Volume 4, Issue 3

Quarter 3 2019

Risk Management Newsletter

Cyber Security update

The world of Cyber Security can be intimidating, so it's good to be able to bring some positive news to our latest newsletter. It has been a good quarter in terms of fighting cyber criminals, and we also include some practical examples of malware as well as Cyber Security advice from PWC .

Some battles won...

Let's start at home - the announcement of the launch of **Cyber Ireland** in May was a welcome development. It has been formed after engagement across private companies, academia and government departments and it's goal is to ensure Ireland becomes a global cybersecurity leader. The cluster should help growth of this industry locally, which will hopefully lead to more job creation.

Internationally, ten members of the GozNym cyber crime network were charged in the US after an international collaboration. The gang had stolen an estimated USD $100 million from over 40,000 people using malware.

Cyber crime awareness generally is on the rise. Events such as those held in May by The International Fraud Prevention Conference in Dublin and IT@Cork's Tech Summit - which included a live hack - can only help.

...but the war isn't over

We all hear and read the various estimates on the cost of cyber crime, both here in Ireland and globally; suffice to say the GozNym loot is a drop in the water. Whatever the exact amount of the proceeds of cyber crime, the fact that it is considered bigger than the drugs trade on a global basis speaks for itself. Vive la résistance!

In this issue

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

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.

Cyber Attacks

What are the most common forms of Cyber attacks affecting companies? And just who are these cyber criminals carrying out these attacks?

Question: What do Cricket Ireland, the Football Association of Ireland and Luas have in common?
Answer: All three were subject to cyber attacks in recent months.

Luas was hacked back in January with over 3,000 user records potentially compromised. The FAI discovered it had been the victim of a hack in June, with speculation that salary and bank account details of FAI employees had been targeted. Also in June, Cricket Ireland had their emails compromised. The hackers then contacted a commercial partner and defrauded them of a 'six figure' sum which has forced the organisation to request advanced funding. This last attack has cost Irish businesses, clubs and individuals over €4.5m this year according to the Sunday Independent.

Gone Phishing

Microsoft's 2018 Security Intelligence Report highlighted that ransomware and malware threats reduced both in Ireland and globally last year. Meanwhile the number of phishing attacks increased. This correlates with what we saw among our own clients, with some very sophisticated fraudulent emails resulting in large losses to our clients - as outlined in previous issues.

The method of attack is largely irrelevant to the victim - incidents that cause damage to IT systems or cause loss of company or client monies can be devastating, regardless of how they occur.

Have laptop, will travel

So who is carrying out these attacks? Firstly, there are plenty of opportunistic individuals looking to make some easy money - it is possible to do so with relatively little knowledge, and a hack takes a lot less physical effort than burgling a house. Larger and more organised attacks tend to originate from well resourced criminal syndicates such as GozNym (prior page) and even from nation states.

Glossary	
Malware	**Mal**icious Soft**ware** which can harm your computer (e.g. virus, ransomware)
Phishing	Fraudulent emails attempting to obtain sensitive info
Ransomware	A type of malware that denies access to files / computer system until a ransom is paid

Estimates on the cost of cyber crime to the economy vary. A recent study looked at the cost charged by criminals to carry out such attacks - click here for external link. Researchers posed as customers enquiring on the cost of a wide variety of cyber-attacks such as tailored malware attacks, phishing campaigns, industrial espionage and insider information and the sample charges are hereunder:

Type of attack	Cost per attack (USD)
Remote logins to corporate networks	$2-$30
Targeted attack on company	$4,500
Targeted attack on individual	$2,000
Phishing kits	$40
Fake Amazon receipts and invoices	$52
Espionage and insider trading	$1,000 - $15,000

Ransomware in action

Baltimore (USA, **not** Co. Cork!) city's government has been on lockdown since May 7th due to Ransomware. This has affected everything from payment of water bills to real estate sales. The Mayor of Baltimore estimates that the disruption will cost the city $18m - a figure which could rise further.

