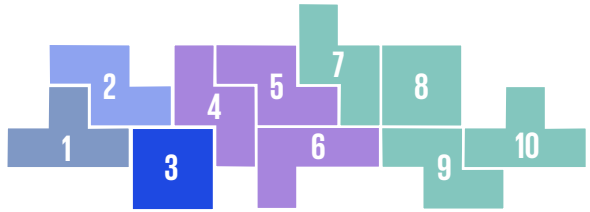
03 Maintaining Cyber & Data Security



Regulatory Signals

- Federal Rationalization
- State Complexity & Divergence
- Data Privacy
- Adaptive Frameworks

Increasingly sophisticated threats to data require organizations and governments to employ advanced technology, adaptive strategies, and skilled professionals to protect critical data and operations.

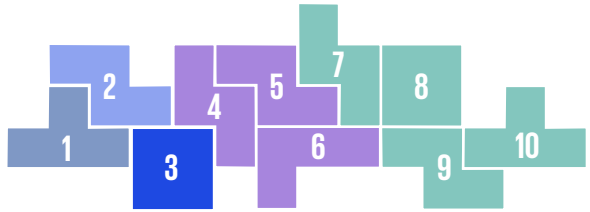
"As we emerge from the era of exploding AI adoption, privacy will be the true differentiating measure of innovation. Leaders' success won't be based on how much data they gather, but how wisely and respectfully they steward the information they were entrusted."

Orson Lucas
Partner
Advisory

"Joining the Cyber Risk Institute's Innovator Program signifies our shared commitment to advancing cyber risk assessment in the financial sector. Through collaboration and supporting industry adoption of the CRI Profile, we aim to enhance the precision and effectiveness of cyber risk assessments, empowering financial institutions to navigate the evolving cyber landscape with confidence."

Matt Miller
Principal
Advisory

03 Maintaining Cyber & Data Security



Regulatory Signals

- **Federal Rationalization**
- State Complexity & Divergence
- Data Privacy
- Adaptive Frameworks

Signal

Expressed need for interagency harmonization to align regulatory expectations, reduce overlap, and streamline reporting requirements, including:

- Establishment of single point of cyber coordination.
- Reauthorization of CISA 2015 and funding of CISA to further its role in information/threat sharing.

Information sharing between industry and government is declining due to staffing and funding reductions, and termination of advisory boards.

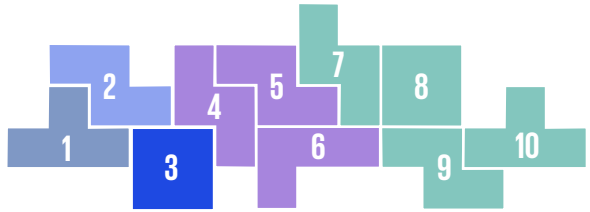
Examples

- Alignment of federal cyber efforts (e.g., support for “clean” reauthorization of CISA 2015, ONCD Statement (Cairncross))
- Industry recommendations to “enhance ONCD authority” and “restore CISA capabilities” (e.g., US CSC 2025 Annual Report)
- Formation of industry coalitions to establish standards (e.g., CRI membership and its Financial Services Cyber Security Profile)

What to Watch

- Release of National Cyber Strategy and “follow-on” action items; anticipated to increase cross-sector agency harmonization
- Potential reauthorization of CISA 2015 and funding for CISA
- Execution of action items in EO 14239, including:
  - Clarification of state role
  - Implementation of a risk-based approach incorporated into the National Resiliency Strategy, National Critical Infrastructure Policy, National Risk Register
- Potential updates to rulemakings (e.g., CISA cyber incident reporting rule, reconsideration of SEC cybersecurity disclosure rule)
- Adoption of the CRI Financial Services Cyber Security Profile and associated Maturity Model

03 Maintaining Cyber & Data Security



Regulatory Signals

- Federal Rationalization
- **State Complexity & Divergence**
- Data Privacy
- Adaptive Frameworks

Signal

Executive directives (e.g., EO 14239, EO 14306) prescribe a more active role in infrastructure resilience and preparedness to the states, resulting in an increase in state legislative activity directed to critical infrastructure and consumers of digital services connected to critical infrastructure.

