The AI Risk Report for State and Municipal Governments

July 2026

Executive Summary

Artificial intelligence is rapidly reshaping the cyber threat landscape confronting state and municipal governments. Current evidence indicates that artificial intelligence is acting primarily as a force multiplier, accelerating the scale, speed, and effectiveness of existing threat vectors rather than creating entirely new categories of cyber risk.

For government organizations, this evolution creates a fundamental shift in cyber risk. Historically, cybersecurity programs concentrated on preventing system compromise, protecting sensitive information, and maintaining operational systems. Those objectives remain critical, but artificial intelligence is expanding the potential consequences of cyber incidents beyond technology disruption alone.

Key areas increasingly affected by artificial intelligence include:

Disruption of citizen-facing services

Political influence and activist-driven cyber operations

Third-party and vendor concentration risk

Critical infrastructure targeting

Identity compromise of government employees and officials

Public trust attacks involving misinformation, impersonation, and synthetic media

The central question for executive leadership is no longer whether artificial intelligence introduces new risks. The question is whether existing governance, resilience, and cybersecurity assumptions remain valid when adversaries can simultaneously target employees, citizens, service providers, and infrastructure through increasingly automated techniques.

Strategic Shift: From System Protection to Institutional Resilience

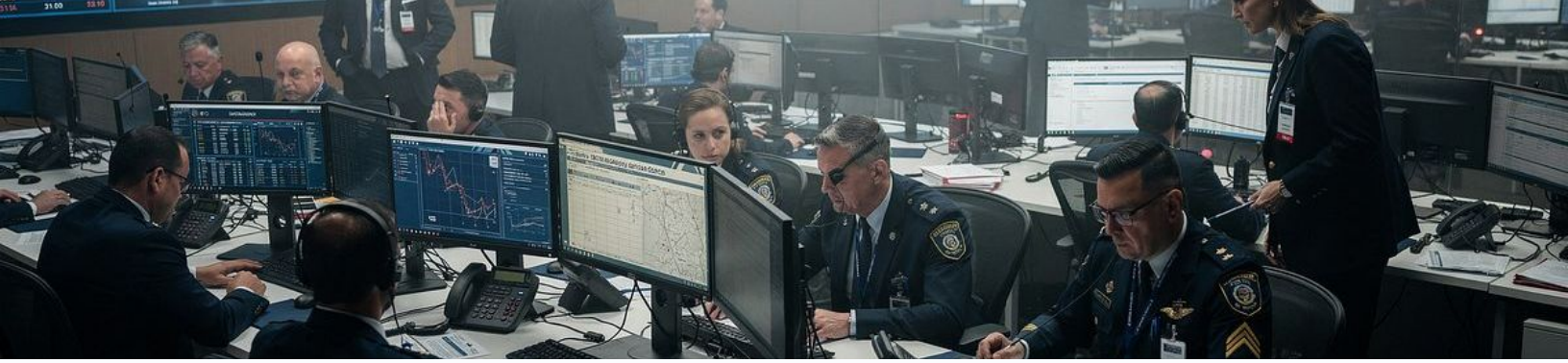
State and municipal governments occupy a unique position within society. They operate citizen services, administer benefits, manage courts, oversee utilities, support public safety, and maintain critical infrastructure. Disruption to these functions affects public welfare, economic activity, and confidence in government institutions.

Artificial intelligence increases the likelihood that a single attack campaign can be executed simultaneously against multiple jurisdictions, creating a shift from isolated incidents toward systemic disruption.

Government resilience will increasingly be measured by an organization's ability to:

- **Sustain services during prolonged disruption**
- **Preserve public confidence during information attacks**
- **Manage dependencies on shared vendors and technology providers**
- **Protect trusted identities and executive decision-making processes**
- **Maintain continuity of critical infrastructure operations**

This represents a strategic evolution from traditional cybersecurity toward enterprise-wide resilience.



Emerging Risk Area One: Service Continuity at Scale

State and local governments rely on citizen-facing platforms that support licensing, permitting, public safety, courts, tax administration, utility services, benefits delivery, and emergency management. These services continue to be high-value targets for threat actors.

