



Cyber Security & Risk Management



Government Cyber Insights: Winter Edition

Adapting for More Resilient Enterprise in the Next Normal

Online → Wednesday, March 2, 2022 | 12pm - 3pm ET

Your Inspiring Speakers



NANCY RAINOSEK
State Chief Information Security Officer
Texas Department of Information Resources



DESHARD STEVENS
Chief Information Security Officer
New York City Commission on Human Rights



DAN WILKINS
Chief Information Security Officer
State of Arizona-DES
(Pending final agency confirmation)



LESTER GODSEY
Chief Information Security Officer
Maricopa County



JOSE LOPEZ
Chief Innovation Officer & Director of Technology
City of Groveland



JENNY HEDDERMAN ESQ.
State Risk Counsel
Comptroller of the Commonwealth of Massachusetts
(Pending final agency confirmation)



TRACY WALKER
Senior Solution Engineer, Americas
SUSE

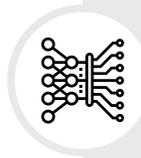


CHRIS JENSEN
Public Sector Business Development
Tenable

Benefits of Attending



Gather insight from government that will help you understand their processes and lessons learned



Examine and address challenges that occur from technology driven initiatives



Discover the latest solutions and services government is using to protect themselves against cyber-attacks



How to maximize your cybersecurity investment with a outcome driven approach

[CLICK HERE TO REGISTER](#)

Transforming Government through Technology Based Initiatives

Governments are being asked to drive change and become more agile and innovative in their public service to citizens. Innovation is achieved when data is unlocked, and trusted people collaborate to leverage the data creatively and efficiently through technology. While this convergence is promising it also marks the point of greatest vulnerability for public sector organizations, driving cyber and security risk to an all-time high. It is necessary to address cyber vulnerabilities before an event occurs to ensure a culture of vigilance and develop safer networks.

Public Sector Network invites you to join the conversation at our Virtual Event: **Government Cyber Insights: Winter Edition**. We will spotlight industry thought leaders and their initiatives from across the United States.



Who You'll Meet

Commissioners/Chiefs/Directors/Managers of:

- Cyber Security
- Information Security
- Cyber Defence
- Endpoint Security
- Zero Trust
- Innovation
- Data & Analytics
- Data Science
- Privacy
- Risk Management
- Risk Mitigation
- Information Technology
- Technology
- AI, Automation & ML
- Learning & Development

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

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

12:20pm ET **Government Keynote: Ransomware and Incident Response: Lessons Learned from Texas August 2019**

In August 2019, 23 local governments in Texas were impacted by a ransomware attack. This government keynote will illustrate how the state successfully responded to this attack, bringing all 23 entities back to operational in a weeks' time, and lessons learned through this incident. The insights from this attack are applicable to any organization that uses remotely administered IT services or managed security providers.

- The single largest factor in the success of this attack was that the remote support administrator console was exposed to the internet.
- Initial access and reconnaissance occurred 14 days prior to the main attack.
- The initial access method: valid credentials that were acquired prior to the attack or exploiting a vulnerability chain in the remote support software

Nancy Rainosek, *State Chief Information Security Officer, Texas Department of Information Resources*

12:40pm ET **Government Case Study: The Buyer's Dilemma: Insight and Tips on Selecting Cybersecurity Support**

Under pressure to prioritize cybersecurity due to continued high profile attacks, the Biden Administration unveiled a comprehensive set of new cybersecurity directives for the U.S. federal government last year. These directives impact an already complicated but critical process: selecting the right cybersecurity support. In this case study the State of Arizona's Department of Economic Security outlines its approach to vendor selection under the new directives, providing key insights and the critical factors that influenced decision-making throughout the process.

Dan Wilkins, *Chief Information Security Officer, State of Arizona-DES (Pending final agency confirmation)*

1:00pm ET **Platinum Keynote: Why Zero Trust Segmentation beats CVE Chasing All Day, Every Day**

Scanning for and remediating vulnerabilities has become a very common - and necessary - security practice in many software development environments. Unfortunately, "CVE chasing" has also become the primary security activity performed early in an SDLC, sometimes even prioritized over other security layers that are overly complex or negatively impact development velocity.

SUSE NeuVector security engineer Tracy Walker will compare CVE Scanning with Zero-Trust segmentation, and offer real examples of organizations automating zero-trust early in their SDLC to block zero-day vulnerabilities that CVE scanning couldn't detect.

Tracy Walker, *Senior Solutions Engineer, Americas, SUSE*

1:15pm ET **Government Case Study: Supply Chain Management: Critical Steps to Mitigating Cybersecurity Risks**

As cyber-attacks against public sector systems, assets, and infrastructure continue to make major headlines, it is imperative that vulnerabilities within government supply chains are identified and exposure to threats mitigated or eliminated. But where are the greatest risks in the supply chain? How to protect against vulnerabilities within the different tiers of the supply chain, particularly your suppliers' suppliers? How to ultimately ensure the secure delivery of critical services and solutions? In this case study presentation Maricopa County outlines their successful approach to minimizing exposure to cybersecurity attacks within their supply chain.

Lester Godsey, *Chief Information Security Officer, Maricopa County*

1:35pm ET

Panel Discussion: Cybersecurity Risk Management: Ransomware Planning, Response, and Recovery

Over the past year, it seems that everywhere you turn, there's another story about a debilitating ransomware attack. Recent high-profile attacks such as the ransomware attack on the utility company, Colonial Pipeline in the USA, demonstrate the lengths that ransomware gangs go to. In this cyber-attack, data was also stolen and used as leverage to add pressure to pay the ransom.

This expert panel will discuss how the public sector can develop an effective cyber-risk management strategy, and best practices. It is imperative to plan for and measure readiness to successfully respond to, mitigate, and recover from a ransomware attack.

- Best practices around business continuity and incident response should you suffer from a ransomware attack.
- What are your options for recovery?
- Who should be on your crisis management team? Who do you call when a ransomware attack occurs?

Jenny Hedderman Esq., *State Risk Counsel, Comptroller of the Commonwealth of Massachusetts (Pending Final Agency Confirmation)*

Lester Godsey, *Chief Information Security Officer, Maricopa County*

Chris Jensen, *Public Sector Business Development, Tenable*

2:05pm ET

Break

2:10pm ET

Gold Spotlight: CrowdStrike

2:25pm ET

Panel Discussion: Mapping your Cybersecurity Plan: Insight & Execution

Creating and implementing a cyber security strategy is more critical than ever as the number of security-related breaches rises. Cybersecurity strategy is the big picture that gives us the chance to begin solving that puzzle, rather than just being experts on a few items. Therefore, it is imperative to have a well thought out plan for execution.

This panel of industry thought experts will share insights and knowledge. From this session you will have a better understanding of:

- What are the most important considerations when developing a cybersecurity incident response plan?
- Identify external data security resources
- Learn how different leaders are building a culture comprised of the right systems, processes, and people to support their strategy.

Deshard Stevens, *Chief Information Security Officer, New York City Commission on Human Rights*

Jose Lopez, *Chief Innovation Officer & Director of Technology, City of Groveland*

2:55pm ET

Closing Remarks from the Chair

3:00pm ET

Virtual Event Adjourns

Thank you to our **Event Partners**

Platinum



Gold



Silver



For partnership opportunities, contact **Andrew Jensen** for more information.

What's On **Next**



**National Cyber Insight:
Spring Edition
Online**

June 8, 2022