govloop

Cybersecurity Is Now a Shared Mission

How Agencies Are Collaborating to Improve Security

A GovLoop Guide

Introduction

Across the public sector, cybersecurity teams are stretched thin, struggling to keep pace with a rapidly evolving threat landscape. Constrained by tight budgets and workforce shortages, they lack the resources to get ahead of new and emerging threats.

But the good news is, they don't have to go it alone. Through strategies such as whole-of-state cybersecurity and information-sharing and analysis centers (ISACs), agencies can pool their knowledge to expand visibility and stop incursions before they spread.

In this guide, you'll meet Ryan Murray, Arizona's Chief Information Security Officer and Deputy Director of the Arizona Department of Homeland Security (AZDHOS), and learn how whole-of-state cybersecurity links threat detection and response efforts across local governments and brings essential security tools to under-resourced communities.

You'll also meet Randy Rose, who leads cyber operations at Multi-State Information Sharing and Analysis Center (MS-ISAC) and is the Center for Internet Security's Vice President of Security Operations and Intelligence. He discussed why collaboration is critical to predicting and preventing cyberattacks, and how shared intelligence builds a cyber community that enhances resilience.

Cybersecurity isn't getting easier. But working together can make it more manageable and effective. We hope you'll find strategies here that will help you strengthen your defenses.

Contents

3 Cybersecurity, by the Numbers

5 To Strengthen Cyber Defense, Agencies Must Close Their Common Security Gaps

6 An AI-Native Defense Against AI-Driven Cyberattacks

7 Whole-of-State: We're in This Together

10 Security Is More Than Prevention: It's Resilience

11 How Centralized Identity Management Improves Resident Experience

12 As Cyber Threats Grow, Information Sharing Becomes More Critical

15 Resilience Keeps Services Running Despite Cyber Threats

16 Continuous ATO Breaks Down Barriers to Innovation

17 Comply-to-Connect Concept Drives Greater Situational Awareness

18 Additional Resources and Acknowledgments

Cybersecurity, by the Numbers

Hackers Have an Edge: Time

ATTACKER SPEED
Time to compromise
72 minutes
(1 hour, 12 minutes)

Attackers can breach systems in just over an hour.

DEFENDER TIMELINE
Time to detect & respond
277 days
(about 9 months)

It can take months to detect and contain a breach.

TIME GAP RATIO ▶ 1 : 5,500+
72 minutes vs. 277 days

In early 2026, the U.S. began seeing a 62% higher attack frequency than the global average.

2.62 billion
The number of federal civilian network cyberattacks that CISA blocked in 2025

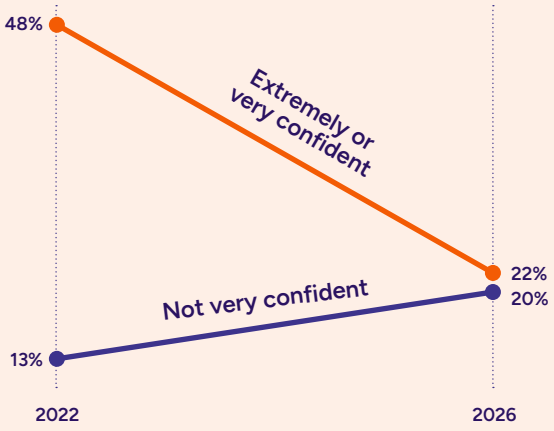
60
The percentage of federal agencies that have delayed, stalled or stopped digital transformation projects due to cyberwarfare risks

Only 22% of state CISOs say their cybersecurity professionals have the competencies they need to keep pace with incoming threats in 2026 — down from 47% two years ago.

Feds are responsible for the cyber protection of 170,000 water and wastewater systems nationwide.

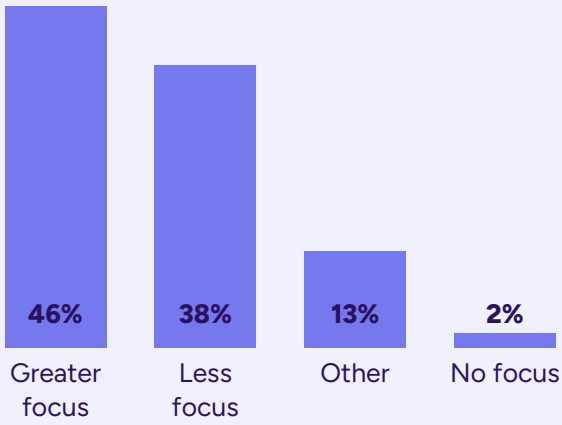
68% of state, local, tribal and territorial governments lack direct funding to implement major cybersecurity priorities.

State CISOs are now significantly less confident that state assets are protected from cybersecurity threats, according to a recent survey.



Note: Percentages may not total 100% because "Somewhat confident" and "Not applicable or do not know" responses are not shown in the figure.

State support for local government/higher education cybersecurity efforts is uneven. In fact, 38% of states are reducing their focus this year, according to a new survey.



