Public Sector Cyber Leader Summit

Wednesday, October 26, 2022
Washington, D.C.

9:00-9:30 am  Registration and Continental Breakfast

9:30-9:45 am  Welcome and Highlights from the CompTIA PTI 2022 Local Government Cybersecurity National Survey: The Top Cyber Issues and Priorities for America's Cities and Counties
The Cyber Leader Summit kicks off with an update on the employee awareness, cyber budgeting, policy issues, access management protocols, cyber insurance, and leadership support issues impacting local government cybersecurity programs.
- Alan Shark, Vice President, Public Sector, CompTIA and CompTIA PTI Executive Director

9:45-10:15 am  Show Me the Money! The Latest on Federal Cyber and Grant Funding Initiatives
There is much anticipation – and confusion – regarding cyber funding opportunities that are being made available through the Investment in Infrastructure and Jobs Act, and other proposed federal initiatives. During this discussion we will provide an update on how the funding programs will work, what local governments can expect, and what IT can do now to hit the ground running when funding is released.

10:15-10:45 am  Cloud and Managed Services Providers: Security Threats and Opportunities
More government agencies are partnering with cloud and managed service providers to increase operational efficiency. At the same time, these services, just like public agencies, are facing increasing threats from adversaries. IT executives can't take a hands-off attitude with their private sector partners. We will explore the questions to ask when choosing a partner, how to improve communications and ultimately build the necessary level of service and trust that is needed to ensure effective cloud security.

10:45-11:00 am  Networking Break

11:00-11:30 am  Does Cyber Insurance Still Make Sense? Can You Afford Not to Have It?
This discussion will explore the changing cybersecurity market and its impact on public sector agencies. Insurance premiums are rising, for some coverage may be inadequate, and requirements set by providers are becoming more stringent.
We will look at how cyber insurance can still be an important tool in an organization's overall cybersecurity strategy - while reinforcing that insurance is not the only defense, the ultimate security blanket that many consider - or hope it to be.

11:30am-12:00 pm  IT Cyber Modernization: What is Working and What is on the Horizon?
To mitigate risk public sector agencies and their private sector partners need to invest in new tools and technologies. We will explore some of the leading-edge tools and practices, to include AI, automation, cloud computing, and Agile development — to ensure a more resilient and adaptable cybersecurity posture.

12:00-1:15 pm  Keynote Lunch: It's Not Just Today but Tomorrow, and the Year After:
Chuck Brooks, a leading evangelist for cybersecurity in both the public and private sectors will share how the trends and threats that are impacting cyber resiliency today can help build a stronger cyber strategy for tomorrow.

1:15-1:30 pm  Networking Break

1:30-2:00 pm  Why is Phishing Still So Successful? Strengthening Cyber Awareness Programs
Humans still account for over 80% of all cyber hacks and phishing continues to be the number one entry point. The speed of a click is very tempting and dangerous. Learn how local governments have beefed up their cyber awareness programs.

2:00-2:30 pm  The Latest Resources and Tools to Help the Public Sector Improve Cyber Resiliency
Organizations engaged in information sharing related to cybersecurity risks and incidents are an important resource for public sector entities. This discussion will highlight the variety of resources - many free - that are available to help public sector entities meet the threats of cyber adversaries.

2:30-3:00 pm  The CIO-CISO: Key Success Leadership Relationship Factors
The relationship between the CIO and CISO can be tense, as the CIO wants to create new IT relationships and service opportunities, while the CISO is concerned about risk. This case study will look at how an effective partnership can be developed and sustained; built on the foundations of trust, the alignment of goals and objectives, and a sound governance strategy.

- **Adam Frumkin**, CIO, Franklin County, Ohio Data Center; CGCIO; Chair, CompTIA PTI City/County Tech Leader Forum
- **Nikki Milburn**, CISO, Franklin County, Ohio Data Center

3:00-3:15 pm  Networking Break

3:15-4:15 pm  Cyber Leader Speed Dating with Outcomes!
Breakout discussions will address Challenges and Opportunities in four main areas (Cyber Workforce, Emerging Technology and Cybersecurity, Cybersecurity and Procurement, and Cybersecurity Policy) with the intent to help CompTIA PTI
and the CompTIA Public Sector Cybersecurity Committee develop its research agenda for 2023.

4:15-4:45 pm  **Breakout Group Findings and Recommendations**
Each of the breakout groups will report on the top issues they identified.

4:45-5:15 pm  **Call in the National Guard!**
The National Guard's cyber force can be a valuable partner for local governments; cyber soldiers are trained to conduct computer network defense, detect malicious activity, and to assist in recovery efforts. Yet many IT executives may not know how to properly use National Guard units deployed to help them in a crisis, due to a lack of knowledge of National Guard capabilities and organizational structure. This discussion will highlight the capabilities and expertise that can be deployed to the greatest advantage in a cyber crisis.

5:15-5:30 pm  **Closing Remarks**
- Alan Shark, Vice President, Public Sector, CompTIA

5:30-6:30 pm  **Networking Reception**