Artificial intelligence allows adversaries to conduct reconnaissance, generate phishing content, customize social engineering attacks, and automate targeting at a level that was previously cost-prohibitive. As a result, the most likely outcome of many future attacks may not be data theft but simultaneous disruption of government operations across multiple jurisdictions.

For executive leadership, the challenge therefore becomes continuity rather than recovery alone.

Government organizations should be able to answer the following questions:

1. **Which services are truly mission essential?**
2. **How long can critical services remain unavailable before significant public impact occurs?**
3. **What manual alternatives exist when digital services become unavailable?**
4. **How can services continue during a large-scale identity compromise event?**

Emerging Risk Area Two: The Weaponization of Public Trust

Public trust represents one of the most important assets of state and municipal government.

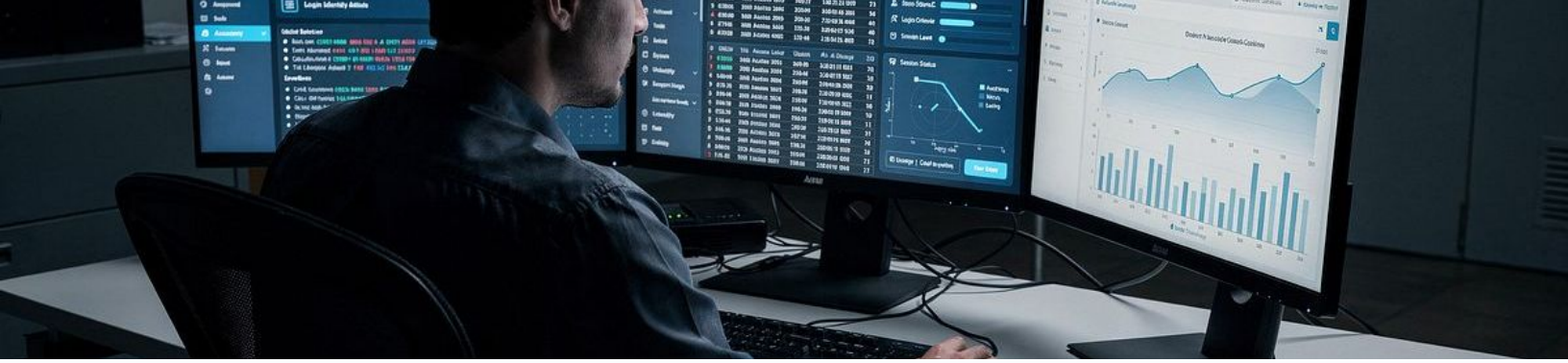
Government agencies serve as authoritative sources of information during emergencies, public health incidents, elections, infrastructure disruptions, and other significant public events. Artificial intelligence introduces growing challenges to that trust relationship.

Advances in synthetic content generation, voice replication, video manipulation, and automated influence operations are lowering the barriers to creating convincing fraudulent communications. Government organizations increasingly face risks associated with fabricated notices, fraudulent advisories, impersonation campaigns, and manipulated public messaging.

Future attacks may involve:

- **Fraudulent emergency notifications**
- **Fabricated public statements**
- **Counterfeit agency communications**
- **Synthetic audio or video impersonating public officials**
- **Coordinated misinformation campaigns**
- **Manipulated narratives designed to undermine confidence in government**

The challenge is no longer limited to protecting access to government websites and systems. Increasingly, the challenge is protecting the authenticity and credibility of government information.



Emerging Risk Area Three: Identity as the New Security Perimeter

Identity security is becoming one of the most significant strategic issues confronting government cybersecurity programs.

Common areas of concern include privileged account exposure, identity management weaknesses, monitoring gaps, session management deficiencies, and access control risks.

Artificial intelligence is accelerating a shift from infrastructure-focused attacks toward attacks targeting trusted individuals. Public officials, system administrators, emergency managers, and executive leadership are increasingly attractive targets because critical decisions depend on trusted identities.

Potential threat scenarios include:

- **Executive impersonation**
- **Fraudulent authorization requests**
- **Manipulated approval workflows**
- **Credential compromise**
- **Synthetic communications from trusted leaders**
- **Deepfake-enabled social engineering**

Identity assurance, executive verification procedures, and privileged access governance should therefore be viewed as critical components of institutional resilience.

