

The Millenium Alliance – Breakfast Keynote Panel

May 14th at 8 AM

"Navigating the AI Security Frontier: Turning Risk into Resilience"

Moderated by:

Dave Chatterjee, Ph.D.

[Author: Cybersecurity Readiness: The Holistic and High-Performance Approach](#)

[Host, The Cybersecurity Readiness Podcast \(https://www.dchatte.com/podcast/\)](https://www.dchatte.com/podcast/)

<https://www.dchatte.com>

<https://www.linkedin.com/in/dchatte/>

Agenda and Discussion Plan

Objective

To explore the evolving landscape of AI-driven cybersecurity risks and opportunities, share real-world insights on managing AI threats, and discuss how organizations can leverage AI responsibly to build cyber resilience.

Discussion Plan

I. Introduction (5 min)

II. The Expanding Threat Landscape (10 min)

Guiding Questions:

- What are the most pressing AI-driven security threats today?
- How are bad actors using generative AI and machine learning for attacks?
- Any real-world examples of AI-powered cyberattacks?

Goal: Establish a clear, practical understanding of emerging risks.

III. AI as a Defensive Tool (10 min)

Guiding Questions:

- How are organizations using AI to enhance threat detection and response?
- What are the limitations of current AI-driven security solutions?
- Can AI help reduce alert fatigue and improve SOC performance?

Goal: Showcase resilience-building use cases of AI in cybersecurity.

IV. Governance, Ethics & Trust (10 min)

Guiding Questions:

- What frameworks or standards are helping govern AI security risks?
- How do we ensure AI models are explainable, fair, and not easily manipulated?
- What role does transparency play in building trust with stakeholders?

Goal: Emphasize the importance of ethical AI and responsible deployment.

V. The Road Ahead – Strategic Insights (10 min)

Guiding Questions:

- What does an AI-resilient organization look like?
- What are the key priorities for the next 12–18 months?
- How should organizations rethink their security architecture in the age of AI?

Goal: Inspire forward-looking thinking and strategic action.

VI. Closing Comments and Q&A (10 min)