

How does mandating cyberattack data sharing among states alter the governance of systemic risk and redefine accountability structures in national cybersecurity defense?

September 14, 2026 | SnugLab Research

Executive Summary

Mandating cyberattack data sharing among states primarily alters systemic risk governance by consolidating national threat visibility under federal agencies like CISA, aiming to identify cross-sector vulnerabilities that individual states cannot manage alone [3, 7]. However, this centralization is significantly counterbalanced by a fragmentation of governance and compliance, as state and local entities face duplicative reporting burdens from numerous federal, state, and sector-specific mandates [8]. Accountability structures are redefined by establishing a federal baseline for incident reporting and national standard-setting [6, 7], yet this often shifts accountability toward localized procedural compliance rather than effective prevention, potentially degrading a jurisdiction's capacity to contain multi-jurisdictional attacks due to premature declarations and data noise [2, 8]. The evidence suggests that while visibility is enhanced, the practical efficacy of these mandates as direct preventive tools is limited, often functioning more as retrospective accountability or resilience mechanisms [2]. A key unresolved uncertainty remains the full operational impact of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), as its mandatory reporting obligations have not yet taken effect [1, 5].

Key Findings

Systemic Risk Governance: Centralized Visibility vs. Fragmented Compliance

Systemic risk governance operationally requires both centralized threat aggregation and decentralized state-level adaptive capabilities to prevent cascading failures [9]. Federal mandates like the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) aim to centralize threat aggregation by requiring critical infrastructure entities to report incidents to CISA, thereby building a coordinated national picture of cross-sector vulnerabilities [7]. This "whole-of-nation" approach seeks to move national defense from ad hoc sharing to

an integrated network capable of identifying cross-sector vulnerabilities that individual states cannot manage alone [3].

However, this centralization of visibility is counterbalanced by significant fragmentation in governance and compliance. The current regulatory environment includes over 54 different federal cyber incident reporting regimes alongside countless state and local requirements, leading to overlapping and duplicative mandates [8]. CISA acknowledges that CIRCIA's requirements are often "different from, or more stringent than" most existing regulations [7]. This structural tension results in a net consolidation of systemic risk *visibility* but a net fragmentation of *governance and compliance*, as state and local entities must navigate concurrent obligations without adequate harmonization [8].

Decentralized state-level adaptive responses are operationalized through collaborative defense networks that integrate state fusion centers alongside federal agencies to analyze threat intelligence and coordinate localized defensive actions [3]. Examples include NYC Cyber Command, which reduced average incident response times from hours to minutes within its first year, processing 90 billion events weekly [4]. New York State has adopted a similar shared responsibility model, and fusion centers in New Jersey and Texas demonstrate coordination with state energy stakeholders [4, 13]. Despite these localized successes, the overall fragmented regulatory landscape diverts scarce resources from operational defense to administrative paperwork [8].

Redefining Accountability: National Standards and Local Burdens

Mandating cyberattack data sharing redefines accountability by establishing a new federal baseline for incident reporting and national standard-setting [7, 11]. CIRCIA, for instance, mandates a 72-hour reporting window for covered cyber incidents and a 24-hour window for ransomware payments, creating a federal floor for reporting and oversight [6, 7]. This aims to ensure critical infrastructure operators are accountable to a national standard of resilience and provides a mechanism for federal threat intelligence to support local entities [3].

However, this shift toward national standard-setting is often accompanied by an increased localized compliance burden. The proliferation of concurrent federal, sector-specific, and state mandates means accountability becomes tied to correctly filing multiple reports rather than securing systems against cascading failures [2, 8]. A 2026 quantitative study examining state-level cybersecurity legislation from 2017 through 2024 found that information sharing as a legislative feature was positively associated with

reported economic losses, suggesting these mandates function more effectively as retrospective accountability or resilience mechanisms rather than direct preventive risk mitigators [2]. This indicates that accountability is redefined around procedural compliance, which can divert scarce resources from operational defense to administrative paperwork and legal risk management [8].

