2025 INFORMS ANNUAL MEETING
October 26–29, 2025 | Atlanta, Georgia

Unlocking Competitive Advantage in the Age of Intelligent Systems

SESSION: AI-Driven Entrepreneurship and Innovation

October 28, 2025

Dave Chatterjee, Ph.D.
Duke University

Disclaimer

Fair Use Notice and Disclaimer

This presentation deck may contain copyrighted material the use of which has not been specifically authorized by the copyright owner. The fair use doctrine allows the presenter limited use of copyrighted material without requiring permission from the rights holders, such as commentary, criticism, news reporting, research, teaching or scholarship. It provides for the legal, non-licensed citation or incorporation of copyrighted material in another author's work under a limited balancing test. The material shall be used to enhance public understanding of cybersecurity preparedness, as such, the presenter believes this constitutes a fair use of any such copyrighted material as provided for in section 107 of the US Copyright Law. In accordance with Title 17 U.S.C. Section 107, this presentation is distributed without profit to those who have expressed a prior interest in receiving the included information for research and educational purposes. If you wish to use potentially copyrighted material from this presentation for purposes of your own that go beyond fair use, you must obtain permission from the copyright owner.

Errors and Omissions Disclaimer

The information contained in this presentation is for general guidance only. The author/presenter assumes no responsibility or liability for any errors or omissions in the content of this presentation. The information contained in this presentation is provided on an "as is" basis with no guarantees of completeness, accuracy, usefulness, or timeliness.

Agenda

- Professional Highlights
- AI as a Catalyst for Competitive Edge
- Founders’ Journey
- The CPD Framework
- Actionable Roadmap for Secure AI Adoption
- Q&A

Professional Highlights

Expertise and Roles

Subject Matter Expertise

- Cybersecurity Governance
- Strategic Management of Technologies
- Supply Chain Management

Roles

- Professor
- Author
- Editor
- Speaker
- Podcastor
- Consultant/Advisor

Author

THE WALL STREET JOURNAL.

