

# Cyber Matters Newsletter

## October 2022

Welcome to our final newsletter of the year. We hope you continue to find this of interest.

### Multi-Factor Authentication (MFA) bypass targets over 10,000 companies

MFA has been heralded by the likes of Microsoft and the cybersecurity industry at large, as well as by Cyber Insurers, as a tool that greatly reduces the likelihood of a successful cyber attack. In theory MFA being enabled means that criminals need to have hacked both your phone (usually) and your computer in order to gain access to IT systems. At this stage we are used to it on everything from banking apps to our own office systems.

However, in July it emerged that criminals had found a way around MFA in an attack that targeted over 10,000 companies. The means by which they did this is too technical for this newsletter, but the Microsoft blog is [available here](#) (external link) for anyone interested. However we mention it just as a reminder that there is no silver bullet for cyber security—the best thing any business can do is implement best practice in conjunction with it's IT team or outsourced specialists, combined with constant training / reinforcement to keep all colleagues on their toes.

### Irish firm hacked

The [Journal.ie website](#) (external link) reported that an Irish firm that works on a number of State infrastructure projects was the victim of a cyber attack in July. This appears to be a ransomware attack as no information had been leaked online at the time of publication.

Such attacks are relatively commonplace and happen against firms of all sizes, so much so that the Gardaí Síochána and the Irish National Cyber Security Centre announced in late-August that they had noticed an increased trend of ransomware attacks targeting SME's. Their press statement is [here](#). Turn to page two for a useful free source for decrypting systems after many ransomware attacks —>

### Off topic – updated house rebuild calculator

*The Society of Chartered Surveyors Ireland*

*updated their rebuild calculator in September. To avoid underinsurance, please ensure your Home*



*Insurance is up to date with the most accurate sum insured.*

*The [link is here](#) on the SCSi website (external link).*

**Our Cyber team is 10-strong nationwide — if you would like to speak with us feel free to contact us — our details are on the last page.**

# Food for thought

## Free Ransomware Decryption Tools



No More Ransom is a public-private initiative set up in 2016 and backed by Europol, the Dutch police and a number of IT companies, among others. It offers 136 tools to enable individuals to decrypt their devices in the event of a ransomware attack, without having to resort to paying a ransom to cyber criminals.

This service has helped over 1.5m people thus far. The link to the website is below.

[Hit by ransomware? No More Ransom now offers 136 free tools to rescue your files | Europol \(europa.eu\)](#)

## Ransomware gangs are...just like us?

The Conti cybercrime group is estimated to have made over \$2.7bn from ransomware in just two years, making them one of the most successful such groups in that period.

A recent leak revealed just how normal their operations are. The company itself is structured like any comparably-sized company, with functions such as finance, HR and R&D.

It also has salaried employees, performance reviews, and even an employee of the month bonus. Conti also fines underperforming staff, something thankfully not as commonplace in legitimate companies!

Alarmingly it appeared that some employees were not even aware that they worked for a cybercrime group, instead thinking that they worked for an advertising company.

## Cyber attack causes physical damage



An Iranian steel factory was the victim of a rare occurrence – a cyber attack leading to physical damage. It appears that a hack led to a serious fire at the plant, with an accompanying video being released by the hackers ([available here](#) on BBC.com).

The hackers waited for employees to step away from the machines before releasing hot metal everywhere, which in turn led to a fire. There are very few other examples of similar attacks – one such was an attack on Iranian uranium enrichment facilities in 2010.

O'Leary Insurances Ltd. is regulated by the Central Bank of Ireland.

### Cyber Insurance—premium analysis

It has been well-publicised that premiums for Cyber Insurance have been increasing, so we took a look at our own renewal book to establish what has happened. We also take a look at future premiums expectations.

Premium increases over the past 12 months were proportionately higher for smaller companies. For example for those with under €5m turnover premiums were up around 80%. A typical premium for such firms was just over €5,000 last year, up from €2,700 the year prior.

For larger firms their primary Cyber Insurance went up around 60%, however those buying higher limits (excess layer insurance) experienced similar or even higher percentage increases right across their insurance programme. We saw some cases where the excess insurance worked out more expensive than the primary layers, and 100%+ premium increases were not uncommon .

#### But what goes up, must come down...

The good news is that many segments are already seeing a slowdown in these increases, with some sectors experiencing premium reductions at their renewals. It is useful to know why this might be.

1. **Claims have reduced in recent times** — see our last issue for a possible explanation for this. One aspect of Cyber Insurance pricing is that it can be adjusted relatively quickly, due to claims settling sooner than with other insurance products. As such any claims reduction will result in reduced pricing (this of course works both ways).
2. **The Cyber market has settled.** There was an initial sharp premium correction due to a number of insurers exiting the market.
3. **More competition**—some insurers that exited have now returned in a more limited form, while some providers have moved into the Cyber space for the first time.

#### Key takeaways

- Increases for SME's were proportionally high, but there are green shoots on the horizon with more competition in this space.
- For larger companies there is an even greater focus by insurers on risk management, with less competition.

Early engagement with your broker is crucial. We have a lot of expertise and strong relationships in this space and would be happy to discuss the best way of presenting your Cyber Insurance 'risk' to the insurance market.



## 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 real-life Irish cases.**

### Employees—gift card fraud

We have had a couple of clients fall victim to a similar type of social engineering fraud. Criminals email an employee pretending to be someone senior within their company. They trick the employee into believing that they need them to purchase some gift cards from a nearby shop — Apple gift cards in both instances. When the employee does so the criminals ask them to send a picture of the card.

In one such instance the criminals convinced the employee to go to another retailer, due to the first one running out of cards. The losses here were €400 and €1,100 respectively, and the vouchers were immediately used so no refunds were available for the companies in question.

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

### Cybercrime

An accountant was hacked. Their client emailed them with instructions to transfer monies. The hackers took over the email chain and amended the bank details. The monies were sent without the bank details being correctly verified internally, and a six-figure amount was lost. Thus far it has not been recovered.

Basic error or carelessness I hear you say, but unfortunately still commonplace.

Office	Contact	Phone	Email
Cork	Brian O'Mara	021 453 6860	<a href="mailto:bomara@oli.ie">bomara@oli.ie</a>
Dublin	Carman Devlin	01 6630604	<a href="mailto:cdevlin@olid.ie">cdevlin@olid.ie</a>
Galway	Joanna O'Donnell	091 454 031	<a href="mailto:jodonnell@olg.ie">jodonnell@olg.ie</a>
Waterford	Fiona Fitzgerald	051 309 130	<a href="mailto:ffitzgerald@oliw.ie">ffitzgerald@oliw.ie</a>

### 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](http://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.**