Emerging Risk Area Four: Accelerated Exploitation Cycles

Artificial intelligence is compressing the timeline between vulnerability discovery and exploitation.

State and municipal governments continue to face challenges associated with:

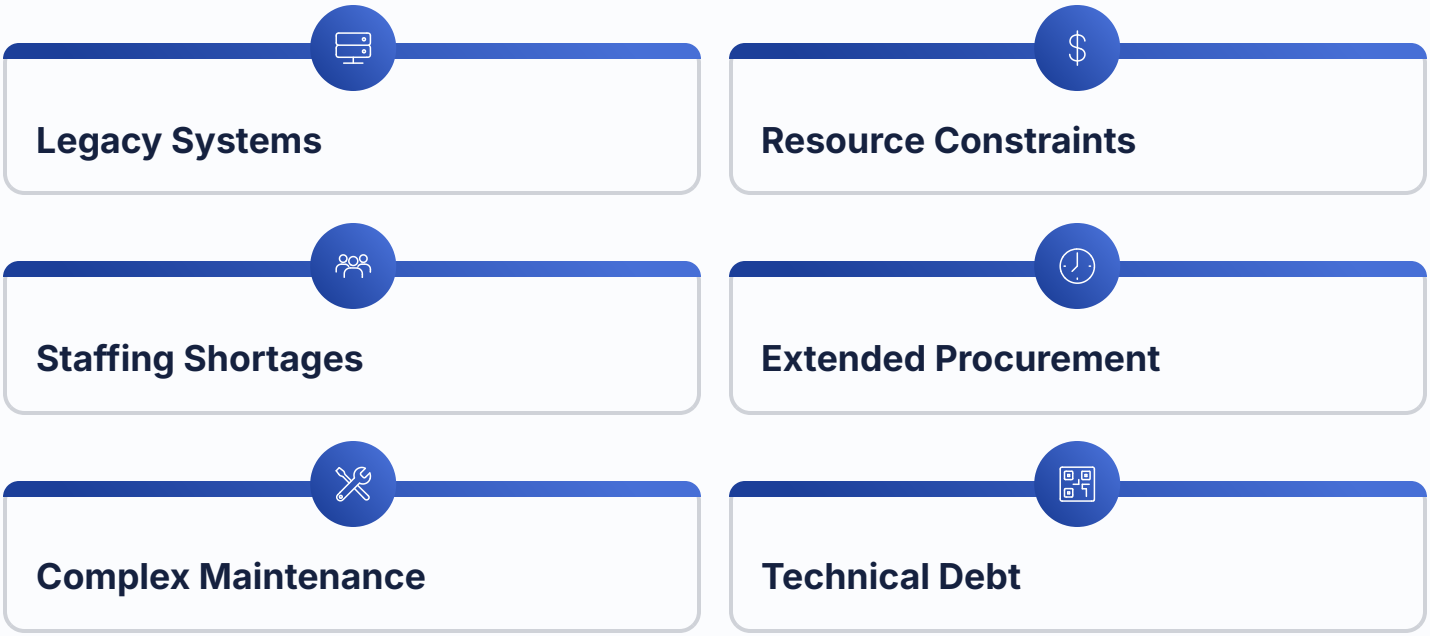
- Legacy systems
- Resource constraints
- Staffing shortages
- Extended procurement timelines
- Complex maintenance requirements
- Technical debt

> Technical debt refers to the accumulated cost — in complexity, fragility, and security risk — of deferred technology upgrades, outdated systems, and shortcuts taken in place of proper long-term solutions.

These conditions create an environment in which threat actors may increasingly gain an advantage through automation and artificial intelligence-assisted exploitation.

Exposure management, continuous monitoring, asset visibility, and risk-based prioritization are becoming increasingly important components of cybersecurity strategy.

The ability to continuously identify and manage exposure may become as important as the ability to patch systems.



Emerging Risk Area Five: Critical Infrastructure and Operational Technology

The convergence of artificial intelligence and critical infrastructure security represents one of the most significant long-term concerns for government organizations.

