Contents

[1.6] Authority Gradient Inhibiting Security Reporting

1. Operational Definition: The observable reluctance of junior staff to report security concerns, policy violations, or potential incidents to higher-ranking individuals due to perceived hierarchical barriers or fear of negative consequences.

2. Main Metric & Algorithm:

- **Metric:** Reporting Gradient Index (RGI). Formula: `RGI = 1 - (N_reports_from_juniors / N_reports_from_seniors)`.
- **Pseudocode:**

  python

  ```
  def calculate_rgi(ticketing_data, hr_data, start_date, end_date):
      # Get all security-related tickets
      sec_tickets = query_tickets(type='security_incident', date_range=(start_date, end_date

      junior_count = 0
      senior_count = 0

      for ticket in sec_tickets:
          reporter_role = get_employee_role(ticket.reporter_id, hr_data)
          if reporter_role in ['junior', 'analyst_i', 'associate']:
              junior_count += 1
          elif reporter_role in ['senior', 'manager', 'director', 'vp']:
              senior_count += 1

      total_reports = junior_count + senior_count
      if total_reports == 0:
          return 0 # Avoid division by zero

      # If juniors and seniors report equally, RGI=0. If only seniors report, RGI=1.
      RGI = 1 - (junior_count / total_reports)
      return RGI
  ```

- **Alert Threshold:** `RGI > 0.7` (i.e., junior staff contribute less than 30% of all security reports).

3. Digital Data Sources (Algorithm Input):

- **Ticketing System API** (ServiceNow, Jira): Fields `reporter`, `created_date`, `type`.
- **HRIS API** (Workday, SAP SuccessFactors): To map `reporter` to their job grade/role (`employee_id`, `job_level`).

4. Human-To-Human Audit Protocol: Run an anonymous survey asking: "Would you feel comfortable reporting a security mistake made by your direct supervisor?" and "Have you ever witnessed a security issue you did not report? If so, why?" Analyze responses by job grade.

5. **Recommended Mitigation Actions:**

   - **Technical/Digital Mitigation:** Implement and heavily promote an completely anonymous reporting channel (e.g., hotline, web form) that is managed by a third party or a separate department like Ethics.
   - **Human/Organizational Mitigation:** Leadership must publicly praise and reward individuals (especially juniors) for coming forward with concerns. Managers should share stories of their own past security mistakes.
   - **Process Mitigation:** Formalize a non-punitive "Near-Miss" reporting process that is decoupled from performance reviews.