Section 1: Headline

We reviewed your At-Bay Specialty Insurance Company cyber insurance policy (form AB-CYB-001.2, 08/2023). We found 0 critical issues, 4 moderate issues, and 2 notes. Overall this is a well-structured policy form with several buyer-friendly provisions, but four clauses could meaningfully reduce a payout in a real claim and deserve a conversation with your broker before you need them.

Note: This document appears to be a specimen or quote form rather than your fully issued policy. The findings below are based on what's visible. Your bound policy may contain additional endorsements or schedules — for a complete review, upload your full policy package.

Section 2: Critical Issues

We found no critical issues in your policy. That's a strong starting point.

Section 3: Moderate Issues

The war exclusion has no visible cyber-terrorism carveback

The policy excludes all losses arising from war, invasion, acts of foreign enemies, hostilities, or warlike operations — but the form contains no language carving back coverage for cyber terrorism or state-sponsored attacks. This matters because the line between a criminal ransomware gang and a state-sponsored threat actor is frequently blurry in practice, and insurers have argued (in cases like Mondelez v. Zurich) that nation-state malware crossing into commercial networks triggers the war exclusion. If your business is hit by an attack that a forensics firm later attributes to a foreign government — even partially — this exclusion could void your entire claim.

Ask your broker whether your bound policy or any attached endorsement includes a cyber-terrorism carveback that explicitly restores coverage for state-sponsored attacks, and get that answer in writing before your next renewal.

Your sublimits reduce your aggregate rather than adding to it

Every sublimit in this policy — ransomware/extortion, business interruption, social engineering, regulatory fines, and anything else shown on your Declarations page — is "part of and not in addition to" the Aggregate Limit of Insurance. That means all your coverage buckets share one pool of money. If you have a $1M aggregate and burn through $500K responding to a ransomware event, you have $500K left for everything else — including a lawsuit filed by patients or customers whose data was exposed in the same incident.

Ask your broker to walk through your specific sublimit structure alongside your aggregate limit and confirm the total is actually sized for your industry's realistic worst-case scenario, not just average claim costs.

The prior knowledge exclusion uses a "reasonably would be regarded as" standard

The policy excludes claims arising from any fact, circumstance, or event that any member of your Control Group (CEO, CFO, CTO, General Counsel, or equivalent) "had knowledge" of, or that "reasonably would be regarded as" the basis for a claim, prior to the Continuity Date on your Declarations page. The "reasonably would be regarded as" language is meaningfully broader than a pure actual-knowledge standard. If a member of your leadership team received a security alert, a vendor warning, or even a routine IT ticket about a vulnerability before your coverage started — and an attacker later exploited that same vulnerability — the insurer could argue that the Control Group should have recognized the risk and decline the claim.

Policy language: "*alleging, based upon, arising out of, or attributable to any fact, circumstance, situation, event, Cyber Event, or Wrongful Act that is, or reasonably would be regarded as, the basis for a Claim or Cyber Event about which any member of the Control Group had knowledge prior to the Continuity Date*"

Before your next renewal, do a documented review of any open security issues, unpatched systems, or prior vendor notifications your leadership team is aware of. Ask your broker what your Continuity Date is and whether anything in your current security posture could be characterized as a known risk under this standard.

Your third-party vendor coverage requires a written contract

The policy covers systems and services operated by outside vendors — cloud platforms, SaaS tools, hosted software — only when those vendors are operating under a written contract with your organization. "External Computer Systems" is defined to include cloud services, IaaS, data hosting, and co-location, but only those run by a third party "under written contract between such third party and Insured." Most enterprise software vendors deliver a formal contract, but many smaller SaaS tools are activated via a click-through Terms of Service. If a critical vendor you rely on — a cloud storage provider, a practice management platform, a payment processor — goes down due to a cyberattack and you discover you only accepted their click-through terms, your contingent business interruption claim may be at risk.

Ask your broker whether click-through Terms of Service agreements qualify as a "written contract" under this policy. Make a list of every cloud tool and hosted service your business depends on and confirm each one has a formal, signed agreement in place.

Section 4: Notes

Your settlement hammer clause is more favorable than market standard

If your insurer recommends a settlement you disagree with, and you refuse, the policy caps your exposure well: the insurer pays the full settlement amount that was on the table, then continues covering 80% of all defense costs and damages that accrue beyond that point. The market standard for many cyber policies is 50% of defense costs only, which leaves you exposed on both damages and a larger share of ongoing legal fees. This policy's structure keeps you better protected if a claim becomes a long, contested litigation.

No action needed — this is a favorable provision. Just be aware it exists and understand what "refusing a recommended settlement" means in practice before you ever find yourself in that conversation.

The policy cannot be rescinded against you

Many insurance policies contain a rescission right that allows the insurer to void coverage from the beginning if it later discovers the application contained material misrepresentations. This policy explicitly states the insurer "shall not be entitled under any circumstances to void or rescind this Policy with respect to any Insured." That is a meaningful protection: if a coverage dispute arises, the insurer's remedy for misrepresentation is limited — it cannot simply declare the policy void and walk away from all claims.

No action needed — this is a buyer-favorable clause worth knowing about.

Section 5: Policy Snapshot

- **Carrier:** At-Bay Specialty Insurance Company
- **Policy form:** AB-CYB-001.2 (08/2023)
- **Aggregate limit:** See your Declarations page (ITEM 4)
- **Retention/Deductible:** See your Declarations page (ITEM 6) — note that separate retentions apply per Insuring Agreement, capped at the largest single retention when multiple coverages apply
- **Retroactive date:** See your Declarations page (ITEM 7)
- **Key sublimits:** See your Declarations page (ITEM 6) — sublimits apply per Insuring Agreement and are part of, not in addition to, the aggregate limit; the Period of Restoration for business interruption is capped at 180 days
- **Settlement clause:** 80% of defense costs and damages (above the original settlement amount) — more generous than the market standard 50%
- **Vendor coverage style:** Open (any third party operating systems for your benefit under a written contract)
- **Cyber-terrorism carveback:** Not present in the form — verify with your broker whether an endorsement provides one

Want a complete Snapshot with your actual numbers? Reply to your report email with your Declarations page (or just the aggregate limit, retention, key sublimits, and retroactive date) and we'll update this

report at no charge.
