Product: Commercial Cyber: Data Protection & Network Interruption

Manufacturer Information

Product information

The Commercial Cyber insurance product is designed for businesses seeking protection against cyber-related losses and liabilities. Depending on the policy wording and jurisdiction, coverage may operate on either a claims-made, claims-made and reported, occurrence, or hybrid basis. The product provides protection against cyber incidents including business interruption, privacy breaches, cyber extortion, incident response costs, destruction of digital assets, regulatory investigations and other cyber-related liabilities. The product is intended for businesses ranging from micro-enterprises to large commercial organisations with exposure to cyber risks.

Core Covers (can include but are not limited to):

- Security and Privacy Liability damages and defence costs as a result of a claim arising from a security breach or privacy breach.
- Regulatory Fines and Penalties and Defence Expenses as a result of a claim arising from a Security Breach or Privacy Breach.
- Multimedia Liability damages and defence expenses as a result of a claim arising from multimedia activities.
- Payment Card Industry Fines, Assessments and Expenses as a result of a Claim arising from a Security Breach or Privacy Breach.
- Business Interruption Financial loss arising from privacy breach, security breach, or system failure impacting the insured's computer system.
- Contingent Business Interruption Financial arising from privacy breach, security breach or system failure impacting the insured's outsource service providers computer system.
- Digital Asset Destruction of data, computer programmes and electronic documents incurred as a direct result of a privacy breach, security breach, or system failure.
- Reputational Harm Financial loss and crisis management costs incurred as a result of an adverse media event arising from a privacy breach, security breach or administrative error.
- Cyber Extortion expenses and ransom demand payments to avoid a privacy or security breach incurred directly as a result of a cyber extortion threat.
- Incident Response Expenses incurred as a result of a privacy breach or security breach.
- Loss of Funds incurred directly as a result of a hack of the insured's computer System.
- Physical Damage following cyber-attack
- Cyber Crime / Social Engineering
- Non-Tech Contingent Business Interruption
- Incident Response (outside of the limit)
- Defence Costs (outside of the limit)
- Cyber helplines and breach response services

Optional Additional Covers Include:

- Hardware replacement costs
- Criminal rewards offered by the insured for information that leads to an arrest of a criminal
- Claim preparation expenses of BI claims
- Court attendance costs

Coverage may be provided on either a claims-made, claims-made and reported, occurrence, or mixed basis depending on the specific wording and cover section being utilised.

- Where coverage is written on a claims-made basis, the relevant claim (or claim and notification) must occur during the policy period and be reported in accordance with policy requirements.
- Where coverage is written on an occurrence basis, the insured event must occur during the period of insurance irrespective of when the claim is subsequently presented. Occurrence based wording may also have a time limit for claims notification (5 years, for example)

Any retroactive dates, continuity provisions, discovery periods or extended reporting periods will be clearly stated within the policy documentation.

Target market

The Commercial Cyber – Data Protection & Network Interruption product is designed for businesses seeking protection against cyber-related risks, including data breaches, and operational disruption. It provides comprehensive coverage and additional services to help mitigate and respond to cyber incidents.

Key characteristics include:

1) Business Size & Type:
   - Micro enterprises, small businesses, mid-sized commercial entities, and large commercial organisations across multiple sectors.
   - Suitable for businesses that rely on digital infrastructure and hold sensitive data, making them vulnerable to cyber threats.

2) Insurance Profile:
   - Customers who purchase commercial insurance through brokers, including those with property or liability policies where cyber cover may be embedded or offered as an additional extension of cover.
   - The product can be sold as a standalone policy or as an add-on to another commercial insurance.

3) Customer Needs & Behaviours:
   - Businesses concerned about financial, operational, and reputational impacts of cyber incidents.
   - Likely to value proactive risk management tools and expert support during and after an incident, including:
     a) 24/7 breach response hotline and triage services.
     b) Access to cyber security tools such as phishing simulations, inbox protection, and vulnerability scanning
     c) Guidance and coordination of specialist resources (IT forensics, legal support) during a cyber event.

4) Geographic Scope:
   - Distributed in the USA, Canada, UK, EEA, Australia/New Zealand, and other licenced jurisdictions globally.

5) Distribution Channel:
   - Sold via insurance brokers through both advised and non-advised processes, ensuring suitability checks even when advice is not provided.
   - Distributed through coverholders, lineslips, open market placements, and group/master policy arrangements.

6) Circumstances Where Product Delivers Greatest Value:
   - Following cyber incidents such as ransomware attacks, data breaches, or system outages where rapid response and financial protection are critical.
   - Businesses lacking in-house cyber expertise and requiring external support for incident management and regulatory compliance.

(7) Customer Understanding Requirements:
   - Where claims-made coverage is provided, the target market should have sufficient understanding, either directly or via their broker, of claims notification requirements, retroactive dates, continuity of cover provisions and the consequences of allowing coverage to lapse.
   - For occurrence-based products, customers should understand that coverage is triggered by the occurrence of an insured event during the policy period.

