Arizona’s lessons learned from its whole-of-state cybersecurity strategy

Introduction

Tim Roemer, Arizona's former CISO and Director of the Arizona Department of Homeland Security, shares firsthand advice on implementing a whole-of-state cybersecurity strategy.

> "We're all going to struggle with sophisticated attacks, workforce development challenges, and other cybersecurity problems. But by coming together, we can solve these problems as one large team."

During his time as Arizona's CISO and Director of the state's Department of Homeland Security, Roemer had to defend Arizona against a wide range of cyberattacks — including complex, well-funded attacks from nations like Russia and China. The team must defend against a large attack surface filled with ever-growing vulnerabilities. And they must do all this across a complex, fragmented set of agencies and institutions.

To do so, they implemented a **whole-of-state cybersecurity strategy.**

In this eBook, we dig into the details of how they successfully brought this strategy to life and the real-world ways it's made Arizona safer.

Cybersecurity is Homeland Security

Roemer began his career with "one really good internship" with the CIA. He was passionate about counterterrorism so he spent 10 years with the agency.

During the final two years of his tenure, he gave national security updates to the President, Vice President, and National Security Council. Those meetings exposed him to the reality of nation-state cyberattacks and the importance of cybersecurity.

Roemer left the CIA and returned to his home state of Arizona. "I wanted to work on security issues that affected friends and family in my own backyard," he explains

He first worked as the deputy director of Arizona's Department of Homeland Security and was eventually appointed the state's CISO and Director of the Arizona Department of Homeland Security.

When Roemer took on these roles, he received two mandates from the Governor - expand statewide cybersecurity and bring it under the Department of Homeland Security because cyber security is homeland security.

> "In state and local cybersecurity, we're expected to hold off national militaries with unlimited resources from around the world — all day, every day."

Fighting a battle with no borders: Why cybersecurity matters to states like Arizona

In some ways, the deck is stacked against states like Arizona. State cybersecurity leaders must meet a far different set of expectations than physical security leaders.

"In no way is the state of Arizona expected to defend our physical border from a nation-state," he explains. "If Russia was physically trying to invade Arizona's southern border, I don't think people would expect us to be able to hold them off."

The opposite is true for the state's cybersecurity efforts.

"In cybersecurity, we're expected to hold off the Russian military, as well as the Chinese, the North Koreans, the Iranians … you name it," Roemer says.

This creates a fundamentally different set of pressures for Roemer and his teams.

"This is why cybersecurity is so important right now — because it has no borders," he explains. "People can attack you with unlimited resources from around the world, and you have to defend against all of it — all day, every day."

To meet these expectations — and to secure his state against a wide range of well-funded global attackers — Roemer needed to make a bold move.

Bringing a whole-of-state cybersecurity strategy to Arizona

Arizona's Governor didn't appoint Roemer to just keep the trains on the tracks. He appointed Roemer to transform how the state approached cybersecurity.

"The governor appointed me to break the status quo and to try new things," Roemer explains. And that process began with an honest evaluation of the current affairs.

"I'm a big believer that you need to know your strengths and your weaknesses," he says. "You can play to your strengths, but your adversaries are coming after your weaknesses — and I knew we had weaknesses and vulnerabilities they could exploit."

Like nearly every state, Arizona had a fragmented approach to cybersecurity. Each agency and institution used its own processes and tools. And best practices built at the state level were not reaching the local level. And no one communicated enough.

Thankfully, Roemer had a solution.

"I saw that implementing a whole-of-state approach would help everyone," he explains. "If state and local leaders could 'buddy up,' come together, and start sharing resources, information, and best practices, then we'd be in a better position."

Whole-of-state is an emerging security strategy. In it, leaders at every level of a state's government collaborate around security issues. The strategy has many goals, but for Roemer, a successful program came down to one thing — increasing teamwork.

"Cybersecurity is a complex problem, and no one has all the answers," he says. "Whole-of-state is important because it's about teamwork. It's about collaborating and bringing the good guys together to fight back against the bad guys."

> **"Whole-of-state is ... about bringing the good guys together to fight back against the bad guys."**

Making whole-of-state real: Focusing on four key elements

Roemer built a successful whole-of-state program by focusing on four elements.

1

Adopt a flexible, long-term mindset

“Whole-of-state — and cybersecurity in general — is a work in progress. We’re fighting an evolving threat, and it changes every day. The moment we think we have it all figured out is the moment when we’re going to get hit,” Roemer says.

2

Build relationships before you need them

“You need to get out of your office. You need to meet people and develop enough trust and collaboration to bring more people to the table — and you have to do it ASAP. We always say within our field, ‘You can’t be passing out business cards in an emergency. At that point, it’s too late,’” Roemer says.

3

Figure out the funding

“You need a grant program. Thankfully, the state of Arizona saw what we were up against in cybersecurity, and we came up with $10 million per year to help school districts, tribes, city, and county governments, and everyone else build cyber resiliency,” Roemer says.

4

Keep governance top-of-mind

“We have a cyber grant task force that’s a two-way street. We listen to locals about their needs, we provide them with solutions, and we find ways to implement those solutions. Our committee and task force travel the state to have those conversations, to pair the right tools with the right organizations, and to make sure those tools work,” Roemer says.

Arizona's whole-of-state goals and outcomes

Roemer evaluated the whole of state program against a set of critical goals and outcomes.

Already, Arizona's whole-of-state program has generated some meaningful benefits — especially when it comes to information sharing at different levels of government.

"I can't protect 7.5 million Arizonans' data from an attacker I don't know about," Roemer says. "But with whole-of-state, we're now sharing information in real time. I'm stronger as a CISO because I know what other people are seeing, and locals are better protecting themselves from attacks we're seeing at the state level."

