Volume 8, Issue 3

Cyber Matters Newsletter July 2023

Welcome to our July newsletter. In terms of content, we have gone against the grain to make this a public-service broadcaster free zone...we will stick to what we know!

Ryan Tubridy will NOT feature in these pages

In this issue we provide an in-depth analysis on a Cyber Insurance claim that we recently finalised, and brought to a successful conclusion— eventually! We believe it makes for an excellent case study. The client had concerns and flagged issues throughout, we had some tough asks of the insurer, and there were a couple of twists and turns that we could not have predicted at the outset.

We believe it is an illuminating case study, and of course if any readers have queries please do let us know.

Cyber Ireland

We continue to be a proud member of Cyber Ireland, a nationwide cluster that we first joined when it launched in 2019. Cyber Ireland has noble goals, namely to:

- ⇒ build out the cross-industry community
- ⇒ develop talent and skills
- ⇒ Enhance research and development collaboration between industry and academia
- ⇒ Aim to support Irish start-ups and SME's to grow and export globally from Ireland

PROUD MEMBER OF CYBER|IRELAND 2023 - 2024

We look forward to working with Cyber Ireland and it's 165 fellow cluster members to try to progress these goals. To that end we have previously mentioned a Baseline Framework for SME's, to enable all types of companies to improve their cybersecurity posture. We hope to have news on this front before the end of the year.

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

Cyber Insurance in action

Earlier this year we settled a Cyber Insurance claim on behalf of a client for over €400,000. Below is a "warts and all" overview of the claim. The initial correspondence highlights just how fluid and stressful the initial incident can be when a company is in 'emergency mode'. The way insurers responded also goes some way to dispelling some common misconceptions about the insurance industry.

Background

This related to a very significant network interruption incident. Crucially, our client was not directly targeted in this incident; their largest client was the victim of the attack. However, their IT systems were linked to those of the much larger third-party that had been hacked — more on that later. The end result was that our client was completely offline for an extended period of time, and incurred significant cost.

All hands on deck

We were advised of the incident on a Friday. It was all hands on deck to start. Our first port of call was to put our client in contact with Cyber Insurers' 24/7 helpline number. Engaging with insurers early is crucial to try to minimise the harm, and also to ensure their expertise input in the decision making process. Our client contacted insurers, who in turn appointed crisis experts to aide the client.

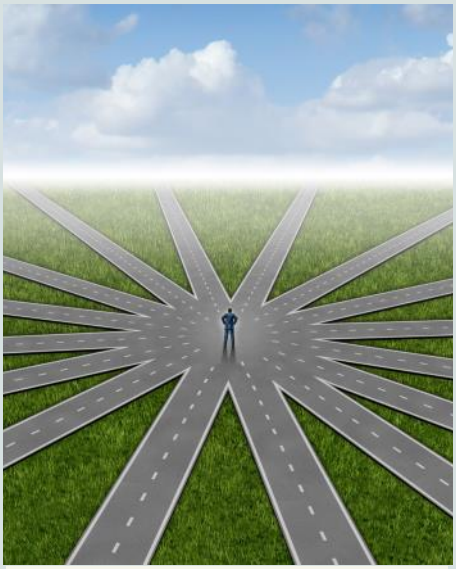
By the following Thursday we had conducted our initial review and sent the client a brief summary of how the policy could potentially respond.

Trouble and strife

Then came our first potential conflicts. Our client contacted us, worried that some of their policy limit was going to be eroded by third party expert fees. Their insurer had pushed to appoint a Cyber Security Firm and Breach Counsel, for their expertise. Our client commented on how stressful the matter was, everything was dropped to resolve the issue.

Another problem arose. The client had suffered a significant data breach. They took out court injunctions to try to prevent sharing of the data, at significant cost. Our client had a long-established relationship with a solicitor, and unfortunately that solicitor was making decisions without engaging insurers. At this stage there was mention by the insurers of no policy cover for these injunction costs, as the insurer wasn't advised of same prior to the costs being incurred.

