ARAGON WAY

Cyber Insurance

Coverage Cheat Sheet

561-830-3360 insure@aragonway.com aragonway.com

Cyber Insurance

Coverage Cheat Sheet

First-Party Coverage

Pays your firm directly for your own losses: response costs, lost income, and data recovery.

Third-Party Coverage

Covers claims brought against your firm by clients, regulators, or partners harmed by a breach at your firm.

Crime Coverage

Addresses direct financial theft triggered by a cyber event; often written as endorsements with separate sublimits

Specialty Coverage

Technology-specific protections, including professional liability for technology services and vendor flexibility.

Systemic & Widespread Events Coverage

When many firms file claims simultaneously, carrier capacity can be constrained in ways that reduce each firm's recovery.

Critical Policy Mechanics

Beyond coverage categories, several policy mechanics determine whether your claim is paid.

Coverage categories and descriptions in this guide are representative of common cyber insurance policy structures and do not constitute a complete list of available coverages. Actual policy forms vary significantly by carrier, program, and policy year. Some coverages described herein may be included as standard, offered as optional endorsements, subject to sublimits, or unavailable depending on the carrier and the insured's specific program. This guide is intended as an educational reference only and should not be used as a substitute for reviewing the actual policy language.

1-561-830-3360 | insure@aragonway.com | aragonway.com

First-Party Coverage

Policy Pays Your Firm Directly

First-party coverages are the foundation of any cyber policy. These are the costs that hit your firm immediately and directly when an incident occurs before any lawsuit is filed, before any regulator calls, and often before you fully understand what happened. For any business managing sensitive data or critical operations, these coverages can play a major role in how well your organization manages the first 72 hours of a breach.

Incident Response Expenses

Covers your immediate response costs: legal counsel, forensic investigators, breach notification to affected parties, credit monitoring services, and public relations. This is often your first and largest expense after a breach. Response costs can be substantial, and the response process begins the moment a breach is discovered.

Business Interruption

Replaces lost net income and covers ongoing operating expenses when your own systems are down due to a cyber event. A ransomware attack that disrupts operations for a week can create significant lost revenue, often well beyond the immediate extortion demand. This coverage bridges that gap while your team works to restore operations.

Contingent Business Interruption

Extends business interruption coverage to losses caused by an outage at a third-party technology provider you depend on, even if your own systems are untouched. If your ERP system, CRM, or cloud provider goes down due to their own breach, your loss is still real. Many firms overlook this until a major cloud outage affects their operations.

Digital Data Recovery

Pays to restore or reconstruct lost, corrupted, or destroyed data and software. After ransomware or a destructive attack, rebuilding your data from backups or from scratch is expensive and time-consuming. For firms with proprietary data, customer records, or years of business history, this coverage is essential.

Network Extortion

Reimburses ransom payments made to end a ransomware or extortion event, plus negotiation and response expenses. Ransomware demands can be significant, and negotiation support can materially affect the outcome. Coverage includes access to professional negotiators who understand the landscape and can often significantly reduce demands.

1-561-830-3360 | insure@aragonway.com | aragonway.com

Third-Party Coverage

Policy Pays on Behalf of Your Firm to Others

Third-party liability coverages activate when someone else suffers harm because of an incident that originated with your firm. For businesses handling customer data or other sensitive information, this category addresses your exposure to lawsuits, regulatory investigations, and contractual penalties. The financial and reputational consequences of a third-party claim can far exceed the cost of the breach itself, **particularly in industries subject to federal and state data protection requirements**.

Defense Costs for Regulatory Investigations & Enforcement

Defense costs for regulatory investigations and enforcement actions related to a cyber event, plus coverage for fines and penalties where permitted by law. Data breach notification laws exist in all 50 states. A breach can trigger investigations by regulators, state attorneys general, or other governing bodies, even when no lawsuit follows. Regulatory defense costs can be significant even before any penalty is assessed.

Cyber, Privacy & Network Security Liability

Liability claims from clients, partners, or regulators alleging that your firm failed to protect their private or confidential information, or that your network security failed and caused harm to others. If a client's data is exposed in a breach at your firm, they can sue. This covers your defense costs and any resulting settlement or judgment, which can be substantial depending on the industry and scope.

