Best Practice Cyber Security for Remote Working

By: Peter Bailey, General Manager, Aura Information Security

With the heightened level of uncertainty enveloping the business community, your company's cyber security processes and policies are more important than ever. Think of the immense reputation damage and difficulty responding if your systems were subjected to a security breach during this volatile time.

Boards should be asking their executive team to make sure their IT processes and policies are adaptable to the home environment. Likewise, Directors should aim to lead by example and make sure they are forming their own good cyber security habits. Peter Bailey, General Manager at Aura Information Security, shares the steps businesses can take to improve cyber security outside the office.

1. **Review existing policies**

If you have not done so already, now is the time to review your cyber security policy and remind staff how to abide by the company security rules, even at home. For those yet to build a robust policy, there are some useful online tools and guides specifically aimed at smaller businesses and start-ups. A good place to start is the CERT website.

2. **Make sure your home router is secure**

When was the last time you changed your router password? If you fall into the large group of people who still have their home router set on the default password, now is a good time to change it. Set a unique password, enable encryption and remember the device itself requires routine software updates. Either find out from your service provider how to log on to do regular updates yourself or arrange for them to perform updates and checks on an ongoing basis.

3. **Don't overlook smartphones and mobile PCs**

With the proliferation of connected devices used in businesses today, there are many more potential access points for cyber criminals to break into your systems. If you work for a company that has an IT department then get their help to make sure all laptops and smartphones are up to date. If not, at the very least aim to do the following:

- Passwords: Always use unique passwords that are difficult to guess. Passphrases, with a mixture of letters and numbers, are the most effective and simpler to remember. Using a password manager is also a good option.

- Auto-lock devices: Make sure all your smartphones, laptops and tablets are set to automatically lock themselves when not in use. Biometrics, such as fingerprint sensors or facial recognition technology, are now available on most modern devices and are effective and simple to implement.

- Keep work devices for work: Don't let family members, especially children, use the devices you use for work. In fact, you should try to have dedicated work and personal devices where practical.

- Be wary of USBs: Avoid using USB drives, as hackers are known for using these as a tool to gain access to your systems. One corrupt USB can easily infect a device or an entire network. Save yourself the stress and avoid them altogether.

4. **Back up, regularly!**

With staff working away from the office in different locations, it's more important than ever to make sure documents and files are safely backed up. Ensuring your devices have an automated backup solution that takes data offsite and stores it in the cloud is a good option. Try to use the same services as those already used within your company to backup files you're working on, such as Office 365 or Google Drive.

5. **Keep software updates in check**

It's incredibly important to ensure your devices are up to date with the latest software - outdated software often has weaknesses that can be exploited by cyber criminals. Any device used for work should be configured for automatic updates or at the very least alert you when an update is available. Remember, companies issue updates for a reason, usually to address newly discovered vulnerabilities. As soon as an update becomes available, install it. While you're at it, ensure all your devices have a reputable internet security package, including antivirus, installed and up to date. This is a basic requirement for anyone who uses the internet.

6. Stay vigilant against 'Covid-19' scams

CERT NZ has already raised an alert warning New Zealanders to be aware of reports that cyber criminals are using Covid-19 themed scams. Phishing emails have been circulating around New Zealand businesses purporting to be from the Ministry of Health, with links to information related to the pandemic. We can also expect to see working from home themed scams targeting remote workers, which may appear to come from business leaders, HR departments or IT departments. While it may be your first instinct to follow the instructions, make sure to check the sender's email address before you act. Remind staff to use caution when receiving any request for log in details and think twice before they click links or download attachments. If you receive a strange email from a known contact or colleague, call the sender to verify the information.

7. No shame, no blame

Remember no business is ever 100 per cent secure and cyber security requires an 'always on' approach. If you think you have been victim to a cyber scam or breach, don't keep it to yourself or try to solve the problem on your own. Alert the company you work for immediately and let them know what information or data might be compromised, or make sure you have an external security team who can get onto it as soon as possible. The faster a breach is identified, the faster it can be shut down, fixed and resolved.