Volume 4, Issue 4 | Quarter 4 2019

Risk Management Newsletter

Data breaches and Ransomware

Something to think about

The primary aim of this newsletter is to make Irish businesses think about risk management, with a particular focus on Cyber security. The formula is simple - introduce topics that may not have occurred to business owners and management.

This issue is a must read. It includes a guest blog on hidden costs of a data breach. When reading the piece, don't forget that such a breach could as easily be accidental as malicious, and that it can involve paper files as well as electronic ones.

We then include real-life examples of Ransomware and Malware incidents from the claims team of a large Cyber Insurance provider. These go a step further than our usual examples which are based on Irish companies (but which are, as usual, included on the last page).

Cyber Ireland membership

In our last issue we highlighted the launch of **Cyber Ireland**, the National Cyber Security Cluster whose aim is to connect the cyber ecosystem in Ireland. It consists of over 100 members including cyber security multinationals and indigenous companies, companies with security-operations, large consumers of cyber security products & services, as well as academic institutes and government agencies. And as of July - us!

We are the only General Insurance broker to have signed up and we look forward to representing our clients and contributing on behalf of the insurance industry.

Tip - Check your Passwords!

The following is a useful tip from a live hack at Futuresec 2019 in Cork. The hackers showed how they can greatly reduce the amount of potential user passwords which assists them in gaining network access.

Where a capital letter, number and character are required in a password, they presume that the capital will be at the start of the word, the number in the middle and the character at the end - and that "!" is by far the most popular character used, e.g. Futuresec2019!

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

Risk Management Newsletter

How much could a data breach cost your company? It's not all about fines - Fiona Mulvaney, Global Head of Business Development at Waterford Technologies looks at hidden costs - both financial and non-financial - which can add up in the event of a breach.

Regulatory Fines

When people think of the cost of regulatory non-compliance, the first thing that comes to the mind is the large GDPR fines of €20 million or 4% of annual revenue.

Many high-profile companies have been hit with these fines including Google (€50 million), British Airways (€204 million) and the Marriot Hotel Group (€110 million).

But what can be lost in all this talk of regulatory fines and what many of the GDPR-led articles you read don't speak about, are the other costs that your company could potentially face along the way to data compliance.

Insurance & GDPR fines

We previously wrote on the topic of GDPR fines; our current advice is to presume they are not insurable.

For more on this please refer back to our Q3 newsletter from 2018: available here

Cost of Diagnosing a Problem

A breach has happened - but which files are affected?

Once you are notified of a data breach, the first thing many companies must do is begin the search for more potential violations to avoid future fines.

For many SMEs, the resources have not been put in place to undertake such a job. For these organisations, a large amount of money and time must be spent to protect them from future data violations.

The amount of time is also a huge factor in this investigation. One study found 1 Terabyte of unstructured data can take up to 9 months to fully investigate internally.

Reputational Cost

These days, if a company experiences a data breach, it is only a matter of time before it becomes public knowledge. The true cost of data compliance can come down to the negative effect that breach investigations and potential fines on a company's reputation.

On a recent study of thousands of consumers, "82% of UK respondents claim they would boycott a company that demonstrated they have no regard for protecting customer data".

So, while your company may have the financial security to pay the fines that are thrown at them, they may never fully recover from the damage that will be done to their organisational reputation as a result of these fines. Though it is hard to quantify the cost of reputational damage, it definitely impacts a companies bottom line.

Due to the increased media interest, you won't find many of your customers who are not aware of GDPR. The same study also showed that 80% of consumers worried most about the financial information held by banks and other financial institutions such as building societies and credit unions.

The above is an edited extract from a blog by Waterford Technologies. The full piece is available here (external link).

Waterford Technologies are experts in unstructured data (email and file) compliance and management.

Email: fmulvaney@waterfrodtechnologies.com Phone: 051 334 967

Risk Management Newsletter

Ransomware & Malware Case Studies

Below are real-life Malware and Ransomware incidents experienced by the claims team of our specialist Cyber Insurer, CFC Underwriting.

We typically include examples from our own client base in our newsletters - see page 4.

CFC insure small to medium sized businesses based all around the world, and the case studies are reflective of this. The below examples could conceivably happen to many Irish businesses, and they should provide food for thought in how to prepare for a worst-case scenario.

Industry	Brief Summary	Key costs	Full case study (external links)
Retailer	An employee opened a phishing email which resulted in a ransomware attack. Of particular note was how ransomware can lead to unintentional and sometimes irreparable damage to electronic files and computer programs - even to a company who don't rely on IT systems to open their doors.	⇒Forensic IT, recreating database / inventory ($20,858) ⇒Loss of gross profit ($21,284)	Link here
Healthcare	A malware outbreak took a medical facility offline. This rendered patient records inaccessible as their IT service provider quarantined their systems.	⇒System damages ($2.6m) ⇒System interruption ($4.5m)	Link here
Property Management	The company fell victim to a ransomware attack. They lost all of their data, as well as a number of clients, due to delays in restoring their systems (over four months).	⇒Forensic IT investigation & recreating database / inventory (£94,083) ⇒Loss of clients (£126,853) ⇒Rebates to unhappy clients (£14,318)	Link here
Electrical Contractor	Another ransomware attack, this time due to an employee clicking on a supposed CV in an email for a job application. Not all of the data could be restored from legacy systems, which was an unintended consequence of the ransomware attack.	⇒Ransom incident ($22,500) ⇒Restore data ($58,887)	Link here
Technology company	A targeted ransomware attack resulted in a particularly high ransom. A second group of cybercriminals also deployed malware with a view to harvesting bank details of clients.	⇒Ransom negotiation & payment ($223,150) ⇒ Forensic IT ($45,000) ⇒Create new servers ($85,000) ⇒Lost income & clients ($291,538)	Link here

The above case studies and many more can be found under the 'Resources' section at https://www.cfcunderwriting.com/.

Glossary	
Malware	Malicious Software which can harm your computer (e.g. virus, ransomware)
Phishing	Fraudulent emails attempting to obtain sensitive info
Ransomware	A type of malware that denies access to files /computer system until a ransom is paid

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.

Identity theft

Cyber criminals purported to be a solicitor over emails with a client. The client in question relied on the bank account detail in the email and transferred €30,000 to the criminals.

Unfortunately this is becoming more common, with clients not having the same checks and procedures a company would. If the hack has happened to the company then there is likely liability. We will discuss this in more detail in our next issue.

Fraudulent invoice

The computer systems of a UK based company with whom a contractor was transacting business were hacked. The contractor received two invoices and bank account details requesting payment. The invoices matched amounts due to be paid, however the bank account turned out not to be and the money was transferred - over €90,000.

Ransomware

A sole trader accountant suffered a Ransomware attack. Their files were encrypted, and a high ransom was demanded. The principal had no backup and had no option but to pay €8,000 by Bitcoin.

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 250 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.