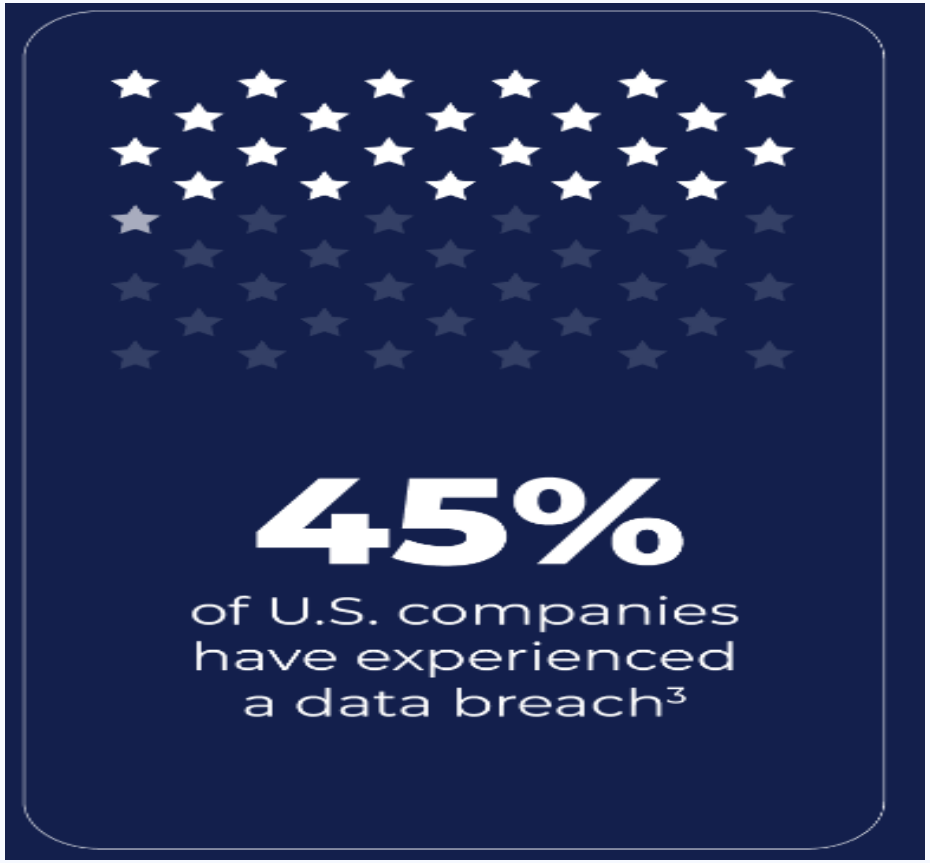
Effective Cybersecurity in the Insurance Industry

Thomas Howell Ferguson P.A.

