5 STEPS TO BEING CYBER SECURE

1 SECURE REMOTE WORKING

It is important that company networks are secure and not susceptible to vulnerabilities due to fragmented remote networks, especially in these times where large parts of the workforce are working from home.

Implementing Multi Factor Authentication or logging in through a Virtual Private Network (VPN) will add another level of protection in order to protect your company's digital assets.

2 DATA BACK-UPS

It is essential that these data back-ups are taken frequently (preferably daily), tested regularly, and that a copy is held off-site to ensure business continuity and to prevent the loss of data.

Whether it be through clicking on a malicious link which deploys malware or targeted by a ransomware campaign, companies can look to mitigate the effect of these attacks by having suitable data back-ups in place from which they can restore their data.

3 INCIDENT MANAGEMENT

In the event of an incident, it is important that you have the right incident management capabilities to deal with the event in the best way possible. In the first instance, with an ATC Cyber Policy, notify the Crawford Incident Response helpline to speak to an expert.

It is also best practice to implement a Business Continuity Plan, Incident Response Plan or a Disaster Recovery strategy, and ensure that these plans are regularly tested.

4 NETWORK SECURITY

At ATC, our cyber policy offers Avast Antivirus Protection for up to 10 devices included with your policy.

Ensure that your network has a suitable level of protection, through the use of commercial grade antivirus protection, firewalls, filtering out unauthorised access and malicious content, monitoring of the network, and applying security patches.

5 ENCRYPTION

No matter what business you conduct, there will always be sensitive data present on your systems.

Loss of this data can lead to a Business Interruption Event and subsequent Business Interruption Losses, Remediation Costs, or potential Reputational Harm to your business.

The first line of defense against this is Encryption, which protects personal data by scrambling the information so that cyber criminals cannot read it.

OUR CYBER UNDERWRITERS:

Lawrence Ormrod
Senior Underwriter
E: lawrenceo@atcis.com.au
P: 02 9928 7107

Jenny Arkell
Senior Underwriter
E: jennya@atcis.com.au
P: 03 9258 1735

ATC INSURANCE SOLUTIONS