Volume 2, Issue 4 Quarter 4 2017

Risk Management Newsletter

Cyber Security for Individuals

In this issue we look at how data breaches can affect individuals, provide some tips to improve your cyber security at home, and we investigate how the insurance market is responding to cyber threats to individuals.

Our reliance on technology doesn't stop when we leave our place of work. Most readers will use online banking, have at least one social media profile, and the more tech-savvy may be able to control their household appliances such as their home heating via phone apps.

However, outside of work we don't have the IT department looking out for our wellbeing! We also have to be conscious of our data - who has what, how it's used, stored and disposed of.

Recent data breaches

What do the Irish National Teachers Organisation (INTO), mobile parking service Parkbytext, HR / pensions administration firm Peoplepoint and Musgraves (owner of Centra, Super Valu, Mace Daybreak and more) have in common? All have had data breaches which have affected Irish people this year.

With new EU-wide data protection legislation on the way in 2018, we're about to go through what citizens in other countries have been experiencing for some time now - correspondence from service providers that our data may have been compromised. It doesn't mean it hasn't happened before, it just means that from May 2018 companies will have to tell the Data Protection Commissioner if they have had a breach of personal information. You will need to consider what action you will take if your data is compromised.

In this edition

Your personal data matters

Should you be concerned if someone has taken data relating to you or your family? It's going to happen anyway, right?

Below are examples of what purposes your personal data can be used for if it is taken in a data breach:. The chart is illustrative only, but hopefully it gives you an idea of why you should care if a breach affects you personally.

Data type	Used for (examples):	Potential value to criminals	Comment
Account password	To gain access to other accounts of yours	€€	If the account in question isn't valuable to criminals, they will try this password on other accounts you may use e.g. banking
Bank logon details	Cybercrime	€€ - €€€€€	Depends on how much funds are in the account
Credit card details	Cybercrime	€€€	Can be cancelled immediately - limited financial loss
Date of birth / driver licence / home address / telephone no. & more	Identity theft, phishing	€	On their own not particularly valuable, but when put together these pieces of information can facilitate identity theft.
Medical information	Insurance fraud, blackmail, identity theft	€€€€€	This data can sell for up to 10 times more than a valid credit card detail on the black market. A card can be cancelled, If you have a medical condition which could cause embarrassment there is little you can do to alter it.

Hole in ~~One~~ Two

We are pleased to advise that our esteemed colleague Evelyn Kelleher has on occasion been asked to obtain insurance for "Hole in One" golf competitions. She has just had her **second** "successful" claim in respect of same!

If you would like to speak with Evelyn regarding this cover (or about next week's lotto numbers!) email ekelleher@oli.ie.

Protect yourself at home

Cyber security risks for individuals are similar to those of businesses - data getting into the wrong hands, damage to our computers or financial loss due to cybercrime.

Cybercrime attack on a pension account

In August, a customer was emailing one of our financial advisors about his pension. However, the customer's email account had been hacked. The criminal built up a profile of how the customer conversed with his advisor and then sent the advisor an email purporting to be the customer. The criminal used the same language the customer would have used in an attempt to have some of the funds cashed in and sent to a bank account. In this case the pension advisor was vigilant and a funds transfer was prevented, which was of great relief to our customer.

Here are some tips that you can implement at home in order to improve your personal cyber security.

No.	Tip	Explanation
1	Spice up your passwords...	Is your online banking password the same as for other logins? If so, what happens if one of those websites is hacked? Hackers now have ALL of your passwords - and they will start testing them!
2	...and change them!	Be honest - when did you last change your password for important websites? As a test, the author just changed his online banking password for the first time in too long - it took just two minutes.
3	Protect yourself	Ensure computer anti-virus is up to date and backup your data regularly.
4	Think about Wi-Fi security	Wi-Fi in airports, cafés, hotels - wouldn't they be great targets for cyber criminals? (HINT - yes). Tens or hundreds of people logging in and browsing the web, reading confidential emails, checking online banking etc. How can you know if these Wi-Fi spots are secure? It is better to conduct 'sensitive' browsing at home - anything involving using a credit card or private information for example.
5	Don't open suspicious emails / links	This one is fairly basic but people can often need reminding!

Don't forget, we include some recent examples of cyber incidents at the end of the newsletter.

