WHITE PAPER

Why State and Local Governments Need a Whole-of-State Cybersecurity Approach

Introduction

Cyberattacks are no longer isolated incidents targeting large corporations—they are systemic threats impacting state and local governments with alarming frequency. From ransomware shutting down county courthouses to hackers compromising personal information of citizens, the stakes for state and local government entities could not be higher.

In 2023, the FBI highlighted government entities as the third most-targeted sector by ransomware attacks, after critical manufacturing and healthcare centers. The average ransom for government organizations was over $1 million. The ever-expanding, complex attack surface, combined with limited budgets and fragmented IT infrastructures, has left many state and local governments ill-equipped to respond effectively.

This is why a **whole-of-state cybersecurity approach** is no longer optional—it's essential. By fostering collaboration, standardizing solutions, and enabling shared resources, governments can better protect sensitive data, increase efficiency, and cultivate trust within their communities.

State and Local Government Cybersecurity Challenges

State and local governments face a host of challenges in managing cybersecurity. Here are a few key pain points:

- **Limited Resources:** Smaller municipalities and local agencies frequently lack the budget and staffing resources to maintain strong cybersecurity defenses, leaving them highly vulnerable.
- **Fragmented Strategies:** Siloed approaches to cybersecurity mean inconsistent protections and gaps in IT systems across different levels of government.
- **Growing Risk Exposure:** From ransomware to data breaches, cyber risks are becoming more sophisticated and widespread, impacting essential public services and citizen safety.

These challenges necessitate a shift from isolated strategies to a cohesive, integrated model that provides robust protections for all layers of government.

How a Whole-of-State Approach Can Help

A whole-of-state cybersecurity approach fosters collaboration across state, local, tribal, and territorial governments, creating shared resources and strategies to counter modern cyber threats. This model enables government entities to tackle challenges that are impossible to address individually. Here's how it delivers value:

1 Improved Collaboration and Information Sharing

By enabling unified efforts, governments can pool their threat intelligence, share lessons learned, and coordinate real-time responses to emerging threats. For example:

- **Rapid Incident Response:** A coordinated system allows for faster containment of threats, minimizing damage.
- **Shared Best Practices:** Local governments, especially underfunded ones, gain access to expertise and methodologies otherwise unavailable to them.

2 Enhanced Budget and Resource Optimization

Centralized efforts reduce redundancies and optimize spending:

- By leveraging shared tools and software, governments can achieve cost savings.
- Centralized management minimizes overhead and streamlines operations.
- Resources can be allocated more effectively, focusing on the highest-priority threats.

3 Streamlined Compliance and Governance

A unified approach ensures consistent governance standards, simplifying audits and supporting regulatory compliance. For example:

- Laws, policies, and frameworks are uniformly implemented.
- Regulatory assessments are streamlined, reducing administrative burden for individual units.

4 Scalable Implementation

This approach allows for scalable security measures that adapt to the evolving threat landscape:

- New tools and policies can be rolled out across multiple entities, from small-town agencies to state-wide operations.
- Security updates and incident response measures can be applied simultaneously across jurisdictions.

Recommendations for Adopting a Whole-of-State Cybersecurity Strategy

To effectively implement a whole-of-state approach, governments should focus on these key components:

1 Policy, Funding & Support

- Secure universal buy-in from stakeholders and adequate funding to support initial and ongoing efforts.

2 Information Sharing

- Foster collaboration between jurisdictions to standardize best practices and expedite incident responses.

3 Incident Response

- Develop a coordinated plan for responding to threats and managing security incidents across all levels.

4 Workforce Development

- Equip IT teams with tools to reduce manual effort and enable automation.

5 Standardized Tools

- Unified, standardized tools ensure consistent protection across all entities.

6 Governance & Validation

- Regular audits and evaluations ensure the approach remains effective and evolves with emerging threats.

Armis is uniquely positioned to support governments across all these areas, guiding them from planning through execution and beyond.

Why Armis Is the Ideal Whole-of-State Partner

Armis stands out as a trusted solution for governments implementing whole-of-state cybersecurity strategies. Armis, the cyber exposure management & security company, sees, protects and manages all physical and virtual assets - from the ground to the cloud - ensuring the entire attack surface is both defended and managed in real time.

Here's how Armis addresses the key needs for whole-of-state cybersecurity strategies:

1 Unmatched Asset Visibility

Armis offers complete, real-time visibility into every device connected to a network—whether managed or unmanaged. This level of insight ensures that no threats slip through the cracks and enables proactive risk mitigation.

2 Enhanced Threat Detection

With advanced anomaly detection, Armis identifies unusual traffic and suspicious behavior, helping governments stay ahead of cyber threats before they escalate.

3 Centralized Management

Empower you whole-of-state approach with intuitive interface and advanced analytics. Armis Centrix™ empowers state and local governments to efficiently gain deep situational awareness and track and manage their assets across diverse environments, ensuring optimal utilization and cost-effectiveness.

4 Asset Intelligence

AI-powered knowledge base, monitoring billions of assets world-wide in order to identify cyber risk patterns and behaviors for state and local governments.

5 Streamlined Collaboration

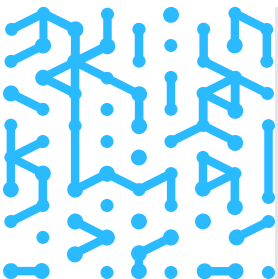
By acting as a unified platform, Armis enables seamless information sharing across state and local governments. This ensures real-time collaboration and resource allocation during critical incidents.

6 Vulnerability Prioritization and Remediation

With high volumes of assets scattered across state and local infrastructure, governments need an end-to-end solution that introduces unparalleled advancements by going beyond vulnerability management to find and consolidate security findings across all sources to holistically understand risk and automate prioritization.

7 Early Warning Detection

For state and local governments, data breach incidents can be extremely costly. Armis Centrix™ for Early Warning provides insights into the vulnerabilities that threat actors are exploiting in the wild or are about to weaponize, allowing organizations to understand their impact and take preemptive action.



8 Scalability and Adaptability

Armis supports organizations of all sizes, making it an effective solution for large-scale state operations with diverse needs. It offers customizable settings catered to the unique requirements of individual entities while maintaining consistency and alignment across the board.

9 Proven Expertise

Armis has a track record of helping state and local governments securely manage their digital landscapes. Its proactive defense strategy ensures better outcomes for communities and citizens.

With Armis, governments don't just protect their assets—they elevate their entire cybersecurity posture.

Case Study Highlight

City of Las Vegas

With a vast IT and OT environment, the city of Las Vegas uses Armis as a core component of its cybersecurity strategy to gain a better understanding of its many IoT assets and their potential vulnerabilities. The Armis platform's Cyber Asset Attack Surface Management (CAASM) capabilities have resolved the security concerns the city previously had about its white-labeled devices, BYOD, and unused assets sitting on the network.

"*Armis helps us to not only understand our environment and our assets, but also to prioritize how we go about using the vital resources we have. If assets aren't being utilized, we can remove those assets from our environment.*"

Building a Secure Future Together

The stakes for state and local governments have never been higher, but the path forward is clear. A whole-of-state cybersecurity approach addresses today's challenges head-on, equipping governments with the tools and strategies they need their citizens.

Armis is here to help you take the first step. **Speak to an Armis expert today** to understand how we can help your organization create a safer, more interconnected cybersecurity environment—one that benefits all levels of government and the communities they serve.

Contact us to learn more and get started on building a comprehensive whole-of-state strategy.