carahsoft®

TOP 5 TAKEAWAYS: What It Takes for State and Local Governments to Stay CYBERSMART

On the road to digital transformation,

government agencies have had pit stops, flat tires and have occasionally run out of gas. With more cargo, or data, to transport than they know what to do with, agencies rely on more online critical infrastructure to store and manage the nation's most vulnerable assets — bringing more risk along for the ride. How can federal, state and local governments protect against the ongoing and ever-evolving risks that come with an advancing technological landscape? In its **2019 CyberSmart live event series**, IT provider **Carahsoft** took a road trip across the country to five different cities to talk security culture, partnerships and policy, ultimately paving the road forward for agencies looking to implement sturdy cybersecurity postures that don't sacrifice innovation.

Want to learn more? Read our takeaways from each city.

Pictured from left: Dr. Abi Salimi, Assistant Professor, Computer Science, University of North Georgia; Ria Aiken, Director, Office of Emergency Preparedness, City of Atlanta; and Richard Cox, Chief Operating Officer, City of Atlanta"

ATLANTA: *Agencies Should Cultivate a Future-Focused Cyber Culture*

When it comes to keeping up with security, there's enough new threats and attack vectors each day to keep any security team busy. But by teaching employees the knowledge they need to stay secure, agencies can make tackling tomorrow's threats that much easier, said experts at the Atlanta Cybersmart event, **"Cultivating a Future-Focused Cyber Culture."**

Ultimately, by creating and promoting a culture of cyber awareness, government decision-makers can open the doors to new and more effective processes that protect vulnerable cyber information and, most importantly, citizens.

"You can talk about problems from all angles," said Eric Toler, **executive director of the Georgia Cyber Center.** "If you just look at our processes, institutional processes, government, academia and private industry, those processes are not allowing us to keep pace with our competitors."

Georgia's Cyber Center, which opened in Augusta, Georgia in July 2018, aims to create an environment where government, academic and private sector IT leaders can share and solve security problems, explains Toler. The center acts as a central state resource to promote cyberhealth and research. "We want to deliver affordable and relevant education and training," said Toler.

Aside from creating a central resource for technical troubleshooting, Toler notes the center also seeks to address **another challenge:** Georgia's approximately 11,600 unfilled cybersecurity jobs.

"Everybody's looking for the unicorns out there, trying to hire the best and the brightest," said Toler. "But they don't exist, or they've already been hired and we're trying to steal talent away from each other. We've got to change our processes and design secondary education to start producing these individuals."

Another key component of a future-proofed cybersecurity culture comes with developing a response structure that allows agencies to not only detect attacks quickly, but also respond accordingly. After a cyber attack **greatly impacted the city of Atlanta last year,** Richard Cox, Atlanta's former chief operating officer, recognized the importance of quick and transparent decision making.

"We were at a decision point pretty quickly," said Cox, who noted that the impact of the attack spread quickly throughout government systems. "One of the most important decisions was to be transparent. We convened city council and had a press conference that day." From there, Cox worked to understand the key players with credibility to defend against the attacks, and pinpointed the processes within the city to act on immediate needs by working with third parties.

"We've got to change our processes and design secondary education to start producing these individuals."

- Eric Toler, Executive Director, Georgia Cyber Center

The experts explained that cultivating a secure infrastructure and stronger cybersecurity culture relies on a combination of IT talent, smart technology investments and strategic partnerships.

"You build a dedicated workforce and you leverage the core competencies of that workforce," said Col. Eric Aslakson, the chief of requirements and integration at the U.S. Army Cyber Center of Excellence. "You build partnerships. You harness the technology and commercial investments in infrastructure. Don't build and bake your own."

AUSTIN: *Cybersecurity Preparation Requires Adaptation*

Preparation is key to enabling secure innovation — but it isn't simple. This was the theme of the Austin Cybersmart event: **"Preparedness and Proactive Threat Response."**

The state of Texas is constantly on high alert, with billions of cybersecurity attacks per month targeting the state's 220 agencies, says Texas Rep. Giovanni Capriglione, District 98. About two months ago, an attack targeted Del Rio, a small city outside of San Antonio, shutting down about 200 computers in the city's systems. "Fortunately, the Department of Public Services had gone in and invested $5 million to beef up their systems the previous year," says Capriglione. "The team helped the city get the right level of support to get up on its feet. The lesson in this is that this was a small city, and it took most of that one team that we had."

For Capriglione, this pointed toward the importance of training. Regular security trainings can prepare city staff for attacks, allow IT teams to develop and tweak response plans appropriately and help agencies better understand the role private sector players can provide in moments of stress and strained resources.

Moreover, outside of emergency situations, a cybersecurity response plan can offer stability and guidance for decision-makers in pivotal moments. The state of Texas is one year into its **strategic cybersecurity plan**, which highlights five key goals: engagement, tooling, staffing, response and outreach.

"Engagement is the thing you have to do first," says Andy Bennett, Texas' deputy chief information security officer. "When you talk about engagement in the context of the state security plan, that means engagement with leaders at the top and with policy makers. If you don't have it, you will get nothing done."

Ultimately, preparation means more than just acquiring new tools — it means working with partners to understand those tools and how to best apply them in fluctuating situations.

"You have to tie everything together and actually respond to an incident," says Bennett.

"The plan isn't a list of actions, but a list of goals with sample outcomes. It's something that all of us can align with to make sure we're going in the same direction and not swimming against each other."

