CYBER SECURITY CHECKLIST

What you need to do

So, what cyber protection and controls do you need to qualify for cyber insurance?

We have compiled a comprehensive checklist to ensure that you can get the cover you need while knowing that you are putting the appropriate protective measures in place.

- **Revenue**
  - Annual revenue
  - Revenue by state or territory

- **Details of previous cyber incidents**
  - Description and date of incidents
  - Financial impact
  - Mitigating steps to avoid future incidents
  - Any current risk factors that could give rise to a Data Breach or Cyber incident

- **IT infrastructure and resourcing including:**
  - Managed service provider
  - Number of servers on your network
  - Number of desktops and laptops
  - Annual IT budget
  - Percentage spent on IT security
  - Any third-party technology partners for IT Infrastructure

- **Data storage and management**
  - Data types
  - Data protection measures (access controls, encryption, network segmentation etc.)
  - Deletion of old records
  - Storage, frequency and testing of backups
  - Number of backup copies and how you prevent multiple copies from being impacted by the same event
  - Recovery time

- **Endpoint security**
  - The Endpoint Protection and Endpoint Detection and Response you use on your network
  - How these products are monitored and managed
  - Whether they cover all endpoints on your network

Perimeter security

- Next-generation firewalls in use
- Regularity of vulnerability scanning of network perimeter
- Frequency of penetration testing of network architecture and whether a third party conducts this
- Multi-factor authentication for remote access to your network
- Methods to secure remote access to your network

Email security

- Multi-factor authentication for remote access to company email accounts
- Use of emailing filtering software

Network security

- How you protect privileged user accounts
- Whether non-IT users have local administrator rights on their computer
- Use of a network monitoring solution to alert you to malicious/suspicious behaviour
- Use of a Security Operations Centre (SOC)
- Whether you have any end-of-life or end-of-support software
- Patch management process to ensure critical patches are applied in a timely process
- Significant changes planned for your IT infrastructure

Staff training

- Phishing testing
- Responsible password practices
- Cyber best practices
- Cyber incident response preparedness

Additional controls that you use

Audit information

Procedures around intellectual property

Legal counsel relating to privacy policy, terms of use, terms of service and customer policies

If you are concerned about your organisation's cyber resilience, get in touch with the Colton team for a check up.

02 6361 1116
sales@colton.com.au
156 Moulder St, Orange NSW 2800