Contents

[3.8] Conformity to Insecure Norms

1. Operational Definition: The tendency for individuals to align their behavior with the perceived normative behavior of their group, even if that behavior is insecure, because deviating from the group carries a social cost.

2. Main Metric & Algorithm:

- **Metric: Norm Deviation Index (NDI)**. Formula: `NDI = 1 - (U_compliant / U_total)`, calculated for a peer group. A high NDI indicates a group norm of non-compliance.
- **Pseudocode:**

  python

  ```
  # Similar to DPP (3.3), but focused on compliance with a specific known policy.
  def calculate_ndi(logs, policy_rules, peer_groups):
      """
      policy_rules: A set of rules that define compliant vs. non-compliant actions.
      """
      ndi_results = {}
      for group, users in peer_groups.items():
          non_compliant_users = 0
          for user in users:
              user_actions = get_actions(logs, user)
              # Check if user violated any of the defined policy rules
              if not is_compliant(user_actions, policy_rules):
                  non_compliant_users += 1

          NDI = non_compliant_users / len(users)
          ndi_results[group] = NDI
      return ndi_results
  ```

- **Alert Threshold:** `NDI > 0.5` (Over 50% of a group is non-compliant with a policy, indicating a strong insecure norm).

3. Digital Data Sources (Algorithm Input):

- **Compliance Scanning Tools (e.g., Qualys PC, Azure Policy, AWS Config):** Directly report compliance status for assets and users against policies. Fields: `user/resource_id`, `compliance_state`, `policy_id`.
- **Various Logs (as in 3.3):** To infer compliance behavior.

4. Human-to-Human Audit Protocol: Use group interviews or focus groups. Present the quantitative data (NDI) to the group and ask: “The data suggests that following [X policy] isn’t the norm here. Why do you think that is? What are the barriers to compliance? What would make it easier for everyone to follow this rule?”.

5. **Recommended Mitigation Actions:**

   - **Technical/Digital Mitigation:** Where possible, use technical enforcement (e.g., enforcing encryption, blocking unauthorized software) over procedural policies to remove the choice to be non-compliant.
   - **Human/Organizational Mitigation:** Identify and work with influencers within the group to model and champion the desired secure behavior, shifting the perceived norm.
   - **Process Mitigation:** Review the problematic policy. Is it unnecessarily cumbersome? Work with the group to simplify the process while maintaining security objectives, increasing buy-in.