PUBLIC SECTOR SEMINAR

WEDNESDAY, OCTOBER 30

8:00 AM – 4:00 PM

Minneapolis Marriott Northwest

14TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

cybersecuritysummit.org

CSS14 / OCTOBER 28–30, 2024 / MPLS., MN

The Public Sector Seminar brings a full day focus to the broad range of persistent threats that challenge government at all levels in Minnesota and beyond. We'll look at the many critical infrastructure efforts that reduce risk, talk about programs, processes and projects that support continuous improvement, and find new ways to bolster our collective cyber posture.

8:00 AM — Opening Remarks

8:30 AM — Beyond MFA and EO 14028: Secure Identities to Protect People

Federal agencies rush to meet new cybersecurity requirements, ensure election security, and address threats, all while sweeping changes hit state and local governments. Learn about data breach incidents and authentication bypass risks that prompted the latest mandates, and the list of considerations related to zero trust architecture. Leave with a better understanding of why this broader set of passwordless, anti-phishing identity capabilities is needed to defend against sophisticated attacks, and how to get it done.

9:00 AM — Deep Dive: Water/Wastewater Panel

Water and wastewater headlines have hit hard, as nation-state and other threat actors focus attention on a human lifeline at the top of the critical infrastructure pyramid. These attacks have turned the tides to pool federal, state, and local municipalities with non-profit resources to strengthen water-related cyber resilience. We will tap into the well of knowledge to evaluate the risk, identify innovative initiatives, and share solutions.

10:15 AM — The New Frontier of Deception: AI, Deep Fakes, and the Dark Web

Learn how advancements in artificial intelligence, the proliferation of deep fake technology, and phishing-as-a-service have revolutionized social engineering. Discover the dark web's ability to democratize access globally and spread criminal tactics and techniques to even low-skilled attackers, and how AI enables phishing that eludes detection and defense at individual and organizational levels. See how deceptive content is crafted to manipulate targets with unprecedented realism, adding a new layer of complexity to business email compromise and other social engineering tactics.

10:45 AM — Digital Trust: The Role of IAL2

In an era of daily remote interactions, securing digital identities is critical. This session highlights the opportunities and pitfalls related to NIST Identity Assurance Level 2 (IAL2). Learn how IAL2 and when it's the wrong choice. We will discuss the concept of component services, the importance of aggregation and orchestration, and alternatives like IAL1+.

12:30 PM — Malicious Insider Threat, Supply Chain and Physical Attack

This panel will explore the Midwest Reliability Organization process used to identify and rank reliability, cybersecurity, and physical security risks to the Bulk Power System (BPS), and its relevance to other sectors. Hear how this grassroots process evolved from the collective knowledge of many, and how it's continuously enhanced by the MRO industry councils to refine risk descriptions, outline typical and worst-case scenarios, and discover high-level risk mitigations. Risks are normalized by MRO staff and its councils and presented on one heatmap in the final Regional Risk Assessment (RRA).

1:30 PM — Disaster Recovery and Identity Fail Over in a Very Cloudy Sky

Forging ahead with new, innovative technologies to make stakeholders' lives easier and more productive is the IT professional's mission. And now, AI and quantum computing bring unforeseen business risk and inevitable conflict to interoperability. Through the lens of a Multi-Cloud and Hybrid Identity Landscape we will identify critical applications to understand how outages affect the business, and ultimately build a DR plan that is less recovery and more automation and orchestration.

3:00 PM — Project Broken Mirror: Origin Story

Project Broken Mirror is a community-driven initiative aimed at protecting the United States from cyber attacks. FRSecure and Security Studio founder Evan Francen will tell the full story behind Project Broken Mirror: why he's doing it, how it works, when it launches, and how you can participate. HINT: attack surface might be part of the equation in this blockbuster tale.

Register at cybersecuritysummit.org

$299 registration fee includes lunch.

Public Sector Seminar Host

STRATA Identity Orchestration

Corporate Partner

MINNESOTA IT SERVICES

Public Sector Supporters

FRSECURE iddataweb RSA

24-09-10