Question: "What is your state's approach to cybersecurity for local government entities and public higher education?"
Note: Percentages may not total 100 due to rounding.

4 Insights Into Local Gov Cybersecurity

A multiyear survey of local government IT, finance, administrative and other professionals revealed four core findings.

1 Cyber risk awareness is high — but uneven.

Respondents consistently rate their state at alevated or high risk, yet awareness of real-world events dropped and training responses became more varied.

2 Budget increases are steady but modest.

Local governments are spending more, but not enough to match the speed and sophistication of modern threats.

3 Technology modernization is accelerating, yet incomplete.

More new systems, fewer on-premises solutions, but persistent fragmentation means cyber exposure remains high.

4 Foundation best practices are not universal.

Zero trust, dot-gov domains and grant use all show large gaps.

Closing Common Security Gaps to Strengthen Cyber Defense

Locking your agency's digital front door isn't enough to keep it safe from potential cybersecurity threats. Cyber attackers are now using AI to help them make their entrance, making them sneakier, faster and more relentless than in the past. As AI proliferates, closing such common-sense cyber gaps becomes increasingly critical. Yet agencies suffer from persistent vulnerabilities that limit their risk reduction. They often have inadequate multi-factor authentication (MFA) and other zero-trust protocols and blind spots created by shadow IT, for example. Many agencies stitch together an ecosystem of tools with little coherence.

A single solution can't solve these challenges, but you start by taking measurements. You might count the number of shadow IT devices on your network, for instance, and determine your attack detection and response times. The goal is to develop a balanced portfolio of reforms to answer the AI threat, said Fadi Fadhil, Field CIO of Palo Alto Networks.

In this video interview, Fadhil discusses why agencies struggle to meaningfully reduce their cyber risk and how to overcome those challenges. Topics include:

- → Specific questions to ask when endeavoring to boost cyber defenses
- → Why MFA, segmentation and other protections are so critical
- → How AI has impacted the cybersecurity environment

"A core concept around AI is that bad actors use AI to multiply themselves, become more sophisticated and get faster at attacking us. Yet, we're constantly lagging a bit behind."

— Fadi Fadhil, Palo Alto Networks

About Palo Alto Networks

Palo Alto Networks is the global cybersecurity leader, committed to making each day safer than the one before with industry-leading, AI-powered solutions in network security, cloud security and security operations.

Learn more about Palo Alto Networks.

paloalto NETWORKS

carahsoft.

An AI-Native Defense Against AI-Driven Cyberattacks

"The folks who are most prepared for attacks are the ones who are saying, 'Let's prioritize the attacks that are most relevant to me. Don't give me a list of thousands of things to go after.'"

— Karan Sondhi, CrowdStrike

Artificial intelligence has a truly impressive ability to invade agency systems. In just seconds, an AI-empowered malicious actor can break through cyber defenses, steal credentials and blend into normal network activity using legitimate administrative tools, essentially hiding in plain sight. Traditional security solutions don't catch the behavior because they look for malicious files that don't exist. Fragmentation and tool sprawl — common in government networks — increase system complexity and make it hard to see telltale signs of cyberattack. And relying on human triage is unsustainable.

Defending against AI-driven threats requires a new model: a single, unified data layer that brings together endpoint, cloud, network and identity telemetry. The approach relies on native AI agents that identify typical network behavior and instantly flag anomalies — then pass the information to humans, giving them the context they need to quickly contain problem areas. But don't chase every potential breach, advises Karan Sondhi, CrowdStrike's Vice President and Chief Technology Officer for Global Public Sector.

In this video interview, Sondhi discusses AI's growing impact on government cybersecurity operations. Topics include:

- → Why accelerated AI adoption creates new cyber threats
- → How security operations will evolve in the next several years
- → The current and future roles of human AI analysts

About CrowdStrike

CrowdStrike protects the people, processes and technologies that drive modern enterprise. A single agent solution to stop breaches, ransomware and cyberattacks — powered by world-class security expertise and deep industry experience.

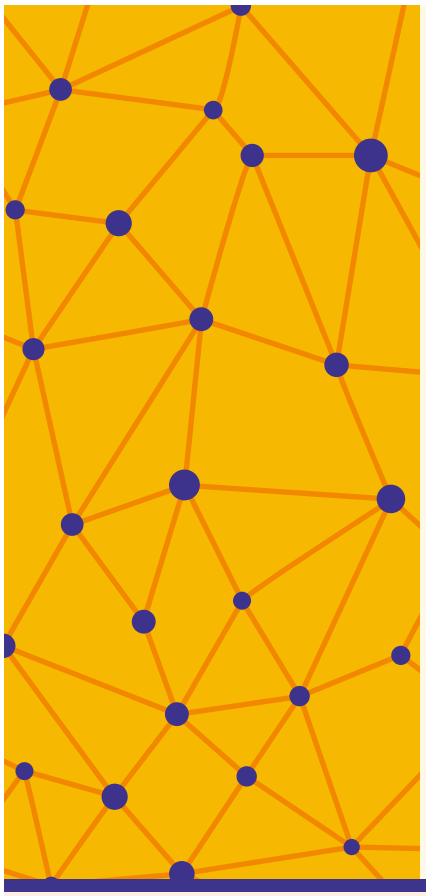
Learn more about CrowdStrike.