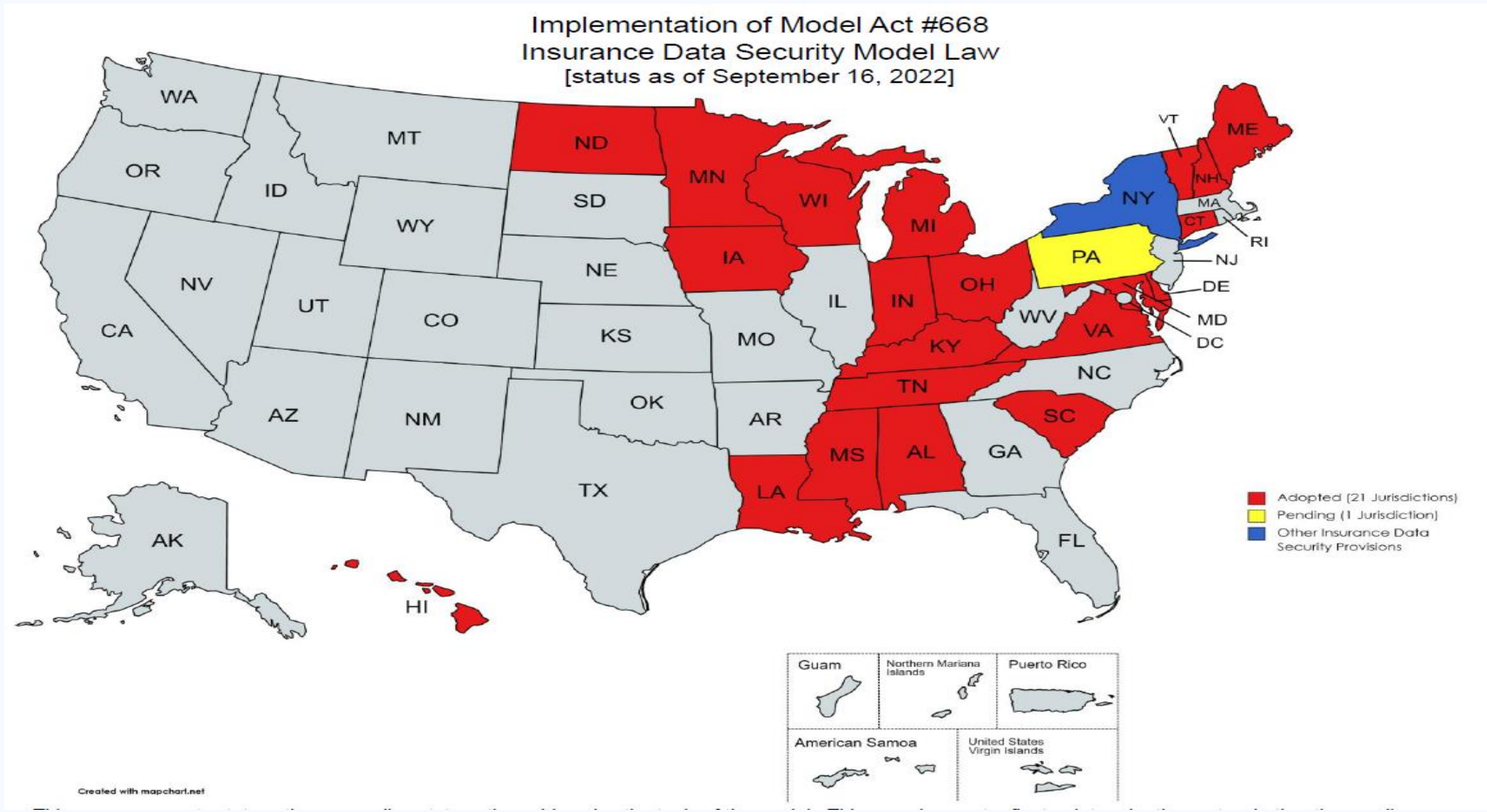
Certified Public Accountants

Interesting Facts



INSURANCE DATA SECURITY MODEL LAW

- Was adopted by the NAIC in October 2017
- The purpose and intent was to establish standards for data security and standards for the investigation of and notification to the State Commissioner of a Cybersecurity Event.


Implementation of Model Act #668
Insurance Data Security Model Law
[status as of September 16, 2022]
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
VT
NH
ME
MA
CT
RI
NJ
DE
MD
DC
AK
HI
Guam
Northern Mariana Islands
Puerto Rico
American Samoa
United States Virgin Islands
Adopted (21 Jurisdictions)
Pending (1 Jurisdiction)
Other Insurance Data Security Provisions
Created with mapchart.net

KEY AREAS OF INSURANCE DATA SECURITY MODEL LAW

- Section 4 Objectives of Security Program
  - Protect the security and confidentiality of nonpublic information and the information system
  - Protect against threats or hazards to security or integrity of nonpublic information and the information system
  - Protect against unauthorized access to nonpublic information
  - Define and periodically reevaluate the retention of nonpublic information and the mechanism for its destruction
  - Develop and perform a Risk Assessment for nonpublic information and information systems
  - Design the information security program to mitigate the identified risks from the risk assessment

KEY AREAS OF INSURANCE DATA SECURITY MODEL LAW

- Section 4 Objectives of Security Program (continued)
  - Oversight by Board of Directors of the information security program
  - Oversight of third-party service provider arrangements
  - Develop and regularly test and update an Incident response Plan
  - Annual Certification to Domiciled State

HOW DO I KNOW IF MY CURRENT POLICY AND PROCEDURES WILL ALIGN WITH THE DATA SECURITY LAW

- Compare your policy and standards against a cybersecurity regulatory guidance.
- This guidance must be flexible, scalable, and practical.
- A nationally recognized framework that embodies those principals is the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

KEY AREAS OF THE NIST CYBERSECURITY FRAMEWORK

DETAIL OF THE FUNCTIONS OF THE CYBERSECURITY FRAMEWORK

- **Identify** - Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect –** Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

DETAIL CATEGORY AREAS OF THE NIST FUNCTIONS

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

HOW TO GET HELP IN EVALUATING THESE CONTROLS

Who is ISACA - Information Systems Audit and Control Association

Provides IT professionals with knowledge, credentials, training and community in IT audit, IT governance, IT risk, and privacy.

What is the CISA designation

Certified Information Systems Auditor

Provides a valid and reliable means for entities to identify technologists who are competent in keeping an entity compliant efficiently and cost effectively.

ISACA has developed a program steps to provide an assessment of the effectiveness of an organization's cyber security identify, protect, detect, respond, and recover processes and activities.

ISACA NIST CYBERSECURITY PROGRAM

Process Sub-Area	Ref. Admin code	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step
Asset Management	ID.AM-1	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	Physical devices and systems within the organization are inventoried.				1. Obtain a copy of physical devices and systems inventory. Review the inventory considering the following: a. Scope of physical devices and systems is based on the organization's risk appetite (e.g., systems that contain sensitive information, allow access to the network, or are critical to business objectives) b. Completeness of inventory (e.g., location, asset number, owner) c. Inventory collection process ensures new devices are collected accurately and in a timely manner (e.g., automated software to detect and/or store the inventory) d. Frequency of inventory reviews
	ID.AM-2		Software platforms and applications within the organization are inventoried.				1. Obtain a copy of software inventory. Review the inventory considering the following: a. Scope of software inventory is based on the organization's risk appetite (e.g., software that processes, stores or accesses sensitive information or is critical to business objectives) b. Completeness of inventory (e.g., version, system, vendor, owner) c. Inventory collection process ensures new software is collected accurately and in a timely manner (e.g., automated software to detect and/or store the inventory) d. Frequency of inventory reviews
	ID.AM-3		Organizational communication and data flows are mapped.				1. Ensure the organization maintains accurate and current copies of data flow diagram(s) (DFD), logical network diagram(s) (LND), and/or other diagrams to show organizational communication and data flow.
							1. If the organization relies on information systems hosted by third parties, obtain a copy of the external systems inventory. Review the third-party inventory considering the following: a. Scope of external systems is based on the organization's risk appetite

WHAT IS YOUR COMPANY'S WEAKEST LINK TO YOUR CYBERSECURITY PROGRAM

It is your employees

We are going to show a video to help emphasis this point

Questions

CONTACT US

Thomas Howell Ferguson P.A. CPAs

Michael Rosciam, CPA.CITP, CISA

Director of IT Assurance,

MLR@thf-cpa.com

Main: 850.668.8100

www.thf.cpa