Cyber Risk Management
Top 10 practical tips

1. Handling sensitive data

How should sensitive data be handled and stored and by who? Consider whether there should be restrictions on access to sensitive information.

2. Remote access

Have a system to ensure security is maintained while accessing work documents from the road or at home.

3. Portable media

Introduce policies for use on devices such as USB drives, CDs and DVDs to safeguard from malware and important data being stolen.

4. Email compromise

Carefully validate ad hoc and suspicious payment instructions as the sender may be a fraudster claiming to be a director, manager or vendor.

5. Secure web pages and software

Look for 'https://' and a padlock symbol on your browser and always review alerts before downloading new software.

6. Smart passwords

Create a long password by using a phrase and replacing some letters with characters and numbers. To be truly secure your password should contain in excess of 25 alpha-numeric characters.

7. Anti-virus software

Use up to date anti-virus software to prevent online attacks (old software may not detect new malware).

8. Business continuity plan

Build cyber threats into your company's business continuity plans alongside other kinds of potential major disruptions.

9. Run a simulation

Running scenario based drills to test the impact and response times to various types of breaches will aid in identifying where your company's greatest weaknesses are so that they can be adequately addressed.

10. Staff education

Keep staff updated on the latest threats and responses you have in place to prevent a breach. Staff are your main exposure but also your best defence, so the better informed they are, the better protected your company is.

Is your business at risk?

Use our online assessment tool at **nzicyber.co.nz** to find out your level of exposure.

NZ6481-3 11/17