Virtual Event

Cyber Security & Risk Management

PUBLIC SECTOR NETWORK

Certified B Corporation

Government Cyber Insights: Summer Edition

Adapting for More Resilient Enterprise in the Next Normal

Online → Thursday, September 29, 2022 | 12:00 - 2:40pm ET

Your Inspiring Speakers

RAY YEPES
Chief Information Security Officer
State of Colorado Governor's Office of Information Technology

CHRIS LETTERMAN
Chief Information Security Officer
State of Alaska, Department of Administration

JENNY HEDDERMAN, ESQ.
State Risk Counsel
Comptroller of the Commonwealth of Massachusetts

ANTHONY RODGERS
Director of Technology Transformation Services
State of Michigan Department of Technology, Management and Budget

WILLIAM CHUMLEY
Chief Customer Officer
State of Colorado Governor's Office of Information Technology

ABEL ABEYTA
Chief Information Security Officer
State of New Mexico Taxation and Revenue Department

WHITNEY PHILLIPS
State Privacy Officer
State of Utah

SHAWN KINGSBERRY
Vice President, Cyber
SAIC Digital Innovation Factory

FADI FADHIL
Cyber Security Strategist
Palo Alto Networks

Benefits of Attending

Gather insight from public sector thought leaders on topis as **privacy awareness, ransomware, and mitigating cybersecurity risks**

Discuss best practices for **top-notch cybersecurity measures to prevent data breaches and online frauds**

Best practices to **build a cyber resilient workforce**

How to **maximize your cybersecurity investment with an outcome driven approach**

CLICK HERE TO REGISTER

Adapting for More Resilient Enterprise in the Next Normal

It was not too long-ago that governments could have robust discussions regarding technology without even mentioning cybersecurity. Today, government institutions have substantial assets and value manifested in digital form, and they are deeply intertwined with remote technology networks. Many acknowledge the serious threats that cyberattacks pose to the public sector; but cybersecurity is no longer something just for technologists to think about. In 2022, it is the responsibility of all team members regardless of their title.

Cybersecurity has always been a never-ending race, but the rate of change is accelerating. The Public Sector is continuing to innovate, which requires investments in technology. Now, we are layering more systems into networks to support remote work, enhancing the customer experience, and generating additional value for the public; all of which creates potential new vulnerabilities. How do you address privacy awareness? What barriers exist to true ransomware defense? And how to mitigate broad based cybersecurity risk?

These are among the questions we will explore at Public Sector Network's Virtual Event: **Government Cyber Insights: Summer Edition**. We will spotlight industry thought leaders and their cyber defense initiatives from across the United States.

Who You'll Meet

Departments: IT, IS, Administration, Transportation, Finance/Treasury, Healthcare, Social Services, Education, Law Enforcement, Public Safety, HR

Commissioners/Chiefs/Deputy Chiefs/Directors/Deputy Directors/Managers of:

- Cyber Security
- Information Security
- Digital Technology
- Digital Service Delivery
- Enterprise Infrastructure
- Innovation
- Enterprise Applications
- Privacy
- Security
- Digital Applications
- Information Technology
- Technology
- Digital Transformation
- Learning & Development

Explore the Agenda

12:00pm ET **Welcome from Public Sector Network**

12:05pm ET **Welcome from Chair**

Shawn Kingsberry, *Vice President, Cyber,* **SAIC Digital Innovation Factory**

12:20pm ET **Government Keynote:**

Risk & Reward: Cybersecurity and Privacy Awareness

Privacy awareness is a crucial component of cyber protection for the public sector – as it helps to define the overall privacy culture in an organization. Mechanisms in place will help to educate employees about the importance of protecting personal data and the potential consequences of not doing so.

- Speaking to Leadership about the importance of cyber and privacy protections
- Ascertaining your cyber perimeter
- Developing a risk-based approach to mitigation.
- Budgeting for Cybersecurity/Privacy/Insurance
- Privacy and Cybersecurity Internal Controls

Jenny Hedderman, Esq., *State Risk Counsel,* **Comptroller of the Commonwealth of Massachusetts**

12:40pm ET **Platinum Partner Session:**

Fadi Fadhil, *Cyber Security Strategist,* **Palo Alto Networks**

12:55pm ET **Panel Discussion:**

Your Data Has Been Kidnapped: Should You Pay the Ransom?

Ransomware attacks have increased dramatically since the beginning of the pandemic. The Colonial Pipeline paid hackers $4.4 million in ransom for a decryption tool that restored oil operations, despite FBI and DHS recommendations that companies avoid paying ransoms. The CEO went before congress to explain that the ransom had to be paid (due to the effects of a declining fuel supply), but it remains a controversial solution.

In the current threat landscape, preparing for cyberattacks and building resilience against hackers must become part of the public sector's infrastructure. But what should the government do in the case of an attack when its own systems and data are on the line?

Abel Abeyta, *Chief Information Security Officer,* **State of New Mexico Taxation and Revenue Department**

Chris Letterman, *Chief Information Security Officer,* **State of Alaska, Department of Administration**

1:25pm ET **Break**

1:30pm ET **Government Case Study:**

How to Approach Cybersecurity Through a New Lense

The State of Colorado Governor's Office of Information Technology has made cybersecurity resilience a top priority. The full scope of cybersecurity needs to be examined. This includes ransomware, infrastructure, risk identification, and your data management. The solution is to approach this with a new lense, anticipating the emerging cyberthreats of the future and understanding the mechanisms today that Colorado can use. Join Ray Yepes, Chief Information Security Officer, and William Chumley, Chief Customer Officer as they provide insight into how consider different approaches to cybersecurity.

Ray Yepes, *Chief Information Security Officer,* **State of Colorado Governor's Office of Information Technology**

William Chumley, *Chief Customer Officer,* **State of Colorado Governor's Office of Information Technology**

1:50pm ET **Panel Discussion:**

It is a Team Sport: How the Public Sector Can Combat Cybersecurity Risks

News of data breaches and online frauds has become a matter of regular occurrence, which serves as a constant reminder that leadership needs to involve the entire team in a strategy for preventing cyber intrusions.

Moreover, successful cyber-attacks are often the result of insider mistakes, such as through phishing emails or business email compromise.

The panel will discuss ways to guard against cybersecurity threats:

- Create a culture of cybersecurity awareness - Employees should be empowered with the skills they need to be proactive and ready to face increasing threats.
- Establish a cybersecurity council – How your agency can gain insights from others to formulate your own public sector policies.
- Cybersecurity Insurance – Perspectives, value, outcomes, and alternatives

Anthony Rodgers, *Director of Technology Transformation Services,* **State of Michigan Department of Technology, Management and Budget**

Whitney Phillips, *State Privacy Officer,* **State of Utah**

2:20pm ET **Closing Remarks from the Chair**

Shawn Kingsberry, *Vice President, Cyber,* **SAIC Digital Innovation Factory**

2:25pm ET **Virtual Event Adjourns**

Thank you to our Event Partners

Chair

SAIC®

Platinum

paloalto® NETWORKS

For partnership opportunities, contact Neil Ashman for more information.

What's On Next

Federal Cyber Insights

Online

October 20, 2022