Volume 1, Issue 2

Quarter 2 2016

Risk Management Newsletter

The Data Protection Edition

In this month's issue we focus on Data Protection, specifically the new EU General Data Protection Regulations (GDPR). It is essential that businesses begin preparing for these now.

- Part 1 includes a summary of just what the proposed changes will be.
- In Part 2 we look at what these changes mean for Irish businesses.
- Part 3 focuses on the importance for senior figures in companies to be up to speed on these regulatory developments and to lead the way.
- We also include an overview of what we are seeing from existing clients.

The new GDPR regulations

WHO is driving the new regulations? The Article 29 Working Party – a European Commission group consisting of representatives from each of the EU Member States' Data Protection Commissioners.

WHAT are they? A set of data protection regulations coming into force across the EU.

WHEN are they being enacted? They were approved by European Parliament in December 2015 and member countries have up to two years to bring them into effect. They are widely predicted to come into effect in quarter one of 2018.

WHERE are they going to be in effect? Any business that is established in the EU, that offers goods or services here, or that monitors the behaviour of EU residents, will be subject to the regulations.

WHY are they required? EU citizens want control of their personal data and how it is used and retained. The new legislation will give citizens more control over this data by modernising data protection legislation and by harmonising the legislation across the EU bloc.

Positive moves most would agree. However there are some important proposals for businesses from the new regulation including:

Mandatory reporting	in the event of a personal data breach a firm must advise their Data Protection Commissioner within 72 hours.
Fines & penalties	firms can be fined up to €20m or 4% of turnover per breach, whichever is the greater.
Processing personal data	clients will have to give "clear affirmative action" to their data being processed.
Data Protection Officers	companies that process sensitive personal data will have to appoint DPO's.

The full EU proposal is available for download by clicking this **link**.

In February we were delighted to take part in a seminar titled ***'Social Media in the Workplace'*** which was held in both Cork and Dublin—it is coming to Galway soon. Our co-presenters were law firm Ronan Daly Jermyn, HR consultants Voltedge and IT security firm Zinopy. The content was very well received, and we carried out a survey of attendees afterwards which revealed some interesting responses:

57% of respondents had experienced at least one type of inappropriate social media incident in the workplace, related to use of:

- Internet **(46%)**
- Mobile phones **(27%)**
- Personal devices at work **(18%)**
- Comments made online **(9%)**

In addition:
- One in five **(21%)** respondents do not feel that their organisation has enough Social Media security policies in force
- **28%** had purchased insurance cover to protect themselves from these exposures

Risk Management Newsletter

We asked **Brian Honan of BH Consulting** exactly what the new EU regulations mean for Irish businesses.

Brian Honan is recognised internationally as an expert in the field of information security and has worked with numerous companies in the private sector and with government departments in Ireland, Europe and throughout the United Kingdom. He has also provided advice to the European Commission on matters relating to information security. In 2013 Brian won the SC Magazine Award for Information Security Person of the Year in recognition of his contributions to information security and he was named as a Top Influencer of Security in 2015 by Tripwire. He has just been inducted to the Infosecurity Europe 2016 Hall of Fame.

Getting Ready for the EU General Data Protection Regulation

Information is the lifeblood of today's business world. With timely and accurate information business decisions can be made quickly and confidently. Thanks to modern technology, today's business environment is no longer constrained by physical premises or office walls. We can work on laptops, smartphones or tablet computers and with nearly ubiquitous internet connectivity we can work from any location.

This technology evolution allows us to be more productive and work with clients in many different ways. We can engage with them over the internet, visit their homes or offices, or they can come into our offices where their requests can be processed quickly and effectively. While bringing many benefits technology also brings with it many threats. With companies gathering more and more information on their customers to provide them with more services there is the increased risk of damage to those individuals should a company suffer a security breach. This information if improperly exposed could cause a lot of embarrassment to the people affected or, should it fall into the hands of cyber criminals, could have severe financial impact on them.

The European Union's Data Protection Directive is concerned about any information, either by itself or used with other pieces of information, that could identify a living person. This information could be items such as email addresses, passport numbers, driver's license numbers, financial details, union membership, medical history or information relating to a person's sexual, religious or political beliefs.

On the 15th of December 2015 the EU agreed to replace the existing EU Data Protection Directive with the EU General Data Protection Regulation (EU GDPR).

The EU GDPR brings in new obligations to companies that handle information belonging to individuals and this will come into effect over the coming 12-18 months. Under the EU GDPR there will be a number of new rules for companies such as companies who process a lot of personnel data will be obliged to appoint a Data Protection Officer, companies who suffer from a security breach will be obliged to notify "the supervisory authority" without delay or within 72 hours, and there will be fines for companies who are proven negligent in the case of a security breach, to name but a few.

There new rules will have implications for how businesses handle and secure the personal data entrusted to it by its customers and staff. While it will take time for the EU GDPR to come into full effect, it will also take time for companies to be properly prepared for that eventuality.

