Arlington/Roe®

ArlingtonRoe.com
(800)878-9891

CYBER INSURANCE DEFINITIONS

- **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 may be payable under the business interruption coverage.
- **BRICKING COVERAGE -** Covers the cost to replace computer and electronic hardware that's rendered inoperable due to failed software, firmware update 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 insured.
- **CONTINGENT BUSINESS INTERRUPTION -** A contingent business interruption loss occurs as result of a third-party supplier, service provider or distributor shutdown whose interruption, due to a cyber incident, directly impacts the insured'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 -** A claim triggered by a cyber breach or other qualifying event where coverage immediately responds to losses directly to the insured.
- **FUNDS TRANSFER FRAUD -** Covers the loss stemming from unauthorized instructions from a third party to a bank without the insured'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).
- **PRIVACY REGULATORY LIABILITY (REGULATORY) -** Covers losses that arise out of an organization's failure to protect sensitive, personal or corporate information in any format.

Arlington/Roe®

ArlingtonRoe.com
(800)878-9891

CYBER INSURANCE DEFINITIONS CONTINUED

- **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 insured alleging that the insured caused some damage to the claimant due to a cyber event.

CYBERSECURITY DEFINITIONS

- **DDOS (DISTRIBUTED DENIAL OF SERVICE) ATTACK -** DDoS attack is a malicious attempt to disrupt or shut down normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
- **MALWARE (MALICIOUS SOFTWARE) -** Any code written for the specific purpose of causing harm, disclosing information or otherwise violating the security or stability of a system.
- **PATCH -** An update or change to an operating system or application. A patch is often used to repair flaws or bugs in deployed code as well as introduce new features and capabilities.
- **PENETRATION TESTING (PENTESTING) -** A security test where security experts mimic hackers to expose weaknesses.
- **PHISHING -** A social engineering attack that attempts to collect information from victims. Phishing attacks can take place over email, text messages, through social networks or via smartphone apps.
- **TWO-FACTOR/MULTI-FACTOR AUTHENTICATION (MFA) -** The means of proving identity using two or more ways to identify the user. It is usually considered stronger than any single-factor authentication.
- **VULNERABILITY -** Any weakness in an asset or security protection which would allow for a threat to cause harm.

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