CYBER SECURITY STANDARDS CHECKLIST

ACP

AUSTBROKERS CYBER PRO

This document is designed to provide organisations with guidance on minimum security standards and processes that cyber insurers are now expecting to see from organisations.

This is not an exhaustive list and organisations should work closely with their IT provider/personnel on ensuring they have strong cyber security protocols in place to protect their business.

The following are key areas that insurers are focusing on at this point in time. Without these controls and procedures organisations will find it difficult to procure cyber insurance moving forward.

Multi Factor Authentication ('MFA')

- Multi Factor Authentication ('MFA') is expected on all remote access into networks (including the use of O365 and other cloud-based platforms).

Privileged Access Controls

- Strong controls are expected in relation to internal privileged access accounts, including a Privileged Access Management ('PAM') tool, the principal of least privilege and the deployment of MFA on those accounts.

Patch Management

- A patch management policy is expected to be in place outlining the patching credence of the organisation and ensuring patches are deployed in a quick and efficient manner.

Business Continuity/Back Ups & Ransomware Planning

- A strong Incident Response, Business Continuity and/or Disaster Recovery plan, which deals with and addresses downtime of IT networks due to a cyber incident is required. The plan must be tested at least annually and confirm Recovery Time Objectives ('RTO').

- Back Ups are to be tested on at least an annual basis for integrity. Back ups need to be taken offline and encrypted.

- Organisations should have specific planning in place in relation to dealing with ransomware events, this includes annual tabletop exercises with key executives and management, along with a ransomware playbook.

Endpoint Detection & Response ('EDR')

- An Endpoint Detection & Response ('EDR') tool should be implemented across all endpoints within the organisation, including workstations, laptops, servers etc.

Vulnerability Scanning & Penetration Testing

- Vulnerability scans and penetration test should be conducted on at least an annual basis by a third-party specialist. Organisations should take immediate steps to address any critical, high, or medium findings that come out of these reports.

End of Life/Unsupported Systems & Software

- End of Life/Unsupported systems and software should be isolated from the network. Organisations need to be able to demonstrate strong controls around these systems and software and provide guidance around plans to decommission and upgrade such systems and software.

Data Encryption & Log Management

- Strong controls are expected in relation to protecting Personally Identifiable Information ('PII') within the IT environment. This data should be encrypted and segmented within the network.

- The use of a Security Information & Event Management ('SIEM') tool should be considered. There should be an audit log retention of at least 180 days.

Cyber Security Training

- Cyber security awareness training should be implemented within the organisation. This training should be undertaken by all staff. This training should include phishing simulation exercises.