CYBER EVENT PROTECTION 005 (CEP-005)

emergence

cyber event protection

Emergence is your award-winning underwriting agency focused on providing flexible, innovative insurance solutions to help protect businesses against cyber risks.

Security to succeed

Our strength and security is 100% Lloyd's - insuring risks for hundreds of years.

Experts on hand

Our dedicated team provides expert support and cyber protection for your business needs.

Comprehensive cover

Insure with confidence and clarity, knowing your business will be covered in the event of a cyber attack.

Agency appetite

We insure start-ups, SMEs and larger corporations across a broad selection of industries.

Services

Policyholders have access to a range of no cost services including ongoing scanning of your internet facing infrastructure and dark web incidents.

Incident response solution

Local experts on call 24/7/365 to manage incidents and minimise business impact.

THE EMERGENCE CYBER COVER INCLUDES

Cyber cover includes:

Cyber event response costs

+ IT forensics
+ Virus extraction
+ Customer notification costs
+ Public relations costs
+ Legal costs

Losses to your business

+ Loss of revenue
+ Increased costs of working
+ Preventative shutdown
+ System failure

Loss to others

+ Third-party litigation
+ Regulatory investigations
+ Fines and penalties
+ Payment Card Industry liability
+ Defence costs
+ Multimedia

Optional cover includes:

Non-IT contingent business interruption and system failure

+ Supplier outage
+ Supplier system failure

Criminal financial loss

+ Cyber theft
+ Socially engineered theft
+ Identity-based theft
+ Push payment theft
+ Telephone phreaking
+ Cryptojacking

D&O liability

Tangible property

Joint ventures/consortiums

Incident response solution

+ 24/7/365 hotline and access to an Emergence Incident Response team member
+ IT investigators
+ Privacy lawyers
+ Public relations consultants
+ Crisis management consultants
+ Customer communications

Complimentary services

+ vCISO Trusted Advisor (one hour consultation)
+ Incident Response Plan Template
+ Real-time Cyber Threat Notification
+ Dark Web Monitoring

→

CYBER EVENT PROTECTION 005 (CEP-005)

cyberSuite

complimentary services

Emergence work in partnership with our sister company cyberSuite to provide our policyholders who purchase the Emergence CEP-005 policy the services outlined below at no cost.

cyberSuite delivers high-quality and practical cyber advisory and privacy services that help businesses manage and reduce their cyber risk.

COMPLIMENTARY SERVICE

vCISO Trusted Advisor

Bespoke advice and resources provided by cyber and privacy experts to assist business managers in understanding and reducing their cyber risks. Examples of bespoke work may include: cyber security strategy development, policy document review, response plan development, etc.

Incident Response Template

In case of a cyber incident, every second counts. We provide a guide to developing your own Incident Response Plan (IRP) that can be tailored to your organisation. The OAIC recommends all businesses have an IRP.

Real-time Cyber Threat Notification

Real-time monitoring of cyber threat intelligence sources to provide businesses with early notifications of detected exploitable vulnerabilities.

Dark Web Monitoring

Using Dark Web Monitoring tools, our threat intelligence team will identify if and when your organisation’s data is shared on the dark web. If it is detected, we will notify you so that you can take appropriate action.

CYBER EVENT PROTECTION 005 (CEP-005)

cyber event protection

Emergence provides cover for first-party and third-party costs if there is a cyber event at or within your business. Cyber events include:

Point of Sale (PoS) Intrusions

Remote attacks against retail transactions for card-present purchases.

Cyber Espionage

Unauthorised network or system access linked to state-affiliated or criminal sources with the motive of espionage.

Miscellaneous errors

People make mistakes. Unintentional actions directly compromising security attributes of information assets.

Cyber extortion

Attacks or threatened attacks against IT, coupled with demands for money to stop attacks.

Web app attacks

Exploiting code-level vulnerabilities in applications.

Privacy error

Your acts or omissions that lead to unauthorised disclosure of data including non-electronic data.

Physical Theft and Loss

Incidents where information assets go missing, through misplacement or malice.

Hacking/Crimeware

Malicious or unauthorised IT access or malware that aims to gain control of systems.

Insider and privilege misuse

Unapproved or malicious use of organisations' IT by insiders or external misuse through collusion.

Payment card skimmers

Skimming devices physically implanted on assets that reads data from payment cards.

Denial of service (DoS)

Intentional compromising of networks and systems' availability. Includes network and application layer attacks.