iapp

# Cybersecurity Regulatory Resilience in an era of AI-driven Cyber Attacks

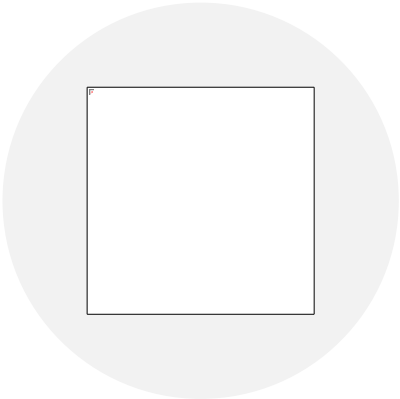
**Thursday, 22 January**
09:00–10:00 PST
12:00–13:00 EST
18:00–19:00 CET

# Panelists

- **Cathy Mulrow-Peattie**, Partner, Privacy, Cybersecurity and AI, Hinshaw & Culbertson
- **Nadia Dombrowski**, Executive Vice President & Chief Legal and Administrative Officer, Pathward
- **Rebecca Hanovice**, Head Privacy Counsel, Mattel, Inc., AIGP, CIPP/E, CIPP/US, CIPM
- **Jennifer Visek**, Managing Director, FTI Consulting

# AI Supercharges Cybersecurity Attacks And More Data to Attack!

NEW ATTACK VECTORS



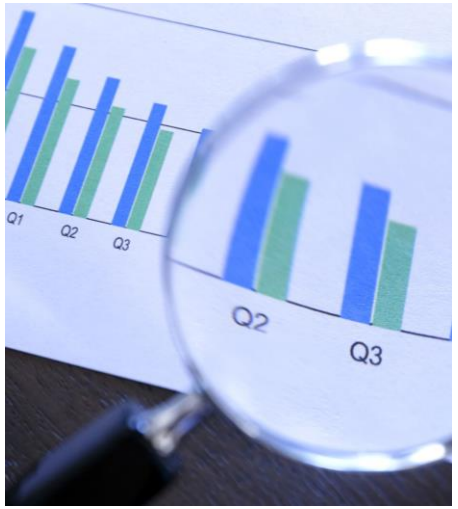
HOW CYBER GOVERNANCE AND COMPLIANCE IS IMPACTED

# Key Learnings from 2025

- The Trump administration is concerned about:
  - Cybersecurity as it relates to personal information attacks on US citizens by foreign threat actors and is concerned that reduced security can lead to more identity theft and fraud. They are also concerned about threats to U.S. business assets and critical infrastructure.
  - Deceptive security promises made to consumers under FTC Act 5.
- State regulators are joining together in increased numbers for cyber compliance and litigation actions. There are 19+ states with reasonable security requirements in privacy laws, more states with security laws, 50 states with data breach reporting laws and a growing consortium of state regulators joining together on concerted actions.
- Increased use of AI by businesses and organizations requires new compliance measures leveraging past practices.

# The CPPA Regulations on Cyber Audits

- Effective January 1, 2026, but beginning in 2027, businesses are required to document the business's plan to address the gaps and weaknesses identified in the audit regarding potential unauthorized activities, including the timeframe in which it will resolve them.
- These audits must be performed by qualified professionals using recognized standards, with an annual certification submitted to the CPPA, and all audit records must be retained for at least five years.
- The audit mandate will be phased in based on company revenue, with the following deadlines:
  - **April 1, 2028:** For businesses exceeding $100 million in 2026 revenue
  - **April 1, 2029:** For businesses with $50 million to $100 million in 2027 revenue
  - **April 1, 2030**: For businesses with less than $50 million in 2028 revenue



# The CPPA Regulation Requires Standard Cyber Practices: Some Key Enforcement Requirements

- End to End Encryption
- MFA Everywhere
- Restricted Account Management and Access Controls
- Secure Configuration of Hardware & Software
- Business Information and PI Inventory
- Limitation & Control of Ports, Services and Protocols
- Oversight of Vendors and Supply Chain
- Employee and Contractor Education and Training
- Incident Response Management and Disaster Recovery Plan

# California's CCPA Regulations on Cyber Audits

- **What are the Critical Terms**? The Cybersecurity Audit Finding must rely on specific evidence and itemize the documents reviewed, sampled, and tested and interviews conducted.
- **The Cybersecurity Audit must assess how security incidents are managed and security incidents are broadly defined!** "Security incident" means an occurrence that actually or imminently jeopardizes the confidentiality, integrity, or availability of the business's information system or the personal information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of the business's cybersecurity program; unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information.
- **Another Key Legal Concerns of this Regulation**?
  - What could be discovered by class action litigators and threat actors and lead to other regulators' subpoenas/inquiries in other states?
    - Businesses are required to identify and describe in detail the status of any gaps or weaknesses of the policies that the auditor deemed to increase the risk of unauthorized access, destruction, use, modification, or disclosure of consumers' personal information; or increase the risk of unauthorized activity resulting in the loss of availability of personal information.
    - Business are required to document their plan to address these gaps.
    - Businesses must submit their certification yearly in writing.