Payment Card Loss, Fines, & PCI Assessments

Covers contractual liabilities to payment card brands and processors arising from a cyber incident that compromised cardholder data. Card brand fines and PCI assessments can be material and are often excluded from standard cyber policies unless explicitly included. Verify this language carefully if your firm accepts any card payments.

Media Liability

Covers liability for defamation, copyright infringement, or trademark infringement that occurs through your website, social media, or other online content. A single post or video that uses unlicensed images, music, or excerpts can trigger a copyright claim. Defense costs alone can be significant even where no judgment is entered against you.

1-561-830-3360 | insure@aragonway.com | aragonway.com

Cyber Crime Coverage

Financial Fraud Triggered by a Cyber Event

Crime coverage addresses one of the most urgent risks for any business: the direct theft of money or assets enabled by a cyber event. Unlike the liability coverages in the previous section, these aren't about defending against someone else's claim; they're about recovering your own money after it's been taken. The critical detail most business owners miss is that these coverages almost always carry their own sublimits, separate from the main policy limit.

Computer Fraud

Covers theft of money or securities that occurs when a third-party gains unauthorized access to your computer systems and initiates or redirects a transfer. This requires evidence of unauthorized computer access, often the narrowest of the three crime coverages in terms of its application.

Funds Transfer Fraud

Covers losses when a third party tricks your bank or financial institution into transferring funds out of your account without necessarily accessing your systems directly. A common source of cyber-related financial loss for many businesses. A spoofed wire instruction or fraudulent transfer request can result in immediate, significant, and often irreversible loss.

Social Engineering Fraud

Covers losses when a third party manipulates an employee through impersonation, deception, or false pretenses into voluntarily transferring money or assets. Business email compromise (BEC) falls here. The funds leave legitimately because the employee believes they are following legitimate instructions and may be unrecoverable without this coverage in place.

Important: Sublimits on Crime Coverages such as Computer Fraud, Funds Transfer Fraud, and Social Engineering are often written as endorsements with their own sublimits separate from your main policy limit. For example, a policy with a $2M overall limit may have a much lower sublimit for crime-related coverages.

Always confirm the actual sublimit.

Do not assume your full policy limit applies to these coverages.

1-561-830-3360 | insure@aragonway.com | aragonway.com

Specialty Coverage

Technology-Specific Protections

Specialty coverages address exposures that don't fit neatly into the first-party or third-party framework. They are particularly relevant for firms that provide any technology-based service to clients, including software platforms, automated tools, and customer portals, as well as for firms that have established vendor relationships they want to preserve during an incident response. Understanding these coverages before you need them can make the difference between a smooth incident response and a contentious one. Additional specialty coverages to consider include reputational harm coverage, voluntary shutdown coverage (proactive costs incurred to prevent a larger loss), and bricking coverage (hardware rendered inoperable by a cyberattack).

Technology Errors & Omissions (Tech E&O)

Covers claims alleging errors, omissions, or failures in technology services or advice you provide, including failures in systems, platforms, or software you deliver to clients.

Why It Matters

This is relevant if your firm provides any technology-based service, platform access, or automated tools to clients. A system failure that causes a client to miss a deadline, lose data, or incur financial loss can trigger an E&O claim that a standard cyber policy will not cover without this endorsement. The line between a technology failure and a professional failure is increasingly blurred in modern business.

Non-Panel Incident Response Service Providers

Most carriers maintain a pre-approved panel of incident response vendors, including forensic investigators, breach coaches, and legal counsel. This coverage reimburses the costs of hiring qualified vendors outside that panel, giving you the flexibility to use established relationships or specialists not on the carrier's list.

Why It Matters

In a fast-moving incident, your existing vendor relationships matter. Your outside counsel knows your business. Your IT firm knows your systems. This coverage preserves your ability to bring in trusted specialists rather than being limited to the carrier's approved list, which may not include the firm best suited to your situation.

1-561-830-3360 | insure@aragonway.com | aragonway.com

Systemic & Widespread Events

When Many Firms Are Hit at Once

A growing class of coverage addresses scenarios where a single cyber event affects thousands of companies simultaneously, a major cloud outage, a widely-deployed software vulnerability, or a supply chain compromise. These events are fundamentally different from a firm-specific attack. When many firms file claims simultaneously, carrier capacity can be constrained in ways that reduce each firm's recovery. Understanding the endorsements and peril categories that govern these events is essential before a major industry-wide incident occurs.

