Cyber Security – Helpful Info and Tips for working from Home

With so many employees across multiple industries currently, or about to, work from home companies need to consider their cyber and privacy protocols.

Working from home can result in a watering down of a company's face to face oversight, its procedures, its compliance and its security. At the same time the company's exposure expands to each employee's home location and the personal devices they use.

On the 23rd March 2020, the Australian Financial Review reported coronavirus-related fraud reports increased by 400% in March. To combat the exposure an effective work from home plan should include a three-stage strategy; pre, during and post.

Before taking the leap, a company will need to determine if all employees have internet access and is the quality strong enough to sustain the entire family being at home. Which employees need access and what level of access is required. What security is in place at the home, are patches updated regularly, is the employee using secured Wi-Fi and could personal computers already have malware imbedded on them.

While working from home ensure an appropriate level of authentication is adopted and only access the company system when required. Know how customers and supply chain partners are operating in the crisis, and if their processes have changed be sure they are communicated to the relevant staff. Be extra vigilant of hackers wanting to take advantage of changing conditions, and of fake instructions to persuade an employee to take an action they shouldn't, such as transferring funds, paying an invoice or sharing private information.

When returning to work employees need to confirm no company material is saved on personal devices. All printed material which contains private information is disposed of in an appropriate manner - not in the household garbage bin! Company access is removed from all personal devices where it is no longer required.

Here are ten quick risk management tips to help transition to working from home:

1. Ensure strong user passwords
2. Activate two factor authentications
3. Use a VPN
4. Set up firewalls
5. Maintain antivirus software
6. Install updates and patches as soon as they are released
7. Regularly back up data
8. Be on the lookout for fake phishing emails or calls
9. Stay up to date with the latest work from home scams
10. Lock your device when not in use

The world is changing, and we all need to adapt accordingly to stay protected.