How would a federal ban on ransomware payments reshape the accountability structures of critical infrastructure operators and alter the power dynamics between state actors and cybercriminal syndicates?

May 16, 2026 | SnugLab Research | readme.snuglab.com

Executive Summary

A federal ban on ransomware payments would moderately reshape the accountability structures of critical infrastructure operators by compelling more resilient entities to invest in robust cybersecurity, while simultaneously risking operational bankruptcies for under-resourced organizations lacking mature backup systems. The ban would alter power dynamics by theoretically disrupting cybercriminal syndicates' financial incentives, but evidence suggests it could also drive payments underground, reducing law enforcement's intelligence visibility and potentially empowering hostile nation-states to shift towards harder-to-attribute disruptive attacks. The primary unresolved uncertainty is whether critical infrastructure operators can achieve sufficient cyber resilience before a ban is implemented, and what specific government support mechanisms would be in place to prevent widespread operational collapse.

Key Findings

Reshaping Accountability: Compelling Resilience vs. Concentrating Risk

A federal ban on ransomware payments would compel cybersecurity investments for critical infrastructure operators with sufficient resources, but risks bankrupting underprepared entities [9, 14, 15]. Proponents argue that removing the payment option eliminates a "moral hazard," forcing organizations to prioritize proactive defense, incident response, and secure backup strategies [4, 5, 6, 10, 11, 14]. This shift would align accountability with genuine risk mitigation, compelling operators to ensure system functionality without attacker cooperation [4, 5, 6].

However, critics, including former acting National Cyber Director Kemba Walden and the Institute for Security and Technology's Ransomware Task Force, argue that an

immediate ban is premature due to the current lack of cybersecurity resilience among many critical infrastructure operators [7, 9, 14]. For under-resourced entities, such as rural hospitals, severing the short-term mitigation pathway of ransom payments could lead to bankruptcy or a fatal dependency on government recovery support [9, 14, 15]. Three-quarters of businesses already view a ransomware attack as an existential threat [15]. State-level bans in North Carolina and Florida have not clearly demonstrated a reduction in attack rates, suggesting that bans alone do not successfully drive proactive defense investments or deter attackers without foundational resilience [7, 12, 15].

Regulatory mechanisms, such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), already mandate reporting cyber incidents within 72 hours and ransomware payments within 24 hours, increasing transparency [3, 5, 8, 14, 16]. A federal ban would intensify regulatory scrutiny, potentially imposing strict liability under the Office of Foreign Assets Control (OFAC) for unintentional payments to sanctioned entities [8, 10, 11]. This could reshape executive accountability, potentially making senior management personally liable for compliance failures, similar to models like the EU's Digital Operational Resilience Act [8].

Altering Power Dynamics: Disrupting Criminals vs. Empowering Nation-States

A federal ban could theoretically disrupt the financial incentives of cybercriminal syndicates by collapsing ransomware-as-a-service (RaaS) markets, but it carries significant risks of unintended strategic shifts [5, 6, 13, 14, 15]. By removing a primary revenue stream, a ban aims to diminish the profitability of financially motivated cybercriminals [5, 6, 13, 14, 15]. Victims paid a record $1.1 billion to cybercriminal groups in 2023, with approximately 75% of incidents yielding over $1 million .

However, cybercriminal syndicates are highly agile and may adapt by shifting targets to countries without bans or evolving their business models to pure data exfiltration and extortion without encryption [13, 15]. State-level bans have not clearly reduced overall attack rates, indicating that localized restrictions may not deter global actors [7, 12, 15].

A substantial risk exists that eliminating financial extortion would inadvertently empower hostile nation-states, such as Russia, China, Iran, and North Korea, to alter their tactics [5, 13, 15]. These states often use ransomware gangs to fund operations or exploit organizations [5, 6, 13]. If financially motivated attacks diminish, state-sponsored attacks aimed purely at causing disruption, chaos, and paralysis of critical infrastructure could

become more prominent [5, 13, 15].

Impact on Law Enforcement Intelligence Visibility

Mandating a payment ban would likely degrade state actors' ability to track and dismantle ransomware networks by reducing law enforcement intelligence visibility [6, 7, 14]. Penalizing payments would disincentivize organizations from reporting incidents, driving ransom transactions underground and "reducing crucial visibility needed for investigations and disruption efforts" [6, 7, 14]. This loss of transparency hinders intelligence gathering, making it harder to identify, attribute, and sanction new or rebranded criminal groups aligned with hostile states [2, 6, 8].

Previous payment restrictions and sanctions have demonstrated how illicit transactions are driven to underground channels. For example, OFAC sanctioned Blender.io in May 2022 after it facilitated over $500 million in Bitcoin laundering [1, 10, 17]. Following the August 2022 OFAC sanctions on Tornado Cash, daily transactions plummeted by up to 97% [18]. However, illicit actors adapted by migrating to Layer 2 networks and using cross-chain bridges and decentralized exchanges (DEXs) to obscure transaction origins, significantly degrading investigative visibility [18, 20]. The TRM Labs 2026 Crypto Crime Report found that illicit crypto volume reached an all-time high of $158 billion in 2025, driven by a shift toward stablecoins and higher-risk services as enforcement tightened [19].

Enforcement Challenges and Legislative Frameworks

U.S. regulators face significant challenges in enforcing a nationwide payment ban without triggering widespread operational bankruptcies, as the strict liability framework conflicts with continuity-of-operations mandates [9, 14, 15]. Many critical infrastructure organizations, particularly under-resourced entities, lack mature backup systems and sufficient cybersecurity resilience to recover data without paying a ransom [9, 14, 15]. The strict liability standards enforced by OFAC, which impose civil penalties even for unintentional payments to sanctioned entities, exacerbate this conflict [8, 10, 11].

