COVID–19 Cyber Threat

In this uncertain period it is critical that you have a comprehensive and clear policy on remote working and that all staff are issued with summary guidelines highlighting the key messages and requirements.

In addition to ensuring there are remote working procedures, it is important to pay attention to the risk of cyber threats which are now more likely to occur due to the increase in home working and the reliance on virtual networks.

1. Phishing scams

With many now working remotely, it is a good time to remind employees of key policies, what to look out for, and the need to be vigilant. Cyber criminals are making the most of the current circumstances and with the increase in email traffic it's likely that phishing/scam emails will become more frequent.

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Cyber criminals have always targeted individuals as well as industries, and with new cases of the Coronavirus being reported daily, cyber criminals have begun to take advantage of the situation and people looking for more information.

A UK security software and hardware company recently spotted emails impersonating the World Health Organization (WHO). The emails ask victims to "click on the button below to download Safety Measures". 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. The BBC recently ran a report base upon research from the cyber security firm Mimecast who flagged a "tax refund" scam. In this an email was sent to individuals and businesses alike notifying them of a tax rebate with a link to a fake GOV.UK website that required you to input your national insurance and tax details.

2. Remote / Home Working

As noted above, it is key that employee are aware and understand the company's policy relating to working from home. This should also extend to wider issues about ways of working; rules for taking hard copy files and documents out of the office, and protocols for telephone/other conversations in public, as well as security precautions to be taken to reduce the risk of lost devices (memory sticks, smart-phones, tablets and laptops) are equally important.

With the UK's borders now closed and the majority of people working from home, cyber criminals are looking to leverage weaknesses in business' remote desktop protocols (RDP). One of our partner Insurers, who specialise in Cyber Insurance noted that in 2019, 80% of all ransomware claims were as a result of attacks initiated through RDP. Businesses should ensure that they are using multi-factor authentication and that their employees are working with their IT departments to secure personal devices. They released a case study regarding one of their clients, a private school, who suffered a loss in such a way. The criminal used software to scan the internet for weak connections, and found that the schools RDP was available to connect to publically, they then ran a brute force program (software which uses thousands of common passwords) to gain access to the administrator account, and unfortunately were successful. As the school had no multi-factor authentication the criminal

was able to commit ransomware and encrypt the school's data in exchange for payment of 2 bitcoins (roughly £10k).

3. Secure Access

Most people use the same or similar version of a password for everything, even between work and home. Unfortunately, this means a single stolen password can be reused on multiple sites to unlock dozens of accounts for hackers. Remembering secure and complex passwords for every account can be difficult, if not impossible. Use password management software to ensure you have strong, unique passwords for everything, because passwords are the foundation of sound online security practices. Additionally ensure that all computers and devices being used to access work systems are operating on up-to-date supported operating systems. For example, as of January 2020, Windows 7 is no longer supported by Microsoft, and computers using this operating system are more prone to cyber attack.

Ultimately it is important to be vigilant, but unlike physical risks cyber risks are often invisible until the inevitable has already occurred - If you are uncertain as to the scope of cover you have concerning your cyber risk, please do not hesitate to contact a member of our team to ensure there is the appropriate level cover is in place.

Nacora Insurance Brokers
Thomas Langridge
Head of Customer Relationships and Development
Thomas.langridge@nacora.com