CROWDSTRIKE

Whole-of-State: We're in This Together

Arizona was among the first states to adopt whole-of-state cybersecurity, launching its Cyber Command in 2021. It linked threat detection and response efforts across local governments and agencies and made essential security tools available, creating a security fabric that better protects everyone.

We talked to Ryan Murray, state CISO and Deputy Director of the AZDOHS, about how the project started and how it works today. He outlined the steps that made the broad approach a reality.



Step One: Recognize That Cybersecurity Is More Than Tech

Officials began by moving the state's cybersecurity operations from IT to AZDOHS, demonstrating that cybersecurity is not simply a technical issue, but a more comprehensive defense. "How do we make sure we're protecting all the small, underserved cities and counties? How do we start talking about the other government entities, like public school districts or transit authorities?" Murray said. "We need to be looking across the entirety of the state of Arizona."

Increasingly, government agencies at all levels are interconnected, "so a threat realized and exploited and manifested in one of those entities is really a threat that we all have to deal with," Murray said.

At the same time, smaller organizations have significantly fewer resources and some lack IT departments altogether. "They're relying on bubblegum and twine just to keep the lights running," Murray said. "So, it made sense for us to say, 'Let's look at this holistically, as a big-picture problem, where we can all come to the table and help each other and protect each other.'"

Step Two: Share Information

In Arizona, outreach began through an existing informal network of officials responsible for cyber in their communities. Information sharing was the critical component early on. "We were reaching out and talking to these entities, saying, 'We have information [about] a specific phishing email or a specific [distributed denial-of-service] attack,' and pushing that out to the broader community," Murray said.

Today's AZ-ISAC is the product of that early information sharing. It now includes more than 1,000 people on a Slack workspace, covering about 400 state and local government entities, as well as links to centers in Maryland and Colorado. "We're sharing and talking to each other in real time [using] that rapid, real-time information-sharing mechanism," Murray said.

Step Three: Make Resources Available

The next step came in 2022-23, when Arizona allocated funds to launch its Cyber Readiness Program, which offers a suite of cyber resources to cities, local government, K-12 schools and tribal agencies. "We were providing them at no cost, knowing that [some organizations may] never be able to afford these tools themselves," Murray said.

Buying centrally also helps agencies that are too small for vendors to consider. "A lot of these companies won't even talk to someone for less than 1,000 users," he explained.

Under the Cyber Readiness Program, agencies can access security awareness training, endpoint detection and response, multifactor authentication, and a web application firewall to protect public-facing services against DDoS attacks and website vandalism. A converged endpoint management system allows the state to push tools and software to the connected agencies and centrally manage updates, software patches and compliance.

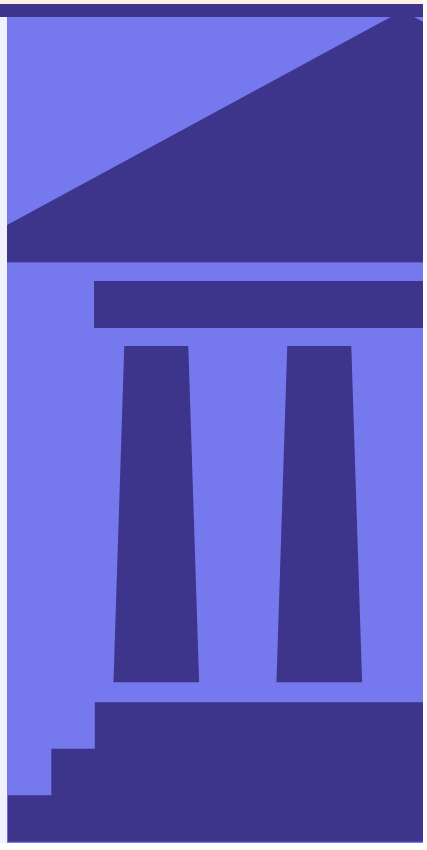
More recently, the program used federal State and Local Cybersecurity Grant Program funds to add protection against malicious email. They've also used SLCGP grants to hire contractors to help customers deploy and configure tools and services.