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) defines critical infrastructure across 16 sectors, including energy, water, healthcare, transportation, finance, and telecommunications [3, 16]. Drafting precise exemptions or grandfathering clauses for a ban is complex, as it would force the government to decide which companies are permitted to survive an attack, potentially requiring official approval

of payments to criminals [6, 7, 15]. Ohio's law, for instance, prohibits payments unless formally approved by legislative authority, highlighting the complexity of such exemptions [11, 12].

Cyber insurance policies are already shifting to exclude reimbursement for payments to sanctioned entities and focus more on recovery costs rather than ransom payouts [12, 13, 15]. A ban would accelerate this market adjustment, forcing operators to reallocate capital toward resilience [12, 13, 15].

Implications

A federal ban on ransomware payments would have several key implications for critical infrastructure operators and the dynamics between state actors and cybercriminal syndicates. For operators, accountability would shift from managing the risk of payment to ensuring robust cyber resilience and recovery capabilities. Those with mature systems would be compelled to further invest in defenses, while under-resourced entities would face heightened operational risk, potentially leading to bankruptcy or increased reliance on government recovery support. This could create a two-tiered system of resilience within critical infrastructure.

For state actors, the power dynamic with cybercriminal syndicates would become more complex. While a ban aims to starve criminals of revenue, it risks driving payments underground, thereby reducing law enforcement's intelligence visibility into attack patterns and threat actor tactics. This loss of transparency could hinder attribution and disruption efforts. Furthermore, the ban could inadvertently push hostile nation-states to prioritize disruptive, non-financially motivated attacks, which are harder to attribute and sanction, thereby altering the nature of the cyber threat landscape. The success of a ban would heavily depend on the government's ability to provide robust, scalable incident response and data recovery assistance, as well as enhanced international cooperation to track illicit funds and disrupt criminal networks.

Limitations and Caveats

The findings draw from a mix of expert opinions, reports, and analyses, and the topic involves predictions about policy outcomes, leading to moderate confidence in definitive conclusions. Direct quantitative data on the long-term impact of federal ransomware payment bans on U.S. critical infrastructure is limited, as no such ban currently exists.

Analogous evidence from state-level bans provides some context but may not fully scale to a national level due to differences in scope and enforcement. Specific budget allocations and staffing levels for federal agencies like CISA and the FBI dedicated to emergency incident response and data recovery for critical infrastructure were not available in the provided research, limiting the assessment of their capacity to support operators unable to pay ransoms. The agility of cybercriminal syndicates and nation-states in adapting to new restrictions also introduces inherent uncertainty into long-term predictions.

Sources

[1] [gov] Products - gao.gov - https://www.gao.gov/products/gao-24-106221

[2] [gov] Crs External Products - congress.gov - https://www.congress.gov/crs_external_products/R/PDF/R46932/R46932.3.pdf

[3] 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

[4] Download - shsu-ir.tdl.org - https://shsu-ir.tdl.org/bitstreams/bb09bfda-6340-43b4-bb84-90e61801056c/download

[5] The Path To Banning Ransomware Payments - centerforcybersecuritypolicy.org - https://www.centerforcybersecuritypolicy.org/insights-and-research/the-path-to-banning-ransomware-payments

[6] What To Do About Ransomware Payments - atlanticcouncil.org - https://www.atlanticcouncil.org/blogs/econographics/what-to-do-about-ransomware-payments/

[7] Ransom Payment Ban Pushback - cybersecuritydive.com - https://www.cybersecuritydive.com/news/ransom-payment-ban-pushback/713206/

[8] Ransomware What You Need To Know - skadden.com - https://www.skadden.com/insights/publications/2026/01/ransomware-what-you-need-to-know

[9] Ban On Ransom Payments Needs More Work Walden Tells Hill - meritalk.com - https://www.meritalk.com/articles/ban-on-ransom-payments-needs-more-work-walden-tells-hill/

[10] Legal Implications Of Ransomware Payments - sentreesystems.com - https://sentreesystems.com/legal-implications-of-ransomware-payments/

[11] Ransomware And Public Entities To Pay Or Not To Pay - greatamericaninsurancegroup.com - https://www.greatamericaninsurancegroup.com/content-hub/loss-control/details/ransomware-and-public-entities-to-pay-or-not-to-pay

[12] Should State Governments Ban Ransomware Payments - govtech.com - https://www.govtech.com/security/should-state-governments-ban-ransomware-payments

[13] Ransomware Payment Prohibitions Do They Work And Will More S - aon.com - https://www.aon.com/risk-services/professional-services/ransomware-payment-prohibitions-do-they-work-and-will-more-states-adopt-them

[14] Federal Ban Ransom Payments - ibm.com - https://www.ibm.com/think/news/federal-ban-ransom-payments

[15] Ransomware Payment Ban Case - techmonitor.ai - https://www.techmonitor.ai/cybersecurity/ransomware-payment-ban-case/

[16] Federal Cyber Mandates Affect Critical Infrastructure Report - mybendersolutions.com - https://mybendersolutions.com/federal-cyber-mandates-affect-critical-infrastructure-reporting/

[17] [gov] Press Releases - home.treasury.gov - https://home.treasury.gov/news/press-releases/jy0768

[18] [edu] Crypto Privacy After Sanctions The Return Of Coin Mixers - jbs.cam.ac.uk - https://www.jbs.cam.ac.uk/2026/crypto-privacy-after-sanctions-the-return-of-coin-mixers/

[19] 2026 Crypto Crime Report - trmlabs.com - https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

[20] [gov] National Security Advisory Open Source Reporting On Risks - banking.senate.gov - https://www.banking.senate.gov/imo/media/doc/national_security_advisory_-_open-source_reporting_on_risks_posed_by_digital_assets.pdf