

MODEL LAW #668 AND UTAH R590-216

Insurance data security requirements and practical safeguards.

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Insurance Summit | Greg Marks

Today's discussion

Real incidents, safeguards and insurance cybersecurity requirements.



Why is insurance a target?

The exposures that attract attackers.



What can we learn? What are the risks?

CNA, Aflac, and the help-desk attack path.



Model Law #668

Insurance Data Security Model Law



So what?

Cybersecurity takeaways

Larson CERTIFIED PUBLIC ACCOUNTANTS



Why insurance is a target

Sensitive data

Identity, financial, health, and claims information.

Money movement

Premiums, payouts, and payment changes.

Connected partners

Agents, MGAs, TPAs, and technology providers.

Larson CERTIFIED PUBLIC ACCOUNTANTS

CNA Financial | March 2021

A fake browser update became a major business disruption.

MARCH 5

Initial access

An employee accepts a fake browser update.

MARCH 5–20

Time inside

Attackers expand access and remain undetected.

MARCH 20–21

Disruption

Ransomware and containment interrupt systems.

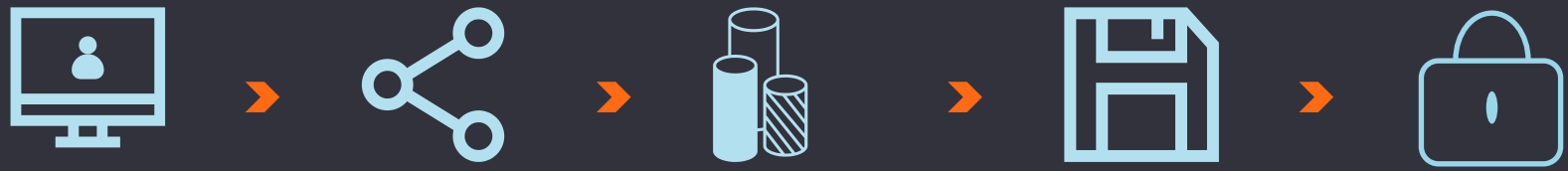
$40 million

Reported ransom payment; not the total incident cost.

Larson CERTIFIED PUBLIC ACCOUNTANTS

Inside the CNA attack

The lesson: safeguards at several stages of an attack.



Entry

Fake browser update

Expanded access

Privileges and network movement

Data theft

Stage and export files via MEGAsync

Disabled defenses

Security tools and some backups

Ransomware

Encryption and disruption

Control connection: risk-based safeguards. Sequence source: CNA notice, reported by BleepingComputer.

Larson CERTIFIED PUBLIC ACCOUNTANTS

How attackers abuse the help desk

Impersonation can undermine a strong authentication system.



Result: the attacker can take over the account.

FBI/CISA document this Scattered Spider method generally; Aflac has not confirmed this exact sequence.

Larson CERTIFIED PUBLIC ACCOUNTANTS

Aflac | June 2025

22.65

million individuals

Personal information involved.

Assess exposure even when operations continue.

"Our systems were not affected by ransomware and remained operational."

Aflac incident update, December 19, 2025. The count is individuals, not records.

AFLAC'S REPORTED RESPONSE

- Contained within hours
- **No ransomware**
- Operations continued

Larson CERTIFIED PUBLIC ACCOUNTANTS

Has Utah adopted Model Law #668?

Yes

No

Not sure

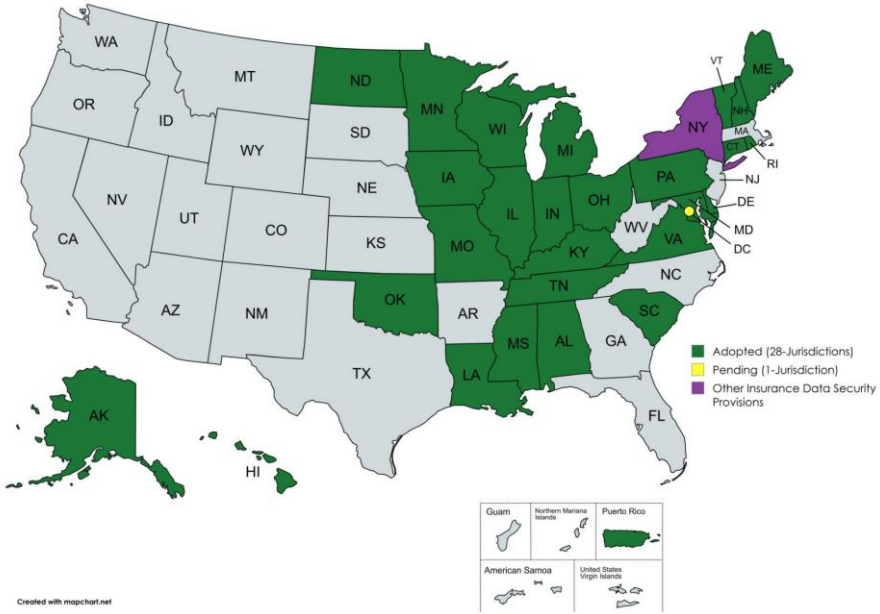
No. Utah's insurance safeguards rule is R590-216.

