Volume 4, Issue 2

Quarter 2 2019

Risk Management Newsletter

Case study & useful tips

Our last issue was very much backward looking - a summary of cyber security losses up to the end of 2018. While finalising that issue, we were very much focused on the present - in the first week of January alone we were notified of two Cyber Crime incidents - it wasn't even a full working week!

Trends that we saw in 2018 with regards cyber crime being quite prevalent are continuing into this year. We include an example of a high-profile claim on the next page.

Some industry-specific incidents should also focus the mind, for example the "extensive cyber-attack" on one of the largest aluminium manufacturers in the world (Norsk Hydro) in March. The hack halted production and forced the company to go back to manual practices. It is reasonable to assume that at a minimum this will lead to reduced revenues and significant costs to repair and restore their systems, be that from back-ups or starting from scratch. Other potential costs include lost clients due to reputational damage, paying a ransom (which they have said they won't do in this case), or costs related to handling a data breach if one occurs.

In this issue

On the topic of data breaches, this month we include some advice from an expert in this area. This includes tips around preventing same and also what to do if a data breach does occur. These tips can be built into your incident response plans.

If there are any topics you would like covered in future issues please email us - cyber@oli.ie

O'Leary Insurances Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Dublin) Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Galway) Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Waterford) Ltd. is regulated by the Central Bank of Ireland.

Cyber Crime case study

The below relates to a Cyber Crime loss which was discovered in January by one of our clients in January.

A nightmare start to the new year. The bookkeeper of the solicitors practice checked, and double-checked, but the fact remained - €96,735 of client funds, supposedly transferred to a financial institution in December, were gone - stolen by cyber criminals. Just €10 was recovered from the bank in question. Within days it had made a national newspaper and was being used as a case study by the Law Society on their website, to serve as a warning to others. Scant consolation for the firm in question...

So what happened?

The firm was transferring funds for a client to a finance company. Like most solicitors, the firm had strong risk management procedures around the electronic transfer of funds - they had just recently successfully defended against another fraudulent attempt related to a separate transaction. Any new bank accounts had to be verified by calling a known person in the finance company, which was duly carried out by the solicitor. The solicitor then emailed the bank details to their bookkeeper.

However, it turned out that the firms systems had been compromised, and the cyber criminals took over this internal email. They intercepted and replaced the legitimate bank account details with their own. They then sent this on to the bookkeeper, and the transfer was authorised. The timing was perfect for the criminals, with the firm shutting down for Christmas break. By the time the fraud was uncovered, the funds were long gone from the fraudulent bank account.

The practical solution

The sheer frequency of these cyber crimes on Friday afternoons or close to Public holidays highlights the need for extra vigilance at these particular times.

The case quoted above highlights the need to verify not just external emails, but also internal ones. One suggestion is to verify by phone. If based in the same office the person verifying the bank details could print them off, sign that they have been verified, and hand them in person to their accounts department. For most businesses this minor inconvenience is acceptable. If not, we recommend you speak with your IT security experts to come up with a solution that works for your business.

Continued on next page———>

O'Leary Insurances Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Dublin) Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Galway) Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Waterford) Ltd. is regulated by the Central Bank of Ireland.

Cyber Crime case study continued

Client account considerations

For solicitors, the client account is sacrosanct. It must always balance, with the Law Society carrying out frequent audits of firms. Any deficit must be quickly rectified to avoid disciplinary action. The default position for a cyber crime loss is that the firms Professional Indemnity Insurance will respond in such instances. The timelines to make the account good are strict - if not done in time, an application will be made to the High Court against the firm in question.

The Insurance solution

Many solicitors purchase Cyber Insurance which includes Cyber Crime. They do so for a number of reasons including cost, broad policy cover and to reduce the effect of cyber crime claims on the mandatory PI policy. The firm in question carried such insurance.

Upon discovering the loss the firm immediately notified ourselves, and we put them in touch with the incident response team of their Cyber insurer. The very next day the insurer confirmed the policy would pay out, and also confirmed they would abide by the Law Society's requirements regarding making good the client account. Insurers conducted their own investigations concurrent to the Law Society's. They looked into whether the funds were recoverable, where the system had been compromised and paid out the full amount, less the policy excess of €2,500.

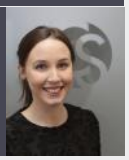
Timeline of the loss

19 December	Firm defrauded of client funds.
02 January	Loss discovered, Law Society and Cyber Insurer notified.
03 January	Insurer advises they "do not envision any coverage issues".
19 March	Claim finalised and payment in full received to the firm from insurers.