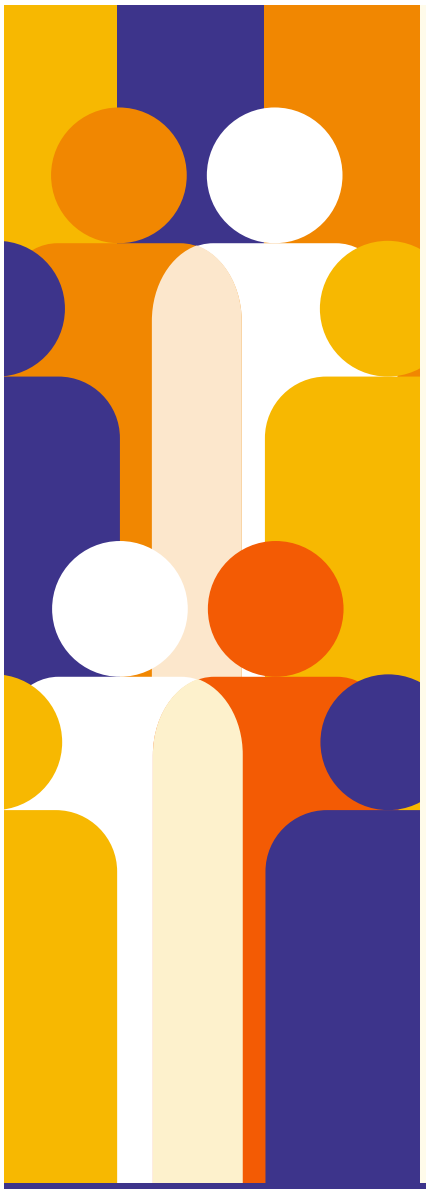
Step Four: Make the Case

To get local organizations onboard, Murray brought the message to them: "In the beginning, I literally drove around the state — me and a couple of my staff members doing these road shows."

With bipartisan support over two state administrations, Murray could reassure agencies that the initiative was free and "as permanent as anything is in government." Even better, it produced data that could help make the financial case. "You can take that to your town council or board of supervisors and say, 'Look, this is how we're saving the city or the county money by participating with the state on this,'" he told them.

Another trust-building factor was a promise not to overreach. "We give them the tools, we help them to get up and running, and then we stand hands-off and let them manage their own environments," Murray said. "We make it very explicit with our stakeholders that we won't make any changes in their environment without their approval. We want to make sure that trust level exists where they know we're not going to just go blow up their stuff without their permission."





Step Five: Expand the Network and the Workforce

The system is a boon for all cities and counties, even those with better funding that can afford their own cyber resources. "As we're deploying the services that are helping to protect these environments, they're also gathering a ton of telemetry of what those attacks look like. If we're all using the same tools, and we're all part of the same community, we can collect that information and then share it with them," said Murray.

AZDOHS is also building a cyber workforce with student-led, state-run regional security operations centers. The pilot is funded by SLCGP, with the hope that the state can eventually support the effort.

"We're looking at this from an operational support standpoint," Murray said. "All these cities and counties are struggling to hire cybersecurity staff. So, we're partnering with our community colleges to put students directly to work, monitoring for cyberattacks and defending against them in their own communities." The students also lighten the load on senior analysts by filtering out false positives and low-level alerts.

The program has additional benefits. It's also a workforce and jobs program that teaches and trains the future cyber workforce. "We're giving them that hands-on experience in a real-world environment," Murray said. "Being able to put on your resume [that you] worked two to four years with the Arizona Department of Homeland Security as a security analyst gives you a major leg up when you're out there looking for jobs."

Cybersecurity Is a Team Sport

Arizona's experience shows that whole-of-state brings people together.

"We often say cybersecurity is a team sport, or it needs to be a community effort," Murray said. "We're really living that. If a city down the road gets hit with a ransomware incident, that's just as much my problem as it is their problem. And it's the citizens' problem, too. Those services are no longer being delivered."

Ultimately, that's why whole-of-state is so important: It keeps agencies up and running.

"Cybersecurity is that core foundation across all of the missions of state and local government," Murray said. "We're investing in quiet days to make sure that we can continue to provide those services to our citizens."

Ryan Murray

State CISO and Deputy Director of the Arizona Department of Homeland Security

Security Is More Than Prevention: It's Resilience

The volume and sophistication of today's cyberattacks make breaches inevitable. Agencies must do everything they can to prevent incursions, but they also need resilience — the ability to respond and recover from a cyber event. Resilience is difficult to achieve, however, because IT environments have become complicated, with devices and applications both on-premises and in the cloud. And despite improvement in software bills of materials (SBOMs), it can be hard to identify all the software that may be at risk.

Tools such as hardened containers, vendored libraries and vulnerability scanners can help, but they depend on an accurate catalog of devices and applications. So the solution starts with a comprehensive asset inventory that identifies vulnerable applications and weeds out legacy carryovers that increase risk.

In this video interview, Josh Bressers, VP of Security at Anchore, discusses strategies to protect ever-more-complex systems, and effective tools that can help. Topics include:

- → Why today's cyber threats call for an approach that goes beyond prevention
- → How agencies can enhance their resilience
- → Why asset inventory is essential to an effective cyber defense

"Without question, the single largest challenge agencies have today is just the amount of infrastructure and software and services and everything that's going on right now. … We have to try to build resilience into a system that's moving faster than we can almost comprehend in many ways."

