

Risk Management Newsletter

2018 - the Year in Review

Data protection grabbed the headlines in 2018, and in particular GDPR . But what did it mean in practice, and did it distract from other cyber security risks? In this issue we look at what effect GDPR has had on companies right across Europe since it's implementation. We then look more specifically at what has happened amongst Irish business in the past twelve months.

GDPR - it came, it saw, has it conquered?

It is hard to believe, but this time last year the Office of the Data Protection Commissioner was conducting a significant PR exercise to make Irish businesses aware that the EU's General Data Protection Regulation was on it's way. Having done the hard yards, we are all now (hopefully!) well aware of it's existence - albeit we may still not be 100% sure what it means for us!



There have been a few high-profile data breaches which have made the news in the past 12 months, and Ireland is at the epicentre of many of these - for example Facebook's data breach in September (over 50 million people affected). Notification of data breaches to regulators has been mandatory across the EU since May - we look at what regulators have been focusing on and how they have been punishing those that have been forced to contact them regarding breaches of the regulations .

In this issue

What happened in 2018:

GDPR fines	Page 2
Ireland overview	Pages 3-4
Cyber incidents	Page 5

Cyber crime on the rise

We have all seen or heard of reports on the global cost of cyber crime - various reports put the figure in the hundreds of billions of dollars - or bigger than the global drugs trade! In 2018 our clients lost more money to Cyber Crime than ever before. In our review we summarise what we saw this year as opposed to what has happened in the past.

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

GDPR fines and penalties

Here in Ireland there have been high profile incidents, such as the Facebook hack. We watch with interest to see what action, if any, is taken by our Data Protection Commissioner. Whilst it's very early days, there have already been case studies from the continent.

Jurisdiction	Summary	Punishment
Portugal	<p>July: a hospital was fined on two counts. Their issues related to (i) poor procedures around access to patient data, with full access given to too many individuals, and (ii) issues related to how they secured patient data.</p> <p>The hospital are appealing the severity of the fine.</p>	€400,000 in total
Austria	<p>September: A betting shop monitored their shop entrance with CCTV. However, the camera was also pointed to the sidewalk outside of their premises. The bookmaker in question was fined for monitoring a public space without proper transparency and notice.</p>	€4,800 fine plus legal costs.
UK	<p>The UK's Information Commissioner's Office has been particularly busy focusing on pre-GDPR incidents - implementing several fines totalling millions throughout 2018 (the UK would historically have had stronger powers of enforcement than the likes of our own Data Protection Commissioner).</p> <p>In September they issued their first proposed GDPR enforcement notice against a company called "Aggregate IQ", for profiling British voters. They were also ordered to cease processing the data of EU citizens. The company is appealing the decision.</p>	<p><u>Pre-GDPR examples:</u> £500,000 - Facebook £500,000 - Equifax £385,000 - Uber £250,000 - Yahoo £77,000 - BT</p> <p><u>Post GDPR</u> Up to £17m - Aggregate IQ</p>
Germany	<p>November: A social media provider suffered a data breach in July, which was discovered in September. 330,000 users were affected, with information including email addresses and passwords taken. The issues were quickly identified and the company in question was fined by their regulator.</p>	€20,000 fine

These fines do not take into account unseen costs such as interruption to the running of the business, lost income, reputational damage, and the costs of notifying those affected. In the case of the German Social Media company, the cost of notifying over 300,000 individuals that the breach occurred could have been a multiple of the fine.

Are GDPR Fines insurable?

This is a common question from our clients. The policy language in most Cyber Insurance wordings is very clear - yes they are covered, where they are insurable by law. The second part of that sentence is crucial.

What is going to be insurable will likely vary from country to country within the EU. From an Irish perspective, the indications from the Data Protection Commissioner are that fines will indeed be partially or wholly punitive. If that is the case, then it is unlikely that an insurer can legally pay a claim, as it would be deemed to go against public policy. For companies that hold / process the personal data of individuals in other EU countries, the situation will vary.

