Client Advisory

Maintaining cyber security during lockdown

With the nation shifting to Coronavirus Alert Level 4, a large number of employees will spend an extended period remotely logging into secure computer network systems to continue their work activities from home.

This unprecedented increase in remote access traffic can create additional vulnerabilities in otherwise secure internal computer systems. During this time in particular, it is important to have some best practice policies in place to minimise the chances of a cyber event or data breach.

The following are some easy steps your business can take to reduce your exposure.

Stay up to date

Ensure all software being used by employees working remotely is up to date. Automatic updates can be turned on in the general computer settings areas of all laptops/PC computers and this will ensure that the computer itself checks for the most up to date operating software for installed applications every day.

It is also recommended that your employees conduct regular virus scans of their computer using the built in or purchased virus protection software. Security programmes such as MacAfee, Norton and MacKeeper all have scan options that will scan all files to ensure no malware or other harmful files exist on the computer. They can also be set to scan incoming attachments and online downloads prior to these being allowed onto the local network to ensure they do not contain malicious content.

Back up your data

Ensure critical business data is backed up, stored and easily recoverable (run tests to ensure the backup works as plan prior to closure). Using external or cloud based service providers is the safest practice as it ensures that your back up data is kept in a location separate to your business operation.

Training/cyber awareness for employees

In the current environment it is increasingly important to ensure your staff are security aware and take the right measures to protect themselves, the company and your customers. As staff work remotely it's a good time to remind employees:

- about the heightened risk that will unfortunately arise from coronavirus-related scams
- to keep their laptops within their physical control, and their screens hidden from others
- never to provide login credentials in response to an email request

- not to use less secure devices, such as the family computer, to obtain or store work information
- not to use personal email accounts to transmit work information
- not to transmit or store work information on their personal cloud storage accounts unless their companies specifically allow that practice
- not to leave written corporate materials in shared or unsecured locations
- even when at home, log off when not using network
- to use strong passwords and ensure they are required to regularly change them
- not to use public Wifi for work related activity
- to use two actor authentication for financial payments as invoice fraud schemes are on the rise in New Zealand.

Ensure your staff know how to spot common phishing attacks as these are already on the rise in the remote environment. Actions such as those outlined below can assist:

- hovering the mouse over the email senders address to verify that it has been sent from an authentic location
- only opening attachments from trusted senders
- ask for a second opinion from a manager in times of doubt before responding to emails.

One of our core responsibilities as a broker is to ensure you have all the information you need to make informed decisions about the risks your business faces. With the effects of coronavirus being felt in a number of ways by our clients across the country, we wanted to share some proactive advice to help you protect your business during this difficult and unprecedented time.

We hope you find the information above helpful, if you have any questions or if you would like to speak to us regarding cyber insurance please talk to your broker.