BH Consulting have prepared a checklist for firms to measure their preparedness for the GDPR and to identify what areas, if any, need addressing. It is separately attached to this newsletter. If you have been forwarded the newsletter and would like a copy please send an email to cyber@oli.ie requesting same.

Risk Management Newsletter

It is essential for management to be aware of the new regulations and to have their organisation prepared by the time they come into effect.

The new GDPR regime – no excuse to bury your head in the sand

The new EU regulations are projected to come into force in 2018. They are being well flagged to Irish businesses; have no doubt that the Data Protection Commissioner will expect companies to be prepared, there won't be a honeymoon period. Be it locking away client files out of office hours, adding encryption to emails on mobile devices or adding another layer of authentication before processing bank transfers, every company is going to have to ensure a culture exists where client and employee data is adequately protected. This must come from the top and permeate through organisations. Cyber security should form part of board meetings and staff need to be adequately trained.

Irish businesses are beginning to wake up to the fact that for all of the obvious benefits of technology, each step forward brings new security issues. Criminals target the weakest security link in firms of all sizes to obtain their data; for example by targeting point-of-sale hardware in retailers. Another method is leaving so-called 'road apples' outside of firms, such as a Smartphone left on the ground with a dead battery; when an unsuspecting employee picks it up and brings it inside to charge (using their computer), the criminals have bypassed security and are 'in'. As the Internet of Things (IoT) expands, ensuring more and more of what we use every day is connected to the worldwide web, it increases potential areas for criminals to exploit. And no matter how good a company's procedures are, there is always room for human error.

Point of sale machines are commonplace in shops, bars and restaraunts

So what hope for senior management in a firm to keep abreast of developments and new threats to their business?

There is still plenty of time to ensure proper procedures are put in place to best protect your firm. If you or your firm are guilty of burying your head in the sand up to now - start small. Banks, government departments, even utility providers have all been hacked. All of the evidence indicates that the majority of people reading this will experience a cyber incident – ransomware, hacks, phishing attempts – in their firm at some stage, if it hasn't already happened. It's how your organisation responds that will count. If your servers are taken down, were they recently backed up elsewhere? Have you contingency plans if staff cannot access your network?

There are simple risk management steps which every company can implement (as featured in our last issue). As insurance brokers we leave this advice to the experts. However we will continue to pass on what we are seeing happen to our clients to spread awareness (see the table on the next page). It's important to filter out what is irrelevant and to focus on what is important to you and your organisation.

Reliance on technology is here to stay. A company can both embrace it and use it as a tool to grow their organisation, or they can ignore it and risk stagnation or extinction. We are seeing clients talk about gaining formal recognition by accredited organisations around their data protection as a means of promoting their business to clients – as people become more aware of their rights firms will need to promote their ability to protect data and to use it properly.

As you will see on the following page, regardless of regulation, cyber risk management is essential across all industries. Even the best IT Security firms will admit that they can't guarantee 100% that they will eliminate all risks to a company. Prudent firms are realising that insurance is a valuable part of the solution as it takes much of this evolving risk away from the company balance sheet.

Risk Management Newsletter

The below are a sample of matters advised to us from firms of all sizes across a range of industries. We share updates on our LinkedIn and Twitter pages to educate our clients, feel free to subscribe:

LinkedIn: https://goo.gl/u06ncG Twitter: @OLearyInsurance

Industry	Description	Loss date	Quantum
Legal	Cyber crime	2015	€40,000
Healthcare	Telephone Hack	2015	€8,500
Financial Services	Phishing	2015	€8,000
Retail	Cyber crime	2015	€20,000
Legal	Cybercrime	2016	€15,000
Construction	Ransomware	2016	Large - lost tender, systems required repair
Financial Services	Ransomware	2016	24 hours business interruption 2 Bitcoin (USD $1,000)
Services	Malware	2016	4 days business interruption 2 days data
Motor	Ransomware	2016	Unknown
Food	Cyber crime	2016	€38,000
Retail	Cyber crime	2016	€19,000
Legal	Cybercrime	2016	€6,500 (halted by bank and recovered)

O'Leary Insurances specialise in placing Cyber and IT insurance for clients across a number of industries. The average premium our client's pay for a comprehensive tailored Cyber policy is under €1,700. For most firms, a proposal form should take no more than 5 minutes to complete.

If you wish to discuss further please contact us.
For new clients please contact Brian O'Mara — bomara@oli.ie or 021 453 6860.

About O'Leary Insurances

Insurance Brokers & Consultants, Est. 1961

From an initial complement of three staff in 1961, Archie O'Leary, now Chairman of O'Leary Insurances, has successfully overseen the growth and development of an Insurance Brokerage which specialises in providing a high level of customer service throughout Ireland.

With over two hundred employees now operating from nine 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 or risk management advice.

Thank you for reading.