

cyber event protection

CEP-005.1 is a cyber insurance product tailored to SMEs, protecting a broad selection of industries against the financial, commercial, and reputational risks of cyber events.

CYBER EVENTS INCLUDE



RANSOMWARE / CYBER EXTORTION

Attacks or threatened attacks against IT, coupled with ransom demands.



PAYMENT CARD SKIMMING

Involving a skimming device being physically implanted through tampering into an item of IT that reads data from a payment card.



MISCELLANEOUS ERRORS

Unintentional actions directly compromising security attributes of information assets.



HACKING

Malicious or unauthorised IT access to IT.



INSIDER AND PRIVILEGE MISUSE

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



CRIMEWARE

Malware designed to cause harm to IT.



POINT OF SALE (POS) INTRUSION

Remote attack against IT where retail transactions are conducted.



PRIVACY ERROR

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



PHYSICAL THEFT AND LOSS

Information assets going missing, through misplacement or malice.



CYBER ESPIONAGE

Unauthorised access to IT linked to state affiliated or criminal sources.



WEB APP ATTACKS

Where a web application was the target of attack against IT.



DENIAL OF SERVICE (DOS)

Uniquely intended to compromise the availability of IT. This includes a distributed denial of service (DDoS).

SMARTER CYBER INSURANCE

Emergence is a specialist underwriting agency focused on providing flexible, innovative insurance solutions to help protect businesses against cyber risks.



cyber emergency 1300 799 562

SECURITY TO SUCCEED



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

cyber event protection

COVER

CEP-005.1 provides cover for first-party and third-party costs if there is a cyber event at or within an insureds business.

 CYBER EVENT RESPONSE COSTS	 LOSSES TO YOUR BUSINESS	 LOSS TO OTHERS
<ul style="list-style-type: none"> • IT forensics • Virus extraction • Customer notification costs • Public relations costs • Legal costs • Data securing costs • Data restoration costs 	<ul style="list-style-type: none"> • Loss of revenue • Increased costs of working • Preventative shutdown • System failure 	<ul style="list-style-type: none"> • Third-party litigation • Regulatory investigations • Fines and penalties • Payment Card Industry liability • Defence costs • Multimedia

COVERAGE HIGHLIGHTS

	INCIDENT RESPONSE OUTSIDE POLICY LIMIT	Emergence Incident Response Services, whether addressing a suspected or confirmed breach, do not erode the policy limit or incur additional costs for the insured. Our in-house experts are available 24/7/365.
	12-MONTH INDEMNITY FOR BUSINESS INTERRUPTION	Up to 365 days' cover for business interruption commencing once an event is discovered—even without downtime—and continuing for an indemnity period up to 365 days.
	EACH INCIDENT LIMIT	The full policy limit automatically resets for each separate, unrelated incident during the policy period at no extra cost to the policyholder.
	REAL-TIME RISK MANAGEMENT	Dark web monitoring and vulnerability scanning notify insureds of threats in real time, enabling risk mitigation before an attack.

OPTIONAL COVER

 NON-IT CONTINGENT BUSINESS INTERRUPTION AND SYSTEM FAILURE	 CRIMINAL FINANCIAL LOSS	 D&O LIABILITY	 TANGIBLE PROPERTY
<ul style="list-style-type: none"> • Supplier outage • Supplier system failure 	<ul style="list-style-type: none"> • Cyber theft • Socially engineered theft • Identity-based theft • Push payment theft • Telephone phreaking • Cryptojacking 	<ul style="list-style-type: none"> • Covering losses your directors or officers are legally liable for because of a cyber wrongful act. 	<ul style="list-style-type: none"> • Covering the cost to repair or replace damaged IT hardware because of a cyber event.

cyber event protection

SMARTER CYBER SERVICES

The following services are available to CEP-005.1 policyholders at no extra cost.



DARK WEB MONITORING

Using Dark Web Monitoring tools, our threat intelligence team identifies whether an insured business's data is shared on the dark web. If detected, we notify, so appropriate action can be taken.



REAL-TIME CYBER THREAT NOTIFICATION

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



VCISO TRUSTED ADVISOR

Bespoke advice and resources provided by cyber and privacy experts to assist business managers in understanding and reducing their cyber risks.



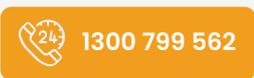
INCIDENT RESPONSE TEMPLATE

In case of a cyber incident, every second counts. We provide a guide to developing an Incident Response Plan (IRP).

INCIDENT RESPONSE & CLAIMS

Our in-house incident response and claims teams help businesses bounce back after a cyber event.

CYBER HOTLINE



Immediate triage of cyber event by IR team



Coverage position issued to the insured / broker



Assessment of business interruption if relevant



Appointment of cyber specialists



Ongoing coordination of incident response to completion



Post-incident reporting – identifying security improvements



Our dedicated incident response experts are on-hand 24/7/365 to trigger an immediate recovery response to a cyber incident, assisted by an armada of specialists.



The Emergence Incident Response (IR) team works closely with our claims team, who assist through the entire lifecycle, until claim closure.

