The Millennium Alliance – Executive Roundtable

Sept 9th 2025 at Noon

" Crafting Better Narratives for the Board "

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

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

Agenda and Discussion Plan

Objective:

Enable CISOs to develop more impactful, business-aligned narratives that earn board trust, support, and funding by addressing risk, resilience, and value creation.

1. **Welcome and Opening Remarks**
    - Introduction of topic and objectives
    - Growing board scrutiny and rising expectations for CISOs as communicators
2. **Real world Examples of Effective and Ineffective Board Communication (10 min)**
    - Share a real-world case of effective communication with the board and the positive impact.
    - Share a real-world case where ineffective communication with the board resulted in budget denial, delayed action, or reputational harm.
3. **The Board's Perspective**
    - What do board members really want to know? (Risk posture? Spend efficiency? Compliance readiness?)
    - How do you prepare for their questions or anticipate pushback?
    - Have you had board champions or skeptics? What did you learn from those interactions?
4. **Translating Technical Risk into Business Impact**
    - What techniques do you use to explain risk exposure in business terms?
    - How do you link cybersecurity priorities to revenue protection, brand trust, or operational continuity?
    - Have you used scenarios or simulations to demonstrate risk likelihood and consequence?
5. **Building Trust, Urgency, and Buy-in**
    - What storytelling devices (e.g., analogies, visuals, incident timelines) have helped you connect with board members?
    - How do you maintain credibility while communicating both urgency and control?
    - What board KPIs or dashboards have been most successful?
6. **Key Takeaways and Closing Thoughts**

Recommendations and Best Practices

Sources

1. Cybersecurity Readiness Podcast (www.cybersecurityreadinesspodcast.com) -- Excerpts from Dr. Dave Chatterjee's conversations with CEOs, CISOs, and other subject matter experts.
2. Research and practitioner articles.

---

1. Speak the Language of Business and Risk

- **Translate technical risk into business impact** (e.g., revenue loss, operational disruption, reputational damage).
- Use **financial analogies** (e.g., "cyber risk is like insurable risk") to help directors grasp severity.
- Prioritize **risk-based narratives** over technical jargon.

2. Use Metrics That Matter

- Present a **concise dashboard** with key cyber risk indicators (KRIs) and trends.
    - Examples: % of critical vulnerabilities remediated, phishing click rates, average time to detect/respond
- Show how cybersecurity supports **strategic objectives** and **regulatory compliance**.

3. Focus on Strategic and Emerging Risks

- Highlight **threats to crown-jewel assets** and what's being done to protect them.
- Proactively brief the board on **emerging threats** (e.g., AI-enabled attacks, ransomware-as-a-service, geopolitical risk).
- Include **threat intelligence** and benchmarking against peers/industry.

4. Align Cybersecurity with Enterprise Priorities

- Position cybersecurity as a **business enabler** rather than a cost center.
- Demonstrate how security initiatives support:
    - Digital transformation
    - M&A due diligence
    - Operational resilience
    - Regulatory readiness (e.g., SEC rules, GDPR, HIPAA)

5. Communicate Preparedness and Gaps Transparently

- Be honest about vulnerabilities, resource gaps, and improvement areas.
- Present clear **risk mitigation plans**, investment needs, and ROI.
- Show maturity trends using frameworks like **NIST CSF, ISO 27001, or FAIR**.

6. Build Ongoing Relationships, Not Just Presentations

- Meet with board members or the risk/audit committee **outside formal sessions**.
- Understand individual directors' priorities and tailor content accordingly.
- Encourage **two-way dialogue**—invite questions and insights.

7. Create a Regular Communication Cadence

- Establish **quarterly briefings** or more frequent updates based on threat activity.
- Include **tabletop exercises** with board participation to reinforce awareness and readiness.

8. **Leverage Visuals and Storytelling**

- Use **scenarios and breach simulations** to illustrate consequences.
- Supplement reports with **infographics** or risk heat maps to convey urgency clearly.