There is a growing awareness among the public of how common such cyber attacks are. While comprehensive Cyber Insurance policies are available, these should be the final step in a company's risk management programme; insurance should not be used to replace good risk management.

Companies must take steps to improve their own risk management, while also having a plan in force of how to react if a cyber attack does occur. The article on the next page offers tips on how to help reduce your cyber-risk.

We also include the usual real-life examples of malware and phishing incidents on page 4.

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.

Risk Management Newsletter

Demystifying Cyber Security

William O'Brien of PwC provides tips for Irish businesses to help reduce their cyber-risk.

What is Cyber Security?

Cyber Security is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users or interrupting normal business as usual activities.

The Challenge

Implementing effective cyber-security measures is particularly challenging in today's environment as there are more electronic devices than people, and cyber-criminals are becoming more innovative. In a space that is experiencing continuous development, such as new technologies like Artificial Intelligence and Machine Learning, the question I often get asked is – "*is it possible for a small to medium enterprise to operate an effective Cyber Security program*?" I believe it is and it is with this in mind I have developed some practical steps any organisation can take to mitigate cyber-risk.

Practical First Steps

The research shows that getting the basics right can drastically lower your risk of a cyber-breach. It is in my experience that small and medium enterprises should begin by focussing on these 10 steps.

Education and Awareness	Staff are the first line of defence. All staff should be educated in security procedures and made aware of threats.
Cyber Risk Management	Cyber Risk Assessments are carried out to identify, analyse and evaluate cyber-risk. Ruthless prioritisation is key for any program with a limited budget and risk assessments should be used to guide your investment of resources. Risk management programs prioritise potential risks based on likelihood and impact, leading to a plan to minimise, monitor and control risk. Risk management can and should be carried out by organisations of all sizes. Directing the area of focus can often reduce cyber-security spend.
Network Security	Connecting to the Internet puts your network at risk. Defend your network perimeter, filter out unauthorised access and malicious content and most importantly test your security controls.
Security Misconfiguration	Security misconfigurations are one of the most common gaps that hackers look to exploit. To safeguard your programme from attack, security measures should be implemented when building and adding network devices.
Monitoring	Monitoring your network is key to detecting and responding to attacks. Effective monitoring is fundamental to building a basic level of Cyber resilience.
User Privileges	Access to sensitive information and permissions should be kept to a 'need to know' basis.
Incident Management	In the era of GDPR the need to be able to quickly and effectively respond to a data breach has never been so high. Incident Response plans should be developed and rehearsed regularly.
Malware Prevention	Anti-malware policies are a must to reduce the risk of malware gaining access to your system during information exchanges.
Removable media controls	Access to removable devices needs to be controlled and monitored and are a vulnerability for many small and medium enterprises.
Mobile and home working	Mobile working exposes the system to new risks. Mobile working policies need to be developed and staff should be trained in accordance.

You can't eliminate Cyber risk and you may not have access to the most sophisticated solutions on the market, but I believe that through prioritisation an effective Cyber Security program is within reach for organisations of all sizes.

Editor's note - Cyber Insurance can be sourced which would be tailored to your business requirements as a final safeguard.

If you have any queries or comments you can contact William as per the below.

¦t¦ 087 194 7803 ¦e¦ will.obrien@pwc.com ¦w¦ www.pwc.ie

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.

Malware

The organisation in question, a clinic, held confidential data on patients. Suspected malware activity resulted in the disappearance of a number of files and folders. Costs were incurred to resolve the initial issue and to restore files.

Phishing

An employee clicked on malicious email link which affected their computer. However, all of that individuals email contacts were then sent the same malicious link, spreading the damage further. This email circumvented internal spam restrictions as it was sent as one message to colleagues and clients.

Hack resulting in data breach

An email address within a solicitors practice was hacked. Of the several hundred files containing personal information that were compromised, a small number were deemed sensitive with one being extremely sensitive. The firm in question had to establish who needed to be notified and to let them know what had occurred. They also had to open a file with the Data Protection Commissioner.

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.

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.