MIT Sloan Management Review

California Management Review

MIS Quarterly

BUSINESS HORIZONS

Journal of Organizational Computing and Electronic Commerce

Taylor and Francis Ltd

S-Logix

IVEY | Publishing

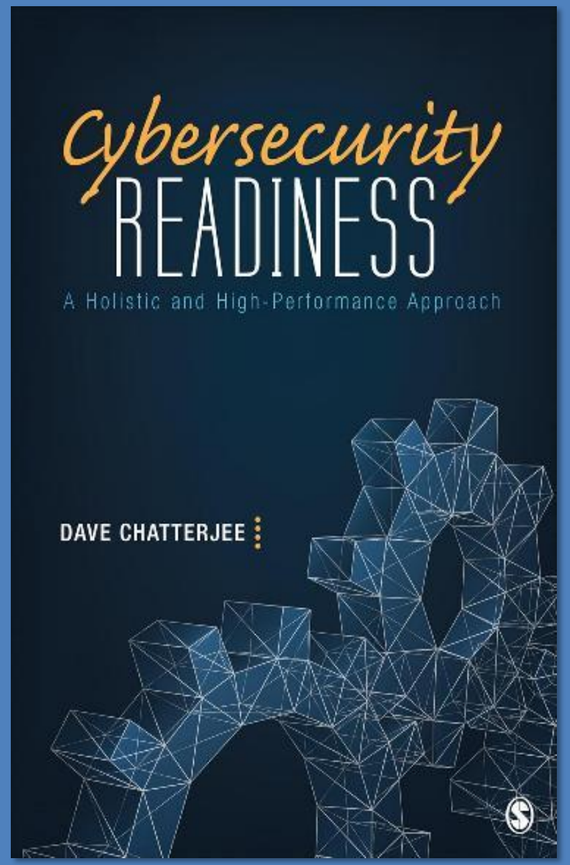
Communications of the ACM

Association for Computing Machinery

S-Logix

I by IMD

SAGE Publishing



Amazon

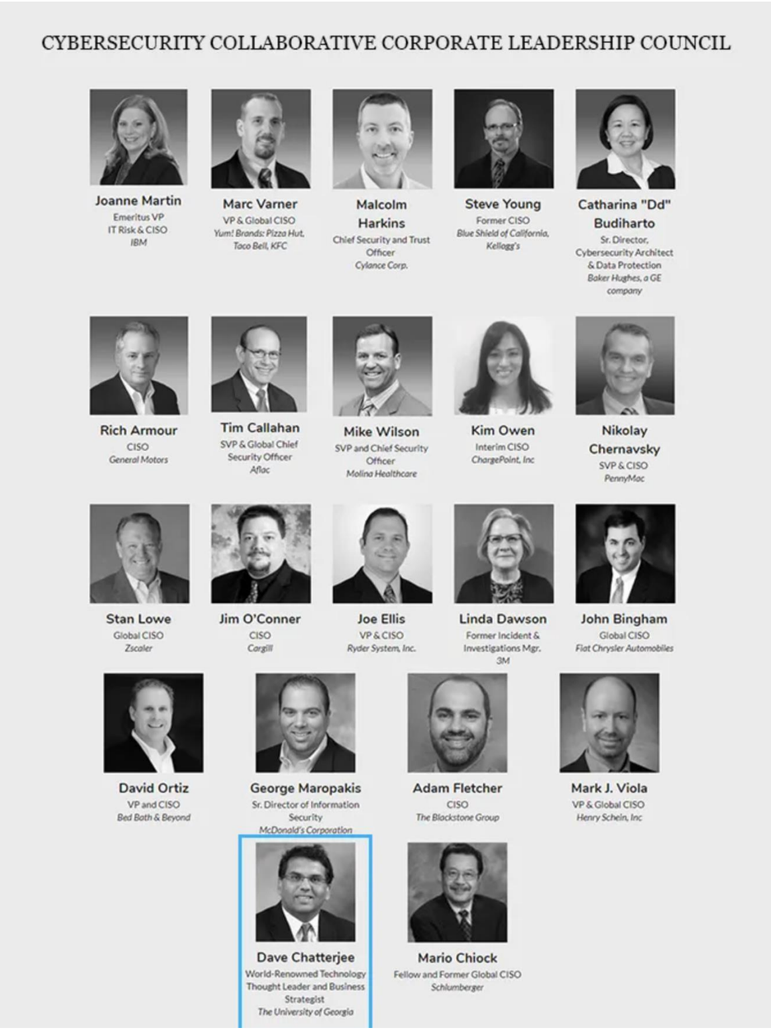
Sage

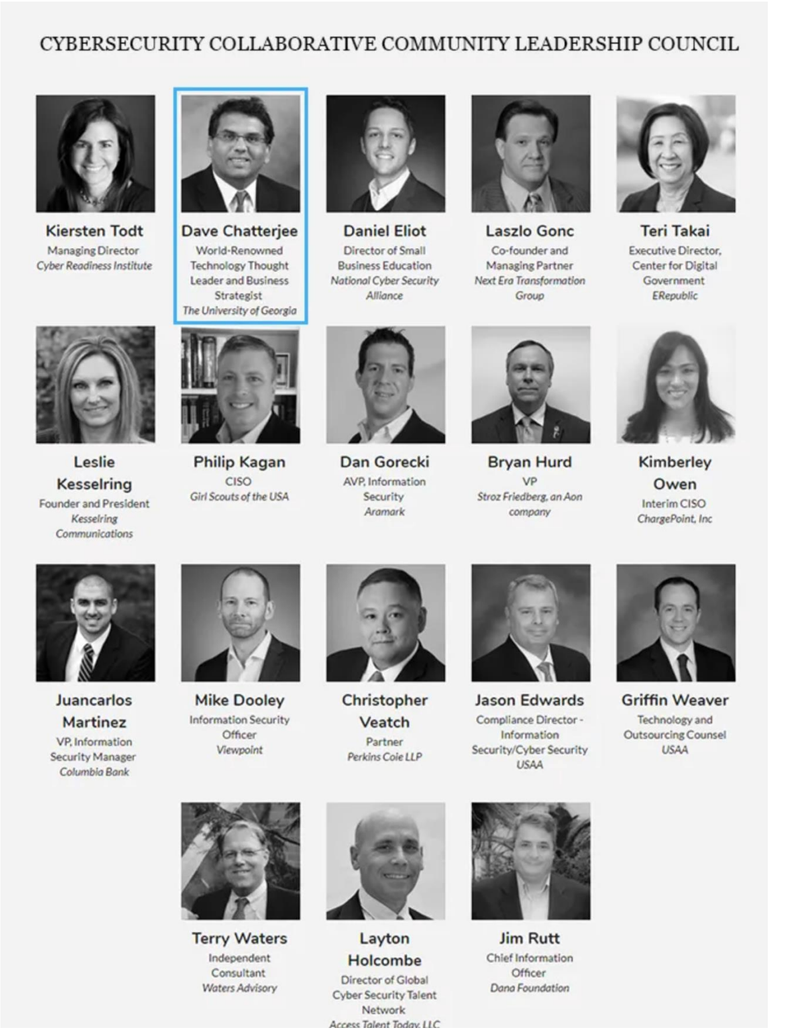
https:www.cybersecurityreadinesspodcast.com