Impact on Incident Containment and Data Quality

The accountability shift toward procedural compliance, particularly rigid reporting deadlines, degrades a jurisdiction's capacity to contain multi-jurisdictional attacks. This occurs by forcing premature incident declarations that generate low-fidelity data, thereby obscuring accurate situational awareness and diverting critical resources [14, 15, 16, 17, 18, 19]. Security professionals anticipate that the 72-hour clock for reporting under CIRCIA will begin when an organization "reasonably believes" a covered incident occurred, rather than after forensics are complete [9, 10]. This "fog of war" problem means organizations cannot wait for complete data before notifying CISA, potentially diverting crucial staff and resources away from active containment efforts [12]. This redefines accountability structures toward rapid information collection over comprehensive accuracy, requiring entities to balance immediate regulatory compliance with operational response priorities [5, 8, 9, 10].

Private Sector Transparency and Litigation Fears

Mandatory cross-state data sharing centralizes threat visibility, but litigation fears and weak privilege protections create governance costs that undermine private-sector transparency. Private entities are frequently hesitant to share cyber incident information due to fears of liability, reputational damage, and regulatory scrutiny [3, 8, 11]. While CIRCIA includes a "no cause of action" clause that limits the federal government's use of reported information for state or local enforcement, it does not explicitly preserve legal privileges like attorney-client privilege or trade secret protection for mandatory reports [11]. This represents a critical departure from the 2015 Cybersecurity Information Sharing Act, which explicitly stated that voluntary sharing would not waive these privileges [11].

Furthermore, CISA retains the authority to disclose information obtained through subpoenas to the Justice Department for enforcement or criminal prosecution, meaning trade secrets and privileged communications remain exposed to federal subpoena authority [11]. As the Department of Treasury reinforced, it "may impose civil penalties for

sanctions violations based on strict liability" [11]. This tension means the systemic benefit of accelerated threat diffusion is partially offset by governance costs, as the very transparency required for centralized visibility may be reduced because entities fear that sharing data will expose them to litigation and regulatory enforcement rather than simply aiding national defense [3, 11]. The SEC's rule, effective December 2023, also mandates public companies disclose material cybersecurity incidents within four business days, adding to this complex landscape [8].

Historical Efficacy of Reporting Mandates

The historical track record of pre-CIRCIAs sector-specific and state-level reporting mandates reveals a significant gap between their theoretical promise and their actual capacity to interrupt cascading cyber failures. A 2026 quantitative study examining state-level cybersecurity legislation from 2017 through 2024 found that features such as mandatory frameworks, enforcement actions, and information sharing did not significantly reduce the ratio of cyberattack victims to establishments [2]. The study discovered that information sharing was positively associated with reported economic losses, suggesting these early legislative features functioned more effectively as retrospective accountability or resilience mechanisms rather than direct preventive risk mitigators [2]. These early frameworks largely created a compliance burden that redefined accountability around correctly filing multiple reports rather than securing systems against cascading failures [2, 8].

Current Status and Operational Gaps of CIRCIAs

As of September 14, 2026, the CIRCIAs final rule remains pending, and the mandatory reporting obligations have not yet taken effect for covered entities [1, 5]. Therefore, there are no specific post-2023 critical infrastructure incidents under CIRCIAs that demonstrate how the 72-hour reporting deadline forced a premature incident declaration that degraded situational awareness during active containment. While the law aims to enhance national cybersecurity defense by fostering a coordinated approach to understanding cyber incidents across critical infrastructure sectors [7], its real-world operational impact on systemic risk governance and accountability structures is yet to be fully observed.

Implications

Mandating cyberattack data sharing among states creates a dual impact on national

cybersecurity defense. It centralizes the *visibility* of systemic risks, enabling federal agencies to develop a more comprehensive national intelligence picture and coordinate responses across critical infrastructure sectors. This shifts accountability towards a federal baseline and national standard-setting, which could theoretically improve overall resilience. However, the current implementation also implies a significant *fragmentation of compliance* and an increased *localized burden* on state and local entities due to overlapping and unharmonized reporting requirements. This can divert resources from active defense to administrative tasks and may lead to a focus on procedural compliance over actual incident containment. Furthermore, the lack of explicit legal privilege protections in mandatory reporting regimes may reduce private-sector transparency, creating a trade-off where the desire for accelerated threat diffusion is undermined by fears of litigation and regulatory scrutiny. The full operational implications of these shifts will become clearer once CIRCIA's mandatory reporting obligations take effect.

