

## CYBER INSURANCE GLOSSARY

### **BUSINESS INTERRUPTION**

Cyber business interruption covers the net profit earned before taxes that would have been earned had there been no interruption due to a cyber event.

### **BI (BUSINESS INTERRUPTION) WAITING PERIOD**

A predetermined amount of time that must elapse before any loss or expenses are considered covered by business interruption insurance.

### **BRICKING**

Covers the cost to replace computer and electronic hardware that's rendered inoperable due to failure or purposeful attacks.

### **COMPUTER FRAUD**

Insures against theft of funds or property specifically stolen by using cyber methods to transfer money or property from the victim.

### **CONTINGENT BUSINESS INTERRUPTION**

A contingent business interruption loss occurs when a third-party supplier or service provider experiences an interruption of service due to a cyber event and that event directly impacts the policy holder's ability to produce a product or provide a service.

### **CYBER CRIME**

Any type of illegal activity that occurs using digital means. Examples of cybercrime are extortion/ransomware, phishing, social engineering, and wire transfer fraud.

### **DATA RECOVERY**

Covers the costs of recovering lost data due to a breach.

### **DATA RESTORATION**

The process of copying backup data from secondary storage and restoring it to its original or a new location. Data restoration is done to return data that has been lost, stolen or damaged.

### **EXTORTION/RANSOMWARE COVERAGE**

Coverage for the damage done to a business due to a cyber breach or attack including possible ransom payments to release key systems and data.

### **FIRST PARTY CLAIM**

Where a policy holder files a claim triggered by a cyber breach or other qualifying event directly with their insurance company.

### **FUNDS TRANSFER FRAUD**

Covers the loss stemming from unauthorized instructions from a third party to a bank without the victim's knowledge.

### **MEDIA (LIABILITY)**

Provides coverage against media-related damage such as libel, privacy invasion, copyright infringement, and plagiarism stemming from the policy holder's media activities (e.g website content, printed articles).

### **NOTIFICATION COSTS**

Covers the cost of notifying affected individuals in the event of a data breach. Customer notification is often required by law.

### **PCI (PAYMENT CARD INDUSTRY)**

Coverage for assessments, fines or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS).

\* All of the above are general terms which may vary based on context. Please consult the quote or ask an agent/broker for precise definitions and details.



## CYBER INSURANCE GLOSSARY (CONTINUED)

**PRIVACY REGULATORY LIABILITY (REGULATORY)**

Covers the loss a company sustains as a result of regulatory investigations and claims.

**SOCIAL ENGINEERING COVERAGE**

Covers unintended payments made to cybercriminals who, through deception, convinced an employee or officer of a company to transfer funds to the criminal.

**THIRD PARTY CLAIM/LIABILITY CLAIM**

When a third party files a claim or lawsuit against the policy holder alleging that the policy holder caused some damage to the third party due to a cyber event.

\* All of the above are general terms which may vary based on context. Please consult the quote or ask an agent/broker for precise definitions and details.