Contents

[3.5] Scarcity-Driven Decisions

1. Operational Definition: The cognitive bias where perceived scarcity (e.g., of time, opportunity, or resources) triggers impulsive decision-making, leading individuals to bypass security controls to avoid missing out.

2. Main Metric & Algorithm:

- **Metric: Urgency Bypass Frequency (UBF)**. Formula: `UBF = Count of security actions performed within a short time (T) of a scarcity-themed communication.`
- **Pseudocode:**

  python

```
def calculate_ubf(access_logs, chat_logs, email_logs, time_window_minutes=30):
    """
    Tracks security actions preceded by urgency cues.
    """
    # 1. Scan communications for scarcity/urgency keywords
    urgency_comms = query_comms(
        [chat_logs, email_logs],
        keywords=["urgent", "ASAP", "last chance", "time-sensitive", "deadline", "today or
        period='14d'
    )

    bypass_actions = []
    # 2. For each urgent communication, check for subsequent security actions
    for comm in urgency_comms:
        user = comm.user
        start_time = comm.timestamp
        end_time = start_time + timedelta(minutes=time_window_minutes)

        # Look for security actions by that user shortly after the message
        actions = get_actions(access_logs, user, start_time, end_time)
        for action in actions:
            if is_security_bypass(action): # e.g., overriding a block, disabling a control
                bypass_actions.append(action)

    # 3. Return the frequency of such events
    UBF = len(bypass_actions)
    return UBF
```

- **Alert Threshold:** `UBF > 5` per team per week.

3. Digital Data Sources (Algorithm Input):

- **Email Server Logs (e.g., Microsoft Graph API):** To scan for urgency keywords in subject lines and bodies. Fields: `sender`, `recipients`, `subject`, `body_preview`, `timestamp`.
- **Communication Platform API (Slack/Teams):** As above.
- **Security Control Logs (e.g., VPN, EDR, Cloud Security):** To detect override actions. Fields: `user`, `event_name` (e.g., `OverrideBlock`, `BypassWarning`), `timestamp`.

4. Human-to-Human Audit Protocol: After a security incident involving a rushed action, conduct a blameless post-mortem. Ask: "What was the perceived consequence of delay? What made the situation feel so urgent? Were there alternative secure paths that could have met the deadline?".

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement technical "circuit breakers" that impose a mandatory short cooling-off period for certain high-risk actions, displaying a warning about scarcity tactics.
- **Human/Organizational Mitigation:** Train employees to recognize linguistic patterns of artificial scarcity used in social engineering and to validate urgent requests through a secondary, offline channel.
- **Process Mitigation:** Pre-authorize and document fast-track procedures for genuine business-critical scenarios, so staff isn't forced to choose between security and missing a real deadline.