No incidents
"What I really want to show is zero successful cybersecurity incidents against our local governments."

Faster remediation
"We want to accelerate our ability to identify and remediate our vulnerabilities."

Measurable improvement
"We want to use metrics to paint a picture about how we're helping organizations better secure themselves than before."

Full utilization
"We hope to see local governments spend every dollar that the state has given us."

More funding
"My goal is to start with the $10 million, prove it's effective, show we're getting good ROI, and then advocate for more funding."

Lessons learned: The need for clear strategy and communication

Building a whole-of-state program has been a daily learning experience for Roemer.

“I’ve just tried to be a sponge and learn everything I can,” he says.

Yet two big lessons stand out for Roemer.

“You have to build comradery amongst the team,” he explains. “Cybersecurity is a very stressful arena to work in right now, and its challenges are extremely difficult. It’s critical to make sure the entire whole-of-state team knows why we’re doing it, what’s at stake, and how we’re going to combat our threats.”

For Roemer, building this true team effort depends on one thing — communication.

“You have to effectively communicate what the strategy is,” he says. “We found that anytime someone didn’t support this program, it was because they didn’t know who we are, what we’re doing, why we’re doing it, how we’re doing it, and what tools we’re giving them.”

Ultimately, the two lessons work hand in hand.

“When everyone knows your strategy — and you communicate it effectively — they come to the table very quickly, and we build good partnerships that keep us safer,” Roemer says.

How a Cyber Command Center drives a whole-of-state strategy

Whole-of-state doesn't just happen.

It requires a coordinated effort to connect, train, and centralize cybersecurity resources across multiple departments, roles, and levels of government.

To make this a reality, Roemer went beyond email chains and web portals. He built a physical Cyber Command Center to be the hub for all cybersecurity efforts in Arizona.

"The Cyber Command Center is located within our state Fusion Center, which is the Arizona Counter Terrorism Information Center (ACTIC)," Roemer explains. "This gives us a one-of-a-kind cyber capability that no other state has at this level."

As Roemer explains, the Cyber Command Center serves multiple purposes and has improved multiple elements of Arizona's cybersecurity efforts. It has:

- **Improved incident response capabilities.** "It gives us the ability to be under one roof with our National Guard response partners and our Department of Public Safety, and it's increased our ability to collaborate with law enforcement and to share information with locals. This gives us surge capacity during cyber incidents and has been great for response from an operational perspective."
- **Created a home for cybersecurity training.** "Real-world scenarios are coming at us quickly, and we have to stay ahead with proper training of our cybersecurity leaders and practitioners at every level of government. We now have a single, central, and effective training facility for all things cybersecurity, and we just didn't have anything like it before."
- **Made a statement.** Symbolically, it shows everybody from around the state that when we said 'cybersecurity is Homeland Security,' we meant it. We put our money where our mouth is. It helps us build trust with our local partners because they see us practicing what we're preaching, and then they want to be part of these programs."

Arizona's new Cyber Command Center offers a tangible example of how a whole-of-state strategy can be brought to life and solve significant cybersecurity challenges.

Three areas where whole-of-state has made Arizona more secure

Roemer shares two areas where an effective whole-of-state strategy has meaningfully improved Arizona's cybersecurity capabilities.

Accelerated incident response

"One of the hardest things about responding to a cyber incident is doing so quickly because minutes really matter," Roemer explains. "We need to respond quickly, with as few surprises and delays as possible — and whole-of-state lets us do that."

For Roemer, whole-of-state accelerates incident response by building the relationships you need to tap during an incident before the incident occurs.

"With the whole-of-state approach, we know who we're working with, and they know us," he says. "They know who's going to be responding. We have the MOUs and NDAs signed. We're practically on a first-name basis. Having these relationships in place lets us share resources and work together during an incident to resolve it fast."

Closing the cybersecurity skills gap

"Workforce development is probably the single biggest cybersecurity challenge worldwide," Roemer explains. "Not having enough people with the right skills contributes to every other problem that CISOs are struggling with."

Roemer's found a whole-of-state approach helps to solve the cybersecurity skills gap.

"Whole-of-state is all about collaboration and teamwork," Roemer says. "If you lack a few cybersecurity FTEs, you're going to be in a better position with a whole-of-state strategy because you're sharing resources and information, you're working smarter to address the issue, and you can leverage skills from other larger, fuller teams."

Making government cybersecurity a fair fight

Even small municipal governments might come under attack from entire nation-states. Whole-of-state evens those odds.

"By coming together, we become one large team," Roemer explains. "An attack on a local school district in Flagstaff, Arizona, is an attack on me, the CISO of the state. They may feel that they're at a huge disadvantage, but they've got others in their backyard with the State of Arizona assisting."

And the more local groups join the whole-of-state program, the bigger the support becomes for every member of the government's cybersecurity efforts. "Beyond the state level, I've also got 15 counties to back me up, and that's not even counting the cities and school districts," Roemer says.

For Roemer, this final point is key for driving home the benefit of whole-of-state.

"This is why whole-of-state is so important when it comes to tackling modern cybersecurity problems — from solving workforce development challenges to pushing back against nation-state attacks. It makes cybersecurity a much fairer fight for everyone."

Conclusion

Cybersecurity threats continue to increase in frequency and sophistication. Fortunately, even small government entities can improve their security hygiene by participating in a whole-of-state cybersecurity strategy. By implementing these broad, inclusive strategies, states can ensure that every government entity has the best training, tools, and insights available to protect their data and infrastructure and to pursue their missions.

Take a deep dive into whole-of-state cybersecurity.

LEARN MORE

At the time of this interview, Tim Roemer was the CISO and Director of the Arizona Department of Homeland Security. He recently left that position and now works in the private sector.