We include more examples of Cyber crime losses at the end of this newsletter.

O'Leary Insurances Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Dublin) Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Galway) Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Waterford) Ltd. is regulated by the Central Bank of Ireland.

Eimear Boyle of **Crowley Solicitors** provides tips for Irish businesses to help reduce the likelihood of data breaches, and also looks at what to do if one does occur.



Five Key Actions to Minimise the Risk of an Incident/Personal Data Breach Occurring

1. Audit and assess what the appropriate technical and organisational measures are for your business to ensure you are securely processing data based on the level of risk profile of the business's data processing activities – do you need to update your firewalls, add an extra layer to your access protocol or maybe implement a clean desk policy? These are all examples of technical and organisational measures that may assist in ensuring security of processing.

2. In light of how much data is stored electronically, pen (penetration) testing is an excellent way to quickly perform a gap analysis on business systems and websites.

3. Uphold the principle of data minimisation – if a business collects and holds personal data solely for what is relevant to their legitimate data processing, a data breach will expose fewer additional questions (and potential flaws) for the business.

4. Simulate a personal data breach – not only will this take away the anticipated fear for the business, simulated breaches allow for a stress test of breach policies and procedures and often prompt valuable revisions to the suite of breach documents in the business. As part of this stress test, analyse whether the type of incident or breach requires notification to your insurers.

5. Train all employees regularly – this is an example of an organisational measure for secure processing and an excellent way to minimise the real risks posed by social engineering, phishing emails and remote working and travel security.

Five Key Actions to Minimise Exposure When an Incident/Personal Data Breach Occurs

1. Follow your tested policy and procedure, which should begin with a key stakeholder meeting and include on the agenda whether or not the business needs to notify its insurers under the terms of its cyber liability insurance policy.

2. Consider whether management of the incident can be handled internally or if the business would benefit from external public relations consultation and specialised legal advice.

3. Don't panic, especially when conducting risk assessments as these are critical to the analysis of whether or not the business is required to notify the Data Protection Commission (DPC) and communicate to data subjects.

4. In line with your incident/breach log, document a summary of the rationale and justification for each action taken, so that the incident can be reflected upon retrospectively and, if necessary, justified to an external party, for example, the DPC.

5. For those borderline instances, err on the side of caution and consider the impact of not notifying the DPC and, if applicable, communicating to data subjects and being found wanting at a later date – the business could face a fine of up to €10 million or up to 2% of the total worldwide annual turnover of the preceding financial year (whichever is higher).

If you have any queries or comments you can contact Eimear: as per the below.

(t) 021 428 9560 (e) eboyle@crowleysolicitors.ie (w) www.crowleysolicitors.ie

O'Leary Insurances Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Dublin) Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Galway) Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Waterford) Ltd. is regulated by the Central Bank of Ireland.

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.

Not for profit - €9,885

The organisation lost monies due to interacting with a fraudulent third party over email. The incident happened in April 2018 but only came to light in Feb 2019 due to a mix-up. The contractor expecting the funds thought they were being withheld until all works on a construction contract were completed, whereas the fact of the matter was that our client had assumed the funds were already paid over to the contractor.

Solicitor - €24,000

The firm have a policy of only sending bank accounts details by post to their clients. However, their IT systems were hacked and the criminals emailed a client with bank details advising that monies were due. The client unwittingly paid over to the criminals, much to the frustration of the firm in question. *Verification by the client could have prevented such a loss. However the solicitor was in a difficult position as it was their systems that were hacked - without this the loss could not have occurred.*

Insurance broker - Ransomware

The Norsk Hydro hack is far from the first time we've come across Ransomware incidents. For example we heard from an insurance broker that was locked out of their systems for a couple of days by such a crime, and they ended up paying the Ransom as their IT specialists advised there was no alternative. Certain insurers would not allow them to use their systems until they improved their IT security, which caused further inconvenience to the business in question.

Office	Contact	Phone	Email
Cork	Brian O'Mara	021 453 6860	bomara@oli.ie
Dublin	Robert O'Leary	01 663 0618	roleary@olid.ie
Galway	Angela Rossborough	091 778 677	arossborough@olg.ie
Waterford	Laura Elliot	051 309 130	lelliott@oliw.ie

About O'Leary Insurances

Insurance Brokers & Consultants, Est. 1961

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.

With over two hundred employees now operating from eight 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.

O'Leary Insurances Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Dublin) Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Galway) Ltd. is regulated by the Central Bank of Ireland. O'Leary Insurances (Waterford) Ltd. is regulated by the Central Bank of Ireland.