— Josh Bressers, Anchore

About Anchore

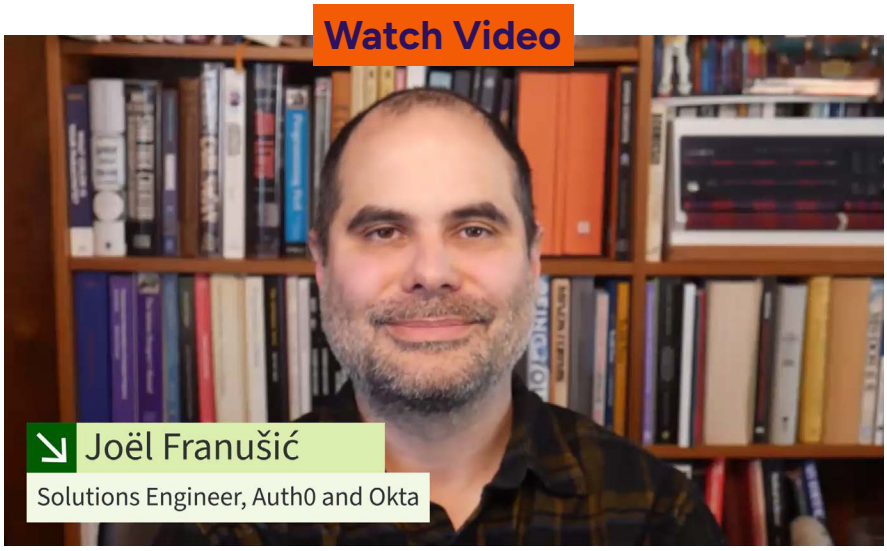
Anchore Enterprise employs SBOMs to inventory software, surfaces security issues to mitigate open source risk, and automates compliance across the software supply chain. Accelerate software delivery with comprehensive SBOM management, industry-leading container vulnerability detection and advanced policy enforcement to ensure continuous compliance.

Learn more about Anchore.

anchore

carahsoft.

How Centralized Identity Management Improves Resident Experience



Public-sector agencies are under increasing pressure to modernize their digital services, yet they face longstanding structural and technological hurdles. New digital services must integrate with a patchwork of legacy applications, mainframes and hybrid systems. This fragmentation also forces users to understand government organizational structure just to complete simple tasks — whether reporting a pothole, paying a utility bill or accessing benefits.

The path forward begins with treating identity as the connective tissue of digital government. Instead of each agency maintaining its own entry point, a unified identity layer gives residents a single, secure way to access all the services they need — regardless of which department runs them. This "no wrong door" approach simplifies digital interactions, reduces user frustration and strengthens trust in public systems.

In this video interview, Joël Franušić, Solutions Engineer at Auth0 and Okta, explains why identity management is the core of modernization, and how the right platform can simplify the task of centralization. Topics include:

- → How to incorporate legacy systems into a modern identity platform
- → Why AI means agencies can no longer put off the identity work they already knew they needed to do
- → How putting identity at the core lets agencies strengthen security and simplify access at the same time

"Having a single way to identify your users and centralizing the way that people get into the applications adds the security to applications that need it. Once you have that baseline, you can take advantage of modern technology to secure not only the modern tools, but also all the legacy systems that are there as well."

— Joël Franušić, Okta

About Auth0

Auth0 takes a modern approach to identity and enables organizations to provide secure access to any application, for any user. Auth0 is a highly customizable product that is as simple as development teams want, and as flexible as they need. Safeguarding billions of login transactions each month, Auth0 delivers convenience, privacy and security so customers can focus on innovation. Auth0 is a part of Okta

Learn more about Auth0.

auth0

As Cyber Threats Grow, Information Sharing Becomes More Critical

For more than two decades, the most comprehensive cyber resource for state, local, tribal and territorial governments (SLTTs) has been the Multi-State Information Sharing and Analysis Center.

With funding from the U.S. DHS, MS-ISAC provided free cybersecurity resources to more than 18,000 public-sector members — until last year, when DHS cut its funding and ended its cooperative agreement with the Center for Internet Security (CIS), the nonprofit that operates MS-ISAC. The move forced the organization to switch to a paid membership model to support its services. It is also working with jurisdictions that can't afford the new payment system.

Randy Rose

Vice President of Security Operations and Intelligence, CIS

Despite that dedication, MS-ISAC's new model may endanger the organization's ability to deliver prevention, prediction, and response and recovery tools and services to a broad coalition of SLTTs, particularly local entities. And this is an especially troubling time for governments to lose visibility into their cyber risk, said Randy Rose, who leads MS-ISAC cyber operations, because hackers are changing the way they attack state and local agencies.

Cyber Threats Have Changed

"What we have found over the last several years is that attacks have increasingly shifted towards a disruptive focus rather than just an opportunistic focus," said Rose, who also is CIS Vice President of Security Operations and Intelligence. Although ransomware is still the primary cyber threat for state and local governments, the attacks are now targeting organizations that provide essential services, such as hospitals, 911 call centers, water treatment facilities and schools — increasing the pressure to pay the ransom.

The community and public safety threat combined with relatively weak cyber defenses make state and local agencies attractive targets. And threat actors are using publicly available agency budget information to size up potential victims.