From May next year, companies will have to disclose if your personal data has been breached under new EU legislation. Some are already doing so as mentioned in our introduction.

Consider how much personal information you give to companies and what you will do if that data is stolen. Think of who has your data, and how much of it they have. There's your bank or building society, and your GP. Do you have a loyalty card with a retailer? What kind of information does your insurance company have? Do you have social media accounts? Email addresses? Shop online?

We've all probably forgotten about giving our personal details to some websites that asked us to register accounts. It's probably a real A to Z - from associations and accountants to your nearest zoo!

If you find out that your data has been taken in a data breach, what should you do?

No.	Tip	Explanation
1	Go to the source	Go to the website of the company that has been breached for up-to-date information on what has happened. Do not trust emails, texts etc. - these could be from opportunistic individuals looking to profit from such breaches.
2	Change that password	Your password may have been taken in the breach - change it immediately. Choose something stronger!
3	Credit card details	If these have been stolen, cancel your card and request a new one.
4	Monitor your bank a/c	In breaches where banking details have been taken, regulators often instruct the company affected to offer complimentary credit monitoring to those affected. Avail of this if it is an option.
5	Think before you type.	For governmental and banking websites your personal details need to be correct. However, for many websites you just want a login to get rid of their annoying pop-ups asking you to register. Do you need to give this particular company your full / real address, date of birth etc.? Should you set up an email address just for these accounts so that their mails don't clog up your inbox?
6	Consider a change	Is this the first such breach? Do you feel the company in question did everything they could to protect your data? If not, would someone else do better?

These are just some suggestions. Have you some tips of your own that you would like to share? Let us know - contact us by email or social media - our details are at the top of page 4.

The insurance market has been very quick to try to respond to the cyber needs of commercial customers. Has this been the case for personal lines customers also? We investigate.

Can I buy Cyber insurance in Ireland as an individual?

Two words - "yes, but". Such cover exists, but thus far it is only available via providers of Household Insurance products.

"*But most people buy Home insurance*" I hear you say.

True, however these 'Cyber' covers are only offered by a limited number of those insurers. More particularly, those insurers that offer bespoke policies to clients - typically higher net worth (HNW) individuals.

Why haven't the other insurers got on board?

The cost; purchasers of Home Insurance are often focused on price when comparing products. And the extra premium required to provide adequate 'cyber cover' may be beyond most household budgets.

Where it is available, what is covered?

Typically :

- computer repair after an incident
- theft of funds after a hack
- cyber extortion
- theft of funds after social engineering / phishing attack
- media liability (e.g. online defamation)

Will this change anytime soon?

Standalone personal cyber insurance does exist, however not yet in Ireland that we know of. As people become more aware of the risk and if individuals continue to experience loss then it is only natural that the demand for this cover will lead to insurers responding. Whether that will be by adding cover to existing policies such as Household or by a separate policy specifically remains to be seen.

If you would like to speak with us about Cyber Insurance, either for a business or as an individual, please contact whoever you normally deal with, email cyber@oli.ie or call us on 021 453 6860.

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: @OLearyInsurances

Below are a selection of cyber incidents that we have come across recently. As usual, these are all real-life Irish cases.

Data protection fine

Our client is a retailer and undertakes marketing campaigns. An individual had opted out of a previous campaign, but the retailers systems failed to realise this and they sent more marketing material to the individual in question. The individual complained to the Data Protection Commissioner (DPC) and our client received a fine. The DPC's enforcement powers are increasing from May 2018 under the GDPR legislation, as referenced in previous issues.

Telephone system hacked

In July, a clients telephone system was hacked. This is something we are seeing more and more of among our clients, quite often due to weak or obvious passwords on voicemail accounts. Calls were forwarded through their exchange to a premium toll number. The phone bill was over € 8,500 and our client was appealing this with their service provider.

Identity theft and reputational damage

Company A was contacted by an individual who had received an invoice from them - despite never having used Company A's services. The criminal had created fraudulent invoices and was (or possibly still is) hoping that an unsuspecting accounts department will think the invoice is legitimate and pay monies to their bank account.

If you wish to discuss further please contact us. For new clients please contact cyber@oli.ie - we have 9 offices around Ireland to respond to your needs.