Volume 7, Issue 1

# Cyber Matters Newsletter January 2022

**Happy New Year to all our readers!** We hope you had a good Christmas and wishing you all the very best for the coming year.

We start 2022 with news of a new App aimed at incrementally educating SME's regarding cyber security (page 3). On page 4 we look at where cyber security is going, with a focus on 'Zero trust'. This issue also includes Food for Thought (page 2) and case studies (page 5).

## Webinar : Cyber Security—what are we doing?

In November we took part in a webinar titled 'Cyber Security—what are we doing' This was hosted by it@Cork and also on the panel were representatives from Dell, EY and the Gardaí. The webinar can be viewed here: link to YouTube.


There were several common threads and items covered included the below (with relevant time in brackets):

- Overview of cyber attack trends from the Gardaí, including Spear Phishing and invoice redirect fraud. Also a useful tip on restricting what is put on company websites! (9:00)
- The importance of assessing inventory and security patches (29:45), logging and monitoring (33:17) - the company 'playbook' is key if something goes wrong.
- How cyber attacks are just a numbers game for criminals —they don't discriminate (34:30).

It was acknowledged more than once that there is no silver bullet when it comes to Cyber Security, but instead to start somewhere and build up. Our guest blog aimed at small businesses on page 3 is particularly timely.

**Social Engineering Warning: "Be careful what you are putting onto your website"**
Inspector Martha Francis from the Garda Síochána lists reasons why businesses should put limited personal information on their company website— starts at 11 minutes.

# Food for thought

## Mandatory Ransomware reporting

An interesting development from Australia, with legislation on the way that will compel companies to notify the government when they have become the victims of Ransomware attacks.

Driving this requirement is the reported 60% increase in such attacks in 2021, a need to monitor national security concerns, along with a desire to drive more co-operation between companies and a need to protect the end users. The stated aim is to enhance the governments understanding of the threat and to support small businesses in particular.

There will be a deadline by which incidents must be reported, with penalties for non-compliance. It will be interesting to see if Europe follows suit.

## CyberQuest training programme

In the webinar mentioned on page 1 it was noted how there is a massive global shortage of qualified staff within the Cyber Security sector. Irish-based companies have a huge need for such a skillset.

For recent graduates, those made unemployed by Covid-19 or even those looking for a change in career, it@Cork and Skillnet Ireland are offering a free training programme called CyberQuest.

CyberQuest combines project work with labs and practical remote working. Here is a brief promotional video : it@cork Skillnet Cyberquest Programme - YouTube.

For anyone interested go to https://www.cyberquest.ie/

## Charity data breach

Irish charity Men Overcoming Violence (MOVE) was given a reprimand and a €1,500 fine by the Data Protection Commissioner (DPC) after it self-reported a GDPR breach in February 2020. This related to losing SD cards with up to 120 recorded video counselling sessions, and in which other individuals would have been named by the men in question. Many have queried the need for such sessions to be recorded, on the basis businesses should presume data can be lost or stolen.

While the small size of the fine has raised eyebrows, it is very much in keeping with form for the Irish DPC, They were quoted as saying that any fine should be *"effective, proportionate and dissuasive having regard to the circumstances of each individual case and the turnover of the data controller".*

**Guest piece: Andrea Manning Founder of CyberPie.** CyberPie is an all-in-one security platform and subscription based service for microbusinesses. They have combined security awareness training, simple tools and a library of resources to help business owners build their defences one small task at a time—all in under 5 minutes a week!

## What does the small business need to know when it comes to cybersecurity?

### 60% of small businesses hit by a cybercrime will close down within 6 months

Andrea Manning -CyberPie

Often portrayed with images of hackers in hoodies, cybersecurity is deemed a technical expertise yet the reality for business is that cybersecurity is about 3 things:

- ✓ Prevention
- ✓ Detection
- ✓ Resilience

For the small business this means build up your defences to protect your data and your business. Use tools and tech to alert you if your data has been compromised and finally, have a plan in place to bounce back and recover should the worst happen.

