Volume 6, Issue 3

# Risk Management Newsletter July 2021

Our April issue was unfortunately quite prescient, featuring as it did a piece entitled *"Ransomware on the Rise"*. What has since befallen our Health Service Executive is appalling, and the cost to human life is yet to be quantified.

## Ransomware has been around for some time


The HSE cyber-attack has been harrowing for many of those affected. It confirmed that cyber-criminals don't have morals, and they don't discriminate. It matters little that the criminals did not intend nor want to take down a national healthcare framework; even though they released the encryption key, it has still caused untold issues for the HSE and for many of it's patients.

This is far from a one-off; for proof just look at some of the companies that have also been affected in recent months:

⇒ **CNA** insurance were widely reported to have paid $40m in March to regain control of it's network.

⇒ The **National College of Ireland** was the victim of such an attach in early April.

⇒ Irish-owned manufacturer **PCH** fell victim to the same hacking group as the HSE. It had it's data published on the darknet after refusing to pay the ransom.

⇒ **JRP**, the world's largest meat processor who spend over $200m annually on IT, paid an $11m ransom in June after a number of their plants globally were shut down due to ransomware.

Just a few days prior to the HSE cyber-attack, a global coalition of nearly 50 technology companies and law enforcement bodies had joined forces to draft 50 recommendations to governments, saying that *"ransomware has become a serious national security threat and public health and safety concern"*.

There is plenty of more detailed comment on Ransomware available elsewhere—for the remainder of this newsletter we will go back to what we do best, providing risk management advice. This quarter we focus on Ransomware and passwords.

**In this issue:**

# Food for thought

## Hi-tech House Tour exposes personal data

In the absence of house viewings, many of us have availed of virtual tours in the past year or so. As reported by BBC News (external link), a UK-based estate agent got into a bit of hot water when it turned out that such a tour included personal data of the vendor.

This included:

- ⇒ A share dividend cheque
- ⇒ An insurance policy document
- ⇒ An invoice
- ⇒ Family photos which were not blurred out
- ⇒ The names of the pets (possible passwords!)

The link contains some wise words from Carissa Veliz, author of Privacy is power - *"if we can't keep (personal data) safe, we shouldn't be collecting it in the first place".*

## LinkedIn Upgrade

In this issue we are highlighting the great work of Brian Honan.

Brian is recognised as a cyber-security expert at both an Irish and an International level. He previously advised Europol on cyber-security and was inducted to the Infosecurity Europe Hall of Fame back in 2016.

If Brian looks familiar it is because he is often featured on national and international news channels, and he contributes to many publications—including this newsletter in prior years.

We encourage people to keep abreast of Cyber Security updates, and Brian Honan's LinkedIn or Twitter are a great place to start.

Brian's LinkedIn is here: click link

His Twitter is @BrianHonan

## GDPR—€90,000 fine

The Irish Credit Bureau DAC became the first recipient of a GDPR fine from the Irish Data Protection Commissioner this calendar year. It related to just over 15,000 closed accounts being inaccurately updated on their database, which ultimately changed credit scores for some customers.

Interestingly, while the DPC noted that *"the level of damage suffered by most of those (affected) data subjects was minimal",* she nonetheless found that *"the gravity of the ICB's infringement of Article 25 (1) was severe"*. An initial fine of €220,000 was reduced to €90,000 due to a number of mitigating factors.

## Ransomware is everywhere — *this piece first appeared in our April issue*

**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 organisations 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.

## Ransomware Insurance

We have prepared a quick note that clarifies how a Cyber Insurance policy could respond to a Ransomware attack.

While policy wordings vary from insurer to insurer, below are areas that are insured under most comprehensive Cyber Insurance policies.

- ✓ Crisis response - initial advice from experts
- ✓ IT forensics to discover the source of a system breach
- ✓ Restoring systems either from your back-ups, or if these are not available from scratch
- ✓ Some policies cover lost income to your business as a result of the attack.

If there is no other alternative than to pay the ransom, and if it is believed that the criminals in question will provide the decryption key upon payment of same, then the insurer will pay up to the relevant limit within the policy. Traditionally this is the overall policy limit, but we are seeing a trend of insurers limiting cover to the Gross Profit of the company in question, or co-insuring with the client.

If there are claims because personal data has been released due to the ransom not being paid, then the policy will cover costs related to this including:

- ✓ The cost of establishing who has been affected, and to what extent
- ✓ The cost of notifying those affected
- ✓ Credit and/or identity theft monitoring, if required
- ✓ Setting up a call centre for those affected
- ✓ Attending a hearing such as with the Data Protection Commissioner
- ✓ Defence and court attendance costs and privacy related liability claims

If you have any queries on this please let us know – cyber@oli.ie.

## Why you should NOT change your password frequently.

Guest piece by Liam Lynch

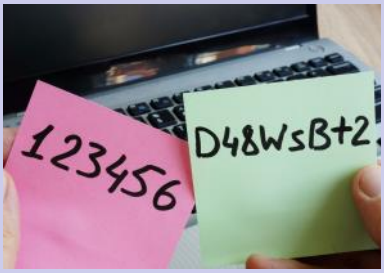
**In the last issue we referenced Liam Lynch's short video advising that we need to re-think changing passwords. We couldn't let that go unchallenged!**


We have been told for a long time that you must change your passwords regularly in case they are cracked by some hackers and used without your knowledge. This came from a time when the internet was much less secure and passwords could easily be cracked with specific software.

In the last 5-10 years, communications on the internet have become much more secure with the data being sent across it being encrypted. It is also much more difficult for hackers to crack modern password security measures. Most people take the easy option when it comes to having to change passwords on a regular basis. They will generally have a number somewhere in the password which they add 1 to it every time they are required to change it.

Hackers are getting access to old email address/password details from sites that they have breached and downloaded this information. If the passwords were short or not protected very well, then once they crack the passwords, they will use software that will take the email and password and try to sign-in to other services like Microsoft 365, Gmail, Yahoo mail and social media sites. If a password has a number in it, then they will keep adding 1 to it and trying again and again until they find the current password.

The National Institute of Standards and Technology (NIST) were the first of the large industry standards bodies to remove frequent password changes from their requirements in 2017. They now recommend the use of a password manager to create long complex passwords that are unique for every service. NIST also recommend the use of two-factor or multi-factor authentication.




The only time you should change a password, is if you suspect it has been compromised and it should then be changed completely across all sites on which it is used. Password managers make this extremely easy.

**About the author: Liam Lynch founded L2 Cyber Security Solution in 2016. Liam has over 30 year's experience working in the IT sector, and we featured Liam's weekend wisdom videos in our last issue.**

**His company website is [L2 Cyber Security Solutions | Cyber Security & GDPR Training/Consulting.]**

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.***

**Engineer—Cyber Crime**

An engineering firm had been hacked. The insurance invoices from their broker were intercepted and then manipulated by cyber criminals — the criminals own bank details were inserted in place of the broker's. The firm relied on the fraudulent invoices and lost over € 50,000.

**Solicitor—data breach**

While posting a file to a client, a staff member inadvertently enclosed documents relating to a sensitive matter relating to another client and a third party that they are in dispute with. To complicate matters the recipient of the documents was slow to return them. The firm had to notify the Data Protection Commissioner and those affected.

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

CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

We are the only Insurance Broker member of Cyber Ireland, Ireland's Cyber Security cluster, having joined at it's inception in 2019.

| 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.**