients. Here we look at the new first line of defence in reducing the likelihood of an IT security incident to your company.

What is Threat Monitoring?

This involves a company scanning a company's network to try to discover any potential vulnerabilities. The aim is to identify same before anyone else—namely a cyber criminal - does.

Is it expensive to hire these firms?

The cost of this service is now being covered by the better Cyber Insurance providers on the market. As such the cost is built into the insurance premium.

Is it not a case of "you get what you pay for" with these policies—if my premium is low, the service must be limited?

To answer this, first put yourself in an insurers shoes; Ransomware, phishing attempts and cyber crime are all on the rise and becoming very hard to manage. The benefit of Threat Monitoring for insurers is that they greatly reduce the likelihood of an incident affecting their clients in the first place. This helps to reduce the number of claims, which in turn helps to keep premiums down.

To give you an idea of scale, the top insurer in this space has 75 such experts working for their policyholders.

Can you give me an example of Threat Monitoring in action?

Below is an example we received in March for a Cyber Insurance policyholder.

"Following a recent scan, we have identified that the following IP address may be vulnerable to attack through an exposed Remote Desktop Protocol (RDP) port…given that cyber criminals are actively hunting for this particular vulnerability and will often use it to deploy ransomware on a network and then seek to extort you, we wanted to highlight this potential issue so they can investigate it. ***Please get in contact with your end client to investigate with their IT team."***

Within three hours the policyholder had confirmed back to us that the issue had been resolved—a good result all round!

Ransomware is everywhere

Ransomware has been around for some time, but recently there are more targeted attacks and higher demands on victims.

Cyber Insurers have been flagging Ransomware as a huge area of claims over the past 6-12 months. This confused us as our data shows that our clients have seen a reduction in Ransomware issues over the past five years. In this piece we delve a bit deeper into what is truly a global issue.

What is Ransomware?

A malicious software that encrypts your data. Criminals usually threaten to destroy or release the data unless a ransom is paid.

Ransomware accounted for around $325m of damages to organisation back in 2015. Various reports estimate the 2020 equivalent figure to be close to $20bn. It is broadly acknowledged by the likes of Interpol that the move to working from home has led to an increase in attacks, with IT networks deemed more vulnerable and employee error also more likely.

Criminals are focused on finding ways to encrypt IT systems as well as a company's back-ups, rendering the victim truly helpless and contributing to the higher demands. Back in 2015, a typical ransom request to our clients would have been around €1-2,000. One insurer we spoke with advised that a typical Ransomware claim payment is now over $1m. In March it was reported that Computer giant Acer has been the victim of a Ransomware attack with a demand of $50m.

On top of that, the company that has been the victim of the Ransomware attack is down on average 8-10 working days, which results in further losses and claim payments.

Insurance payments & ethics

One issue that has raised its head is whether paying Ransomware demands via Cyber Insurance is ethical, or is it contributing to higher ransom demands. Insurers would point out that not all companies have appropriate cover for such incidents. For those that do, the ransom is only paid where there is no viable alternative such as working from back-ups.

Certain insurers are now tailoring their policies to limit the Ransomware cover to what the company would have been able to pay in the absence of insurance. This serves two purposes; insurers combat accusations of contributing to Ransomware inflation, and they can also better manage their own risk.

Going back to our comments in paragraph one above, maybe our clients have been lucky, or maybe they are well-educated due to reading newsletters such as this. Vigilance is key! If you want to discuss insuring against this threat feel free to contact us.

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.

Agriculture—Cyber Crime

A company was purchasing a piece of agricultural equipment from overseas. The vendor had been hacked, and the hackers emailed fraudulent bank details to the company. Over €70,000 was lost and the funds could not be recovered by the time it was realised what had happened.

Solicitor— Data Breach

The firm was hacked. The criminals drafted an email including an alleged link to a VAT invoice. The idea would have been that of the circa 500 people contacted, a small number would be awaiting such an invoice and would follow the link. The link was malicious and may have given access to the recipients own system. At this stage it is being investigated and we are hoping no-one fell victim to the scam.

If you have further questions on anything in this newsletter please let us know— details below.

Office	Contact	Phone	Email
Cork	Brian O'Mara	021 453 6860	bomara@oli.ie
Dublin	Brian McDonnell	01 660 8211	bmcdonnell@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

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. The O'Leary Insurances group of companies are all wholly owned subsidiaries of Brown & Brown, Inc. one of the largest and most respected independent insurance intermediaries in the United States of America (NYSE BRO). You can find out more about us at www.olearyinsurances.ie".

With over two hundred and fifty insurance professionals 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.