TOKIO MARINE KILN

Cyber Ctrl: **Policy Enhancement**

Cyber Ctrl insurance provides cover for events such as computer attacks, mistakes made by employees, network failures and data breaches. When events like this happen they can completely paralyse an organisation. TMK's 24-hour hotline helps you respond to an incident and minimise damage to your business.

Who is it for?

Tokio Marine Kiln's Cyber Ctrl insurance is designed to enhance existing policies (such as property or liability insurance) to give protection against a wide range of cyber-related risks. The product is aimed at small to medium sized businesses.

What we provide

- Cyber wording
- Rating guidelines
- Established 24/7 incident response hotline
- Support and guidance including marketing
- Informative website for all insureds
- Coverholder commission

How do I get it?

Our cyber insurance can easily be added onto existing policies written under the Binding Authority Agreement. All you need to do is provide us with the following information:

1. Approximate revenue range of insureds
2. Number of policies
3. Industry profile

Overview of the cover provided

Cover	Overview of what's included	Particularly suited to
Business interruption	Loss of gross earnings and extra expense, caused by either a mistake in the use of or a security breach of the Insured's computer system.	Companies whose business income depends on an available IT infrastructure, e.g. online retail, manufacturers, utilities, financial institutions or trading systems.
Digital asset destruction	Costs to restore or recreate data caused by either a mistake in the use of or a breach of the Insured's computer system.	
Incident response expenses	Costs to manage a data breach including IT forensic costs, public relations and legal expenses as well as the cost of notifying customers of the situation and providing credit or monitoring to them.	Any company that maintains personal information (customer or employee) including financial services firms, healthcare, retailers and other B2C companies.
Regulatory defence and penalties	Fines and penalties resulting from a regulatory action following a security breach of the computer system or a breach of privacy.	
Payment card industry fines and expenses	Fines and expenses that relate to credit card breaches from non-compliance with payment card industry data security standards.	Any company that accepts credit cards as a form of payment.
Security and privacy liability	Damages and defence expenses from a legal suit which the Insured is legally obligated to pay as a result of a security breach or privacy breach.	Any company storing personal and/or confidential information.
Multimedia liability	Liability and defence costs incurred as a result of infringement of offline/online media.	Companies who publish and advertise online and offline media content as part of business operations.

Access to dedicated **24-hour emergency hotline for all policyholders** powered by CyberScout™.

cyber ctrl

Insurance Products Cyber Ctrl: Policy Enhancement

Policy extensions available

Cover	Overview of what's included	Particularly suited to
Extortion	Extortion monies and costs incurred if you are subject to a ransom demand relating to your data or computer systems.	All companies. Ransomware is a growing problem that all companies face.
Reputational Harm	Ongoing loss of profit resulting from brand damage as well as crisis communication expenses.	Any organisation that wants to protect their brand.

Our coverage is available globally with the following limits	
Maximum limit	USD25,000 or USD50,000
Deductible	USD2,500

Higher limits are available for the standalone product, subject to the insured completing a warranty statement or a proposal form.

Policy highlights

- Privacy breaches that are not linked to or triggered by a computer or electronic data breach, so customers are covered for paper file or other privacy breaches
- Costs to notify customers following a data breach, even where not required by law
- The maximum business interruption indemnity period is up to the date of full system restoration and up to 30 days thereafter
- Business interruption triggers include:
  - Administrative error in the operation of the computer system
  - Malicious attacks of the computer system
  - Power failure if the power supply is under the direct operational control of the Insured
- No retroactive date
- Automatic 30-day ERP available
- Duty to defend clause
- Access to dedicated 24-hour emergency hotline for all policyholders following discovery of a cyber incident

About CyberScout

Since 2003, CyberScout has protected consumers, businesses and institutions alike against hackers, thieves, and human error. They provide solutions that deliver valuable identity fraud protection and education, proactive protection services as well as swift data incident response for their clients.

We have partnered with CyberScout™ to provide our policyholders with proactive services to minimise the likelihood of a data breach and post-breach services to provide expert assistance if one occurs.

CYBERSCOUT™

To find out more about this product please contact Jonny Groves
jonny.groves@tokiomarinekiln.com

cyber ctrl