Our recommendation: Until such a time as there is sufficient legal precedent to refer to, companies should act as a 'prudent uninsured' - they should presume that such fines are not going to be insured.

Email cyber@oli.ie if you would like more information.



The Irish Perspective - where do claims arise?

The below figures are based on information received from our own client base across Ireland.

Type of incidents affecting our clients 2016-2018

Classification	2016	2017	2018
Cyber crime	47%	55%	55%
Data breach	6%	6%	16%
Identity theft - 3rd party	0%	6%	13%
Privacy Liability	3%	6%	10%
Damage to Systems	44%	16%	6%
Telephone hacking	0%	11%	0%

€1,096,756

Total direct financial loss to Cyber Crime among our clients in 2018

Cyber crime: theft of funds by Cyber means. Includes CEO Fraud, Identity theft resulting in loss to our insured, funds transfer fraud, phishing and social engineering.

Identity theft affecting third parties: For example you are hacked and your clients receive a fraudulent invoice purporting to be from you - and they pay it. (See example on page 5).

We do not count such losses in our figures, but they could conceivably result in claims against the firms that were hacked.

Privacy Liability: linked to data breaches - where they lead to claims from third parties.

Damage to Systems: incidents such as Denial of Service attacks, hacking, malware and ransomware.

Cyber Crime	2016	2017	2018
Most common area of loss	Funds transfer fraud	CEO Fraud	Funds transfer fraud
Number of incidents (total)	16	10	18
No. of incidents where funds lost	6	7	13
Average loss per incident	€53,500	€83,329	€84,366

Continued on page 4 [----->](#)



The Irish Perspective - where do claims arise?

Continued from previous page

Top individual losses 2016-2018:

- 1) €300,000 Identity theft 2018
- 2) €277,300 CEO Fraud 2017
- 3) €226,500 FTF 2018
- 4) €207,000 FTF 2018
- 5) €166,500 FTF 2017

FTF = Funds Transfer Fraud

Percentage of incidents notified to Cyber insurers by year:

2016	18%
2017	6%
2018	76%*

* mandatory notification under GDPR
since 25 May 2018

Percentage of Cyber incidents (2016-18)

Sector	%
Legal	35%
Construction	11%
Retail	9%
Financial services	8%
Hospitality & Leisure	6%
Healthcare	5%
Outsourced customer services	5%
Charity / Not for profit	3%
Technology	2%
Transport	2%
Travel	2%
Other	10%

Is the threat of Ransomware reducing?

The number of Ransomware attempts being notified to us is significantly down year-on-year.

However, in 2017 a client received - and felt they had to pay - a ransom demand for €15,000. Anecdotal stories support that the amounts being requested are increasing.

A potential factor in the reduced notifications is that our figures are based on what our clients tell us - it is possible that we are no longer being advised of smaller Ransomware demands.

Advice provided in this newsletter is intended as a general guide and is brief by nature. For queries specific to your own insurances, please contact us to discuss.



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.

Identity theft affecting third parties

A solicitor told their client that they would post their bank details to their client. The solicitor was then hacked and criminals emailed the client with their own bank details (from the solicitor's email). The client relied on the email and transferred €27,000 to the criminals. The Solicitor advised they would end up paying this amount to their client to avoid a Professional Indemnity claim.

Retailer - funds transfer fraud

A retailer suffered financial loss on two fronts. Firstly, their personal account was cleared out to the value of tens of thousands. Also, the business itself was defrauded of another €9,000 due to their emails being hacked and they receiving updated bank details, supposedly from their solicitor.

Solicitor - Data breach

A solicitor sent confidential documents to the incorrect address. These were unintentionally opened by the neighbour of their client. Private financial details were included in the correspondence.

If you wish to discuss further please contact us. For new clients please contact cyber@oli.ie - we have 8 offices around Ireland to respond to your needs.

Interesting Insurance Fact:

The most expensive single-car insurance claim ever paid was for Rowan Atkinson's McClaren F1. The repair bill was a whopping £910,000!

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.

