CYBERSECURITY AND DIGITAL RISK STRATEGY

How State and Local Governments Can Strengthen Cybersecurity—and Trust

By Neveen Awad, Lina Bankert, Nadya Bartol, Jen Hoffbauer, Akshat Kalra, and Heidi Kim

ARTICLE SEPTEMBER 17, 2025 8 MIN READ

Cybersecurity is more than a technical necessity. For state and local governments in the US, it's a cornerstone of public trust.

Citizens increasingly expect online public-sector services, such as renewing a driver's license or applying for Medicaid, to match the seamless, secure experiences delivered by leading private-sector companies. Yet, in BCG's 2024 Digital Government Citizen Survey, 74% of respondents said they have faced problems accessing government services over the past two years. (The survey did not distinguish between state and local government services.) Each failed interaction erodes public trust.

Data breaches, which have frequently targeted both state and local governments, are perhaps even more problematic. Breaches of state government systems have risen more than 70% in the past three years. In one instance, a ransomware attack targeted a state portal used for health insurance and social services. The attack exposed the personal information of hundreds of thousands of users, forcing the state to temporarily take the system offline.

The risks for governments are already high. But the rapid growth of AI has raised the stakes further by giving attackers new, faster, and more effective hacking tools. At the same time, AI can strengthen cyber defenses by identifying suspicious behavior and automating security tasks previously performed by people.

Challenges Facing State and Local Governments

Some state and local governments have focused with some success on elements of cybersecurity. Colorado and Michigan, for example, are adopting DevSecOps, a collaborative and iterative approach that builds security into IT projects from the start. Oklahoma has created efficiencies and stronger defenses by standardizing and centralizing IT and security across state government.

But few governments have tackled cybersecurity as comprehensively as the current threat demands. People, process, and technology challenges stand in the way of progress.

People. Individual state and local government departments often have their own cybersecurity and IT leadership teams. Even when cybersecurity is centralized, chief information officers (CIOs) and chief information security officers (CISOs) frequently report through multiple governmental layers, limiting their influence and slowing critical decisions. In many governments, responsibility for cybersecurity is so fragmented that it ultimately is nobody's responsibility.

A severe systemic shortage of cybersecurity professionals persists globally and within the US. In each of these four states—California, Florida, Texas, and New York—there are more than 400 cybersecurity job openings in state and local government, according to CyberSeek, a workforce analytics service that collaborates with the National Initiative for Cybersecurity Education, the federal program responsible for cyber workforce development.

Processes. Process inefficiencies—from service delivery to procurement—create friction at every stage in the development of secure digital services. Teams frequently build features in isolation and bolt on compliance at the end, rather than treat security and usability as equally essential product features to be designed into the system upfront.

Procurement practices further complicate matters. Requests for proposal often do not include clear service level agreements or measurable resilience standards. Once a vendor is selected, performance tracking, compliance checks, and clear escalation paths may be lacking.

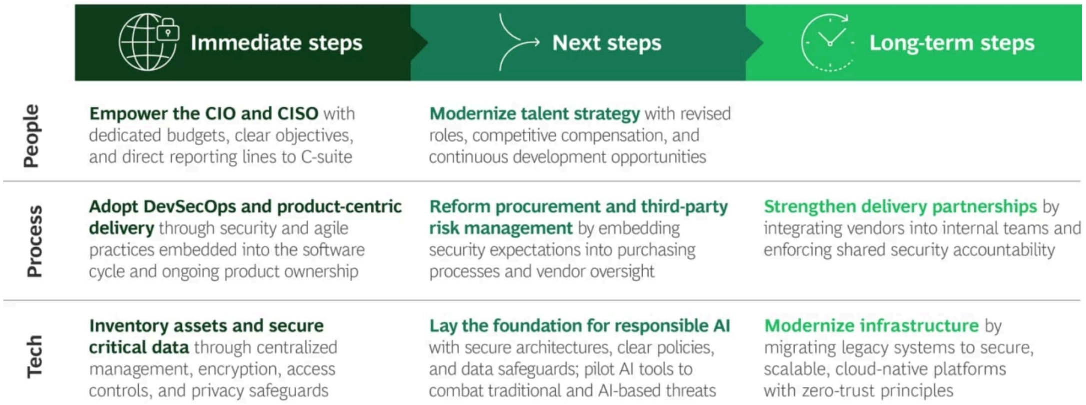
Technology. Critical data—from Social Security numbers to tax and benefit records—are frequently stored in legacy systems. These fragmented systems are an easy target for cyber attackers. Again, many modernization efforts focus on the front end rather than strategic back-end overhauls, leaving vulnerable architectures in place.

A pattern of chronic underinvestment underlies these weaknesses. The adoption of modern commercial platforms and secure, scalable cloud architectures can be hard to justify and approve when state budgets are constrained.

A Staged Approach to Achieve Cybersecurity

The recommendations below offer a practical staged roadmap for improving cybersecurity capabilities in state and local governments. The people, process, and technology steps all lead toward trust, innovation, resilience, and compliance. (See the exhibit.)

