Cybersecurity Through Collaboration

How Governments Can Work Securely With Each Other — And Their Partners

The growing volumes and severity of cybersecurity threats are making it harder than ever for state and local governments to ensure the safety and security of their communication channels. In this Q&A, former Utah CIO Michael Hussey, now an Oracle industry executive director for state and local strategy, discusses techniques for collaboration and opportunities to address long-standing barriers.

What are some of the most critical cybersecurity challenges faced by state and local governments?

The number of attempts is increasing at an exponential rate, while at the same time the playbook is evolving for bad actors. These cybercriminals monetize their efforts by infecting systems with ransomware and then holding them hostage.

The other half of the equation is that governments don't have the resources, especially if they're trying to go it alone. Some jurisdictions are having trouble even finding IT help; I heard of one who hired a high school senior to help with their challenges.

In what ways can federal, state and local jurisdictions collaborate and learn from each other, and what are the obstacles?

In Utah, we stood up all our state resources under one roof in partnership with our federal partners in the Utah Cyber Center, where we can broker the resources needed.

The obstacles are largely self-imposed hurdles, often more for political than technical reasons. It takes time for everyone to understand there's an opportunity to come together and fight the common enemy. That's really how you solve the resource challenge.

Election security continues to be an area of concern. How can governments use election security efforts as a springboard for broader collaboration?

It was election security that really helped us break down some of those barriers. A lot of jurisdictions come together just for an election to occur, so how do you make sure there's a unified approach?

We brought in the Department of Homeland Security to do penetration testing of county systems through the Utah Cyber Center, then held personal meetings in the counties to help them plug any holes. We were focused on elections, but we actually looked at other county issues, and also received help from the FBI. This method was the icebreaker, and a great model going forward.

What lessons learned during the COVID pandemic will help safeguard constituent data going forward?

You're trying to respond to a pandemic and save lives, and at the same time you're trying to balance the privacy concerns. Our first app did contact tracing, but the data was not private. Months later, IoS and Android devices were enabled to anonymize the data. But the pandemic underscored what we already knew: Governments have a lot of confidential information, and keeping it safe should be a top priority. That's why cybersecurity is the No. 1 goal for state CIOs in every survey — and it should be.

How can cloud-based solutions simplify the process of securing data and systems for governments?

When you start to partner with major cloud providers, you're leveraging the resources these providers have baked into the solution. The guardrails are there, and countless staff hours have gone into protecting and securing the data. Cloud-based solutions take the worry off the table so you don't have to find yourself outside those guardrails.

Governments should make sure they leverage one another's resources at each level, use a system like elections to start breaking down those self-imposed barriers, and take advantage of the support of your partners. That's how to improve your posture across all these areas.

Oracle offers integrated suites of applications plus secure, autonomous infrastructure in the Oracle Cloud. Learn more about Oracle for state and local government at **oracle.com/stateandlocal**.

ORACLE