Coverage Definitions

3rd Party Coverage	Definition
Cyber / Privacy Liability	Defense and indemnity for claims against you related to cyber events / data breaches
Media Liability	Defense and Indemnity for claims of libel, slander, copyright infringement, trademark infringement, invasion of privacy, etc.
Regulatory Defense & Fines	Defense and indemnity coverage for claims brought by federal, state, local or foreign governing body related to privacy regulations, data breaches, cyber events, and fines and penalties where insurable by law
PCI Fines & Assessments	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)
Management Liability	Defense and indemnity coverage for management should they be deemed legally responsible for a breach; Excess D&O coverage for cyber-related events only
Defense (Outside the Limits)	Additional defense coverage outside of the limits of liability.
Contractual Liability	Defense and indemnity coverage for events that are part of a contractual agreement; Affirmative coverage or a carve back to a breach of contract exclusion
Bodily Injury / Property Damage	Defense and indemnity coverage when a cyber event results in physical damage or injury
1st Party Liability	**Definition**
Breach Response & Remediation	Coverage for response and remediation costs associated with a breach; This includes legal fees, customer notification, IT/digital forensics, and crisis media relations, among others
Cyber Business Interruption	Coverage for financial losses due to a cyber event that causes degradation to your computer system; Usually requires a time retention (see Business Interruption Waiting Period)
Dependent Business Interruption	Coverage for financial losses due to a cyber event when a 3rd party provider experiences an outage that causes you disruption; 3rd parties often include cloud providers or other software/services providers
System Failure	Coverage for business interruption resulting from an unplanned or unintentional outage, often caused by employee error or power outage
Business Interruption Waiting Period	Time retention typically applied to cyber business interruption, dependent business interruption, and system failure.
Cyber Extortion / Ransomware	Coverage for the costs to respond to a cyber extortion (ransomware) event, including forensics experts to investigate the attack, experienced negotiators, and sometimes ransom payments in virtual currencies
Ransomware Payment Provision	Provision for how the policy responds to a ransomware claim; “Pay on behalf” indicates the carrier will tender payments due when a ransom event occurs; “Reimbursement” indicates the insured will pay out of pocket and then seek reimbursement for covered losses
Digital Asset Damage	Coverage for costs to rebuild electronic data and other digital assets after a cyber-event, like recovering offsite backups, etc.

1st Party Coverage (continued)	Definition
Cyber Crime	Coverage for the theft of funds from a failure in your security, often by a hacker stealing login credentials; This is often referred to as fund transfer fraud and may be covered on a crime policy
Social Engineering	Coverage for theft of funds by using deception or impersonation, where a criminal tricks you into parting with your funds; Often ties into a business email compromise
Client Funds	Coverage extension to cover theft of client funds in the insured's care, custody, or control
Invoice Manipulation	Coverage for the release or distribution of a fraudulent invoice or fraudulent payment instruction to a third party as a result of a cyber-event
Telephone Hacking	Coverage for costs associated with unauthorized and fraudulent telephone calls
Crypto Jacking	Coverage for costs associated with unauthorized use of the insured's computer processing power to mine crypto currency
Reputational Harm	Coverage for lost income from an adverse media event due to a cyber event that damages the insured's reputation
Breach Response (Outside the Limit)	Coverage for 1st party breach costs outside of and in addition to the policy aggregate limit
Bricking	Coverage for physical damage to IT hardware resulting from a cyber event that renders the equipment useless and unable to be safely repaired
Bodily Injury / Property Damage	Coverage for bodily injury or property damage which results from a cyber-event.
Pollution	Coverage that would apply should the insured experience a cyber-event which causes a pollution condition
BYOD	Coverage for any device used by the company's employees in the course of normal business operations, no matter who the device belongs to
Additional Services	
Cyber Risk Report	An assessment of the company's business cyber security often providing a score and actionable security recommendations; Carriers that can provide this usually only need the company's URL to do an outside-in scan and provide this for all quotes
Proactive System Monitoring	Ongoing and regular scanning to monitor for security vulnerabilities; If an issues are flagged, carrier will proactively notify the insured and offer assistance to mitigate; Only provided to policy holders
Pre-claim Assistance	Access to software and services including cyber risk applications, breach response plans, data breach calculators, and other risk management tools to manage cyber risk
Expert Security Advice	Open access to Cybersecurity experts to ask questions about the company's security; usually access is provided via phone or email