After a breach report: what a state insurance regulator is likely to ask for

Two texts set the pattern. The NAIC Insurance Data Security Model Law, in force in 28 jurisdictions as of October 2026, gives an insurer, agency or other licensee 72 hours from determining that a cybersecurity event has occurred to notify the commissioner, with a 13-item notice and a continuing duty to update. New York's 23 NYCRR Part 500 gives every DFS-regulated firm the same 72 hours, plus 24 hours to report an extortion payment and an annual certification by 15 April. Both require a written program, a risk assessment, board oversight and a tested incident response plan, and both exempt the smallest firms from the program but not from the notice. These are the records the rules require, so they are what an examiner asks for.

Where the NAIC model law applies.

28 jurisdictions

had implemented Model Law 668 as of 8 October 2026, 27 states and Puerto Rico (NAIC Government Affairs brief, October 2026). New York runs Part 500 instead.

DFS penalties in one cybersecurity action.

$19.1m eight insurers

paid by eight auto insurers on 14 October 2025 for Part 500 failures; two also reported late. Since then: Delta Dental, $2.25 million (April 2026); two mortgage servicers, $6.75 million (19 November 2026).

ITEM & DESCRIPTION	REGULATION
☐ **1. The 72-hour notice and every update.** The initial filing and the continuing updates the rules require. → Have it ready: the filed form, the determination and filing timestamps, the 13 items.	Model 668 s.6A, 6B; 500.17(a)
☐ **2. Incident response plan.** The written plan in force on the day, and proof it was tested. → Have it ready: the current version, roles, the last test date and results.	Model 668 s.4H; 500.16
☐ **3. Information security program.** The written program, its policies and the person responsible. → Have it ready: the program, its approval record and the CISO designation.	Model 668 s.4A to 4D; 500.2 to 500.4
☐ **4. Risk assessment.** The documented assessment that drove the controls, updated annually. → Have it ready: the dated assessment, method and risk register.	Model 668 s.4C; 500.9
☐ **5. Board oversight and the annual certification.** Proof leadership saw the program and signed the filing. → Have it ready: minutes, management's annual report, the February or April filing.	Model 668 s.4E, 4I; 500.4, 500.17(b)
☐ **6. Third-party service provider records.** Who holds your data, on what terms, and what they told you when. → Have it ready: the vendor list, due diligence, contract clauses, any vendor notice.	Model 668 s.4F; 500.11
☐ **7. MFA and access evidence.** Who could get in and how, with any written compensating-control approval. → Have it ready: MFA configuration, privileged-account list, access logs.	Model 668 s.4D; 500.12
☐ **8. Asset and data inventory.** What systems and data exist, where, and who owns them. → Have it ready: the inventory with owner, location, classification and recovery objectives.	Model 668 s.4B, 4D; 500.13
☐ **9. Forensic report and timeline.** What happened, when, to what data, and the root cause. → Have it ready: the report, period of compromise, consumer counts by state, remediation log.	Model 668 s.5D, 6B; 500.16
☐ **10. Consumer notice and who was told when.** The notice sent under the state breach law and the regulator copies. → Have it ready: the letter, send dates, counts, regulator and police notifications.	Model 668 s.6C; 500.17(a)

IF YOU ONLY DO ONE THING

Fix the clock. Both regimes give 72 hours from the moment you determine an event has occurred, including one at a vendor. Write down who makes that determination and how it is time-stamped, then test that the plan can produce the first notice inside the window. The DFS actions of 2025 and 2026 turned on late notice, missing MFA and stale risk assessments, so keep those three dated all year.