# What's Regulations Should be Onboard: New York State Department of Financial Services Requirements on MFA and Data Inventories

- Two additional NYSDFS Part 500 obligations went into effect on November 1, 2025.
  - **500.12 Multi-factor authentication.** Multi-factor authentication shall be utilized for any individual accessing any information systems of a covered entity.
  - **500.13 Asset management and data retention requirements.** As part of its cybersecurity program, each covered entity shall implement written policies and procedures designed to produce and maintain a complete, accurate and documented asset inventory of the covered entity's information systems. The asset inventory shall be maintained in accordance with written policies and procedures. At a minimum, such policies and procedures shall include: (1) a method to track key information for each asset, including, as applicable, the following: (i) owner; (ii) location; (iii) classification or sensitivity; (iv) support expiration date; and (v) recovery time objectives; and (2) the frequency required to update and validate the covered entity's asset inventory.

# Reaching Compliance with the NYS DFS Guidance on Mitigating Cyber Risk of 3rd Party Service Providers

- NYS DFS issued Guidance on 10/21/25 on Supply Chain Cybersecurity Risk
  - DFS has emphasized the need for robust contractual provisions with third party providers and risk management policies and procedures tailored to your data, information systems and risk, with the appropriate oversight by your organizations senior executive team.
  - DFS emphasized critical due diligence provisions, including understanding who are the downstream service providers and what are their cyber security controls.
  - Critical to many companies, following in line with other federal and state regulators, NYSDFS stated that if your business outsources your IT solutions, that your business's legal compliance obligations under Part 500 cannot be delegated.

# Add in the Cyber Risks in Using AI– What does Cyber Resilience Look Like?

Before security departments dive deep into AI they need to make sure that they have a solid foundation—with risk assessments, contractual procurement terms and cybersecurity reviews.

Understand what cybersecurity threats supply chain vendors are facing and how they are protecting themselves from such threats, and how if those protections fail the how you will be impacted.  Require key cyber safeguards such as access controls, encryption, monitoring, training, MFA and breach notification requirements.

Regulators will expect that businesses assess their service providers based on the risk they present and the adequacy of their safeguards.

# Best Practices for the Department of Justices' Bulk Data Law

The DOJ's Bulk Data Law went into effect on October 6, 2025.

This is a National Security law where, the U.S. federal government is restricting access to certain Bulk Sensitive Data of U.S. citizens from foreign adversaries in China, Russia, Cuba, Venezuela, Iran and North Korea. The term foreign adversaries includes vendors and investments owned by persons from these countries.

The data involved includes biometric, human omic, health, financial, certain identification data and geolocation data, as well as data linked to current or former U.S. government employees or contractors in certain bulk level quantities.

What is a covered data transaction? A covered data transaction is any transaction that involves access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data and that involves: (1) data brokerage; (2) a vendor agreement; (3) an employment agreement; or (4) an investment agreement.