Water systems, wastewater operations, energy infrastructure, industrial control environments, and other operational technology assets remain persistent areas of concern. Recurring challenges include segmentation deficiencies, remote-access exposure, infrastructure visibility gaps, and utility-related risks.

Artificial intelligence is expected to improve adversaries' ability to:

- **Identify exposed operational technology assets**
- **Map infrastructure dependencies**
- **Discover weak remote-access pathways**
- **Correlate vulnerabilities across systems**
- **Automate attack planning**
- **Target critical services at greater scale**

For government leaders, this represents more than a cybersecurity issue. Disruption of critical infrastructure can affect public health, economic activity, emergency response, and public confidence simultaneously.

Forecast Outlook: Artificial Intelligence as an Accelerator of Existing Government Risk

Based on recent state and municipal government cyber risk assessments, the outlook for artificial intelligence is best characterized as **acceleration rather than transformation**.

Artificial intelligence does not currently constitute a new standalone category of cyber risk. Instead, it is making existing threats materialize faster, more frequently, and at greater scale. Artificial intelligence is amplifying existing vulnerabilities, increasing attack efficiency, and expanding the reach of threat actors across interconnected government ecosystems.

The strategic implication for government leaders is straightforward: the most likely near-term impact of artificial intelligence will not be the emergence of entirely new attack methodologies. Rather, existing threats will materialize faster, spread further, and generate broader operational consequences.

AI Acts as a Force Multiplier

Existing threats are amplified, not replaced

Faster Materialization

Threats emerge more quickly than before

Greater Frequency

Attacks occur more often across more targets

Broader Scale

Impact spreads further across interconnected government ecosystems

Wider Operational Consequences

Downstream effects grow more severe

Thirty-Day Outlook: Artificial Intelligence Becomes a Force Multiplier

The next thirty days represent the highest-confidence forecasting horizon because the underlying attack patterns are already observable.

Current indicators point to elevated risks associated with ransomware, espionage, hacktivist activity, and third-party compromise. Supply-chain and vendor ecosystems represent some of the most significant near-term exposure pathways.

Municipal and state assessments indicate that artificial intelligence-enhanced phishing and accelerated vulnerability weaponization are increasing the effectiveness of existing attack paths rather than creating entirely new threats.

Immediate priorities include:

Citizen-service survivability

Vendor visibility and dependency management

Public portal resilience

Water and wastewater preparedness

Identity protection and verification

Most Likely Artificial Intelligence-Enabled Activity

1. Artificial intelligence-generated phishing targeting government employees
2. Artificial intelligence-assisted reconnaissance of state and municipal vendors
3. Artificial intelligence-enhanced exploitation of newly disclosed vulnerabilities
4. Artificial intelligence-generated social engineering targeting citizen-service operations
5. Increased hacktivist messaging and disruption campaigns targeting public-facing portals

Executive Question: Which shared vendor, cloud provider, software-as-a-service platform, or managed service would create the greatest operational disruption if compromised tomorrow?

Sixty-Day Outlook: Scale and Automation Become More Visible

By the sixty-day horizon, the operational impact of artificial intelligence is expected to become increasingly evident.

Threat actors are expected to leverage automation more extensively across cloud environments, collaboration platforms, software supply chains, and shared technology ecosystems.

At this stage, artificial intelligence increasingly supports attacker workflow automation, including reconnaissance, vulnerability correlation, attack-path identification, and the scaling of operations across multiple targets.

Most Likely Artificial Intelligence-Enabled Activity

1. More sophisticated deepfake and impersonation campaigns
2. Artificial intelligence-assisted vulnerability chaining against internet-facing systems
3. Artificial intelligence-supported targeting of shared government software platforms
4. Automated harvesting of citizen and government data repositories
5. Increased use of artificial intelligence within denial-of-service and public-service disruption operations

Concentration risk remains a dominant concern because commonly deployed communications, network-edge, identity, and information technology management platforms create opportunities for a single vulnerability to affect multiple jurisdictions simultaneously.

> **Executive Question:** Are we prepared for a single vendor compromise affecting multiple jurisdictions simultaneously?

The likelihood of this scenario appears greater than the emergence of a completely novel artificial intelligence-specific attack category.

