

Cyber Matters Newsletter

April 2022

It has been a busy start to 2022 for those of us specialising in Cyber Security and Insurance.

We saw some large claims to start the year, and these are referenced on the last page—we also include a tip on how to try to prevent such incidents affecting your company. The sheer amount of claims in this space is leading to a 'hard' Cyber market — see below.

Cyber market conditions

The Cyber Insurance market is proving particularly tough at the moment, with large rate increases as insurers try to get a handle on claim frequency. We look at some of the reasons for this in more depth on page 3.

Our best advice to clients is to discuss what insurers want to see in terms of cyber security measures and to get the proposal forms back to us promptly to allow us as much time as possible to work on your renewal. The more time we have the better a job we can do in what is a difficult market.



Can we help you?

We at O'Leary Insurances like to think that we can make cyber security issues understandable, relatable, and crucially that we can offer solutions to problems as they arrive. Hopefully these newsletters are proof of that!

We also regularly present in-person on the topic of Cyber Security. For example in March we carried out a CPD for the Law Society of Ireland's Small Practice Support Service, at the invite of their Technology Committee.

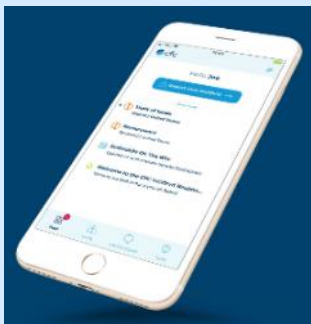
We have carried out dozens of such webinars, presentations and seminars over the past few years including conferences for the Irish Travel Agents Association and The Irish Hotels Federation, and to the likes of the legal profession. We are also regular contributors to seminars on specific topics for example issues around social media exposure. We regularly speak with individual companies, whether that be at board level or with appropriate IT personnel at the 'coal face'.

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

Cyber Insurance App benefits

One of the large Cyber Insurers has been making it mandatory for customers to download their App. The benefits of this are two-fold. Firstly, the client can access policy details and notify a claim, which may be useful if computer systems were down or if they are away from the office when an incident occurs.



Secondly, the insurer can send targeted cyber security alerts to clients. This is of such benefit that the National Cyber Security Centre in the UK is now using the App to broadcast urgent cyber security alerts to businesses.

Autocomplete email address issues

The annual Data Protection Commissioners report was published in late February. One item in particular caught our attention – related to email addresses autocompleting:

“The DPC has also seen a vast increase in the number of breaches caused by email correspondence issuing to an incorrect recipient due to the message service employed which predicts the recipient’s email address based on the first characters entered.”



This is entirely relatable to most – and it is a setting that can be disabled for those that have concerns!

The full report is available here: [external link](#)

Direct debits - beware!

The RDS were the victim of a data breach in February, which affected staff, suppliers and members. Their initial correspondence to those affected noted that for a “small number of cases, bank details may have been compromised in respect of those who paid their membership fee by direct debit”.

We don’t know if this affected any members, as the RDS themselves were investigating at the time. However a colleague affected posed a general question—should people be limiting DDs where possible, to reduce the likelihood of bank details being compromised? It would be foolish to think that all organisations have the same security procedures, so it is certainly worth asking how companies store your sensitive data, and only agreeing to share it if satisfied with the response.

The cost of cyber attacks

In this piece we look at how costly such attacks can be, along with ransomware trends and some positive news on actions taken by law enforcement agencies.

Cyber attacks are costly

Gloucester City Council in the UK was the victim of a system breach in December. In March it was reported that the initial reserve of £630,000 set aside may be nowhere near enough to cover the cost to the council. One local politician, quoted by the BBC, stated that the ruling Conservatives were *"either refusing to estimate the final bill or doesn't have a clue to what it could be"*.

Leading Cyber insurer CFC's experience is that ransomware activity frequency is flat since late 2018, but the severity of such instances is the key. Lindsey Nelson, Cyber development leader at CFC advises that "ransomware accounts for 18% of the number of claims, but 75% of the total claim cost". Ransomware is not the preserve of the large companies – it is a big issue for small and medium sized companies also, and can be much more devastating to smaller companies.



Lindsey Nelson, CFC

It is important to note that the insurer does what it can not to pay such a ransom, but sometimes critical infrastructure is involved and there is little choice due to the urgency to get back up and running. The insurer can present the case to the insured, and the business decision rests with the victim of the attack. Around 50% of ransom demands are actually paid for this reason.

Law enforcement fights back

The good news is that law enforcement is fighting back where it can. In our last issue we mentioned a webinar we carried out with the Gardaí. They outlined how they are stepping up their resources nationally to fight cybercrime. It is by its nature a cross-border issue, and as such many policing agencies collaborate with a common purpose.



In November the US Department of Justice and Europol announced that 7 members of the high-profile REvil cybercrime gang had been arrested in Kuwait, Romania, South Korea and Ukraine, In addition over \$6m in ransom payments had been clawed back.

Just last week a 16-year old in England was identified as being a leader of the Lapsus\$ cybercrime gang, and having personally amassed \$14m from hacking. UK policy had arrested 7 people aged 16-21 alleged to be gang members, although it is not yet clear if he is one of those.

The message is clear – law enforcement won't give up. Some battles have been won, but the war against cybercrime continues.



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.

Cybercrime loss – various

Clients of our office experienced cybercrime incidents in December that resulted in losses of over €1m in total. Sometimes the firm was duped out of monies, while in other incidents they were hacked and their clients were defrauded – the criminals emailed purporting to be the company in question.

It is worth highlighting that we have noticed such attacks are much more devastating coming up to periods where the offices are closed. Often success in recovering these transfers comes down to hours, not days. Where monies were transferred before Christmas, the losses were then only discovered when the offices re-opened in January. This gives the criminals ample time to move the monies on to other accounts and means it is much harder to recover funds.

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

Tip: We recommend increased caution around electronic fund transfers coming up to periods of annual leave for the relevant staff, or where the office will be closed.

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.