Amazon

Professional Highlights

Cybersecurity Leadership Council and SWAT Team





Professional Highlights

Speaker/Moderator

AI as a Catalyst for Competitive Edge

Identity and Access Innovation

- **Passwordless and device-bound authentication** (Beyond Identity, Badge).
- **Multi-cloud identity orchestration** (Strata Identity).
- **Deepfake-resilient verification** (Nametag).

Goal: Shrink attack surfaces while creating seamless, trusted user experiences.

Autonomous Cyber Defense

- **Agentic AI for patching and remediation** (Root, Vicarius).
- **AI-driven model and data-layer protection** (HiddenLayer, Nightfall).
- **Autonomous DDoS and behavioral defense** (NETSCOUT, DTEX).

Goal: Accelerate detection and response beyond human reaction time.

AI Trust, Safety & Compliance

- **Post-quantum and crypto-ready infrastructure** (Futurex).
- **Data classification and compliance automation** (Normalyze/Proofpoint).
- **Governance dashboards for AI risk oversight** (Pangea)

Goal: Ensure that innovation keeps pace with evolving legal and ethical standards.

Founders’ Journey

Motivations

Firsthand Exposure to Risk:

- Several founders came from security or identity management backgrounds and had seen how traditional defenses collapsed under new forms of attack.
- Their ventures were born out of a determination to close those gaps—
  - whether that meant eliminating passwords (as in Beyond Identity and Badge);
  - defending AI models from manipulation (HiddenLayer); or
  - authenticating humans in a world of deepfakes (Nametag).

Belief in Trust as a Differentiator:

- They recognized that trust—once a compliance box—was becoming a market-winning feature.