-Andy Bennett (above), Texas Deputy Chief Information Security Officer

LOS ANGELES: *Harness the Power of Cybersecurity Partnerships*

As the nation's second-largest city, Los Angeles provides protection for millions of citizens while pioneering new tools and processes to ensure the security of critical information assets.

"Cyber risk has existed as long as technology has existed," said George Khalil, chief innovation officers for the city of Riverside, California, during the Los Angeles Cybersmart event: **"Strengthening Security Posture Through Partnerships."** "In this day and age, our borders and perimeters are essentially dissolving where we're moving into the cloud. Our users are mobile — going home, working remotely, going to conferences and connecting to external networks. Our attack vectors have expanded significantly."

To keep up with this evolving threat landscape, prevention is ideal, but detection is a must, said Khalil. For state and local governments, improving detection means bringing in new methods of thinking and communicating, which hinges on strong collaboration and information sharing practices.

"We think of partnerships as how industry is impacted and how it impacts us," says Dr. Clifford Neuman, director of the USC Center for Computer Systems Security. Neuman pointed toward the ports of Los Angeles and Long Beach, where the cities and private companies would both receive impact from cyber attacks within the same vicinity. A partnership between the two, in this case, bolsters the area's cybersecurity infrastructure.

With access to appropriate, shared information, governments can embrace more nimble and agile approaches to cybersecurity problems.

"Information sharing is key to identifying, responding, restoring and recovering from any crisis, especially in the cyber arena," says Jim Featherstone, president and CIO of the **Los Angeles Homeland Security Advisory Council**, a nonprofit organization that facilitates public safety collaboration. Featherstone's team works actively to convene with the private and public sector to address cyber issues as they start to look forward.

"We had been working with the mayor's office when the **command center** was stood up," Featherstone said. "Using our influence and our outreach among the private sector community, we began to multiply the participation of the private sector. Government does a lot of things well, but the government doesn't always have the ability to reach out and bring in non-governmental partners."

"Information sharing is key to identifying, responding, restoring and recovering from any crisis, especially in the cyber arena."

-Jim Featherstone, (below) President & CIO
LA Homeland Security Advisory Council

DENVER:
Cybersecurity Is an Everyone Problem

The Carahsoft CyberSmart Smart Series stopped in Denver for its event entitled **"Protecting Citizens through Vigilant Threat Prevention.I"** which addressed how innovation, awareness, training, vigilance and can leverage partnerships can work together to help the public sector secure critical assets.

"This is not a 'me' problem, this is not a 'you' problem, or a 'they'[problem — this is an 'us' problem," says Ike Barnes, assistant to the Special Agent in Charge, Electronic Crimes Task Force in the U.S. Secret Service Denver Field Office. "Without all of us collaborating our resources together, sharing information and talking cross sector about what the threats are and what some possible solutions are, we aren't going to help solve this problem."

When it comes to cybersecurity, the speakers emphasized the need to include security into systems, policies and practices from the ground up. "You have to build in security by design as your protocol," said Barnes, noting that adhering to **National Institute of Standards and Technology** frameworks often doesn't go far enough. "You may pass the audit but you're running to the lowest common denominator. You need to take the next step for extra security, and make sure it's worth your investment."

Barnes emphasized agencies' need to articulate and monitor their most critical assets, pinpoint their threat actors and their techniques, and identify the tools in that environment that are specific to that agency's needs and legacy infrastructure.

Baking security into infrastructure and IT can prevent cyber incidents, instead of tacking it on as an afterthought, which plays a major role in building security by design, explained Greg Sternberg, the chief information security officer for the Denver Information System Security Association.

"Security is not just there at deployment or at writing code, but when somebody in another department has an idea or roles out a new tool, let's put security on there as well. That's where it needs to start," he noted.

WASHINGTON, DC: *Match Modernization with IT Security*

Modernizing IT and enabling digital government are hot topics for federal government agencies, underlined by new legislation that encourages innovation. But incorporating new and emerging technologies, such as 5G and artificial intelligence, comes with risks that IT leaders should be conscious of throughout the modernization process.

"With all the things like AI, drones and whatever you may use to make the new bigger pipeline more reliable, you can't forget about that you need to secure it first," said Vincent Sritapan, the program manager for the Science and Technology Directorate at the Department of Homeland Security, speaking at the D.C. Cybersmart event: **"Priorities in Securing Tomorrow's Federal and Defense Landscape."**

For Sritapan and others security and innovation should go hand-in-hand." Across the board, we're leveraging regulatory executive orders and trying to work with public private partnerships to really look at innovation," said Sritapan. This can mean reevaluating partners, setting guidelines to test out and understand the level of trust between partners, or noting vulnerable supply chain areas that leave room for compromises.

"In order to get to where America can innovate, we have to make sure the core of the infrastructure and the devices themselves are secure."

-Vincent Sritapan, Program Manager, Science and Technology Directorate, Department of Homeland Security

By doing this, IT leaders can ensure today's advances don't become tomorrow's vulnerabilities.

"As we have an eye to tomorrow, we also need to keep an eye to today," said Curtis Dukes, executive vice president of security best practices at the Center for Internet Security.

Pictured from Left: Curtis Dukes, Executive VP of Security Best Practices, Center for Internet Security; Jeff Harris, Chief Information Security Officer, Small Business Administration; Amélie Koran, CTO, Department of Health and Human Services Office of the Inspector General; Vincent Sritapan, Program Manager, Science & Technology Directorate, Department of Homeland Security; and Ian Wallace, Director, Cybersecurity Initiative, New America