Pre-Shutdown Four-Check Quick Card

Broker Cyber Policy Precautionary Offline Protocol • Grounded in Post 1194

Current version — Oct 31, 2026. Update history: https://riskcoveragehub.com/what-should-a-broker-check-about-a-clients-cyber-policy-before-a-precautionary-shutdown/
Notice: For licensed insurance broker use. All policy wording must be verified against client declarations and form endorsements prior to executing an operational shutdown.

The Operational Context (PHP Oct 21 Emergency Advisory): PHP released critical remote code execution fixes (CVE-2026-109618, CVE-2026-109619; CVSS 9.2). Supported fixes: PHP 8.5.12, 8.4.27, 8.3.36, 8.2.35. PHP 8.1 and older receive no update. Exposures include PHP-FPM, Apache mod_php (highest risk), php-cgi, FrankenPHP, LiteSpeed. CISA advises taking systems offline if unable to patch immediately. Coalition observed in-the-wild exploit attempts >5 hours before release. *Cowbell CCO Simon Hughes Rule:* "Businesses that switch off as a precaution, and the brokers advising them, should check now how their cyber policy treats a voluntary shutdown and what waiting period applies, rather than finding out at claim stage."

CHECK 1: WAITING PERIOD & CLOCK-START ARITHMETIC

DEDUCTIBLE IN TIME Declaration Hours

- **Cyber vs Traditional BI Benchmark:** Cyber BI waiting periods are almost always <24 hours (usually **6 to 12 hours**), compared to a typical **72 hours** under traditional property/BI forms (Broker Hylant comparison).
- **Retained Loss Rule:** Income lost inside the waiting period is 100% the client's money, not the insurer's. Chubb PremierTech2 wording states expressly: business interruption loss does not include amounts accrued during the waiting period.

CLOCK-START EVENT Actual Interruption Trigger

- **Beazley Breach Response 5.0 Standard:** Waiting period begins upon the *actual interruption* of business operations caused by a security breach — expressly including a voluntary shutdown — or a system failure, and runs for the hours listed in declarations.
- **Patch vs Waiting Period Formula:** If the client's realistic patch-and-test window is shorter than the waiting period (e.g., 4-hour maintenance vs 8-hour waiting period), the entire financial loss is retained by the client.

CHECK 2: TRIGGER DOOR MATCHER (INTRUSION VS THREAT)

The PHP Fact Pattern Stress Test: A client faces a critical CVE, active internet scanning, and a CISA recommendation to shut down — but has *no evidence* of an active intrusion into its own systems. Cyber forms provide three distinct trigger doors:

Carrier Form	Voluntary Shutdown Trigger Language	Precautionary Outage Status
Beazley Breach Response 5.0	Covered only to the extent necessary to limit loss during an *"active or ongoing Unauthorized Access or Use... or an infection... by malicious code"*, or expressly required by a governmental entity resulting from that situation.	**DOOR CLOSED** Pure threat or vulnerability advisory alone does not satisfy trigger without active unauthorized intrusion.
Cowbell Prime One / HSB Total Cyber	Cowbell: shutdown taken to *"minimise, avoid, or reduce further damage as a result of a covered incident."* HSB: shutdown *"in an effort to mitigate effects of or recover from the attack."*	**DOOR CONDITIONAL** Requires linking the threat to an imminent attack or defined covered incident under policy terms.
Chubb PremierTech2	Covered incident expressly includes *"the reasonable and necessary shutdown"* of a covered system *"in an attempt to prevent or mitigate the effects of"* a malicious act, unauthorized access, human error, network security failure or programming error.	**DOOR OPEN** Expressly permits shutdown in an attempt to *prevent* listed causes. Reasonable and necessary evidence required.

Broker Golden Rule: Never tell a client "voluntary shutdown is covered" off the strength of the defined term alone. Identify which of the three doors the policy actually has, in writing, before systems are severed from the internet.

Current version — Oct 31, 2026. Update history: https://riskcoveragehub.com/what-should-a-broker-check-about-a-clients-cyber-policy-before-a-precautionary-shutdown/

CHECK 3: PATCH CONDITIONS & KNOWN-VULNERABILITY LANGUAGE

COALITION POSITION **Carrier Specific**

Daniel Woods (Head of Emerging Risks, Coalition):

"We don't have a clause in the policy that bars coverage if they don't apply the patch. In practice, we find customers are very cooperative."

CRITICAL CAVEAT: This is one carrier's position on the record, not a general cyber insurance market rule. It does not govern other carriers' exclusions or warranties.

3-QUESTION ISOLATION **Do Not Merge**

Brokers must review form conditions and separate three questions clients habitually confuse:

- **Q1: Shutdown Coverage:** Does the policy pay income lost during a voluntary preventative shutdown?
- **Q2: Subsequent Breach Coverage:** Does coverage respond if an unpatched flaw is later breached?
- **Q3: Patch Timeline Defenses:** Does staying unpatched violate maintenance warranties or application representations?

CHECK 4: CIVIL AUTHORITY — DO NOT REACH FOR IT

The Property Coverage Reflex: When CISA or another federal body issues an advisory, insureds immediately assume "Civil Authority" coverage applies. This extension answers a fundamentally different problem.

Connell Foley Physical-Damage Rule: Civil authority responds strictly to orders tied to *actual physical damage to nearby property*. Losses from government orders issued because of "merely a threat of, or potential or anticipated, damage are not covered."

CISA Alert ≠ Civil Authority Order: CISA's advisory is a voluntary operational recommendation to patch or disconnect, not a mandatory legal order arising from property damage.

Cyber Government Order Grants: Under forms addressing government orders (e.g., Beazley Breach Response 5.0), the shutdown must be "*expressly required by a governmental entity*" resulting from an active intrusion situation, not a vulnerability bulletin.

CHECK 5 / THE PAPER: 5-PART PRE-SHUTDOWN MASTER FOLDER

Create Before Systems Go Offline: A precautionary shutdown claim is won or lost on contemporaneous evidence created before and during the outage. Establish these five folders immediately:

File Component	Required Records & Substantiation	Authoritative Benchmark
1. Decision Record	Document who decided to shut down, exact timestamp, officers involved, IT lead concurrence, and specific advisories relied upon (PHP alert, CISA bulletin).	Proves commercial reasonableness & prevention attempt.
2. IT Operations Timeline	Synchronized server logs showing exact disconnection timestamp, isolation of web services (PHP-FPM, Apache), patch application, staging tests, and go-live.	Crestview Public Adjusters downtime duration standards.
3. Compromise Check Log	Audit logs inspecting Coalition's 4 signs of compromise: (a) PHP spawning shells, (b) web-root file changes, (c) new cron jobs/accounts, (d) upload requests + OOM errors.	Coalition threat advisory & prompt claims notice mandate.
4. Financial Baseline	Daily operational records for loss period and prior year; monthly billings/collections (≥1 year); prior tax return; monthly P&L; weekly payroll; cancelled vs made-up sales schedule; saved expenses.	Beazley Forensic Accountant claims audit list.
5. Extra Expenses & Threat Proof	Invoices for external IT/forensics, emergency patching overtime; preserved copies of vendor alerts, CISA advisory, Coalition Oct 20 alert; written claims notice log.	Chubb & Crestview extra-expense mitigation recovery.

Notice Discipline Mandate: Coalition instructs policyholders who observe signs of compromise to contact claims immediately. Giving prompt notice of a precautionary shutdown costs nothing and eliminates carrier late-notice defenses.