Emerging Realities for State Government Cybersecurity

Ransomware, Fraud, and Data Breaches with **Financial Impact**

ResilientTech Advisors

May 2025

High-Impact Cyber Incidents (2012–2024)

This table captures high-impact cyber incidents across U.S. state and local governments. All involved either ransom payments, operational shutdowns, or significant recovery costs.

You'll notice repeat patterns in attacker behavior-particularly in under-resourced environments like localities, shared services, or education sectors.

Year	State/Local Entity	Incident Description	Financial Impact
2024	Fort Bend County, Texas	Cyberattack on library system.	$2.6 million in recovery expenses.
2024	Jackson County, Georgia	Cybercriminals demanded ransom after ransomware infection; full shutdown required.	$400,000 ransom demanded; significant recovery costs incurred.
2024	Texas: 22 local government entities	Coordinated ransomware attack on 22 entities; disrupted various services.	Undisclosed ransom; significant operational challenges.
2023	North Carolina State Agencies	31 agencies impacted.	$2 million+ stolen; $958,000 due to cyber-related fraud.
2023	Virginia Commonwealth University Health	Phishing attack led to a data breach involving over 4,000 patient records.	Regulatory penalties likely; reputational damage
2021	Virginia Legislature (DLAS)	Ransomware attack disrupted bill drafting systems ahead of the General Assembly session.	Operational disruption; exact cost undisclosed.
2019	Baltimore, Maryland	RobbinHood ransomware attack disrupted city services for months.	$18 million in recovery costs.
2019	Riviera Beach, Florida	Ransomware attack led to payment of ransom to restore systems.	$600,000 ransom paid.
2019	Jackson County, Georgia	Ransomware attack resulted in payment to regain system access.	$400,000 ransom paid.
2019	New Orleans, Louisiana	Ransomware forced shutdown of city systems; extensive recovery needed.	$7 million in recovery costs.
2018	Atlanta, Georgia	SamSam ransomware attack affected multiple municipal services.	$2.7 million initially spent; total recovery estimated at $9.5 million.
2018	Colorado Dept. of Transportation	SamSam ransomware attack shut down 2,000+ systems; recovery through internal IT efforts.	Estimated recovery cost exceeded $1 million.
2012	South Carolina Dept. of Revenue	Data breach exposed millions of tax records; state provided identity protection services.	$12 million spent on identity theft protection.

Sources: StateScoop, AP News, BleepingComputer, HIPAA Journal, OCR Breach Portal, ABC11, Houston Chronicle, WTOP, FOIA Disclosures, AASA Bulletins

What the Data Tells Us

1. Repeat ransomware strains (e.g., SamSam) highlight persistent vulnerabilities.

2. Paying ransom doesn’t reduce total cost - recovery often exceeds ransom amount.

3. State and local agencies are frequent targets due to decentralized security.