howden

# Cyber Risks and Work from Home

With social unrest and then the spread of Covid-19, many employers have encouraged or mandated their employees to work from home. This is a progressive step and has many benefits for employees and businesses but also comes with risks. As the rest of the world adopts what Hong Kong has been doing for months, several reports indicate a significant rise in cyber-attack and cybercrime, much of it playing on the anxiety caused by the Covid-19 virus.

Similarly, the amount written on cyber hygiene has been prolific. This document aims to provide a few short points to bear in mind without being too technical.

- Work from home means work from home. Resist the temptation to use the free wi-fi from the coffee shop. We all know they are less secure. If you must work away from home use a company VPN to access the network.
- Secure your home router with a strong password and, definitely, do not use the pre-set administrator one. You might want to do this anyway to stop your neighbour using it.
- Be even more careful about what you share on social media. Never share your online meeting ID or the URL to an online meeting, even through a direct message.
- Be even more careful about phishing emails. Most people are generally aware of these, but our guard goes down in times of anxiety. Be very careful about what you share online.
- If possible, do not use your home computer for work. Work issued laptops are generally more secure and contain up to date virus protection.
- Do not download apps to your work computer without your IT dept. permission. Often the company software will prevent this but that will not always be the case when working remotely. Resist the temptation, however flashy they look.
- Always log off from the VPN when not working and always lock your computer screen when not using it. This is especially true if you’ve ignored the first rule and are not at home.

There are a few measures that companies can take to mitigate their risk.

- Issue an IT procedure manual and ensure that all employees are familiar with it. Conduct training to reinforce the procedures.
- Set up a VPN for use by employees working remotely.
- Maintain up to date virus and anti-malware systems and ensure that remote laptops are updated regularly.
- Back up data regularly.
- Require employees to use strong passwords and to change them regularly.

A cyber insurance policy cannot prevent you being targeted and cannot prevent your employees accidentally compromising your networks. But it can help you through the recovery process by providing

- Incident response
- Business continuity support
- Third party liability insurance

Work from home is likely to become a permanent feature of business in Hong Kong. So, the cyber risk will not abate as the biological one eventually will. Maybe now is the time to make this protection part of your risk management and insurance programme.