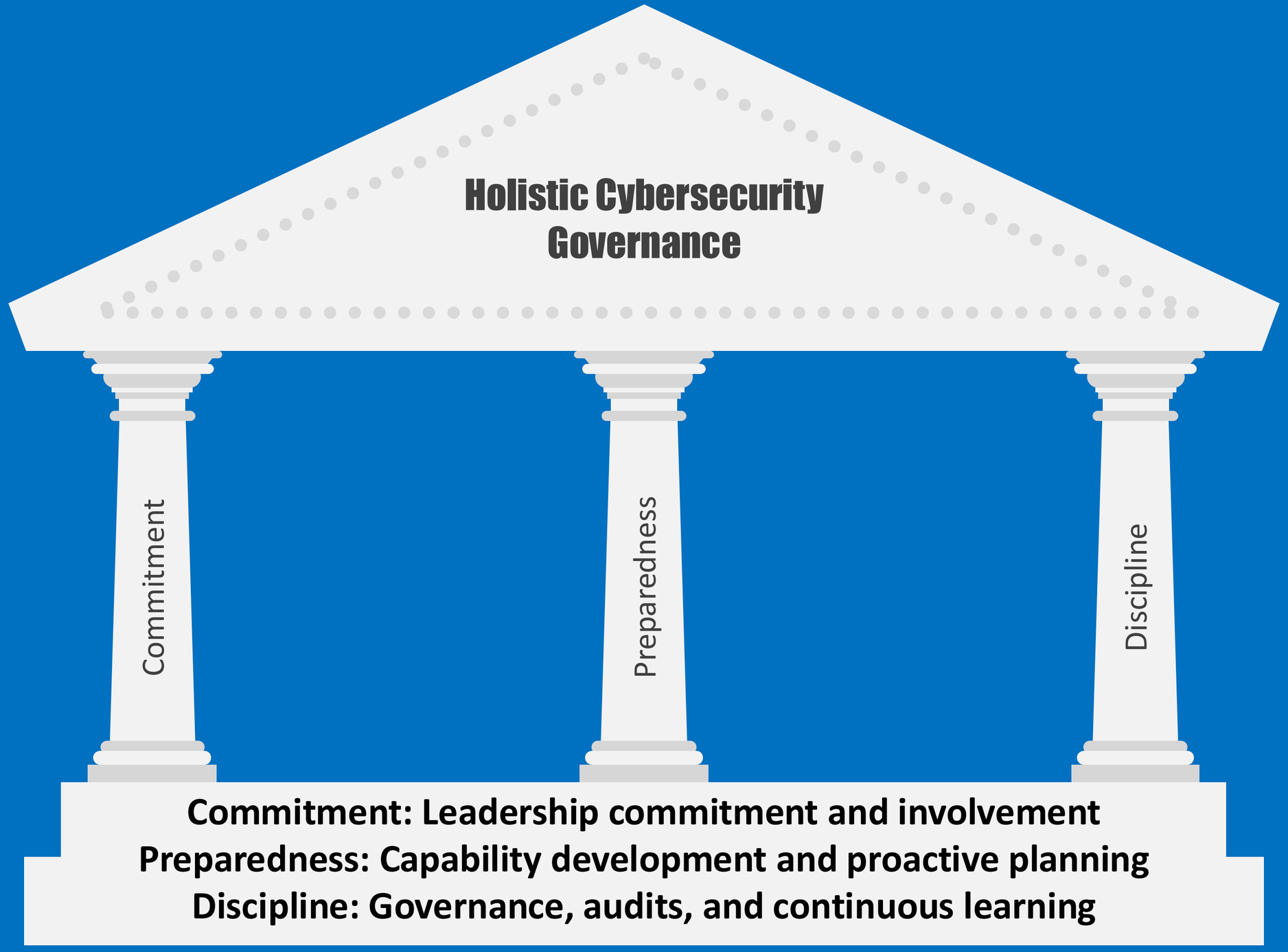
Hurdles Encountered

- **Market Skepticism and Investor Fatigue:**
  - Early adopters were cautious about replacing legacy systems with AI-driven defenses.
  - Convincing boards and CISOs
- **Talent and Technical Complexity:**
  - Recruiting specialized AI security talent
  - Build teams capable of both pioneering new algorithms and translating them into practical, compliant solutions.
- **Regulatory and Ethical Grey Zones:**
  - As AI outpaced existing laws, companies faced ambiguity around privacy, fairness, and liability.
  - Had to impose higher ethical standards on themselves

Overcoming Adversity

- **Relentless Experimentation**
  - Each setback—failed pilots, funding gaps, regulatory delays—made them even more determined.
- **Strong Belief and Vision**
  - **Long-term vision: make security an enabler and not an obstacle**.
- **Strategic Partnerships**
  - Collaborations with cloud providers, cybersecurity firms, and government agencies lent credibility and helped scale adoption.
- **Transparency and Education:**
  - Founders made openness a strategy—
    - Publishing research;
    - Open-sourcing tools; and
    - Engaging in dialogue with regulators to set new benchmarks for AI safety and accountability.

