Cyber Risk Aware's: Do's and Don't for working remotely

The recent outbreak of the **COVID-19** virus has seen more people working remotely for their own and their colleagues' safety. Whilst there are many benefits to working remotely, we wanted to raise awareness that in doing so, there is an increase in cyber risk to the business, and while it is important to consider your employees' safety, it is imperative to ensure the security of your company data and the reputation of the business. Below are the most important **Do's** and **Don't** to keep your business safe from cyber threats when working remotely.

DO

Be extra vigilant to Phishing emails

Cyber criminals will actively use this crisis to their advantage and run scams such as pretending to offer government tax rebates or seek fake donations that steal your cash and credit card details for example. We strongly advise running simulated phishing campaigns and delivering security awareness training to highlight what a real phishing attack will look like and inform staff how they can report such emails to IT Security.

Use secure, company provided systems

While using personal Cloud systems for sharing or storing files when out of the office might seem to be efficient, it can come at a massive cost to your company. Using the Cloud isn't necessarily a risk in itself, but when misconfigured or using personal accounts rather than company accounts, it can allow unauthorized access and lead to sensitive data being stolen leading to potentially a reportable event to the local Data Protection authorities. Ensure you always use secure company provided systems and company credentials to manage your data and ensure all company data is backed up centrally and is not just stored on staff laptops or desktops.

Do put protocols and processes in place

Should a cyber incident occur, it's important you have protocols and processes in place,ensuring your staff know how to report, and to whom. Cyber Risk Aware offers PhishHuk, a free outlook plugin, which staff can use in their email ribbon to report phishing emails to IT Security.

Do have clear lines of communication

Often people will use unsecure means to communicate with each other, such as social media or Whatsapp, which can expose sensitive data. Do ensure you have safe means of communication in place, and that this is communicated to your staff. If email was to be suddenly unavailable owing to a cyber incident, how would you communicate with each other?

Do equip your staff

Provide employees with security standard, encrypted devices and a VPN where possible to ensure secure access to your company's internet without worrying about being targeted by cyber criminals. Also make sure all device systems are up to date with system and application patches, and that the anti-virus software and firewall is turned on.

Do consider cyber insurance

As we do not know how long the current situation will last, it is worth considering cyber insurance policies to ensure you are covered in case of an unfortunate security incident. Be sure to check the policies coverage and we would recommend both our partners CFC Underwriting and AXIS Capital who have the best policies on the market.

DON'T

Don't take the easy route

Shadow IT is a term for technology systems that are built and used within organizations without explicit organizational approval, and an increasing threat to businesses' cyber security. This can involve installing free software to help ease your workload such as a Macro for Excel, or software to grab screenshots, which, although efficient, can be the cause of a cyber incident as it may not come from a reputable source. Nothing is free in this world! If it sounds too good to be true, that is usually the case!

Don't connect to public WiFi

Connecting to open networks can lead cyber criminals to monitor all computer generated traffic, steal staff credentials and access sensitive company data such as intellectual property or personal identifiable information, which can be detrimental to your company and create liability issues. Use a company provided VPN or mobile data if accessing sensitive work systems or using company login credentials.

Don't forget to backup centrally

So important it is worth mentioning twice. Whether it be the concern of system crash or the risk posed by a ransomware attack, please ensure all backups are made daily, to a central location and that restores are tested regularly by IT staff.

Don't allow use of personal computing devices

The more devices you allow your staff, the higher the risk of a cyber incident. If they can do all their work using a company issued device, then that is what you should tell them to do. Staff must never use household, personal computers as they may be wholly insecure owing to a lack of security defenses, outdated operating systems or worse they may already be compromised unbeknownst to the staff member.

Don't forget password protection

When working remotely, make sure all devices are password or pin code protected, all files are password protected and if they need to be shared, use an encrypted zip file. If employees access networks remotely using only usernames and passwords, you need to include multi-factor identification to avoid credential stuffing attacks. It is also critically important not to have the same password across different accounts and we would highly recommend using a password manager. E.g. Lastpass, Thycotic for example