Volume 3, Issue 1 | Quarter 1 2018

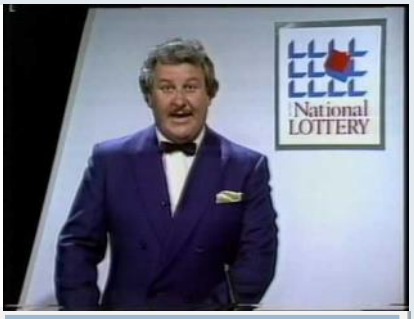
Risk Management Newsletter

The cost of a data breach

From 25 May, the General Data Protection Regulation (commonly referred to as GDPR) comes into effect across the EU. The enhanced powers of the Data Protection Commissioner include the ability to impose significant fines and penalties on those deemed non-compliant. In this issue we look at what this means for Irish businesses as well as other costs related to a breach.

The incumbent - Data Protection Act 1988 (Amended in 2003)

1988 was the year Ireland enacted The Data Protection Act. While it was updated in 2003, it is fair to say that this legislation has not kept with the times and is no longer fit for purpose.



Times have changed since the original Act in 1988

While the Data Protection Commissioner's (DPC) powers are currently fairly limited, they have had some ability to enforce the Act via prosecutions in the courts system.

For example, a retailer recently conducted a marketing campaign. An individual had previously opted out of being contacted, but the retailers systems didn't pick this up. The business in question was fined €2,000 for their system failure.

The DPC have also temporarily shut down firms that were deemed non compliant via Enforcement Notices. More serious cases are included as Case Studies in their Annual Reports.

The new regime - GDPR

As of 25 May, the DPC will have the power to impose fines of their own without the need to bring a firm to court. The increase in fines and penalties have grabbed most of the headlines - up to €20m or 4% of global turnover, whichever is greater.

The DPC has been very careful not to quantify potential fines for breaches of legislation. They have simply pointed out that Article 83 of the GDPR allows for them to levy a fine that is "effective, proportionate and dissuasive," as well as highlighting that they will enforce a "maximum" fine if they see the need. They have also stressed that there will **not** be a leeway period after 25 May - if anything one suspects they will look to make examples of non compliant businesses.

1988	2018
The National Lottery started it's live draw	We can buy our Lotto tickets via our smartphones
Ireland beat England 1-0 in the Euros.	Ireland unfortunately won't be at the World Cup
Paddy Power was founded	Paddy Power Betfair PLC is the number one online gambling company in the world
David Norris successfully took Ireland to court over it's criminalisation of homosexuals	Marriage equality is enshrined in legislation
Orinoco Flow topped the charts for four weeks	Ed Sheeran will probably top the charts for the whole year

The costs of a data breach include more than a potential fine. There are a number of issues which may need to be resolved and which could cost your business a lot of money.

IT & legal

Let's imagine that you have just been made aware that a breach of your IT systems has taken place . The first thing you will want to do is to

(i) discover the source of the breach, to close it off and
(ii) determine how many of your clients or employees have been affected
(iii) notify the DPC within 72 hours as per GDPR regulations

As such you will need IT experts to come in and investigate your systems and possibly seek legal advice.

Notification

When you have an idea of who's data has been compromised, it is likely that you will either want, or be instructed, to let them know. The total cost of this can be staggering - while the figure has been coming down year-on-year, it is still well over €100 per record according to IBM and the Ponemon Institute's latest study in 2017.

Monitoring

The data in question could potentially be used by criminals for financial gain. An obvious example is using your credit card details to purchase goods, but criminals have other uses for your data such as using it to perpetrate identity theft. It is conceivable that you may have to offer credit or identity theft monitoring in order to reduce the fallout from a breach.

Restore and repair

If you do have a breach , there will be costs associated with repairing and restoring your systems and data. Your business may not be able to fully function while this is all being resolved, which could result in a drop in turnover. We have seen real life breaches where it has taken businesses weeks and even months to become fully operational again.

Court costs

Aside from the potential for fines, there may also be liability if you are deemed negligent in how the data was stored or disposed of for example.

It also costs money to take senior staff out of your business for a period of time in order to respond to regulatory investigations or to deal with claims through the courts system. Defence costs and court attendance expenses can stack up very quickly.

As usual we include incidents we have come across on the last page of our newsletter

Cyber Insurance assists in becoming fully operational after an incident. Below are some benefits that comes with buying a policy - it could be an invaluable investment if something does go wrong.

Access to expertise

Insurers collate huge amounts of data. Take the WannaCry ransomware, or Locky in 2016. Insurers in-house analysts see these same incidents from all over the world and they quickly build up expertise on how to respond. For example they might tell you that there is no point in making payment as you're files won't be encrypted or they may even have come across a way around a particular issue such as a piece of code to remove it from your system.

Low cost risk transfer

The Cyber Insurance market is projected to grow exponentially over the coming years, which attracts most if not all of the big insurers. This is good news for businesses as insurers are keen to pick up this type of business. Premiums are currently extremely competitive for the level of cover on offer. The insurance could be the difference between continuing to trade or shutting the doors in the event of a catastrophic incident.

24/7 response

Cyber exposures don't tend to go away after the office closes. Any insurer that is offering this product must have the capability to respond to incidents anytime and anywhere. Some insurers will have consultants that will go straight to your office and co-ordinate an incident response if it's required. For more straightforward issues they should be able to assist over the phone or by email.

Helpful apps

Some insurers are upping their game with apps that can be downloaded to your phone or tablet and used to report incidents, request urgent assistance or even to review your policy details. The apps are free when the insurance is purchased and multiple employees can download them using a single common login.

Comprehensive Cyber Insurance policies are designed to respond to data breaches (including the physical loss of data). Policies can include:

- ✓ 24/7 incident response to help manage the incident - a great comfort if disaster occurs
- ✓ IT forensic costs to discover the source of the breach
- ✓ The cost of notifying those affected
- ✓ Credit and identity theft monitoring,
- ✓ The cost of attending investigations with regulators i.e. the Data Protection Commissioner
- ✓ Fines and penalties once they are insurable (not criminal fines)
- ✓ Liability that arises from the breach (i.e. claims from those affected) and court attendance costs
- ✓ Public Relations costs if the matter is going to cause adverse publicity for the firm

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.

CEO fraud

Criminals represented themselves as being the CEO of a firm in emails. In our experience, this type of fraud is prevented more often than not. However, it came during a busy time for the firm and an individual in accounts approved a payment of €15,000. We have previously highlighted similar losses which cost companies six figures.

Cyber crime

A contractor was defrauded out of over €50,000 in two fraudulent attempts. The accountant was asked to update bank details of a supplier. The firm in question did not verify that the instruction was genuine by picking up the phone - it was in fact a fraudulent email. Two invoices were paid to the bank accounts before the fraud was brought to light.

Network interruption due to hack

The headquarters of a business was hacked. The IT department were able to reinstate all consumer facing services within a couple of days. However they continued to suffer internal turmoil - they lost all old emails, had no internet access and had to close off their internal IT systems while they carried out repairs. This interruption lasted for several weeks.

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.

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, buildings 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.