Contents

[1.3] Authority Figure Impersonation Susceptibility

1. Operational Definition: The measurable likelihood that an employee will comply with a security request (e.g., sharing credentials, bypassing a control) from an individual they perceive to be an authority figure, without performing adequate verification.

2. Main Metric & Algorithm:

- **Metric:** Impersonation Success Rate (ISR). Formula: `ISR = N_successful_impersonations / N_impersonation_attempts`.
- **Pseudocode:**

  python

  ```
  def calculate_isr(security_events, start_date, end_date):
      # Query simulated phishing/pen-test data for authority-based campaigns
      impersonation_attempts = query_security_events(
          source='phishing_simulator',
          event_type='authority_impersonation',
          date_range=(start_date, end_date)
      )
      successful_attempts = [e for e in impersonation_attempts if e.status == 'clicked' or e

      total_attempts = len(impersonation_attempts)
      successful_count = len(successful_attempts)

      ISR = successful_count / total_attempts if total_attempts > 0 else 0
      return ISR
  ```

- **Alert Threshold:** `ISR > 0.15` (i.e., more than 15% of attempts are successful).

3. Digital Data Sources (Algorithm Input):

- **Phishing Simulation Platform API** (e.g., KnowBe4, Cofense): Campaign results filtered by template theme (e.g., "CEO Fraud", "IT Helpdesk").
- **Email Security Gateway Logs** (e.g., Mimecast, Proofpoint): Logs of emails with spoofed headers from internal authority domains that were delivered to the inbox.
- **EDR/Identity Audit Logs** (e.g., CrowdStrike, Azure AD): Events where a user performed a high-risk action (e.g., password change, MFA reset) immediately after receiving an email from a suspicious external address.

4. Human-to-Human Audit Protocol: Conduct a controlled, debriefed simulation. After a planned phishing test, interview a sample of employees who complied. Ask: "What about this message made it seem legitimate? What, if anything, did you do to verify the sender's identity before taking action?" Look for patterns in the lack of verification steps.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement strict DMARC, DKIM, and SPF policies to reduce email spoofing. Deploy identity verification tools that provide visual indicators for internal emails.
- **Human/Organizational Mitigation:** Conduct targeted training on authority impersonation tactics, emphasizing a mandatory, easy-to-use verification protocol (e.g., "Call the person using a known number from the company directory").
- **Process Mitigation:** Institute a formal, non-punitive process for reporting suspected impersonation attempts to reinforce the desired behavior.