General Glossary on Cyber Insurance

Disclaimer: The definitions and examples provided below are for general, informational purposes only. Notably, these definitions do not set forth all possible scenarios and/or situations applicable to the described events. Policyholders should always refer to their own Policy for specific terms and definitions applicable to their Policy. Nothing in this document is intended to describe or define any coverage offered by Cowbell. However, should you need further information or assistance, please do not hesitate to reach out to us at Cowbell - we would be happy to help with any questions or concerns that you may have.

Insurance

Admitted (or state-admitted): The coverage offered by insurance providers who are licensed to operate by state insurance agencies. Admitted insurance companies must adhere to state regulations regarding policy forms, rate approvals, and claims handling.

Surplus: A segment of the insurance market that allows businesses to buy specialty insurance through the non-admitted market. It is also sometimes referred to as E&S, specialty lines, surplus insurance, and hard-to-place business.

Excess: An excess policy, also called secondary policy, extends the limit of insurance coverage of the primary policy or the underlying liability policy.

Underwriting Guidelines/Rules: A set of rules and requirements an insurer used to underwrite risk. These guidelines are used to make decisions regarding the acceptance, modification, or rejection of a prospective insured.

[Insurance] Coverage: The type and amount of risk or liability that is covered for an individual or entity by way of an insurance policy.

[Insurance] Claim: A formal request by a policyholder to its insurer to pay for something that the policyholder's insurance covers.

Standalone: An insurance product that a business or individual purchases to cover a specific risk or cost. It is the opposite of "packaged insurance" where the policy combines multiple coverages for different types of risk in a variety of scenarios.

Business Owner Policy (BOP): A business owner policy is a package policy that bundles all basic Property and Liability insurance into one policy.

Errors and Omissions (E&O) insurance: E&O insurance generally protects service businesses from errors and/or omissions made by a business owner, employee, or contractor working on behalf of the company. Cyber insurance typically does not cover E&O and E&O does not cover cyber incidents.

Technology Errors & Omission (Tech E&O): A type of insurance designed to cover providers of technology services or products. For example, application developers and website designers provide technology services, while computer software and computer manufacturers offer technology products.

Cyber Insurance

Cyber Insurance: A specialty insurance product intended to protect businesses from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities.

First-party loss: Losses or damage sustained by the insured, such as business interruption, or stolen devices.

First-party expenses: Expenses sustained by the insured to return to normal operations in the aftermath of a cyberattack, such as hiring forensic investigators, sending out notifications to impacted stakeholders, or ransom payments.

Third-party liability: Expenses sustained by the insured through lawsuits of impacted third parties, i.e. when sensitive customer data has been leaked during a breach.

Exposure: The state of being subject to loss because of some hazard or contingency.

Incident Response Plan: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit the consequences of a malicious cyberattack against an organization's information system(s).

Cryptocurrency: A type of digital currency that is often the form of payment demanded as ransom by hackers because it’s untraceable. Bitcoin is the most common example of cryptocurrency.

Fraudulent Funds Transfer: Funds that are illegally taken via an unapproved transfer to someone else, often via a cyber manipulation of employees' trust (example: phishing email or phone scam). This crime is dangerous as it involves access to a business's financial information, where small or even large amounts can be transferred and disappear rapidly prior to being caught.

Social Engineering: A broad term that can encompass several common types of cybercrime. For example, when people approve or interact with a prompt that allows individuals to steal from a business. For example, opening a phishing email that appears to be from an employee's boss asking them to transfer funds to X.

Cybercrime: An umbrella term for types of crime committed solely through cyberspace. (note that the word "Cybercrime" is used in many different ways in the insurance and security world and should always be clarified).

Data Breach: When an unapproved entity accesses private personally identifiable information on a business, its employees, and/or its customers.

Extortion: When a company's system is held hostage by an unauthorized entity and won't be released until they have been paid a ransom.

Personally Identifiable Information (PII): The private information entrusted to a business by their employees or clients: made up of names, email addresses, phone numbers, health information, order history, etc.

Phishing: A common way to breach a business's computer system is by sending a fraudulent communication that deceives the recipient into opening content that could compromise their computer system. The most common way phishing links are sent is via email, or in some cases, SMS text messages (this is called "smishing").

Class of Business: Industry in the insurance world like a patient is a customer for a doctor or a hospital. A class of business typically refers to specific NAICS codes.

Ransomware attack: A type of extortion attack that highjacks a business's systems and data and employs encryption to hold the victim's information at ransom. The cybercriminals threaten to perpetually block access to systems or data unless a ransom is paid.

Double ransomware: A ransomware with a double extortion threat is a ransomware attack that in addition to demanding payment to regain access to systems and data also threatens to publish highjacked data if the payment is not made.

Triple threat ransomware: In addition to the above, if the business still refuses to pay the ransom, the criminals initiate a denial-of-service attack which might trigger an interruption of internet services.

Cybersecurity

MFA or 2FA: Multi-factor authentication or two-factor authentication.

CVE (Common Vulnerabilities and Exposures): A list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw that's been assigned a CVE ID number.
Main site: https://www.cve.org/ Example: CVE-2022-20016

Exploit: An exploit is a code that takes advantage of a software vulnerability or security flaw. A CVE might not be a serious software issue until there is a means to take advantage of the vulnerability to penetrate a system or cause damage to it.

Zero-day vulnerability: A zero-day is a newly discovered computer-software vulnerability unknown to those who should be interested in its mitigation (example: the software provider) or known but without a patch to correct it.

Zero-day exploit: This is an exploit targeted at a zero-day vulnerability.

CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart

The Cowbell Fundamentals

Cowbell Cyber: Cowbell is the leading provider of cyber insurance for small and medium-sized enterprises. Cowbell is signaling a new era in cyber insurance by harnessing technology and data to provide businesses with advanced warning of cyber risk exposures bundled with cyber insurance coverage adaptable to today's and tomorrow's threats.

Cowbell Prime™: Cowbell's portfolio of cyber insurance programs targeted at enterprises with up to $250m in revenue.

Cowbell Prime 100: Cowbell's admitted cyber insurance program targeted at enterprises with up to $100 Million in revenue.

Cowbell Prime 250: Cowbell's admitted and surplus cyber insurance program targeted at enterprises with revenue ranging from $100 Million to $250 Million.

Cowbell Prime Plus: Cowbell Prime Plus offers excess cyber risk insurance on top of primary cyber insurance. Cowbell Prime Plus serves enterprises that need higher limits than what's offered with their primary policy.

Cowbell Factors™: Cowbell's set of proprietary risk ratings that define an organization's risk profile in comparison with Cowbell's risk pool of 25 million US accounts (as of Q3 2022).

Cowbell Platform: The technology, data, and cloud services that enable Cowbell Cyber to offer and deliver differentiated cyber insurance programs.

Closed-loop Risk Management: A term coined by Cowbell to define a holistic approach to risk management. The four pillars of Cowbell's closed-loop risk management - ASSESS, INSURE, IMPROVE, RESPOND cover the entire lifecycle of risk from identification, visibility, and understanding to quantification, remediation, incident response, and recovery when a cyber event occurs.

Risk Aggregation: Risk aggregation is a common concept in risk management contexts. Overall, it relates to the process of summing (or aggregating) and showing the interaction between single or individual risks, to see the bigger picture.