

# Risk Management Newsletter

## Mining for Data

It can be difficult to quantify to a business why the data they hold is valuable to third parties, so we take a look at just how valuable it may be. We also look at data breaches that have affected our clients - the sheer variety gives food for thought. We also examine an actual data breach and the disruption it caused.

Many believe that the data they hold is of little or no value, or the amount they have isn't enough to make them a target for criminals. To start, let's consider this from the perspective of those whose data has been taken.

### Why is Personal Data so valuable?

It's easy to understand why stolen credit card details may be valuable to third parties - they can be used for immediate financial gain. But if your email or your date of birth is now known to third parties due to a data breach - so what? Or if a password is stolen from a website you haven't used in years - what harm?

On its own, an item of information might be innocuous. But if other pieces of data were taken in similar breaches, criminals can piece those together like a jigsaw to build up a profile of you. This profile can then be used for criminal purposes such as identity theft or insurance fraud. If passwords are used on other accounts, criminals may test this out and obtain even more information. We discussed this in more detail in our October 2017 issue, [available here](#).



Your data is very valuable when pieced together

**Personal Data** is anything that can be used to identify an individual. It includes :

Name	Driving license detail
Address	Passport number
Email	Phone number
Date of birth	Medical Information
PPS number	Gender

This is also referred to as Personally Identifiable Information (PII).

### What does this mean for your business?

Businesses need adequate safeguards and processes in place around their use of Personal Data. Ignorance is no defence if something does go wrong.

Firstly, anyone whose data you store will have expectations around how it is handled. If there is a breach, they will look to you to communicate it effectively and to appropriately deal with their queries. In addition, GDPR has already been well publicised, with requirements relating to how data is gathered, processed and stored now subject to a strict regulatory regime.

Data breaches can result in significant reputational harm to businesses, resulting in lost clients, income, and even privacy related court cases. Falling foul of GDPR could result in being the subject of investigations as well as fines and penalties.

In the following pages we include an example of a well-handled data breach, and the difference that prior preparation made to our client.

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.

### Types of data breach

What comes to mind when you think of a data breach? Probably similar to what we see on the news - criminals hacking an organisation and stealing their data.

That is just one example of a data breach - our clients have experienced several others.

#### Types of data breach

##### Confidential document

A company accidentally sent a confidential file to the wrong party. This included sensitive personal information of a particular client. The firm had to ask for the correspondence to be returned, advise their client and regulatory body, as well as the Data Protection Commissioner.

##### Office move

After an office relocation, it was discovered that a filing cabinet containing sensitive Personal Data relating to employees had gone missing. While the organisation in question believed it was dumped in error by the contractor, they had to notify the Data Protection Commissioner and speak with their solicitor.

##### Employee theft

The family of an employee highlighted that the individual in question had taken credit card details of customers and used them to purchase goods. The firm in question had to make a notification of this to the Data Protection Commissioner and to make necessary changes company-wide to prevent it happening again.

##### Employee data breach

An employee was seconded to another organisation. While there, they came across sensitive information regarding an individual - information which they released to a third party, possibly for financial gain. This happened several years ago, but only came to light recently.



##### Workplace accident

An employee suffered a very serious workplace accident which was caught on CCTV. Another employee obtained footage of the incident and showed it to colleagues and third parties. A solicitors letter was sent to the employer stating that the CCTV should not have been passed on to third parties.

##### Third party breach

A company relied on an online service to run competitions for their customers. The website in question suffered a hack, which resulted in the data of several thousands of individuals being stolen. Our client, as the Data Controller, had to deal with the breach themselves. We look at this incident in more detail on the next page.



As usual we include some examples of cyber losses on the last page of this newsletter



### How much does a data breach cost?

We see astronomical figures quoted for high profile data breaches. But what do they really cost? Here, we analyse an Irish data breach that was covered by Cyber Insurance, and look at how the costs quickly racked up.

#### The breach

Our client runs competitions for their customers. Those taking part followed an email link which brought them to a third party website, where they inputted their personal details. The third party suffered a data breach. Personal information of several thousand customers of our client were taken.

Under GDPR, the third party is considered a Data Processor. Our client is considered the Data Controller - they are responsible for securely storing their customers data. As such, they were expected to handle communication of the data breach themselves.

#### The fallout

The data in question was not overly sensitive, however affected individuals needed to be notified. The company have strong internal procedures in force around data protection, and they purchase a comprehensive Cyber Insurance policy. They notified ourselves, and we immediately notified insurers. Senior management of the company were greatly assisted by the insurer-appointed crisis consultant, who co-ordinated their response.

This included:

- ⇒ Identifying exactly how much data was taken
- ⇒ providing advice around notifying those affected
- ⇒ setting up a call centre and training staff to handle enquiries
- ⇒ responding promptly to email enquiries
- ⇒ Notifying the Data Protection Commissioner (DPC) to comply with GDPR
- ⇒ Preparing a comprehensive report for the DPC, and answering their queries
- ⇒ Appointing a Public Relations consultant to assist with handling of the breach



#### The end result

The data breach was handled expertly and reputational harm was avoided. This was not the case for one of the company's peers, who featured in national newspapers for the exact same breach.

The costs of handling the breach were far from negligible - costing tens of thousands of euros, as well as significant interruption at senior management level - but reputational damage could have been worse. These costs were covered by their insurance policy after the payment of the policy excess.

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.**

### Finance - Identity theft

This company took on a new client from overseas. They went through their normal rigorous routine in verifying that they were complying with various regulations, such as Anti Money Laundering. They then authorised a transaction based on their new clients instructions.

It turned out that the 'client' was the victim of identity theft. The originating bank returned the attempted drawdown of monies , leaving our client out of pocket for around € 300,000.

### Solicitor - Cyber Crime

A practice emailed their bank details to their client. The emails were intercepted as one parties' emails had been hacked. The end result was that the practices client received fraudulent bank details by email, and transferred over € 50,000 to criminals based on this.

If you wish to discuss further please contact us.

For new clients please contact [cyber@oli.ie](mailto:cyber@oli.ie) - we have 8 offices around Ireland to respond to your needs.

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

### 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.

