Altius CYBER INSURANCE

Protecting Digital Future

Aligned with modern insurance needs, arising from technological developments, Altius Insurance Ltd enhances its portfolio with a Cyber Insurance program.

WHY CYBER INSURANCE IS NECESSARY
In today's world, digital transactions constitute the dominant method of conducting business, making cybersecurity more essential than ever. At the same time, cyberattacks have increased globally in recent years, affecting both organisations and individuals.

WHO IT IS FOR
All types of businesses and organisations (excluding high-risk businesses).

WHAT THE COMMERCIAL COVERAGE PLAN INCLUDES - COMMCYBER

INCIDENT RESPONSE
Includes incident response expenses, confidentiality events, privacy event or a breach of computer system security.

What it covers:
- Detection and containment of the breach
- Incident analysis
- Documentation and preservation of evidence
- Technical support and recovery
- Investigation by cybersecurity specialists
- Data and system recovery
- Legal and regulatory compliance
- Advice on legal and regulatory requirements
- Management of notifications sent to authorities and clients
- Public relations and communication management
- Protection of company reputation
- Communication strategy for clients and the media
- Response expenses
- Specialists and lawyers' fees
- Recovery and communication expenses

DATA RESTORATION
Includes data restoration expenses resulting from a breach of the insured systems' security.

What it covers:
Technical Recovery
- Data restoration, recovery or reconstruction of lost or damaged data due to an attack.
- System repair and recovery - Restoration of cloud infrastructure and software.
- Investigation and digital data analysis to detect and manage cyberattacks (forensic analysis) – Expert examination to identify the cause and scope of the breach.
- Security enhancement - Implementation of additional protective measures to prevent future attacks.

Financial Impact
Crisis management expenses – Communication advice, PR, and company reputation management.

Specialised Services
Provision of credit monitoring services - Coverage for expenses for fraud protection services (credit monitoring)

EXTORTION
Includes damage caused by extortion of the insured, as a direct consequence of a privacy or confidentiality event.

What it covers:
Ransomware negotiation services – Expert assistance for potential data recovery.
Reimbursement of paid amounts to hackers to restore access to important data or prevent data leaks.

BUSINESS INTERRUPTION
Covers losses from lost profits due to:
1. inability to use data assets that have been corrupted or encrypted.
2. reduced availability of computer systems or data assets as a direct result of a security breach due to a cyberattack.

What it covers:
Loss of profit - Reimbursement for operational downtime due to a cyberattack (up to 12 months)

LEGAL LIABILITY OF THE INSURED

Covers damages due to a privacy or confidentiality event, resulting in the:
α) transmission of malware,
β) unauthorized destruction, corruption, erasure, or encryption of third-party data,
γ) unauthorized denial of service affecting a third party.

What it covers:
•Reimbursement for the insured's legal liability resulting from a privacy event.
•Customer notification expenses.

REGULATORY SANCTIONS

In the event of personal data protection breaches.
It covers:
• Payment of fines and penalties imposed by regulatory authorities due to data protection law violations.
• Legal costs for defending the business against regulatory investigations or prosecutions.
• Compliance costs with regulatory requirements after the breach, such as expenses for improving security measures.
• Management of investigations held by government or supervisory authorities, regarding the breach.

PAYMENT CARD INDUSTRY (PCI) COSTS

Includes costs and consequences related to non-compliance or data breaches involving credit/debit cards.

What it covers:
• PCI DSS fines and penalties - Coverage of fines imposed by payment providers (Visa, MasterCard, etc.) for card data breaches.
• Digital forensic expenses to detect and manage cyberattacks – Expert investigation to detect how the cyberattack occurred and assess compliance with PCI DSS. (PCI DSS are security standards which govern the protection of cardholder data).
• PCI Re-certification costs - If the business loses PCI DSS compliance, the policy may cover the restoration and re-certification cost.
• Reimbursement to banks and partners - Coverage for costs incurred by banks and payment providers affected by data breaches.
• Customer notification expenses - Informing cardholders and providing fraud protection services (credit monitoring).

WHAT THE CYBER INSURANCE POLICY DOES NOT COVER
The policy does not cover:
• Biometric data
• Bodily injury
• Business financial losses
• Contractual obligations
• Directors' duties
• Discrimination
• Dishonest acts
• Electromagnetic interference
• Employment practices
• Government orders
• Infrastructure
• Insolvency
• Radioactivity
• Patents
• Natural hazard
• Prior acts
• Physical damage
• Connected parties
• Sanctions
• Statutory violations
• Terrorism and political violence
• Third-party capitals
• Unfair and deceptive practices
• Unauthorised surveillance
• War
• Wear and tear

The Company does not cover and is not liable to reimburse to the extent that doing so would result in violation of sanctions, prohibitions, or restrictions imposed by the United Nations, or under the trade sanctions, laws, or regulations of the European Union, United Kingdom, or United States.

For more information, please visit our offices.

AltiusInsurance
Skopa 8, 1075 Nicosia, P.O.Box. 26516, 1640 Nicosia, Tel.: (+357) 22379999
customer_service@altiusinsurance.com.cy
www.altiusinsurance.net