Contents

[3.9] Social Identity Threats

1. Operational Definition: The perception that a security protocol or its enforcement threatens an individual's sense of belonging, status, or self-worth within a group, leading to resistance, non-compliance, or covert bypassing.

2. Main Metric & Algorithm:

- **Metric: Threat Perception Sentiment Score (TPSS)**. This requires NLP analysis of communications following security-related announcements or enforcements.
- **Pseudocode:**

  python

  ```
  def calculate_tpss(chat_logs, comms_channel, time_after_event_hours=24):
      """
      Analyzes sentiment in a channel after a security update is announced.
      """
      # 1. Get timestamp of security announcement (e.g., "new MFA required")
      announcement_time = get_announcement_time(comms_channel)

      # 2. Get messages in the window after the announcement
      start = announcement_time
      end = start + timedelta(hours=time_after_event_hours)
      messages = get_messages_in_window(chat_logs, comms_channel, start, end)

      # 3. Perform sentiment analysis on these messages
      sentiment_scores = []
      for msg in messages:
          score = analyze_sentiment(msg.text) # Returns a score between -1 (negative) and 1
          sentiment_scores.append(score)

      # 4. Calculate average sentiment. A strongly negative score indicates high TPSS.
      TPSS = sum(sentiment_scores) / len(sentiment_scores) if sentiment_scores else 0
      return TPSS
  ```

- **Alert Threshold:** `TPSS < -0.3` (Significantly negative sentiment following a security initiative).

3. Digital Data Sources (Algorithm Input):

- **Communication Platform API (Slack/Teams):** The primary source for measuring reaction to announcements. Fields: `channel`, `text`, `reactions`, `timestamp`.
- **Email/Intranet Platforms:** To get the timestamp and content of the original security announcement.

4. Human-to-Human Audit Protocol: Conduct "pulse checks" or surveys after rolling out new security measures. Ask questions like: "Do you feel this new security measure helps or hinders

your team's ability to work effectively?" "Do you understand why this change was made for our security?".

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Ensure the user experience of security tools is as seamless as possible to minimize perceived friction and threat to efficiency.
- **Human/Organizational Mitigation:** Frame security not as a set of restrictive rules, but as a shared value and collective responsibility that protects the entire group ("us vs. the threat actors").
- **Process Mitigation:** Involve teams early in the design and testing phase of new security processes. Their feedback can help shape the rollout in a way that minimizes perceived threats to identity and status.