

# AGENDA

The Future of IT & Cybersecurity

# CIO & CISO Think Tank

[Click Here to Register](#)



October 29, 2026

Eastern Time

**Registration**

8:30 AM-9:00 AM

**Morning Networking**

9:00 AM-9:30 AM

**Opening Remarks**

9:30 AM-9:40 AM

**VISION VOICES KEYNOTE**

**The Accountability Shift: IT & Security as  
Business Risk Owners**

9:40 AM-10:05 AM

Technology and security leaders are no longer operating as support functions. As AI, cloud, and digital ecosystems expand, CIOs and CISOs are increasingly accountable for enterprise risk, resilience, and business continuity. This discussion explores how leaders are redefining their role at the executive level, aligning IT and security decisions with business outcomes, and navigating growing expectations from boards and stakeholders.

**KEYNOTE**

**AI Is Changing the Threat Model Faster Than We  
Can Secure It**

10:10 AM-10:35 AM

AI is transforming how organizations operate, but it is also reshaping how attacks are executed, scaled, and concealed. Many security frameworks were not designed for systems that learn, adapt, and act autonomously.

This session examines how leaders are evolving their security strategies to address AI-driven threats, and whether current approaches are sufficient in an environment where risk is becoming less predictable

## Coffee Break

10:35 AM-10:55 AM

### PANEL

## The Governance Gap: Decentralized Innovation, Centralized Risk

10:55 AM-11:40 AM

AI and digital innovation are increasingly distributed across teams, business units, and platforms. While this accelerates progress, it also creates fragmented accountability and inconsistent oversight.

This conversation focuses on how organizations are establishing governance models that balance speed with control, and how leaders are defining ownership in a landscape where risk is shared but not always clearly managed.

### DISRUPTOR

## Zero Trust Under Pressure: Where the Model Starts to Break

11:45 AM-12:00 PM

Zero Trust has become a foundational approach, but its effectiveness is being tested by dynamic identities, machine-to-machine interactions, and AI-driven workflows.

This discussion explores where Zero Trust holds up, where it falls short, and how organizations are evolving toward more adaptive, intelligence-driven security models.

### LUNCH & DISRUPTOR SHOWCASE

## Lunch & Disruptor Showcase

12:00 PM-1:00 PM

## Cocktail Networking

4:15 PM-5:00 PM

## Closing Remarks & Raffle Giveaway

4:00 PM-4:15 PM

### PANEL

## Leading Through Uncertainty: Decision-Making When the Playbook No Longer Applies

3:35 PM-4:00 PM

The pace of technological change, driven by AI, evolving threats, and shifting regulatory expectations, is outpacing traditional decision-making models. CIOs and CISOs are increasingly required to make high-stakes decisions without complete information, clear precedents, or stable ground.

This closing discussion explores how leaders are navigating ambiguity, building confidence in imperfect decisions, and aligning organizations when certainty is no longer guaranteed. It will focus on judgment, communication, and leadership in an environment where the cost of waiting can be just as high as the risk of acting.

### VISION VOICES

## From Reactive to Predictive: The Future of

3:05 PM-3:30 PM

# Enterprise Security

Cybersecurity is evolving from reactive defense to predictive, intelligence-driven strategies. AI and data are enabling earlier detection, faster response, and more proactive risk management.

This session explores what it takes to build a forward-looking security posture, and how organizations are preparing for a future where anticipating risk is just as critical as responding to it.

## FIRESIDE CHAT

2:30 PM-3:00 PM

### Security at Scale: Are We Protecting Everything or Protecting What Matters?

As digital ecosystems expand, so do the demands on security teams. Attempting to secure everything equally is becoming unsustainable from both a cost and operational perspective.

This discussion addresses how leaders are making difficult prioritization decisions, aligning security investments with business risk, and accepting that not all assets can be protected the same way.

## Networking Break

2:15 PM-2:30 PM

## VISION VOICES

1:50 PM-2:15 PM

### The AI Visibility Problem: You Can't Secure What You Can't See

As AI systems become embedded across the enterprise, visibility into how they operate, make decisions, and fail is becoming increasingly limited. This lack of transparency creates new blind spots for both IT and security teams.

This session explores how organizations are approaching AI observability, and what it takes to maintain control and confidence in systems that are no longer fully explainable.

## DISRUPTOR

1:30 PM-1:45 PM

### Cyber Resilience vs. Cyber Perfection: What Are We Actually Optimizing For?

The idea of fully eliminating risk is no longer realistic. As environments grow more complex, organizations must decide how much risk to accept and where to prioritize resilience over prevention.

This conversation explores how leaders are redefining success in cybersecurity, shifting from prevention-focused strategies to models built on response, recovery, and continuity.

## VISION VOICES

1:00 PM-1:25 PM

### Human Risk Is Still the Biggest Risk

Despite advances in automation and tooling, human behavior remains one of the most unpredictable elements of cybersecurity. Social engineering, insider risk, and decision fatigue continue to expose vulnerabilities.

This session examines how leaders are addressing human risk not just through training, but through culture, design, and accountability.

## PARTNERS

*We are currently accepting partnership opportunities for this event.*