Contents

[6.1] Groupthink security blind spots

1. Operational Definition: A mode of thinking in a cohesive group where the desire for harmony or conformity results in an irrational or dysfunctional decision-making outcome, suppressing dissenting opinions and critical evaluation of alternative security strategies.

2. Main Metric & Algorithm:

- **Metric:** Dissent Suppression Ratio (DSR). Formula: `DSR = (Number of meetings where no alternative viewpoints were raised) / (Total number of security strategy meetings)`.
- **Pseudocode:**

  python

  ```
  def calculate_dsr(meeting_transcripts, start_date, end_date):
      """
      meeting_transcripts: from meeting recording/transcription tools
      """
      # 1. Get all meetings related to security strategy in the time period
      security_meetings = get_meetings_by_topic(meeting_transcripts, ['security', 'risk', 'a

      meetings_without_dissent = 0
      for meeting in security_meetings:
          # 2. Perform NLP analysis on the transcript
          # - Check for uniformity of agreement (low semantic diversity on key points)
          # - Check for phrases that shut down discussion ("let's just move on", "that's a s
          # - Check if initial proposed solution is accepted without challenge
          if not contains_alternative_viewpoints(meeting.transcript):
              meetings_without_dissent += 1

      # 3. Calculate DSR
      total_meetings = len(security_meetings)
      DSR = meetings_without_dissent / total_meetings if total_meetings > 0 else 0
      return DSR
  ```

- **Alert Threshold:** `DSR > 0.6` (Over 60% of strategy meetings show signs of suppressed dissent)

3. Digital Data Sources (Algorithm Input):

- **Meeting Transcription Tools (e.g., Microsoft Teams Transcripts, Otter.ai):** Raw text of meetings tagged as related to security.
- **NLP Libraries:** For semantic analysis, keyword spotting, and sentiment detection to identify patterns of agreement and suppression.

4. Human-to-Human Audit Protocol: An external facilitator conducts anonymous surveys after key meetings: "Were you able to voice opinions different from the majority?" "Did you feel

pressured to agree with the group?" Alternatively, appoint a designated "devil's advocate" in every meeting and have them report on the group's receptiveness to challenging views.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Use anonymous polling or idea generation tools at the start of meetings to collect initial opinions on solutions before group discussion can create pressure to conform.
- **Human/Organizational Mitigation:** Leadership must explicitly reward constructive dissent and model this behavior. Train team leads on techniques to actively solicit alternative opinions ("Let's hear from someone who hasn't spoken yet" or "What are two potential flaws in this plan?").
- **Process Mitigation:** Integrate a formal "pre-mortem" step into the incident review and strategy process, where the team assumes a future failure and works backward to identify reasons for that failure, inherently encouraging critical thinking.