Widespread Event Endorsement

Provides specific limits, retentions, and coinsurance terms for widespread events, clarifying what you'll actually recover when the entire industry is affected simultaneously. Without this, a catastrophic widespread event may exhaust a shared pool of carrier capacity in ways that reduce your individual recovery below what your policy limits suggest.

Ransomware Encounter Endorsement

Allows you to customize your coverage limits, retention, and coinsurance specifically for ransomware losses, separate from the rest of the policy. Useful when ransomware is your primary concern, and you want to ensure those limits reflect your actual exposure rather than sharing headroom with other coverage lines.

Neglected Software Exploit Endorsement

Provides a grace period, which varies by carrier, to patch known vulnerabilities listed in NIST's National Vulnerability Database. After the grace period, your coverage share shifts progressively, meaning unpatched systems increasingly become your financial responsibility.

Covered Peril Categories

How Widespread Events Are Classified

Known Vulnerability Exploit

Attacks launched against a known, unpatched software vulnerability. Typically, easy to exploit remotely, requiring limited privileges, and capable of significant damage.

Software Supply Chain Exploit

A bad actor compromises trusted or certified software used by many organizations, simultaneously using legitimate software as a delivery vehicle for a widespread attack.

Zero-Day Exploit

Attacks from a vulnerability known to attackers but not yet publicly disclosed; no patch exists yet. A particularly challenging exploit, as there is no patch or established defense at the time of attack.

All Other Widespread Events

A broad catch-all for large-scale cyber events that affect many victims simultaneously, such as widespread cloud service outages caused by a cyberattack.

1-561-830-3360 | insure@aragonway.com | aragonway.com

Critical Policy Mechanics

What Every Policyholder Should Understand

Beyond coverage categories, several policy mechanics determine whether your claim is paid. These structural features are easy to overlook during the buying process but can be the difference between full recovery and a denied claim. Understanding them before renewal gives you the leverage to negotiate better terms.

Claims-Made Policies & Duty to Report

Virtually all cyber policies are written on a claims-made basis, meaning the policy in effect when the claim is reported is the one that responds, not the policy in effect when the incident occurred. Late notice can create serious coverage issues and may jeopardize a claim.

Why It Matters

Report incidents to your carrier as soon as you suspect a breach, even before the full scope is known. Many policies require notice "as soon as practicable," and waiting until you have all the facts can jeopardize coverage. Your policy may also include an Extended Reporting Period (ERP) or "tail" option, which is critical if you switch carriers or let coverage lapse.

Retroactive Dates & Prior Acts Coverage

Your retroactive date determines how far back your policy will look for incidents. Coverage typically only applies to incidents first discovered after this date. If you switch carriers, the new policy may set a fresh retroactive date, creating a gap for any incidents that occurred before the switch but are discovered afterward.

Why It Matters

When purchasing cyber insurance for the first time or switching carriers, negotiate for the earliest possible retroactive date, ideally "full prior acts" coverage with no retroactive date limitation. A policy with a retroactive date set to the policy inception date provides zero protection for breaches that occurred before you bought coverage but were not yet discovered, which can create a meaningful coverage gap for incidents that occurred earlier but were discovered later.

1-561-830-3360 | insure@aragonway.com | aragonway.com

Cyber Insurance

Start With a Conversation

Get a Cyber Insurance Quote

View Application

Complete the cyber quote form, and we will identify the coverage options for your risk profile. We walk through your options in plain terms and explain what each policy actually covers before you make any decisions.

Schedule a Coverage Consultation

Schedule a Consultation

Not sure where to start? We walk through your risk exposure, explain how coverage holds up in a real claim scenario, and help you find the right fit without the pressure.

Review Your Existing Policy

Already have cyber coverage? We can review your policy, identify gaps or mismatched limits, and help you understand how it is likely to respond to a claim. No cost, no obligation.

Request a Coverage Checklist

Take our plain-language checklist to your next renewal. It covers the key coverages and policy mechanics that businesses may overlook until a claim is denied.

1-561-830-3360
https://aragonway.com
Schedule a Call
insure@aragonway.com

Cyber Insurance Quote