Examples

More than 800 cybersecurity bills introduced across 49 states in 2025 with at least 200 bills enacted in 44 states[2]. Focus areas include:

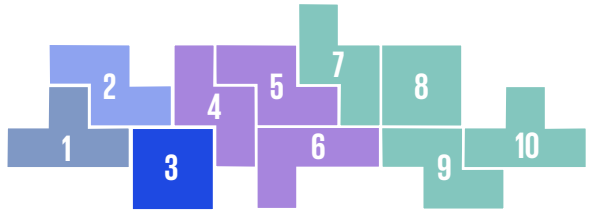
- Agency leadership structures for cyber coordination
- Technical safeguards and best practices
- Compliance and reporting requirements
- Incident response plans

What to Watch

- Continuing legislative and regulatory activity to strengthen state and local cybersecurity protection related to critical infrastructure and social media; focus areas to include detection, reporting, risk assessment, TPRM, and privacy
- Increasing fragmentation and federal-state and state-state divergence
- Potential skills-based workforce constraints
- Potential rulemaking or policy guidance to clarify federal vs. state cybersecurity roles

[1]Derived from NCSL.org

03 Maintaining Cyber & Data Security



Regulatory Signals

- Federal Rationalization
- State Complexity & Divergence
- **Data Privacy**
- Adaptive Frameworks

Signal

Continued focus at the federal level on national security, sensitive data (e.g., biometric, geolocation), and deepfakes, with a lessened focus on broader consumer protections.

Expansion of state laws and regulations, often in combination with cyber and AI laws, including ongoing attention to children's privacy and the definition of sensitive data.

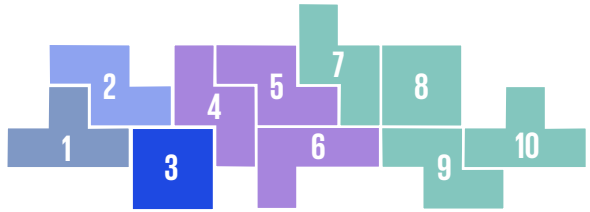
Examples

- Restrictions on transfer of sensitive data to select countries (e.g., DOJ bulk sensitive data rule, FCC connected vehicles and subsea cables ownership proposals)
- Development of frameworks to export full-stack AI technology packages (e.g., DOC RFI implementing EO 14320)
- Strengthened protections for children, including "personal data" (e.g., biometric data), data retention and deletion, and parental consent (e.g., FTC COPPA rule, multiple state laws)

What to Watch

- Forthcoming reconsideration of CFPB Personal Financial Data Rights Rule (Section 1033); potential ongoing legal challenges
- Potential rulemakings related to cross-border data sharing/technology sales
- Increasing compliance challenges, federal-state-global (e.g., India DPDPA, EU-US DPF)
- Strengthened protections for children's data, sometimes coupled with AI laws and regulations (e.g., verifiable parental consent, unsolicited direct messaging) and expansion of age thresholds (e.g., ages 13-17) with enhanced verification systems
- Ongoing state level enforcement of privacy protections (e.g., CA CCPA actions re: policy disclosure, opt-out rights, data sales)

03 Maintaining Cyber & Data Security



Regulatory Signals

- Federal Rationalization
- State Complexity & Divergence
- Data Privacy
- **Adaptive Frameworks**

Signal

Development and application of new approaches to cybersecurity and digital infrastructure, secure software/cloud service providers, and innovative technologies.

Examples

- Federal contracting requirements to protect sensitive unclassified information, including in supply chains (e.g., DOD CMMC Final Rule)
- Updated standards and security protocols (e.g., NIST Cybersecurity Framework and related guidance)
- Enhanced TPRM expectations to include fourth parties, specific contract requirements, continuous monitoring of vendor security risks, and threat information sharing with critical vendors

What to Watch

Expectations for enhanced approaches to cybersecurity and data protection, including:

- Prioritization of data governance, including protections for customer data, models and algorithms, data sharing and protocols for collection, retention, deletion, and archiving
- Governance frameworks designed to be scalable, integrated across the business, informed by lessons learned, and supported by workforce training and development
- Application of new tools (e.g., Security-By-Design principles, AI threat detection systems, quantum-safe encryption)
- Potential increases in regulatory requirements with penalties for noncompliance (e.g., federal, state, global)

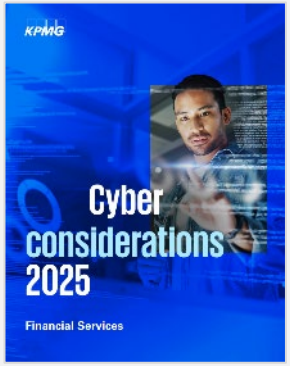
03 Maintaining Cyber & Data Security

Regulatory Signals

- Federal Rationalization
- State Complexity & Divergence
- Data Privacy
- Adaptive Frameworks

Relevant Thought Leadership

The Importance of an Integrated Approach to Data Privacy Regulations in Cybersecurity



Cybersecurity considerations 2025: Financial services sector

Top Related Regulatory Challenges

02 Adopting Disruptive Tech & AI

05 Averting Fraud & Scams

06 Protecting Fairness

07 Ensuring Resiliency

10 Enhancing Parties & Workforce