A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER

DIGITAL STATES

How Public Sector Leaders Are Reframing Government Cyber Strategy

SPONSORED BY

ARMIS

Government agencies at every level must reduce cyber risks while maximizing limited resources. But without an accurate understanding of their overall technology ecosystems — something many still lack — their efforts fall short.

The experiences of three former top agency officials — former New York City CTO Mike Bimonte, former Florida CISO Jeremy Rodgers and former Washington state CISO Vinod Brahmapuram — show how public sector organizations can achieve smarter, faster and more secure operations by transitioning from siloed tools to unified visibility.

The Cost of Inadequate Visibility

Many agencies operate with fragmented or incomplete asset visibility. This often leads to bloated inventories, overlapping cloud use and inconsistent software licensing tracking. These gaps can slow response efforts and make it harder to identify or contain threats quickly.

Bimonte recalls facing significant "true-up costs," sometimes in the six-, seven- or eight-figure range, because New York City lacked accurate data about what was deployed and whether those tools were accurately being used.

Rodgers' early statewide enterprise initiative in Florida revealed that most agencies lacked real-time visibility and accountability for their IT and OT assets.

Brahmapuram says Washington's cybersecurity teams were forced to rely on cumbersome spreadsheets during urgent zero-day responses, such as the Log4j event, underscoring how fragmented data hinders crisis management.

These are not isolated challenges. They are systemic realities showing that even the most capable government IT and security teams grapple with a lack of comprehensive insight, which leads to inefficiencies and increased vulnerability.

Operational Effectiveness Starts with Real-Time Visibility

Today's public sector IT environments, characterized by sprawling and decentralized components, are under constant pressure from evolving threats, shrinking budgets and rising expectations.

As Bimonte says, "You can't protect what you can't see." Asset visibility should be considered an operational cornerstone, not a security checkbox. Agencies must have live insight into their IT, operational technology, Internet of Things assets — what's deployed, where it resides and how each component performs. Relying on outdated reports and fragmented tools causes response delays, misalignment across teams, and inefficiencies in both time and budget. Without a continuous and comprehensive view of assets, critical decisions are based on guesswork.

When unified visibility is done right, it aligns IT, security and operations teams around a shared source of truth, creating the conditions for faster, more confident decision-making.

Lessons from the Front Lines

The successes of Rodgers, Brahmapuram and Bimonte provide compelling evidence of how unified visibility can transform government agencies.

When unified visibility is done right, it aligns IT, security and operations teams around **a shared sense of truth.**

In Florida, Rodgers spearheaded an enterprise rollout that achieved visibility across hundreds of thousands of devices spanning dozens of state and local agencies. That visibility enabled the state to act quickly during cybersecurity emergencies. For example, when the Cybersecurity and Infrastructure Security Agency issued an urgent alert on certain vulnerabilities, Florida was able to identify affected systems before the weekend deadline.

Brahmapuram attributes Washington state's success in advancing cybersecurity to strong collaboration across executive branch agencies, which allowed the state to successfully implement five major enterprise security services in less than two years. Those efforts helped protect connected assets and ensured the state was delivering resilient, secure and equitable public services.

According to Bimonte, in New York City, responding to law enforcement requests for user and device activity used to take days and involve multiple teams. Now, with unified asset visibility, that same process can take just seconds.

These examples show integrated visibility is not just theoretical. It drives tangible improvements in efficiency and security and brings speed, trust and clarity to high-pressure, high-impact situations.

Being Effective with What You Already Have

Transformation doesn't have to mean disruption. There are visibility tools that integrate with current systems; improve data fidelity; and dramatically reduce wasted time, money and effort.

Visibility into your current assets can reap various benefits, including reduced cloud and software bloat, more accurate license negotiations and vendor oversight, and faster risk identification and prioritization. It also leads to reclaimed staff hours (what Bimonte calls "FTE giveback") and an improved operational focus that comes from having a single-pane-of-glass view.

Agencies can't afford to focus solely on emerging threats. In many cases, long-standing, unpatched vulnerabilities present an even greater risk. Without comprehensive visibility, these hidden weaknesses persist, leaving critical systems exposed.

From Insight to Action: Advice for Leaders

- **Don't start with tools; start with outcomes.** Before investing in technology solutions, leaders should first identify the specific risks they need to reduce and the decision-making processes they need to speed up.
- **Think like an adversary.** Brahmapuram recommends reverse-engineering your preparedness based on how fast today's attackers operate. If adversaries can act in minutes, agencies must be able to respond with comparable speed.
- **Build shared accountability.** Cross-functional visibility ensures teams aren't working at cross purposes. Everyone needs access to the same data to ensure alignment and collaborative effort. Leaders or teams with different levels of leadership and responsibility may be responsible for risk, patching or threat intelligence, but all must work from the same data.
- **Make visibility dynamic.** Yearly inventories aren't enough in today's rapidly changing threat landscape. Real-time insight is essential to keep up with evolving threats and emerging opportunities.

Conclusion

Visibility is a leadership issue. It underpins accountability, empowers smarter action and makes government more adaptive. With a clear, real-time view into their environments, agencies can coordinate more effectively and better protect critical services.

This piece was written and produced by the Government Technology Content Studio, with information and input from Armis.

government technology

Produced by Government Technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

ARMIS

Sponsored by Armis

Armis, the cyber exposure management and security company, defends the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, secure, prioritize and manage all critical assets. Armis secures Fortune 100-, 200- and 500-scale companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7. Armis is a privately held company headquartered in California.

ADOBESTOCK/AI GENERATED