CYBER EVENT PROTECTION (CEP-005.1)

emergence

policy coverage overview

This document provides a summary of the coverage provided in the Emergence Cyber Event Protection policy. It follows the sectional layout of the policy. It is not an exhaustive summary, nor does it form part of the policy wording. Emergence policies are available on the Emergence website.

Coverage under the policy can be triggered by Cyber Events or reasonably suspected Cyber Event which includes:

- Crimeware
- Cyber espionage
- Cyber extortion
- Denial of service
- Hacking
- Insider and privilege misuse
- Miscellaneous errors
- Privacy error
- Payment card skimming
- Physical theft and loss
- Web app attacks
- Point of sale (POS) intrusion

COVERAGE SECTION A: LOSSES TO YOUR BUSINESS	CEP-005.1
Losses to your business coverage provides these protections:	
Impact on Business Costs if there is a Cyber Event	
In your business	✓
In your IT contractor's business'	✓
Waiting Period	8 hours
Impact on Business Costs if there is a System Failure	
In your business	3
In your IT contractor's business'	3
Waiting Period	48 hours
Preventative Shutdown	
Preventative Shutdown Allowance	48 hours
Indemnity Period	30 to 365 days
COVERAGE SECTION B: LOSS TO OTHERS COVERAGE	**CEP-005.1**
Loss to others provides protection:	
Against your legal liability because of a Cyber Event	✓
A Multimedia Injury	✓
Your Payment Card Industry Liability	✓
This cover includes:	
Defence Costs	✓
Settlements / Awards / Damages	✓
Civil Fines or Regulatory Fines and Penalties	✓
Mandatory Notices from Regulators	✓

CYBER EVENT PROTECTION (CEP-005.1)

policy coverage overview

COVERAGE SECTION C: CYBER EVENT RESPONSE COSTS	CEP-005.1
Cyber Event Response if there is a Cyber Event in your business	✓
Cyber Event Response if there is a Cyber Event in your IT Contractor's business	✓
Cyber Event Response if there is a Cyber Event in your Data Processor's business	✓
This cover includes:	
Credit and Identity Monitoring Costs	✓
Cyber Extortion Costs	✓
Data Restoration Costs	✓
Data Securing Costs	✓
External Management Costs (Crisis Management / Reputational Harm)	✓
Identity Theft Response Costs	✓
IT Forensic Costs	✓
Legal Advice Costs	✓
Notification Costs	✓
Public Relations Costs	✓
Pursuit Costs (for a Cyber Event in your business only)	✓
Virus Extraction Costs	✓
COVERAGE SECTION D: OPTIONAL COVERS	**CEP-005.1**
Optional Covers may be available. Various sublimits may be available	
Non-IT Contingent Business Interruption and System Failure	
Supplier Outage	✓
Supplier System Failure	✓
Criminal Financial Loss (cover for Direct Financial Loss)	
Cyber Theft	✓
Socially Engineered Theft	✓
Identity-based Theft	✓
Push Payment Theft	✓
Physical Goods Theft	✓
Telephone Phreaking	✓
Cryptojacking	✓

CYBER EVENT PROTECTION (CEP-005.1)

policy coverage overview

Tangible Property (IT hardware repair or replacement due to a Cyber Event)	✓
D&O Liability Cover (directors or officers liability due to a cyber wrongful act)	✓
Joint Venture and Consortium Cover	✓
Emergence can also apply US Jurisdiction on application	✓
OTHER FEATURES	
Other selected features of the policy include:	
Policy limits	$250,000 to $10m
Excess	From $0
Territorial limits	Worldwide
Security	100% Lloyds
Emergence Incident Response Service	Australia Based 24/7/365
Smarter Services provided by Emergence	
vCISO Trusted Advisor (one hour consultation)	✓
Incident Response Plan Template	✓
Real-time Cyber Threat Notification	✓
Dark Web Monitoring	✓

emergence