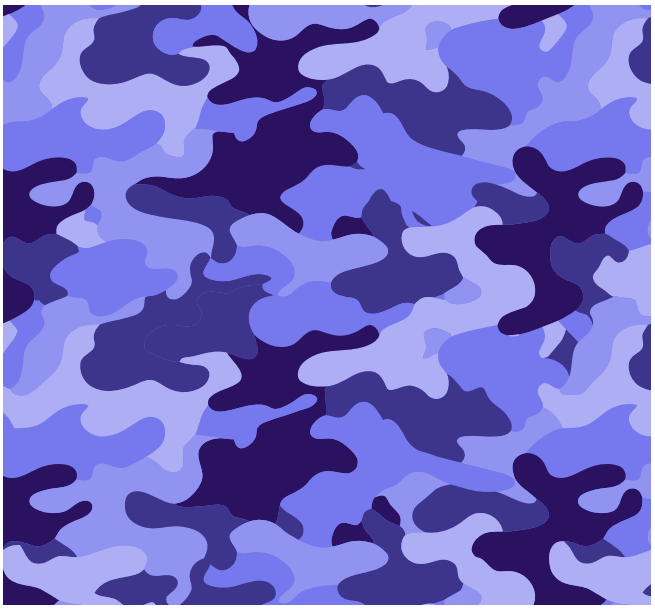
"Even smaller government organizations can have seemingly large budgets," Rose said. "So, if you're targeting a rural school district, and you see a $50 million budget, you're like, 'Hey, that's a pretty good payday for me.'"

Cybercriminals also have access to tools that once were available only to nation-state adversaries. Ransomware-as-a-service and generative AI allow low-level hackers to do much more damage. "We're starting to see them move into disruptive and destructive attacks because they can," Rose said. "We've seen a blurring of state actors and cybercriminals and hacktivists."

For many agencies, however, resources haven't kept up with these growing challenges. That's where ISACs can help.

"Shared-service models are critical for bridging the resource gap between large metropolitan areas and smaller, fiscally-constrained, and often rural jurisdictions."

— MS-ISAC



Sharing Knowledge for a Stronger Defense

"No single entity has the full threat picture," said Rose. "The idea behind ISACs was to create this communitywide or sector-wide visibility [so] there will be a better capture of the full threat picture, because as a community, we can come together and share information."

An intelligence component also is important; sometimes an anomaly is a false alarm. "Has it been correlated and enriched and verified? That's something that a cyber threat intelligence analyst would [do]," noted Rose.

MS-ISAC fields a robust set of tools and services that may serve as aspirational goals for narrower ISACs. Those include a 24/7 security operations center for real-time monitoring and support, cyber incident response, threat intelligence, a red team that mimics adversaries to find and fortify weaknesses, and a multidimensional threat team that evaluates cyber threats with physical impacts in the real world.

"Ultimately, the goal of MS-ISAC is … turning an isolated incident into shared threat intelligence that's timely, actionable and relevant for the community at large," Rose said. "We aim to take the information about one attack and turn that into proactive defense for everybody else."

Other Ways to Share

ISACs can complement cyber initiatives such as whole-of-state programs. Rose notes that ISACs may include local nonprofits or small businesses, broadening visibility beyond government entities. That can be especially helpful in an environment where hackers may be identifying organizations that aren't government agencies but have a city or state in their name.

"If an actor wants to go after Brooklyn, they're hitting everything with Brooklyn in the name, whether it's a business or a nonprofit or a local government," he said. "We can actually raise the baseline defense for a lot of these organizations that would otherwise essentially be left out alone in the cold."

At the same time, a state-focused approach may miss signals from outside its borders, although threats don't generally stop at the state line. MS-ISAC or another sector-based ISAC may provide a more "whole-of-nation" perspective.

Other types of information-sharing models include New York state's Regional Information Centers, which provide IT and cybersecurity services to school districts and connect schools that may have similar populations or resources. Also, ISACs can share threat intelligence and coordinate responses among related entities.

Beyond Cyber: The Power of Community

These knowledge exchanges do more than strengthen cyber defenses. "**When we have membership calls, the collaboration that happens just in the chat of those while the presentation's happening is unbelievable**," said Rose. "You're creating a community where people are literally answering questions for each other and helping each other out, sharing resources in real time. The social aspect of doing defense together is something that I don't think anybody really could have predicted, but it really helps improve resilience beyond just cybersecurity."

For many in public service, cybersecurity can be a lonely and thankless job. "They're not paid what their commercial counterparts are," explained Rose. "They don't have as many resources, and they're now being hit with attacks from the Russian government or the Chinese government. And they're like, 'I'm just an IT person at a school. I don't know how to deal with this stuff!' So, having that community provides some psychological safety and emotional resilience in addition to the cybersecurity resilience."

When Iranian Hacktivists Came to Call

The conflict between the United States, Israel and Iran highlighted the risk of pro-Iran hacktivists, Rose said.