Ninety-Day Outlook: Trust, Identity, and Infrastructure Become Primary Concerns

By the ninety-day horizon, the overall threat landscape remains remarkably consistent.

Ransomware, espionage, hacktivism, third-party compromise, and operational technology exposure continue to represent the most significant sources of government cyber risk. Artificial intelligence continues to amplify these risks rather than replace them.

Most Likely Artificial Intelligence-Enabled Activity

1. Deepfake-assisted executive impersonation
2. Artificial intelligence-driven misinformation and public-trust attacks
3. Artificial intelligence-enhanced attacks against municipal portals and citizen-service platforms
4. Artificial intelligence-assisted discovery of operational technology weaknesses
5. Increased targeting of water and wastewater environments
6. Greater automation of ransomware and extortion operations

The primary focus at this horizon shifts toward trust, identity, public communications, critical infrastructure resilience, and citizen-service continuity.

> **Executive Question:** How would our organization verify the authenticity of a critical executive communication during a cyber incident involving synthetic voice, video, or messaging content?

As artificial intelligence capabilities mature, trust validation may become as important as traditional cybersecurity controls.

Executive Forecast Summary

Time Horizon	Most Likely Direction of Artificial Intelligence Risk
Next 30 Days	Accelerated phishing, social engineering, vendor targeting, and vulnerability exploitation
Next 60 Days	Increased automation across vendors, cloud environments, citizen-service platforms, and shared government software ecosystems
Next 90 Days	Increased targeting of trust, identity, public communications, critical infrastructure, and operational technology environments

Bottom Line

The most probable artificial intelligence-related risk facing state and municipal governments over the next ninety days is **not autonomous artificial intelligence attacks against government infrastructure**.

The most probable outcomes are:

1. Artificial intelligence-assisted phishing and impersonation
2. Artificial intelligence-assisted exploitation of known vulnerabilities
3. Artificial intelligence-amplified vendor and supply-chain compromise
4. Artificial intelligence-enhanced hacktivist and public-disruption activity
5. Artificial intelligence-supported attacks targeting water, wastewater, and other critical public services

The dominant theme emerging across state and municipal government assessments is that **artificial intelligence is turning government cyber risk into a scale problem.**

Threat actors can now target more jurisdictions, more employees, more vendors, and more citizen-facing systems simultaneously, increasing the likelihood of service disruption, infrastructure impacts, and erosion of public trust.

Governance Considerations for Executive Leadership

Boards, executive leadership teams, chief information officers, and chief information security officers should reconsider several assumptions that have historically shaped cybersecurity strategy.

Service Continuity

- Which government services are truly mission essential?
- How long can those services remain unavailable before public impact becomes unacceptable?
- What manual alternatives exist for critical operations?

Public Trust

- How is public trust measured and protected during a cyber crisis?
- How would officials communicate if primary communications channels were compromised?
- How would the organization validate the authenticity of public messaging?

Identity Resilience

- Are identity-verification controls sufficient for executive decision-making?
- Can high-risk approvals be independently verified?
- Are executive impersonation scenarios incorporated into incident response planning?

Third-Party Risk

- What single dependency presents the greatest concentration risk?
- How many essential services depend upon the same vendor ecosystem?
- Are contingency plans in place for critical provider failures?

Critical Infrastructure

- How resilient are operational technology and critical infrastructure environments?
- Are water, wastewater, energy, and public-safety systems appropriately segmented?
- How quickly can essential infrastructure operations continue under degraded conditions?

Conclusion

Artificial intelligence is not fundamentally changing what threat actors seek to accomplish. It is fundamentally changing the speed, scale, and efficiency with which they pursue those objectives.

For state and municipal governments, the defining challenge of the next phase of cybersecurity will not simply be defending information systems. It will be maintaining citizen trust, sustaining critical services, protecting critical infrastructure, and ensuring resilience across increasingly interconnected government ecosystems.

Organizations that recognize artificial intelligence as an amplifier of existing weaknesses—and adapt governance, resilience, and cybersecurity strategies accordingly—will be best positioned to navigate the evolving public-sector threat landscape.

Contact **Charlene@CyberRiskModels.com** to discuss this and other critical risk concerns.