This product appeals to organisations seeking peace of mind, operational resilience, and expert-led incident response, particularly those exposed to increasing cyber threats and regulatory scrutiny.

Types of customer for whom the product would be unsuitable

The Commercial Cyber product would not be appropriate for:

1) Individuals or Personal Lines Customers
   - The product is designed exclusively for commercial entities and does not provide cover for personal cyber risks.

2) Businesses Without Meaningful Cyber Exposure
   - Organisations that do not rely on digital systems, store sensitive data, or conduct online transactions, as they have negligible exposure to cyber threats.

3) Entities Seeking Direct Purchase Without a Broker
   - Customers who wish to buy insurance directly without engaging a regulated insurance broker, as the product is distributed through broker-led channels to ensure suitability and compliance.

4) Organisations Domiciled Outside Licensed Jurisdictions
   - Businesses domiciled in regions where TMK/Lloyd's does not hold a license to operate.

Any notable exclusions or circumstances where the product will not respond

Limitations:

- Any incurred loss during the waiting period as stated in the schedule will be uninsured.
- Incidents to be reported as soon a reasonably practicable.
- Insured to not make and payments, assume any obligations, incur expenses, enter onto any settlement without TMKS written consent.
- Accurate and complete information must be supplied as requested.

Exclusions include but not limited to:

- Bodily injury
- Betterment
- Breach of contract, warranty, guarantee or promise and assumed liability.
- Loss of funds
- Terrorism
- Use of illegal or unlicensed programs or software
- War or uprising
- Insured misconduct
- Infrastructure failures including but not limited to internet and utilities - except where the insured owns or controls such infrastructure
- Ordinary payroll
- Breach of securities law

Claims-Made Conditions (where applicable):

- Claims and/or circumstances must be notified during the policy period or any applicable extended reporting period.
- Claims arising from circumstances known prior to inception may be excluded.
- Retroactive dates may apply.
- Continuous coverage requirements may apply.
- Failure to comply with notification provisions may prejudice coverage.

Occurrence Basis Conditions (where applicable):

- The insured event must occur during the policy period.
- Evidence may be required to establish when the loss-causing event occurred.

Limits of Liability:

- Various limits of liability may be applied based on the method of distribution and insured's needs. All limits of liability are clearly stated in the insured's policy schedule.
- Limits may apply on an aggregate, annual aggregate, per claim, per event or per occurrence basis depending on the section of cover.

Retention Amount

- Various excesses/deductible apply and are clearly stated in the insured's policy schedule.

The applicable structure will be clearly stated within the policy wording and schedule.

Other information which may be relevant to distributors

This product is permitted for sale with up to 4 distributors in the chain e.g.

- Lloyd's Broker;
- A delegated authority arrangement with a coverholder
- Wholesale broker;
- Retail/ producing broker.

No further distributors in the chain are permitted without TMKS' approval. Any such approval will include consideration of their impact on product value.

This product can be sold with or without advice in line with FCA regulations or local regulations if distributor is not regulated by the FCA.

All distributors are expected to fully understand the eligibility criteria, covers and exclusions of the product.

Sales journeys must identify customer eligibility and ensure that key information and choices to be made are presented to customers in a way that supports a customer through the process of understanding core cover and configuring optional elements of insurance to suit their specific demands and needs.

This product can be sold face to face, via telephone, online rating engine or electronic communication or a mix of these methods, as long as customers are provided with sufficient information to make an informed decision regarding the suitability of the product.

Where Distributor 1 sells this Product via multiple other distributors (via sub-delegation or sub-broking), it is their responsibility to ensure all distributors have been provided this document, have reviewed it and understand the content. If there is any additional remuneration, including commissions, fees or other 'non-standard' remuneration charged to the customer by other distributors, it is the responsibility of Distributor 1 to inform TMK of these details accurately and in full.

Commission & Fees

If there is a coverholder in the chain, they are expected to ensure that maximum commission rates do not exceed those stipulated within the Binding Authority Agreement.

The coverholder is expected to maintain oversight of all broker commissions (where applicable) and, where there may be a risk to product value, remedial action should be taken immediately including notification to Tokio Marine Kiln.

Brokers are reminded of their own regulatory obligations in relation to remuneration under PROD 4.3.6 as well as the requirements to make all necessary disclosures to the customer.

Where there are any fees charged by any member of the distribution chain these should be:

- commensurate with the service provided by the distribution.
- not have an adverse impact on customer value; and
- distributor should ensure that TMKS is made aware of the fee amount and/ or method of calculation.

Fees of up to £100 per policy can be charged by the producing broker.

How value is assessed

Value is assessed based on a number of metrics, including underwriting, claims and complaints information as well as through broker and coverholder engagement.

Remuneration paid as set out in our agreements with distributors has been considered as part of the product review.

If additional add-ons (including premium finance) are sold alongside this product or additional remuneration is charged, this may affect the value for the customer.

Further information on our product approval processes can be obtained on request.

Date Fair Value assessment completed	April 2026
Expected date of next assessment	April 2027