One such group began targeting internet-connected surveillance cameras in Israel and other Middle Eastern countries. MS-ISAC started scanning for that type of attack and warned hundreds of state and local organizations that their internet-facing cameras likely were vulnerable. The network of members worked together to mitigate the risk, taking cameras off the internet or applying security patches.

"Another quick win," Rose said of the effort. "**The information-sharing model allows small organizations to punch well above their weight.** We can raise their capabilities through the shared defense model. I think that's really the best thing about collaboration."

Resilience Keeps Services Running Despite Cyber Threats

State and local governments are a favorite target for cyberattacks because they provide essential services and must secure critical infrastructure — responsibilities that have far-reaching impacts. In the current environment, though, successful breaches are inevitable, so agencies need the resilience to continue operations even when malicious actors invade agency systems. Hackers often do crippling damage once inside a network.

To be truly resilient, organizations must contain any incursion. Segmentation, for example, confines damage to a small part of the system, which protects the rest of an agency's data and network. IT teams then can focus on the areas that hackers breached, while operations elsewhere continue to function.

In this video interview, Gary Barlet, Public Sector Chief Technology Officer at Illumio, explains how agencies can protect vital functions in the event of a successful cyber breach. Topics include:

- How cyberattacks can impact state and local agencies' ability to deliver services
- What resilience means in the context of service continuity
- How segmentation can limit damage from a cyber breach and keep operations running

"Nowadays, you need to accept the fact that you're going to be breached, and you need to ask yourself, 'How can I maintain services during that breach? As I'm fighting through that breach? As I'm responding to that breach?' And the answer can't be, 'I just turn everything off.'"

— Gary Barlet, Illumio

About Illumio

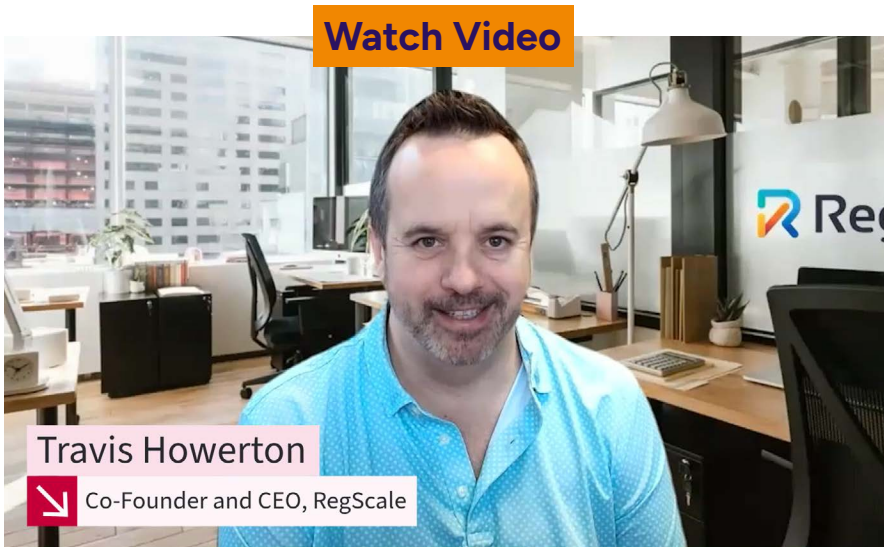
Illumio, the breach containment leader, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio Zero Trust Segmentation Platform visualizes how workloads and devices are communicating, creates granular segmentation policies which allow only necessary communication, and automatically isolates ransomware and breaches.

ZTS is proven to help organizations of all sizes, from Fortune 100 companies to small business, stop breaches and ransomware in minutes, save millions in downtime, and build operational resilience.

Learn more about Illumio.

illumio carahsoft

Continuous ATO Breaks Down Barriers to Innovation



The current wave of IT innovation is hitting a big bottleneck in government: the Authority to Operate (ATO) process. Agencies can code quickly with AI agents, deploy quickly with DevSecOps and continuous improvement/continuous delivery (CI/CD) pipelines, and scale quickly with the cloud. While the ATO process serves as a vital security check, it remains largely mired in the same manual processes and spreadsheets that agencies have used for decades. The reliance on these periodic, point-in-time security snapshots makes it difficult to keep up with today's rapidly changing IT environment.

Increasingly, agencies realize they need to adopt a continuous ATO, or cATO, process that provides real-time monitoring of National Institute of Standards and Technology Risk Management Framework controls, ensuring that systems remain compliant and secure as they evolve. CATO entails a fundamental shift from tracking controls in spreadsheets and documents to using machine-readable formats, such as the Open Security Controls Assessment Language, to streamline and automate the ATO process. This compliance-as-code approach enables the ATO process to keep pace with innovation, said Travis Howerton, Co-Founder and CEO of RegScale.

In this video interview, Howerton explains how agencies can shift to a cATO process. Topics include:

- → Leveraging OSCAL to assess security in real time
- → Getting more insights out of your existing cyber telemetry
- → The emerging role of AI agents

"Everybody's wanting to get closer to real time on this, so that as soon as there's a problem, we can respond the same way we do in our Security Operations Center."

