Volume 5, Issue 2 Quarter 2 2020

Risk Management Newsletter

Remote Working

COVID-19 has resulted in a marked change in how we work, and how we will work into the foreseeable future. It is important for companies to be cognisant that there are cyber security considerations that come with remote working,

Are you 'wfh'?

Since the outbreak of the virus here in Ireland, 'Working from Home' has become part of our everyday lexicon. It is a fantastic resource for those that can avail of it, offering the opportunity to keep working during these difficult times.

Many companies are expanding their capabilities so that even more employees can log on from home. It is important that this does not come at the expense of good cyber security.

Coronavirus - an opportunity to some

Cyber criminals consider themselves exempt from most of the positive examples of human decency that we have been seeing at this unusual time. On the contrary, many are using the virus as an opportunity to ramp up their activities. Cyber security firm CheckPoint have advised that Coronavirus-themed domains are 50% more likely to be malicious than other domains.

Many of us will have experienced increased phishing emails in recent weeks — we include examples overleaf. Also, individuals in key supply chains (shipping, transport and retail) are being sent attachments claiming to include safety measures — once opened a ransomware strain is released. As usual, employer training and employee vigilance are key.

If there is anything you would like us to include in future newsletters please let us know - cyber@oli.ie.

Cybercriminals exploiting Coronavirus

Public concern and working-from-home mandates are providing opportunities for cybercriminals.

The below is from an advisory by CFC Underwriting, a specialist Cyber Insurer.

Coronavirus increasingly being used in phishing attempts

As new cases of the Coronavirus continue to be reported daily, cybercriminals have been leveraging the situation to take advantage of those looking for information on the outbreak. Scams include the following and are changing each day:

- The Sophos Security Team has spotted emails impersonating the World Health Organization (WHO). The emails ask victims to "click on the button below to download Safety Measure". Users are then asked to verify their email by entering their credentials, redirecting those who fall for the scam to the legitimate WHO page, and delivering their credentials straight to the phisher.
- Interpol has warned of a large increase in fraudulent websites claiming to sell masks, medical supplies and other high demand items that simply take money from victims and never deliver the promised goods. It is advisable that internet users purchase items only from established and reputable sources.

- There have been reports of airlines and travel companies being impersonated by fraudsters in a bid to either obtain sensitive information, like passport numbers, or install malware on victims' computers. They may say they want to advise you of COVID-19 infected passengers on past flights you've taken or offer discounts on future flights. When in doubt, we advise users to be vigilant when clicking on any links, delete any suspicious emails, and not disclose sensitive information if you are approached unexpectedly.
- Fraudsters are also developing fake charitable donation campaigns which claim to help individuals and communities impacted by the Coronavirus. Any money donated is sent to fraudulent accounts. Again, if you are wanting to support relief efforts, make sure to research the organizations you are looking to donate to.
- A Twitter user has identified another malware campaign purporting to be a "Coronavirus Update: China Operations". The emails have attachments linking to malicious software.

As global concern about the coronavirus grows, it is likely that threat actors will continue to abuse this outbreak to their advantage.

Cybercriminals exploiting Coronavirus continued

Increased remote working can open gateway to hackers

Remote desktop protocol (RDP), when set up correctly, is a great tool for remote working. However, using it without multi-factor authentication (MFA) enabled or on an insecure network can open the gateway to hackers.

> "In fact, in 2019, 80% of the ransomware attacks we handled were initiated through RDP."

Businesses that start using RDP for remote working during the outbreak should be aware of some of the cybersecurity risks it can pose and ensure it is being used securely. Employees should always log on within a trusted network and ideally work with their IT department to secure personal devices – and implement MFA – prior to remote working.

CFC recommendations - we suggest implementing the following steps to bolster security:

1. Test remote log-in capabilities

Not only should personal devices be configured for secure remote working, but business should ensure that multi-factor authentication (MFA) is set up immediately. MFA is an authentication process that requires more than just a password to protect an email account or digital identity and is used to ensure that a person is who they say they are by requiring a minimum of two pieces of unique data that corroborates their identity. Implementing this significantly reduces the chances of cybercriminals being able to log into a business's RDP.

2. Train your employees on how to spot a phishing email

As a CFC cyber policyholder, you can get free access to a range of risk management tools, including CyberRiskAware, an e-learning tool focusing on phishing attacks. This valuable tool teaches people within your business to be more vigilant when in comes to opening attachments, clicking on links, transferring money, or sending sensitive information.

3. Prepare for operational disruption in advance

Put simply, prepare for the worst. As with so many cyber incidents, time is of the essence so ensure you have an incident response plan in place, a template for which you can access for free as a CFC cyber policyholder. And as ever, if you believe that one of your employees has fallen victim or that you are experiencing any kind of cyber event, notify CFC as soon as possible so that we can help you.

4. Finally, be vigilant

What's becoming clear as this pandemic plays out is that cybercriminals are shifting tactics daily. If you see something on social media or receive an unsolicited email that seems too good to be true, it probably is. Aside from learning how to spot phishing emails, make sure to do your research, use reputable companies, and follow-up requests for money or information with a phone call using a number from a separate, trusted source.

To access links related to points 1 & 2, please visit the CFC website: click here.

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.

Solicitor - Cyber Crime / Data Breach

We included an example in a previous newsletter whereby a solicitors practice was hacked and the end result was that the practices client received fraudulent bank details by email, and transferred over €50,000 to criminals based on this.

By way of update, the firm in question made a claim under their Cyber Crime Insurance policy. During investigations it became apparent that IT security settings were not in place, despite a previous breach. The Cyber insurer in question made no issue of this as their wording has no way of avoiding cover for human error—many other policies would not have paid the claim. This highlights the importance of a good policy wording.

Technology firm — Ransomware leading to a data breach

The company in question provided software to an association in the UK. The tech company agreed to act as data processor and put in place appropriate measures to ensure security to member's data. A ransomware attack was made on the tech company's computer system in October 2019 but was only discovered by them in January 2020. They have notified both the association and the ICO (UK Data Protection office).

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	Maria Murphy	091 778 677	mmurphy@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.