Cybersecurity is a billion dollar industry and growing in line with the exponential rise in cybercrime. Yet the solutions on the market are often feature heavy and not designed to meet the unique needs of the micro-business who make up 90% of Irish businesses. If you're one of the 90% chances are you may not have dedicated IT support, you have limited resources in terms of time, money and technical know-how, and security awareness training is a once off event or still on your to do list.

CyberPie is a new cybersecurity platform that recognises the micro-business is a distinct sector with unique cybersecurity needs. Putting education at the heart of a defensive strategy, the platform delivers Weekly Slices of cybersecurity advice and micro-tasks that take under 5 minutes a week to complete. Using the one-bite-at-a- time approach small firms can build up their defences, access simple cybersecurity tools and resources and benefitting from industry best practice in a way that works for them.

In Cybersecurity we say that security is a process not a product. And the first step is your personal security; an inventory looking at where you might be vulnerable, then systematically checking off each step as you plug the gap. Call it a digital health check.

**Reader offer:** To kick off 2022 CyberPie is offering the first 22 respondents a full digital health audit—which usually costs €195—for €22. LINK

CyberPie is free to sign up. Join today and start building your defences one bite at a time. LINK

## The 'Zero Trust' approach to Cyber Security

No business is impenetrable to cyber attack. The US government have come to realise that by mandating that Federal Government 'advance towards Zero Trust Architecture'. In this piece we look at what that means for private companies.

### What is it?

The main principle behind Zero Trust security is that devices should not be trusted, even if they were previously verified as being safe. It is a mindset change, encouraging organisations to move past believing that they have a safe 'perimeter' within which their IT security is safe. Zero Trust is a reflection that networks now are very different from what they were in the past, with all kinds of devices having access.

Think of a typical household, where previously the totality of the network may have been the internet modem, a computer and a printer. Now this same home network is also accessed by the Internet of Things. Most homes are now connected to at least some of the following: smartphones, tablets, smart TVs or fridges, a smart Assistant such as Alexa. Toilets, light settings, home heating, radios, fish tanks can all be connected to the network...the list goes on!


### If we can't stop a breach, what hope have we?

IBM's professional hacker Charles Henderson put this best— if your aim is to keep a hacker out, you will lose. Instead, businesses should focus on protecting their key data—presume that their systems can be penetrated, and work from there. The aim is to buy yourself time if it does happen, and to contain any attack.

Think of this in practical terms. In a previous issue we reported on a GDPR fine for a hospital where any staff member could access any patients file. A Zero Trust approach would encourage restricted file access, so that patient files are accessible on a need-to-know basis i.e. the relevant medical team.

With Cyber Security continuing to evolve, this is surely not the last time we will hear the term 'Zero Trust' Security.

**The Zero Trust approach—summary**

⇒ Automatically 'distrust' all users of your network

⇒ Require frequent 'affirmations' from all users, to prove they are who they say they are

⇒ Review supply-chain partner access

⇒ Protect critical data

# Risk Management Newsletter

**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 reaHife Irish cases.***

**Estate Agent—Cybercrime**

An employee unknowingly clicked a malicious link on an email. This gave system access to cyber criminals. They manipulated emails and were able to convince the parties to transfer a house deposit to their account. A 'Zero Trust' approach to Cyber Security may have helped here.

**Manufacturer—Ransomware**

A manufacturing facility was the victim of a cyber-attack, with systems encrypted by the criminals. This locked down the facility. A ransom was demanded and the Gardaí were involved. All systems were offline for the duration.

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

**Solicitor —Cybercrime**

The firm was asked to transfer sterling funds to the UK from a legitimate-looking, yet ultimately fraudulent, email. There was no background to the request, yet the transfer was authorised by a staff member. This implies that staff training either did not happen or was not regularly reinforced. The request was for two large six-figure amounts —one of the transfers was eventually recovered.

| Office | Contact | Phone | Email |
|---|---|---|---|
| Cork | Brian O'Mara | 021 453 6860 | bomara@oli.ie |
| Dublin | Carman Devlin | 01 6630604 | cdevlin@olid.ie |
| Galway | Joanna O'Donnell | 091 454 031 | jodonnell@olg.ie |
| Waterford | Fiona Fitzgerald | 051 309 130 | ffitzgerald@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 operating from seven 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.**