Strengthen Cybersecurity—and Public Trust—in Stages



	Immediate steps	Next steps	Long-term steps
People	**Empower the CIO and CISO** with dedicated budgets, clear objectives, and direct reporting lines to C-suite	**Modernize talent strategy** with revised roles, competitive compensation, and continuous development opportunities	
Process	**Adopt DevSecOps and product-centric delivery** through security and agile practices embedded into the software cycle and ongoing product ownership	**Reform procurement and third-party risk management** by embedding security expectations into purchasing processes and vendor oversight	**Strengthen delivery partnerships** by integrating vendors into internal teams and enforcing shared security accountability
Tech	**Inventory assets and secure critical data** through centralized management, encryption, access controls, and privacy safeguards	**Lay the foundation for responsible AI** with secure architectures, clear policies, and data safeguards; pilot AI tools to combat traditional and AI-based threats	**Modernize infrastructure** by migrating legacy systems to secure, scalable, cloud-native platforms with zero-trust principles

Source: BCG.

Immediate Steps

Embed cybersecurity as a fundamental requirement by strengthening leadership and processes and securing critical technology assets.

People: Empower the CIO and CISO. Cybersecurity needs a seat at the table with key leaders. Elevate cybersecurity leadership by providing direct reporting lines for CIOs, CISOs, and other critical roles to agency executives. Equip them with dedicated budgets and clear objectives that shift responsibilities from checklist compliance to strategic accountability and innovation.

Process: Adopt DevSecOps and product-centric delivery. The current approach of introducing security measures at the end of system development is not working. Instead, fully integrate agile DevSecOps practices into the software life cycle for both externally and internally developed systems. Deploy, or require vendors to marshal, cross-functional teams to continually gather real-time user feedback, perform threat modeling, and engage in iterative testing. Shift from one-off projects to ongoing product ownership. Make CISOs and security engineers strategic design partners to help craft seamless, trustworthy user experiences.

Technology: Inventory assets and secure critical data. Teams need a single source of truth. Implement comprehensive, statewide asset management systems and processes. Catalogue critical assets and data and enforce encryption, access controls, and privacy standards. Break down silos by creating a centralized asset management. Use this foundation to develop risk-based protection strategies and advanced analytics.

Next Steps

Once the foundational steps have been taken, the focus shifts to building momentum through strategic talent management, procurement reform, and responsible AI adoption.

People: Modernize talent strategy. Legacy practices prevent state and local governments from proceeding as fast or as thoroughly as they might. Overhaul state cybersecurity talent practices, revising job roles and compensation to attract skilled cybersecurity professionals. Introduce flexible work arrangements and establish educational partnerships to build a steady pipeline of cybersecurity talent and provide continual professional development.

Process: Reform procurement and third-party risk management. Revised procurement practices can speed the establishment of cybersecurity practices. Embed stringent cybersecurity expectations into procurement processes. Standardize RFP language with measurable security requirements, structured vendor assessments, and strong oversight, including performance scorecards and compliance checks. Utilize federal funding and cooperative purchasing agreements to scale and reinforce these improvements efficiently.

Technology: Lay the foundation for responsible AI. Introducing new services without proper guardrails in place can introduce new vulnerabilities. Prepare secure and transparent practices and approaches for AI adoption. Develop zero-trust identity and modern data architectures alongside clear policies addressing transparency, bias, and security. Prioritize AI use cases with clearly defined security, data privacy, and usability standards to safely enhance services. Pilot AI tools that can combat traditional and AI-based threats.

Long-Term Steps

Long-term priorities should focus on institutionalizing resilience through strong vendor partnerships and modern infrastructure.

Process: Strengthen delivery partnerships. Traditional buyer-seller relationships with vendors stand in the way of progress. Develop collaborations that fully integrate vendors with internal teams. Standardize secure delivery practices, consistent documentation, and rigorous quality checkpoints. Build shared accountability that enforces high standards of security and performance in vendor partnerships.

Technology: Modernize infrastructure. Piecemeal patching does not scale. Fully transform outdated infrastructures by migrating legacy systems to secure, scalable, cloud-native platforms. Embed zero-trust principles, automate security controls, and prioritize comprehensive upgrades over temporary solutions to ensure lasting resilience, scalability, and cost effectiveness.

Investing in cybersecurity is investing in public trust. In addition to creating digital services that work better and more safely, state and local leaders can create services that inspire confidence in government itself.

Authors

Neveen Awad

Managing Director & Senior Partner
Detroit

✉

Lina Bankert

Managing Director & Partner
Chicago

✉

Nadya Bartol

Managing Director, BCG Platinion
Washington, DC

✉

Jen Hoffbauer

Platinion Manager, Cybersecurity
San Diego

✉

Akshat Kalra

Project Leader
Chicago

✉

Heidi Kim

Managing Director & Partner
Los Angeles

✉

ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

For information or permission to reprint, please contact BCG at permissions@bcg.com. To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com. Follow Boston Consulting Group on Facebook and X (formerly Twitter).