

A Roadmap for Stronger Cybersecurity

Using new federal funding to move toward zero-trust maturity



The need for state and local governments to strengthen cybersecurity has never been more urgent.

Government agencies have become prime targets for cyber attackers, especially with wider adoption of remote work and digital services. Agencies also are grappling with legacy systems that hinder their efficiency and increase their security exposure.

In 2020, at least 79 ransomware attacks successfully hit government organizations, amounting to nearly \$19 billion in downtime and recovery costs.¹ Separate research indicates 34% of local governments worldwide were hit by ransomware in 2021.²

Federal funding programs — including \$1 billion in cybersecurity grants soon to be available from the Infrastructure Investment and Jobs (IIJA)³ and remaining funds from the American Rescue Plan Act (ARPA) — offer governments an opportunity to address current cybersecurity vulnerabilities and make strategic investments to prepare for future threats.

“The more we think about cybersecurity as foundational to our technology, the better off we all will be.”

Chris Hein, Director of Customer Engineering, Google Cloud

Ultimately, state and local governments must use these and other resources to integrate stronger cybersecurity into everything they do, says Chris Hein, director of customer engineering for Google Cloud.

“Cybercrime has become an incredibly lucrative business, and it’s now a national security problem,” he says. “The more we think about cybersecurity as foundational to our technology, the better off we all will be.”

The Zero-Trust Journey

Hein says governments need to create cybersecurity strategies that immediately strengthen their security posture while also providing a roadmap for mid- and long-term investments that advance cyber maturity.

Zero trust likely will be the North Star for state and local cybersecurity strategy going forward. Zero trust isn’t a particular security technology. Instead, it’s a collection of concepts, policies and tools intended to protect data in today’s heightened risk environment, where users are often mobile, transactions are increasingly virtual, and security threats are more numerous and sophisticated.

Zero trust is a security framework that requires all users — inside or outside the organization’s network — to be authenticated and continuously validated before they can access applications and data. As its name implies, zero trust doesn’t assume implicit trust, but rather that every access request could be a potential threat.

As state and local governments focus on their cybersecurity planning in 2022, they can use federal funding to move incrementally toward a zero-trust model.

Immediate Security Investments

Agencies can take several immediate steps to reduce cyber vulnerabilities, starting with implementing multifactor authentication to verify identities for employees, contractors and temporary staff, says Hein.

“For your most privileged users who have access to core systems, you even want to get to the point where you’re enforcing hardware-based token authentication,” he says. This approach requires users to have a token or other dedicated physical device in addition to a password to access network resources.

Replacing legacy identity and access management systems with cloud-based, AI-driven platforms that employ the principle of least privilege — a concept that says users should only have the minimum access privileges they need to do their job — is another important step. Agencies should look for systems with integrated capabilities such as single sign-on, streamlined user provisioning and deprovisioning, real-time analytics and alerts, anomaly detection, predictive security monitoring, and granular application access controls.

Agencies must also deploy modern, secure email and collaboration platforms to support permanent remote and hybrid workforces. Google Workspace, for example, includes integrated

security features that transmit data through HTTPS-encrypted tunnels using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption protocols. In addition, Google Workspace offers built-in tools to detect and prevent phishing and malware attacks,⁴ and it runs on custom-designed servers for optimal security and performance.⁵

“It’s really important to make sure you’re using best-of-breed solutions for your organization’s browsers and mobile devices and securing these things using modern workforce tooling,” Hein says. “If you do these two things alone, you’ll shut down the vast majority of the threats that come to you.”

Mid-Term Security Investments

Transitioning away from on-premises technology and adopting secure-by-design, cloud-based solutions can help agencies advance their security maturity.

“The cloud has some significant security benefits,” Hein says. “It’s not a cure-all, but it can help you build your security infrastructure.”

IJA funding gives agencies a once-in-a-generation opportunity to invest in both physical and digital infrastructure — and agencies can use these dollars for cloud-based operational technology (OT) and IT security solutions as they modernize. For example, cloud-based asset management tools that incorporate AI-driven real-time monitoring and analytics can help agencies strengthen infrastructure security and improve maintenance.

State and local agencies should also consider adopting cloud-based security information and event management (SIEM) and security orchestration, automation and response (SOAR) platforms. These tools provide real-time threat detection and intelligence.

Multi-jurisdictional security collaboration is another important move. Many states are launching regional security initiatives, such as New York’s recently announced joint security operations center that will serve as a hub for threat intelligence sharing and cybersecurity coordination across the state.⁶

“It’s a really valuable concept to look at how statewide security offices can help individual cities, counties and school districts because they’re often the folks who are being attacked,” Hein says.

Long-Term Security Investments

Along with continuing to mature their zero-trust capabilities, agencies should make strengthening data backup and recovery capabilities a fundamental part of their long-term cybersecurity strategy. Besides deploying these solutions, agencies must test them regularly to ensure they function correctly, adds Hein.

“If you’ve made a backup, but you actually can’t recover from that backup, then it’s worthless,” he says.

As part of this process, agencies must understand their recovery point objectives (RPO) and recovery time objectives (RTO). RPO focuses on the organization’s acceptable level of data loss after a security incident and RTO covers how quickly systems and processes must be restored to avoid a massive disruption to day-to-day operations. These metrics are key to any disaster recovery plan and can be applied differently depending on the criticality of the data, systems and applications an organization must restore.

Building More Secure State and Local Government

Government agencies must steadily build and strengthen their security infrastructure by making immediate, mid- and long-term security investments. This roadmap for zero trust and disaster recovery maturity can help agencies plan and prioritize security initiatives and make the most of available funding.

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

Endnotes

1. Ransomware attacks on US government organizations cost \$18.9b in 2020. CompariTech. <https://www.comparitech.com/blog/information-security/government-ransomware-attacks>
2. State of ransomware in government 2021. SOPHOS. <https://cdn.statescoop.com/state-of-ransomware-in-government-2021.pdf>
3. Infrastructure Investment and Jobs Act. <https://www.congress.gov/bills/117/congress/house-bill/3684/text>
4. Google Workspace admin help. Advanced phishing and malware protection <https://support.google.com/a/answer/9157861?hl=en>
5. Google Cloud help. Security. <https://support.google.com/googlecloud/answer/6056693#zippy=%2Cis-it-safe-for-my-organization-to-access-google-cloud-over-the-internet%2Cchow-do-i-know-that-other-customers-sharing-the-same-servers-cant-access-my-data%2Cdoes-google-workspace-offer-sstls-connectivity%2Cchow-does-google-protect-against-hackers-hacktivists-governments-and-other-intruders>
6. Governor Hochul announces formation of joint security operations center to oversee cybersecurity across the state. <https://www.governor.ny.gov/news/governor-hochul-announces-formation-joint-security-operations-center-oversee-cybersecurity>



Produced by:

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



Sponsored by:

Visit sessions from the [Google Cloud Security Summit](#) to learn from experts, explore the latest tools and hear best practices to drive your agency’s cybersecurity strategy.