Cybersecurity Readiness Podcast Series

Episode 97: AI's Missing Puzzle Piece — Why Information Readiness Determines AI Success

Host: Dr. Dave Chatterjee, Duke University

Guest: Greg Clark, Senior Director of Product Management & Strategy, OpenText

Podcast Portal: https://www.cybersecurityreadinesspodcast.com/

Summary Pitch

In this insightful episode, Dr. Dave Chatterjee speaks with Greg Clark—longtime enterprise content management and cybersecurity leader—about a foundational but overlooked ingredient of AI success: **information readiness**. While organizations rush to implement artificial intelligence, many neglect the quality, governance, security, and contextual integrity of the data fueling these systems. As Clark notes, without clean, curated, and governed information, even the most advanced AI models will misfire—sometimes with damaging or legally significant consequences.

Together, they explore why "garbage in, garbage out" is more relevant than ever in the AI era, especially as enterprises confront fragmented data, weak metadata, inconsistent governance, and high regulatory scrutiny. Dr. Chatterjee weaves in his **Commitment–Preparedness–Discipline (CPD)** governance framework, demonstrating why information readiness must be treated as a **strategic capability**, not a technical afterthought. The conversation illuminates how trust, data integrity, and responsible model oversight are emerging as competitive differentiators in the age of GenAI and agentic AI.

Discussion Highlights

Information Readiness: The Bedrock of AI Success

Clark defines information readiness as the ability to supply AI with **clean, contextual, secure, and ethically governed data**. Organizations that deeply understand their information—its lineage, value, and risks—are better positioned to adopt AI responsibly and effectively.

Why Data Chaos Undermines Trust

Fragmented data, poor metadata standards, weak unstructured data governance, and inconsistent privacy controls create blind spots and erode trust. Clark cites research showing CIOs are overwhelmed by tool sprawl—averaging 15 cybersecurity platforms—which complicates risk interpretation and governance.

Real-World Consequences of Poor Information Quality

The discussion highlights the 2024 Air Canada chatbot case, where faulty AI-generated responses triggered legal liability. Both emphasize that organizations—not the AI—remain fully accountable for the accuracy and reliability of automated outputs.

Applying the CPD Framework to AI Governance

Dr. Chatterjee maps **Commitment, Preparedness, and Discipline** to information readiness:

- **Commitment** → Leadership prioritizing data ethics, transparency, and governance.
- **Preparedness** → Investments in metadata management, validation pipelines, secure integrations, and stewardship roles.
- **Discipline** → Continuous audits, model validation, oversight, and real-time monitoring.

Operationalizing Information Governance

Clark notes that many companies treat data hygiene as a "project," not a discipline. Mature organizations institutionalize governance with budgets, metrics, and board engagement—some even appoint **Chief AI Officers** or establish formal oversight bodies like JPMorgan's Responsible AI Council.

Metrics that Matter

Both emphasize the need for meaningful, context-specific metrics. Proxy metrics often suffice if tied to strategic outcomes such as reduced financial risk exposure, decreased time-to-respond, or lower data hygiene costs.

Sector Example: Mayo Clinic's AI Governance Model

The conversation highlights Mayo Clinic's radiology AI program, which embeds bias detection, data readiness checkpoints, and compliance reviews throughout the model lifecycle—illustrating how rigorous governance enhances accuracy and trustworthiness.

Enablement Through Zero Trust & Least Privilege

Clark explains how understanding data value enables practical zero trust: protecting high-value data, applying least privilege, enforcing policy-as-code, encrypting sensitive fields, and monitoring access behaviors.

The Dangers of Siloed AI Adoption

With marketing, finance, and legal teams spinning up their own AI projects, organizations risk exposure, duplication, and lack of oversight. Clark warns that the coming wave of **agentic AI** will magnify these vulnerabilities.

Human-in-the-Loop and Regulatory Expectations

Dr. Chatterjee and Clark stress the need for human oversight to audit decisions and validate outputs. They reference the German credit scoring case where lack of explainability violated GDPR, demonstrating regulators' growing insistence on transparency and traceability.

Actionable Recommendations

- **Prioritize Information Readiness Early**
  Build data hygiene, metadata discipline, and governance before deploying AI systems.
- **Adopt Zero Trust Principles**
  Classify data, restrict access, monitor behaviors, and encrypt or tokenize sensitive elements.
- **Operationalize Governance**
  Move beyond one-off projects—treat information readiness as an ongoing practice with leadership sponsorship.
- **Use Organizationally Relevant Metrics**
  Tie outcomes to financial exposure, operational efficiency, compliance posture, and business resilience.
- **Embed Human Oversight**
  Implement human-in-the-loop reviews, real-time audits, and explainability requirements.
- **Create Enterprise-Level AI Oversight**
  Establish centralized governance councils to review risk, data quality, and model transparency.
- **Prepare for Agentic AI**
  Strengthen controls now—before autonomous systems introduce exponential complexity.

- **Apply CPD for Cultural Alignment**
  Leadership commitment, operational preparedness, and disciplined execution are must-haves for AI-era resilience.

Time Stamps

00:49 — Dave introduces Greg Clark

02:43 — Clark's 20+ year journey

07:14 — Defining information readiness

08:32 — Importance of understanding data

09:58 — Data chaos and pitfalls

12:00 — Trust erosion

13:29 — Air Canada chatbot case

16:22 — Auditability and explainability

18:51 — CPD applied to AI governance

20:43 — Operational maturity

22:53 — JPMorgan's Responsible AI Council

25:43 — Security as strategic capability

27:35 — Zero trust and data protection

30:32 — Mayo Clinic example

31:25 — Metrics for buy-in

32:50 — Destroy-your-business scenarios

34:21 — Trust-first culture

36:09 — Human-in-the-loop

37:20 — GDPR case

38:23 — Final reflections

Memorable Quotes

“Innovation without trust is a liability.” — Greg Clark

“AI without information readiness is risk.” — Dr. Dave Chatterjee

“The better you understand your data, the more responsibly you can adopt AI.” — Greg Clark

“Information readiness must be a strategic enabler, not an afterthought.” — Dr. Dave Chatterjee

“Human-in-the-loop oversight is essential—autonomy without accountability is unacceptable.” — Greg Clark