Sources: NAIC Summer 2026 state chart; Utah R590-216

Larson CERTIFIED PUBLIC ACCOUNTANTS

Model #668 adoption

State adoption continues. Utah has a separate safeguards rule.



Source: NAIC implementation map. State laws and effective dates vary.

28 jurisdictions

27 states + Puerto Rico

UTAH

Utah has not adopted Model #668. R590-216 governs its insurance safeguards program.

NAIC status: October 8, 2026

Larson CERTIFIED PUBLIC ACCOUNTANTS

Model #668 at a glance

The program, the investigation and the notice are the core.

§4

Build it

Information security program

§5

Investigate

Scope, information and restoration

§6

Notify

Commissioner and other affected parties

§§1–3 Purpose and definitions §§7–8 Powers and confidentiality
§§9–13 Exceptions, penalties, rules, severability and effective date

Source: NAIC Model #668 §§1–13

Larson CERTIFIED PUBLIC ACCOUNTANTS

The four terms that matter

Is it a Cybersecurity Event? Vote yes or no on each scenario.

LICENSEE

Licensed, authorized or registered under state insurance law.

NONPUBLIC INFORMATION

Sensitive business information, consumer identifiers and health information.

CYBERSECURITY EVENT

Unauthorized access, disruption or misuse; specified carve-outs apply.

THIRD-PARTY SERVICE PROVIDER

A non-licensee providing services with access to Nonpublic Information.

Source: NAIC Model #668 §3

1. Ransomware locks claims systems. No evidence data left.

   Yes. Disruption is enough.

2. Encrypted laptop stolen. Encryption key remains secure.

   No, if the encryption carve-out applies.

3. Claim file emailed to wrong recipient. Deletion confirmed and documented.

   No, carve out in Model Law 668

Larson CERTIFIED PUBLIC ACCOUNTANTS

Build the program

Model #668 §4A–C

§4A Written and scaled

Administrative, technical and physical safeguards based on risk.

§4B Clear objectives

Protect information and systems. Set retention and destruction rules.

§4C Risk assessment

Name an owner. Assess threats. Test key controls annually.

Assess → Design → Implement → Test → Adjust

Source: NAIC Model #668 §4A–C

Larson CERTIFIED PUBLIC ACCOUNTANTS

The safeguards menu

Determine which are appropriate, then implement them.

- **a** Access controls
- **b** Asset management
- **c** Physical access
- **d** Transit / portable encryption
- **e** Secure development / app testing
- **f** Change management
- **g** Authentication, potentially MFA
- **h** Regular testing and monitoring
- **i** Audit trails
- **j** Fire, water and technology failures
- **k** Secure disposal

Also required: enterprise risk integration, threat awareness and staff training.

How many could you evidence tomorrow? 10–11 / 7–9 / 6 or fewer

Source: NAIC Model #668 §4D

Larson CERTIFIED PUBLIC ACCOUNTANTS

Board and third parties

Oversight continues when responsibilities are delegated.

BOARD, IF ONE EXISTS

Require management to maintain the program.

Receive a written report at least annually.

Oversee delegated responsibilities and reporting.

THIRD-PARTY SERVICE PROVIDERS

Exercise due diligence when selecting providers.

Require appropriate safeguards for accessible information and systems.

Source: NAIC Model #668 §4E–F

Incident response

A written plan for responding to and recovering from cybersecurity events.

1. Internal response process
2. Goals of the incident response plan
3. Roles, responsibilities and decision authority
4. Internal and external communications
5. Remediation of identified weaknesses
6. Documentation and reporting
7. Review and revision after an event

Source: NAIC Model #668 §4H

Larson
CERTIFIED PUBLIC ACCOUNTANTS

The five-year paper trail

Annual certification and event investigations create separate record obligations.

ANNUAL CERTIFICATION

February 15

Domiciled insurers certify §4 compliance.
Keep supporting records for five years.

Document material improvements and remediation.

INVESTIGATION

Prompt investigation

Determine occurrence, scope and affected information.
Restore security; confirm vendor investigation.
Keep event records at least five years.

Source: NAIC Model #668 §4I; §5

Larson CERTIFIED PUBLIC ACCOUNTANTS

The 72-hour clock

Discovery prompts investigation. Determination starts the model's clock.



DISCOVERY

Prompt investigation

DETERMINATION

Clock starts

72 HOURS

Latest notice

Notify when the domicile / home-state trigger applies, OR 250+ residents plus a qualifying notice or material-harm condition.
Provide available notice details and continue updating the Commissioner.