# Enforcement Actions: Federal Trade Commission Go Daddy Settlement Order 2025

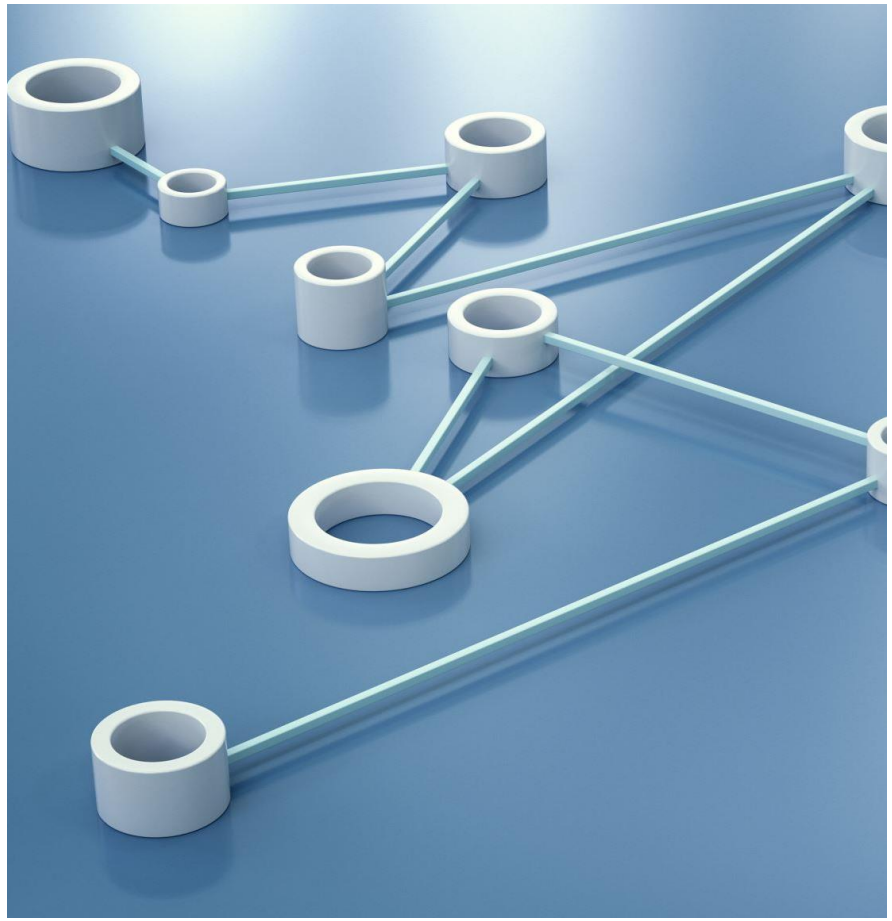
- FTC alleged that since 2018, GoDaddy failed to implement reasonable and appropriate security measures to protect and monitor its website-hosting environments for security threats, and misled customers about the extent of its data security protections on its website hosting services.

As part of the Settlement Go Daddy, in addition to 20 years of compliance monitoring, Go Daddy is required to do the following.

- Implement and maintain centralized system component inventories, including of hardware, software, and firmware elements, that track the out-of-date and vulnerable versions of each managed software program, operating system file, and firmware that is installed on any tracked asset, and create an alert for each asset that is using an out-of-date or vulnerable version.
- Select and retain service providers capable of safeguarding Hosting Services and Information they access through or receive from Go Daddy and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Hosting Services.

# FTC Enforcement Letters regarding Cyber Threats in 2025: Actions to comply with Global Law could Reduce Security from What is Promised is to Consumer Maybe A Violation of FTC Act 5

- Federal Trade Commission Chairman Andrew N. Ferguson issued letters to several tech, data security, services, cloud computing, and app companies about reducing security controls, such as end-to-end encryption, in response to regulatory demands of foreign powers, which could lead to "an increased risk of identity theft and fraud or U.S. citizens."
- Ferguson stated that "companies that promise that their service is secure or encrypted, but fail to use end-to-end encryption where appropriate, might deceive consumers who reasonably expect that level of confidentiality. Further, certain circumstances may require reasonable security measures such as end-to-end encryption, and the failure to implement such measures might constitute an unfair practice."



HINSHAW

# FTC Case Against Nomad in December 2025 –Meet Your Security Promises

- The FTC alleged that Nomad touted its security in its advertising, claiming that it offered "security-first" services. The FTC, however, alleged that the company failed to live up to these promises by failing to: use secure coding practices; implement processes for receiving and addressing vulnerability reports and responding to security incidents; and utilize known technologies that might have helped mitigate consumer losses.
- The FTC settled with Nomad in December 2025 under the proposed settlement, Nomad will:
  - Implement a comprehensive information security program that is designed to protect consumers from theft or other unauthorized access and address the security issues outlined in the FTC's complaint;
  - Obtain biennial assessments for a period of 10 years of its information security program by an independent third party and cooperate with the third-party assessor.

# State Enforcement Continues: New York State AG Rides the Wave of Enforcement for Data Breach Lack of Reasonable Security

NYS Attorney General Letitia James on 10/14/25 secured a $14.5 M settlement from 8 car insurance companies relating to their data breaches.

Hackers stole driver license information and used it to submit unemployment claims.

The companies were sanctioned for not having reasonable security measures in place like MFA, data inventories,& adequate threat response systems.

# How to Prepare & What's Next?



# Web Conference
# Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

**Click here: https://iappwf.questionpro.com/t/AbBPvZ7pN6**

**Thank you in advance!**

For more information: www.iapp.org

## Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the original broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

## Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact: livewebconteam@iapp.org

# Thank you

## Cybersecurity Regulatory Resilience

Cathy Mulrow-Peattie

212.655.3875 | cmulrow@hinshawlaw.com

HINSHAW