**Board Level Balanced Scorecard for Cyber Resilience**

**Goal**: To create a balanced scorecard to help Boards of Directors engage in critical conversation regarding cyber security and align cyber resilience with business needs

Mridula Prakash & Dr. Keri Pearlson

---

1. **Traditional Cybersecurity Reporting Provides the Wrong Information for Boards of Directors**

   What is the right information for Boards of Directors to perform oversight for cyber risk? Cybersecurity dashboard tools are complicated for many reasons:
   - Lack of common language to describe in terms of business value
   - Varying information across various departments makes it difficult to standardize reporting
   - Traditional security reporting focuses on what is being done and are usually manually compiled spreadsheets.
   - Boards and committees receive dozens of reports which are usually poorly structured and inconsistent.

2. **Boards of Directors Need Cybersecurity Information to Enable Strategic Business Decisions**

   Our research focus is to create a balanced scorecard for the Boards of Directors:
   - A balanced scorecard includes information on financial, technological, organizational, and supply-chain risks.
   - Boards want to know how resilient the organization is.
   - Board also need to know the action plan operational managers are taking to address risks.
   - Boards prefer measurable performance indicators.

3. **A Balanced Scorecard Approach Provides a Comprehensive View of Cyber Risks**

   Key takeaways of the research:
   - Boards need more than technology risks assessment for cyber security oversight.
   - Boards language is business risk and balanced scorecard articulates business risk.
   - Cyber resilience is a function of financial, technological, organizational, and supply-chain risks.

4. **Sample Balanced Scorecard for Boards of Directors**

   - **Financial**
     - **Biggest Risk**: Loss of market momentum due to increase possibility of stolen IP
     - **Action Plan**: Investigating IP insurance
   - **Technological**
     - **Biggest Risk**: Vulnerability testing and compliance not automated
     - **Action Plan**: Bringing on new system to automate vulnerability testing
   - **Organizational**
     - **Biggest Risk**: Employees not effectively implementing what they learned in awareness training
     - **Action Plan**: Promoting cyber resilience awareness with new campaigns
   - **Supply-Chain**
     - **Biggest Risk**: Potential leak of our data held by vendors
     - **Action Plan**: Working with vendors to ensure adequate cybersecurity state

   **45% Resilient**

   **The percentages are function of key performance indicators previously agreed by the management**

5. **Join our CAMS Research**

   We are seeking input and feedback on our balanced scorecard.

   Please reach out to mridula@mit.edu