It is the broker's role to gauge how involved to be in a particular claim. In crisis mode, streamlined communication from insurers to our client were key, so we remained on a watching brief. However at this point we took a more hands-on approach. We engaged with the insurers and negotiated some allowances from them regarding the handling of the claim. We also reassured the client that the engaged experts were very much to their benefit, focussing on getting systems restarted and functioning again after the incident.



Complex claims such as this can go in any number of directions, at any time

After the dust has settled...

Once the first fortnight had passed, the focus switched away from the initial triage stage. Now the client raised a pressing concern.

As mentioned at the outset, it was a third party client that was hacked. As would be standard under a commercial insurance policy, insurer's rights are that they can look to recover costs from a third party deemed responsible for an insured incident. However — this third party was the single biggest source of revenue for our client. They simply could not afford to take an action against them.

Restricting an insurers right to recovery would greatly impact their bottom line. However, after negotiation with ourselves they thankfully agreed to waive their right, and they put this in writing to the insured

"Although it is not Insurers' usual course of action, Insurers are on this occasion prepared to waive any potential subrogation rights against (the third party) to ensure that (the insurer) can provide (the client) with the expert assistance it requires in response to the ransomware attack and data breach."

But this claim wasn't finished yet....the board of management of the client met the next day and much to our main point of contact's shock, and to ours, they withdrew the claim. They felt there were "too many issues", and the overarching concern was fear of fallout with the third party client. Perhaps what we had negotiated sounded too good to be true?

Insurers ~~don't~~ pay claims

The insurer in question had already made the decision to exit Cyber Insurance due to this being a lossmaking insurance product for them. The premium this client had paid to them was a fraction of the potential claim. Most readers might assume that they would not be looking a gift horse in the mouth.

Three weeks later, unprompted, the insurer sent a letter to the client acknowledging the claim being withdrawn. However, they also included a line by line summary of what could potentially be covered by such a claim — a figure in the hundreds of thousands. The insurer was still open to dialogue, and the client was now reassured enough to opt to pursue settlement. Lesson learned....never assume!

We now progressed to settle the claim. This was a complex process for a number of reasons. It involved a lot of correspondence between the client and the insurers solicitors. There was much back and forth, swapping projections and data with forensic accountants for the insurer, who had to analyse various details e.g. replacement hardware costs, overtime, future overtime and more.

The upshot of this was that the vast majority of what was claimed for was paid. Result!

Lessons Learned

1. Early engagement with your broker / insurer is key.
2. Insurers will not spend money for no reason— if they are doing so it comes from experience.
3. If using your own solicitors, keep insurers appraised and obtain their agreement for proposed costs.
4. Cyber Insurance pays claims— sometimes even where clients don't want to be paid!

Each claim is different, as you can appreciate. Hopefully you will never need to have an appreciation for our claims handling expertise, but if you do this may shed some light. These claims can be quite complex, with us needing to balance the needs of our clients against what is pre-agreed within the insurance policy.

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

Defamation of employee

A director emailed allegedly disparaging comments about an employee to a colleague. The employee in question was at their colleagues desk at the time and they saw the email.

After a clear-the-air meeting, the director sent an internal email to another director, but they accidentally copied in the employee. There were allegations of further defamation and an action is now being brought.

The Cyber Insurance policy is responding to this under the Media Liability section.

Cybercrime loss

A member of staff with authority to transfer funds received an email purporting to be from a client. The email requested a transfer of €60,000 urgently. Under pressure, the member of staff made the transfer without verifying the validity of the request or the bank details over the phone.

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

Soon after the criminals requested higher amounts, and the employee tried to transfer same. Thankfully there were insufficient funds and the transfers could not be made. However the original transfer was not recovered. This amount was indmenified by Cyber Insurance.

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.