Limitations and Caveats

The research provides limited direct quantitative data on the actual containment success rates of specific state-level cross-state data sharing mandates compared to federal CISA deadlines [2]. Furthermore, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) final rule remains pending, and its mandatory reporting obligations have not yet taken effect [1, 5]. Consequently, real-world operational data on how CIRCIA's deadlines impact situational awareness during active containment is not yet available. The research also lacks specific data comparing the cost of compliance with new mandates to the average financial loss per breach for small-to-mid-sized enterprises (SMEs) or determining if the reporting burden disproportionately affects resource-constrained jurisdictions. No specific private-sector litigation cases between 2025 and 2026 resulting in significant damages due to shared mandate data were identified. Additionally, the top three sectors with the highest 'data noise' ratios or specific legislative exemptions for trade secrets from the 2017-2024 data analysis were not identified.

Sources

[1] Cyber Incident Reporting Critical Infrastructure Act 2022 Ci - cisa.gov -

<https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>

[2] [edu] Viewcontent.Cgi - digitalcommons.liberty.edu -

<https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=9789&context=doctoral>

[3] Toward Collaborative Cyber Defense And Enhanced Threat Intel - belfercenter.org -

<https://www.belfercenter.org/publication/toward-collaborative-cyber-defense-and-enhanced-threat-intelligence-structure>

[4] [blog] Shared Responsibility Model For Cybersecurity - aspendigital.org - <https://www.aspendigital.org/blog/shared-responsibility-model-for-cybersecurity/>

[5] How Climate Risks Are Reshaping Systemic Risk Governance - cetex.org - <https://cetex.org/news/how-climate-risks-are-reshaping-systemic-risk-governance/>

[6] IIF Responds US CISA Request For Information On Cyber Incident - iif.com - <https://www.iif.com/Publications/ID/5148/IIF-responds--US-CISA-request-for-information-on-Cyber-Incident-Reporting>

[7] Cyber Incident Reporting - pwc.com - <https://www.pwc.com/us/en/services/consulting/cybersecurity-data-tech-risk/library/cyber-incident-reporting.html>

[8] The Shifting Nature Of Cyber Incident Regulatory Reporting - globalinvestigationsreview.com - <https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/fourth-edition/article/the-shifting-nature-of-cyber-incident-regulatory-reporting-obligations-in-the-united-states>

[9] Redefining Systemic Cybersecurity Risk In Interconnected Env - acijournal.com - <https://www.acijournal.com/Redefining-Systemic-Cybersecurity-Risk-in-Interconnected-Environments,192119,0,2.html>

[10] [gov] Of Contagion Index - financialresearch.gov - <https://www.financialresearch.gov/bank-systemic-risk-monitor/ofr-contagion-index/>

[11] Cyber Reporting Proposals Assessing Liability Protections - lawfaremedia.org - <https://www.lawfaremedia.org/article/cyber-reporting-proposals-assessing-liability-protections-and-legal-privileges>

[12] [gov] DHS Congressional Report Harmonization Of Cyber Incident Reporting - dhs.gov - <https://www.dhs.gov/sites/default/files/2023-09/DHS%20Congressional%20Report%20-%20Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf>

[13] [gov] Cybersecurity Risk Management Strategy Governance And Incident Disclosure - federalregister.gov - <https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure>

[14] [peer-reviewed] Strengthening Health Security at Ground Border Crossings - Authors: Diana G Sami; Sungsoo Chun - Journal: Healthcare - <https://pmc.ncbi.nlm.nih.gov/articles/PMC11476094/>

[15] [gov] Chapter 5: Management of State Response and ... - <https://www.aspr.gov/readiness-response/healthcare-readiness/performance-measures-guidance-reports/mfcc/chapter-5-management-state-response-coordination>

[16] [gov] Crisis Response and Disaster Resilience 2030 - https://www.fema.gov/sites/default/files/2020-09/fema_crisis_response_disaster_resilience_2030_progress_report_2010_2011_insights_strategic_foresight_initiative_01-13-2012.pdf

[17] Recommendations to Promote Alignment and ... - <https://www.fsb.org/2024/12/recommendations-to-promote-alignment-and-interoperability-across-data-frameworks-related-to-cross-border-payments-final-report/>

[18] Cross-border payments in 2026: Friction and reform - <https://thepaymentsassociation.org/article/cross-border-payments-2026-friction-reform/>

[19] No 167 Cross-border payment technologies: innovations ... - <https://www.bis.org/publications/paper-167-cross-border-payment-technologies-innovations-and-challenges.pdf>