



Offensive security for the insurance industry

Offensive security testing built for NAIC compliance

Insurance providers hold some of the most sensitive PII and PHI of any industry, often on systems built long before today's compliance requirements existed. The NAIC Insurance Data Security Model Law (#668) raises the bar for how that data gets protected, and testing is how you show your program holds up in practice, not just on paper.

Why offensive security matters under Model Law #668

Model Law #668 requires a written information security program built on an annual risk assessment. A program that looks complete on paper is not the same as one that holds up under a real attack. Offensive security testing is how you find out whether your controls, your third-party oversight, and your incident response actually work, before a regulator, an auditor, or an attacker finds out for you.

What Model Law #668 requires

- Maintain a written information security program based on an annual risk assessment
- Designate an employee, or a third party, responsible for that program
- Investigate cybersecurity events and notify the state insurance commissioner
- Oversee the third-party service providers that handle nonpublic information
- Regularly test and monitor systems to detect actual and attempted attacks, scaled to the risk assessment¹

Risk-based, not one-size-fits-all

Model Law #668 does not set a fixed annual cadence for pentests. It requires testing intensity to match your own risk assessment. That puts the responsibility on you to scope testing around where your real exposure sits: for example, undocumented APIs, legacy systems still in production, and the parts of your environment no audit has fully mapped yet.

1. NAIC Insurance Data Security Model Law (#668), National Association of Insurance Commissioners, adopted 2017.

A program that matches how you actually operate

Insurance providers should develop testing that maps to how you actually run your systems: the systems your policyholders touch every day, the systems your subsidiaries and affiliates operate independently, and any newly developed or undocumented systems.

Scope of testing program

Application security

- **Web App Pentest.** Policyholder portals, agent and broker interfaces, claims systems: the interfaces your business depends on every day.
- **API Pentest.** REST, SOAP, and GraphQL interfaces behind claims and eligibility systems, often the least documented part of the attack surface.
- **Mobile App Pentest.** Policyholder and claims apps on iOS and Android, a growing channel for PII exposure.
- **AI and LLM Application Pentest.** Claims chatbots and coverage-decision assistants, tested for prompt injection and data leakage as AI adoption accelerates.

Network and infrastructure

- **External Network Pentest.** Public-facing infrastructure: firewalls, DNS, email servers, where an attacker's first attempt lands.
- **Internal Network Pentest.** Active Directory, internal servers, and insider-attack simulation, confirming a breach at the edge does not become a breach of everything.

Enterprise and brand risk

- **Red Team and Digital Risk Assessment.** Subsidiary and affiliate exposure, leaked credentials, and OSINT, for insurers whose security posture depends on dozens of underwriting affiliates and resellers.

"Cobalt has redefined what it means to be a leader in offensive security. While many continuous solutions rely solely on AI and scripts, the human validation provided at Cobalt is the key differentiator."

Jon Cheuvront
Sr. Security Engineer, Gallagher

Talk to Cobalt about your insurance testing program

See how Cobalt maps a testing program to your environment, your subsidiaries, and your NAIC obligations.

cobalt.io/get-started