The Commitment-Preparedness-Discipline (CPD) Framework


Holistic Cybersecurity Governance
Commitment
Preparedness
Discipline
Commitment: Leadership commitment and involvement
Preparedness: Capability development and proactive planning
Discipline: Governance, audits, and continuous learning

The ‘Commitment’ Dimension

Success Factors

The ‘Preparedness’ Dimension

Success Factors

The ‘Discipline’ Dimension

Success Factors

Actionable Roadmap for Secure AI Adoption

1. Commitment – Secure AI Starts at the Top

Goal: Ensure leadership buy-in, clear governance, and ethical alignment before AI deployment.

Action Step	Deliverable	Example in Practice
1.1 Executive Alignment	Board-approved AI security charter	A hospital board ratifies an AI governance policy mandating bias testing, explainability, and robust security controls.
1.2 Ethical & Regulatory Commitment	AI ethics code aligned with sector-specific laws (HIPAA, GDPR, etc.)	A financial services firm integrates AI compliance into its enterprise risk management framework
1.3 Budget & Resource Allocation	Dedicated AI security funding and cross-functional team	AI security lead appointed with budget for red-teaming and continuous monitoring tools.

Checkpoint: Leadership signs an AI security pledge, making it part of annual strategic objectives.

2. Preparedness – Building a Resilient AI Ecosystem

Goal: Architect, test, and train before deploying AI into critical workflows.

Action Step	Deliverable	Example in Practice
2.1 Threat Modeling & Risk Assessment	AI-specific threat matrix (data poisoning, adversarial ML, model inversion, prompt injection, etc.)	Pharma R&D lab runs tabletop exercises on model manipulation during drug discovery.
2.2 Secure AI Design	Security-by-design AI architecture with layered defenses	Zero Trust principles applied to AI pipelines (restricted data flows, encrypted model storage).
2.3 Data Protection & Quality	Verified data lineage and integrity controls	Manufacturing AI models use digitally signed sensor data to prevent spoofing.
2.4 Workforce Preparedness	AI-specific security training	Staff learn to detect and report adversarial prompts or suspicious AI outputs.
2.5 Simulation & Testing	Pre-production adversarial testing	Bank uses red teams to simulate fraud attempts exploiting generative AI chatbots.

Checkpoint: AI system passes adversarial penetration test and compliance audit before production launch.

3. Discipline – Sustaining Security Over Time

Goal: Maintain vigilance and adaptability as threats evolve.

Action Step	Deliverable	Example in Practice
3.1 Continuous Monitoring & Anomaly Detection	AI security dashboard with real-time alerts	Healthcare AI tool flags anomalous diagnostic suggestions for human review.
3.2 Model & Data Drift Management	Quarterly retraining with bias and security checks	Insurance AI models are retrained to account for new fraud patterns.
3.3 Incident Response Integration	AI-inclusive IR playbook	Cybersecurity team has specific steps for AI model compromise scenarios.
3.4 Governance Reviews & Audits	Annual AI ethics and compliance review	Independent auditors validate model fairness and robustness.
3.5 Cross-Industry Intelligence Sharing	Membership in AI threat-sharing consortiums	Energy company shares adversarial AI attack indicators with sector peers.

Checkpoint: Post-deployment reviews show adherence to security SLAs, minimal bias drift, and timely incident handling.

Phased Timeline

- **Phase 1 (0–3 Months):** Commitment
  - Establish governance, security budget, create AI ethics & security charter.
- **Phase 2 (3–9 Months):** Preparedness
  - Threat model, secure AI design, red-team testing, workforce upskilling.
- **Phase 3 (Ongoing):** Discipline
  - Deploy continuous monitoring, audits, intelligence sharing, and retraining cycles.

