

Contents

[10.5] Black Swan Blindness	1
---------------------------------------	---

[10.5] Black Swan Blindness

1. Operational Definition: The inability of an organization to recognize or prepare for extreme, high-impact events that are statistically rare but lie outside the realm of regular expectations. Measured by the lack of preparedness for high-impact, low-probability scenarios.

2. Main Metric & Algorithm:

- **Metric:** Black Swan Preparedness Index (BSPI). This is a composite score (0-100) based on a checklist of preparedness activities. Formula: $BSPI = (\text{Sum_of_Weighted_Scores} / \text{Total_Possible_Score}) * 100$.

- **Pseudocode:**

```
python

def calculate_bspi(preparedness_checklist):
    total_score = 0
    max_possible = 0

    for item in preparedness_checklist:
        # item has: 'question', 'weight', 'score' (0-5)
        total_score += item['score'] * item['weight']
        max_possible += 5 * item['weight'] # assuming max score of 5 per item

    if max_possible == 0:
        return 0
    bspi = (total_score / max_possible) * 100
    return bspi
```

- **Alert Threshold:** $BSPI < 50$ (Less than 50% preparedness for extreme events).

3. Digital Data Sources (Algorithm Input):

- **GRC Platform:** Questionnaire or checklist module where the CISO team answers and scores items like: “Do we have a playbook for a zero-day in our primary VPN?” or “Have we tested restoring from backups after a ransomware attack on the backup server itself?”.

4. Human-to-Human Audit Protocol: Conduct a facilitated war-gaming session with senior leadership. Present a plausible but extreme scenario (e.g., “A state actor has compromised our build servers and shipped backdoored software to all customers”). Evaluate the response not for technical perfection, but for the existence of any plan and the decision-making process.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Isolate and rigorously protect crown jewel assets with extreme controls, assuming other defenses may fail.
- **Human/Organizational Mitigation:** Appoint a senior individual to be a “Devil’s Advocate” whose role is to challenge assumptions and propose worst-case scenarios during planning meetings.

- **Process Mitigation:** Integrate one “black swan” scenario into the annual incident response testing schedule to stress-test the organization’s resilience and improvisation capabilities.