Detected Monday 9 a.m. • Determined Wednesday 10 a.m.
What is the latest model deadline for a qualifying event?

Thu 9 a.m. / Sat 10 a.m. / Fri 5 p.m. / Next business day

Saturday 10 a.m.

Source: NAIC Model #668 §5; §6A–B

Larson CERTIFIED PUBLIC ACCOUNTANTS

Model #668 vs. Utah R590-216

Two distinct frameworks. Both require a written security program.

	NAIC Model #668	Utah R590-216
Legal basis	Model act enacted through state law	Utah rule implementing GLBA
Information	Consumer, health and business information	Nonpublic financial and health customer information
Notice	72-hour model deadline; triggers apply	No incident-notification provision here
Certification	Domiciled insurers, by February 15	No annual certification in this rule

Sources: Model #668 §§3–6; R590-216-2 through -7

Larson CERTIFIED PUBLIC ACCOUNTANTS

Adopted does not mean identical

Keep a state notification matrix beside the common security program.

Feature	The model	State examples / variations
Regulator notice	72 hours	SC 72 hours; MO 4 business days; MN 5 business days; MI 10 business days
Effective dates	§4: one year; §4F: two years	Each state sets its own dates
Exceptions	Small licensees; HIPAA; covered agents	Eligibility and conditions vary

Sources: Model #668; SC §38-99-40; MO §375.1410; MN §60A.9853; MI §500.559

Larson
CERTIFIED PUBLIC ACCOUNTANTS

A Utah carrier's position

A Utah domicile does not settle your obligations in other states.

UTAH STATUS	Utah is not listed as a Model #668 adopting state.
UTAH REQUIREMENTS	Written safeguards program and applicable general breach-notification duties.
MULTI-STATE EXPOSURE	Check each adopting state's scope, exceptions and notification triggers.

Sources: NAIC Summer 2026 state chart; R590-216; Utah Code §13-44-202

Larson CERTIFIED PUBLIC ACCOUNTANTS

If this raised questions

If any of this raised questions for your team, we're glad to help.

We've completed NIST CSF assessments to assess compliance with Model #668, including mappings between the two.

Greg Marks IT Risk Manager • gmarks@larsco.com

Larson CERTIFIED PUBLIC ACCOUNTANTS

Takeaways

1. **Know where the rules apply**
   Map licenses, state deadlines and exceptions. Utah has its own rule.
2. **Maintain safeguards that work**
   Name an owner, assess risks and test key controls annually.
3. **Practice the incident response**
   Assign decisions and notices. The model's 72-hour clock starts at determination.
4. **Oversee providers and the information security program**
   Confirm provider safeguards and notice terms. Report annually to the board, if applicable.
5. **Keep compliance evidence ready**
   Retain required five-year records and support any applicable February 15 certification.

Sources: Model #668 §§4–6; NAIC adoption map; Utah R590-216. State scope and exceptions apply.

Larson
CERTIFIED PUBLIC ACCOUNTANTS

Sources | Incident examples

1. **House Oversight ransomware investigation**
   November 16, 2021
2. **CNA technical incident timeline — BleepingComputer**
   July 22, 2021
3. **Aflac initial incident disclosure**
   June 20, 2025
4. **Aflac incident update**
   December 19, 2025

Source titles are clickable. Full URLs and attribution details are in speaker notes.

Larson CERTIFIED PUBLIC ACCOUNTANTS

Sources | Threats and requirements

5 **FBI/CISA: Scattered Spider advisory**

Updated July 29, 2025

6 **Coalition 2026 Cyber Claims Report announcement**

March 5, 2026 — data covers 2025

7 **NAIC Insurance Data Security Model Law #668**

Model law; check applicable state enactments

Source titles are clickable. Full URLs and attribution details are in speaker notes.

Larson CERTIFIED PUBLIC ACCOUNTANTS

Sources and legal reference guide

NAIC Insurance Data Security Model Law #668

§§3–6 program, investigation and notice; §§7–10 powers and exceptions

Utah R590-216 • Official current rule

Current rule effective June 9, 2023; §§4–5 mandatory, §6 illustrative

Utah general breach-notification statute

Utah Code §13-44-202; separate from the insurance safeguards rule

NAIC Model #673 • GLBA safeguards comparison

Parallel title, purpose and safeguards structure; distinct from #668

Primary sources checked October 20, 2026. Click titles to open.

Larson CERTIFIED PUBLIC ACCOUNTANTS

Sources | Adoption and state variations

NAIC adoption baseline and implementation map

October 2026 brief; October 8, 2026 map; Summer 2026 state chart

State notification deadlines

SC §38-99-40; MN §60A.9853; MI §500.559; MO §375.1410

Historical adoption growth

Faegre Drinker: October 16, 2020 and August 3, 2021

Full URLs, verification dates and qualifications are in speaker notes.

Larson CERTIFIED PUBLIC ACCOUNTANTS