Key Success Metrices

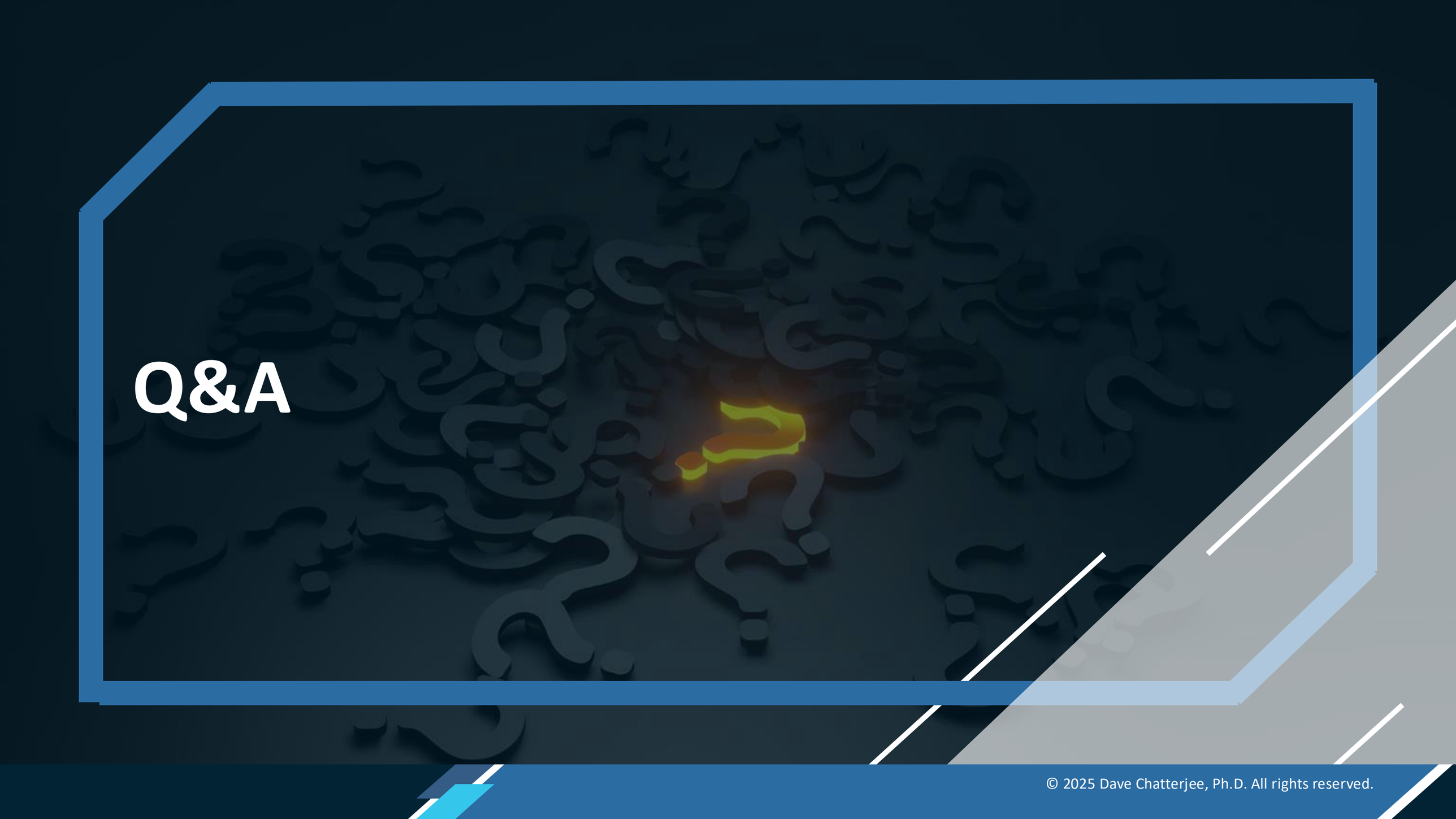
- **Governance**: % of AI projects passing pre-deployment security and ethics review.
- **Resilience**: Mean time to detect/respond to AI incidents.
- **Compliance**: Audit pass rates for AI-related regulatory requirements.
- **Trust**: Stakeholder satisfaction with AI transparency and reliability.

Concluding Thoughts

Concluding Thoughts

- AI is both an enabler and a risk amplifier—advantage flows from responsible adoption.
- Founder journeys reveal how adversity and expertise drive globally relevant innovation.
- CPD ensures AI is deployed securely, ethically, and at scale.
- Leaders who integrate trust and resilience into AI strategy will shape the future of competition.

Q&A



THANK YOU!!