CYBER ENTERPRISE SOLUTION

emergence

appetite guide

Primary and excess cyber risks with revenue > $250m.
Aggregate limits up to $25m.

Emergence has appetite for a broad range of industries, with key industries outlined as follows:

Target business

+ Financial Institutions
+ Retail and Hospitality
+ Construction and Engineering
+ Manufacturing (with strong BCP)
+ Property Owners and Developers
+ Wholesale (Distribution Outsourced)
+ Agribusiness
+ Mining (excluding thermal coal and risks with autonomous vehicles)

Selective appetite

+ Professional Services
+ Healthcare
+ Education
+ Technology Firms (up to $1bn revenue)
+ Government Owned Corporations
+ Local Governments
+ Hotels
+ Aged Care Facilities

Limited appetite

+ Airlines
+ Adult Content
+ Critical Infrastructure / Power Gen
+ Federal and State Governments
+ Hospitals
+ Logistics & Freight-forwarding
+ Exchanges Platforms
+ Petrochemical
+ Telecommunications and ISPs
+ Payment Processors
+ Mass Transit
+ Military Defence

The cyber maturity of our Policyholders is a key consideration for our underwriters:

Minimum cybersecurity and risk governance controls

- Multifactor authentication for all remote access, email inbox access and O365/M365 (if applicable)
- Strong patch management procedures
- Strong privileged access controls (role-based access control and principle of least privilege)
- Back-ups stored securely, preferably offline and encrypted
- Back-ups tested annually
- Incident Response Plan, Business Continuity Plan, and/or Disaster Recovery Plan tested annually (ideally including ransomware scenarios)

Preferred cybersecurity controls

- Risk-based network segmentation to prevent lateral movement
- Next-gen antivirus and endpoint detection & response
- EOL software isolated from wider network
- Penetration tests conducted annually
- 24/7 Security Operations Centre (own or via MSSP)
- SIEM and audit log retention of at least 90 days
- PII and sensitive data encrypted
- Application whitelisting

emergence