Run a scenario from A to Z

Let’s walk through a cybersecurity incident scenario, covering each stage and explaining when to engage each stakeholder and take critical actions.

Scenario

Phishing Attack with Data Exposure An employee unknowingly clicks on a phishing email link, which leads to unauthorized access to a database containing personal customer information.

Step-by-Step Incident Response

1. **Detection and Initial Assessment**

- Action: SOC (Security Operations Center) or security detection system flags unusual access patterns on the database.
- Assess: Determine the scope — **confirm if it’s an actual incident**, and **identify what systems and data are impacted**.
- Notify: **Contact managers as soon as the incident is verified**.

2. **Containment**

- Action: **Isolate** affected systems to prevent further unauthorized access.
- Internal Coordination:
    - **Inform legal** if PII or sensitive data exposure is suspected. Legal will begin reviewing regulatory requirements and prepare for potential disclosure obligations.
    - **Brief managers** to ensure immediate containment resources and communicate with affected teams.
- User Involvement: If users’ accounts are directly impacted, **consider notifying them to be vigilant of suspicious activity**.

3. **Eradication**

- Action: Analyze and **remove** phishing emails from the system, **close** exploited vulnerabilities, and enhance controls.
- Legal Review: Reconfirm if there’s a need for regulatory reporting.
- Directors Briefing: Notify directors if the attack is part of a larger threat pattern or could escalate to impact operations or reputation.

4. **Recovery**

- Action: **Restore** systems and **monitor** closely to **prevent recurrence**.
- Users Notified: If personal information was accessed, **inform impacted users per regulatory guidelines**.
- Management Update: Ensure managers and directors are **updated with timelines and recovery status**.

5. **Post-Incident Review**

- Action: **Conduct a root cause analysis, review the response process, and improve controls**.

- **Management Debrief**: Report findings and lessons learned to managers and directors.
- Legal Follow-Up: Legal may support final reporting or **address compliance concerns** that arose.
- Users Communication: For significant incidents, **inform users** of corrective actions taken to improve security.

Summary

This A-to-Z scenario demonstrates a structured approach:

- **Early containment** and **collaboration with legal for compliance**.
- **Timely updates to managers and directors** to ensure alignment on resources and response strategy.
- **Transparent user communication** where relevant to maintain trust.