Volume 9, Issue 1

Cyber Matters Newsletter January 2024

Welcome to our first newsletter of 2024. Apologies that this one is a bit late —but thanks to those that chased us up, it is rewarding to know that you read it!

We are now in year 9 of issuing this newsletter to businesses of all sizes across Ireland. During that time we have seen cybercriminals hone their craft, governments respond with new legislation, better-resourced policing and several education campaigns. We hope you continue to find this to be both original and interesting.

You are only as strong as your weakest link

In November a company providing IT services to law firms was taken offline by a cyber-incident. This affected the IT systems of around 80 law firms in the Ireland and the UK. The following week tales began to emerge of house completions failing to go through as a result. It took a month for the IT firm to get back up and running.

It bears repeating — most businesses are heavily reliant on third parties for a range of services. An outage to them could be catastrophic to your business. Ensuring that such firms carry adequate Cyber Insurance at least gives peace of mind that they have assistance and financial resources to get back up and running after an insured incident.

Israeli-related water hack in Mayo

A sentence we didn't ever envision typing. A private water scheme in Mayo had their water pump system shut down. The manufacturers were targeted because they are Israeli. 180 homeowners were affected—one would presume others on other schemes may have experienced similar disruption.

While this may seem small in the scheme of things, it brings focus to how detrimental such cyber attacks can be, as we saw with the HSE. Replace local water scheme with Uisce Eireann and you can imagine the media attention it would garner.

Thanks for reading. If you have queries on Cyber or any other insurances feel free to contact us on cyber@oli.ie.

What to avoid if a cyber incident occurs

Below are excerpts from an article by Ashley Burdon of CFC, a specialist provider of Cyber Insurance

What's the key to a smooth claims process when you suffer a cyber incident? Here are four big things he says to avoid—and advice on what you should always do.

A cyber incident is the time for cool heads and clear thinking. Having a pre-prepared plan to refer to is key.

Avoid

1) **Engaging vendors before anything else.** In the hurry to get back online, it's tempting to immediately reach out to different vendors you believe will help resolve the incident. But since there are many nuances to consider, doing so will only slow the process down and potentially have a negative impact on your claim.

1) **Negotiating the ransom yourself**. Negotiating with threat actors is a balancing act where one false move can result in disaster.

1) **Restoring data on your own.** If it was easy to restore data, cybercriminals would be out of a job. One slight error when attempting a fix can end up wiping out everything, even if your backups hadn't originally been destroyed.

1) **Disclosing too much too soon.** When an incident occurs, businesses often have an obligation to make a public statement. But once a statement is out there, there's no going back; the incident could turn out to be less serious than first feared, but the reputational damage would already have been done.

The full text of this piece is available here: Claims expert: 4 things to avoid if you suffer a cyber incident | CFC

What *should* you do?

Engage your insurers straight away, either directly or via your insurance broker.

You pay them for their expertise and their advices. If something does go wrong — this is what they are set up to do, so let them show their expertise.

Social Media in the Workplace – an employer's guide

By Fredericka Sheppard, Joint Managing Director, Voltedge

We often think that social media in the workplace refers to the great work marketing and PR teams do, but here's another completely different aspect for you to consider and to be aware of. Whether the company has a social media presence or not, you can be pretty sure that at least some of your employees are active on social media so that means there is a definite overlap that needs to be managed.

What does that really mean?

Well for starters it means that what you or your company does may be discussed out there in the social media forums not because your marketing department has been busy promoting the company but because your employees are sharing and communicating about their lives and experiences and, guess what, it's open season when it comes to telling pals about work colleagues, work events, or even company news. Those photos from the Christmas party or the company night out may be getting shared on Facebook or Twitter as we speak and you don't even know about it. Also consider news about a customer, a product you are designing at work, the new intern in the office, there are no limits. It may appear to be a bit of chit chat but what happens when someone doesn't see it that way?

Employees are using social media more and more for day to day activities, finding a new job, getting background on a company, finding out what they should be paid, who else works there. A little check of an employees Facebook pages will soon reveal if its "a fun place to work" or what staff think of the MD, it can all be done from their desk, while waiting for a meeting, or queuing for a coffee in the canteen.

Déjà vu? If so, great memory– this article featured in our Q4 2016 newsletter. It reads as relevant to-day as it did back then, although the likes of Tik-Tok might get a mention in 2024!

So, as employers, it's important you create a work environment that treats everyone fairly, where there's no inappropriate conduct, where company policy is followed to resolve issues – but do you have appropriate policies?

What if this social chit chat is not in their personal time but in their work time - that means "Company" time? What if it's not their personal business and it's your "company or colleagues'" business or what if they are so upset with a colleague or manager that they decide to give them a telling off in rather unrestrained and colourful terms on Facebook? The "cyber" world that craves entertainment, breaking news, office gossip etc. - it all has the potential for a perfect storm.

Top tips employers should consider	
Have social media policies in place that staff can fully understand	Review and ensure good management practices are in place
Train your managers and educate employees	Utilise systems & technology to monitor and safe guard activity
Embrace and utilise the best from Social Media - keep learning about it	Don't forget cultural aspects and your staff demographics
Follow good governance at all times	Remember the value of your EMPLOYER BRAND

Fredericka set up Voltedge Management Limited with her business partner Joyce Rigby-Jones in 2011. Voltedge aim to bring expert HR services to SME's across all sectors and be an integral part of a variety of entrepreneurship programmes. T: 01 525 2914 E: Fredericka@voltedge.ie

Cyber Matters 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

Recent case studies of cyber incidents from our client base

Clients of company lose monies

Our client was hacked. The hackers contacted two of their customers who owed them monies. One of these customers transferred over €200,000 to the cybercriminals.

Their customer thankfully managed to recover the funds. Our client engaged their Cyber Insurers to carry out an audit of their systems and also to provide further advices to prevent such an incident re-occurring. These costs—over €20,000 - were covered by the insurer, after a nominal policy excess.

Cybercrime loss

Hackers gained access to a client's computer systems. The criminals hijacked selected internal emails, namely around a bank transfer taking place. They duped employees within the company into sending €160,000 to the criminals' bank account. These monies were not recovered.

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	Carman Devlin	01 663 0604	cdevlin@oli.ie
Galway	Brendan Devlin	091 454 042	bdevlin@oli.ie
Waterford	Fiona Fitzgerald	051 309 130	ffitzgerald@oli.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.

Cyber Risk is now recognised as a top threat to all types of businesses. We at O'Leary Insurances were quick to realise the potential risk to our clients, and have acted accordingly. We have recruited and researched so that we can advise and provide our clients with up-to-date details of the exposure, and our ability to engage with organisations in this space is only possible because of our determination to do everything we can to protect our clients.

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.