— Travis Howerton, RegScale

About RegScale

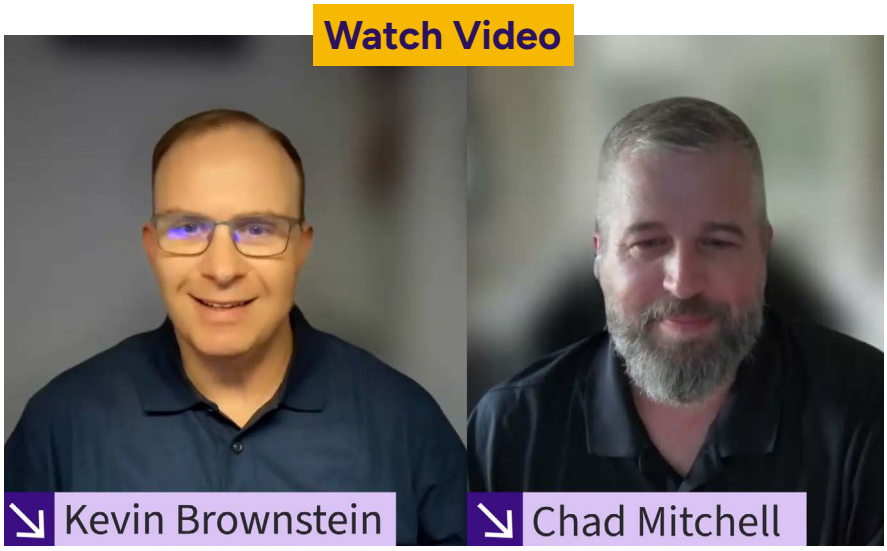
RegScale's AI-powered CCM platform transforms GRC by automating compliance, reducing costs, streamlining processes, and integrating seamlessly into DevSecOps for faster, more efficient risk management.

Learn more about RegScale.

RegScale

carahsoft

Comply-to-Connect Concept Drives Greater Situational Awareness



The Defense Department's Comply-to-Connect, or C2C, program will play a critical role in improving the security of defense networks in the years ahead. The goal is to create an automated process for verifying that every endpoint device is authorized and meets critical security requirements before allowing it to access the network — and ensure it stays in compliance. But to work effectively, C2C hinges on automating an array of cyber capabilities, said Chad Mitchell, a Systems Engineer for U.S. Public Sector at Cisco.

The payoff, however, can be significant. C2C processes generate a wealth of data that, pulled into a central repository for reporting requirements, provides unprecedented situational awareness on all aspects of the infrastructure, said Kevin Brownstein, Senior Manager for Security Solutions Architecture at Splunk, a Cisco company.

In this video interview, Mitchell and Brownstein discuss how agencies across the public sector can build on the C2C vi sion to develop greater visibility into the network infrastructure. Topics include:

- → The value of a C2C solution for civilian agencies
- → Using C2C data to support advanced cyber automation
- → Extending C2C data to support other cyber use cases

"Whether we're looking at C2C ... or whatever is on the horizon beyond that, we're in this state now where a solution to a problem is never just a single product. It's always going to take an integrated solution."

— Chad Mitchell, Cisco

About Cisco

Discover how Cisco helps organizations securely connect and protect everything in the AI-powered world.

Learn more about Cisco.

About Splunk

Splunk, the cybersecurity and observability leader, helps build a safer and more resilient digital world. Organizations trust Splunk to prevent security, infrastructure and application incidents from becoming major issues, remediate threats and disruptions faster, and adapt quickly to new opportunities.

Learn more about Splunk.

cisco DISTRIBUTOR splunk> a CISCO company carahsoft.

Additional Resources

Check out GovLoop's previous guides for more about the state of cybersecurity.

Preparing Agencies for Cyber Disruptions: How to Build Resilience

Government agencies are long past imagining they can stop all cyber threats and incursions, but that doesn't mean they need to give up. The secret is resilience — the ability to contain and recover from attacks with minimal downtime. This guide examines how to foster resilience inside an agency and defend against the threats outside it.

The AI Cyber Arms Race Is On

Government agencies know what they are up against. Malicious actors are leveraging AI to launch a higher volume of attacks and make attacks more targeted and harder to detect. This guide explores recent developments that will shape security strategies in 2026 and beyond.

Focus on Cyber Force Multipliers

Cybersecurity teams, like everyone in government, deal with tight budgets and staffing limits. At the same time, the IT environment is growing more complex and the cyber threats more sophisticated. This guide explores technologies and tactics that can serve as force multipliers for cyber teams, helping them do more with less.

About GovLoop

GovLoop's mission is to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

Thank You

Thank you to Anchore, Auth0, Carahsoft, Cisco, CrowdStrike, Illumio, Palo Alto Networks, RegScale and Splunk for their support of this valuable resource for public-sector professionals.

Authors

Lauren Walker, Senior Staff Writer

Candace Thorson, Managing Editor

John Monroe, Director of Content

Designer

Kaitlyn Baker, Senior Creative Manager