MUBEEN GUL MALIK

DEP TASK 3

### IT Company Scenario: Developing Incident Response Plans

**Company Name:** TechGuard Solutions  
**Industry:** IT Services and Software Development  
**Size:** Medium-sized enterprise with 250 employees  
**Location:** Headquarters in New York, with remote teams across the globe  
**IT Infrastructure:**

* **Data Centers:** 2 on-premises data centers and cloud services on AWS.
* **Networks:** Corporate LAN and multiple VPNs for remote access.
* **Systems:** Internal systems for software development, customer support, and financial operations.
* **Clients:** Small to large businesses relying on TechGuard for secure, reliable software and IT solutions.

#### **Objective**

* **Goal:** Develop a comprehensive Incident Response Plan (IRP) to effectively handle security incidents within TechGuard Solutions.
* **Purpose:** Ensure the plan minimizes operational disruption, mitigates damage, protects client data, and facilitates rapid recovery.

### ****Key Steps:****

#### **1. Identifying Potential Security Incidents and Scenarios**

* **Threat Identification:**
  + **Phishing Attack:** A phishing email targets employees, leading to a potential compromise of credentials.
  + **Ransomware Attack:** A sophisticated ransomware variant encrypts critical business data, demanding payment for decryption.
  + **Insider Threat:** A disgruntled employee attempts to leak sensitive client information.
  + **DDoS Attack:** A Distributed Denial of Service (DDoS) attack overwhelms the company’s web servers, disrupting client services.
  + **Cloud Service Breach:** Unauthorized access to cloud-based resources storing customer data.
* **Impact Analysis:**
  + **Critical Systems Compromise:** Loss of client data, operational downtime, reputational damage.
  + **Service Disruption:** Failure to meet service level agreements (SLAs) with clients.

#### **2. Defining Roles and Responsibilities for the Response Team**

* **Incident Response Team (IRT):**
  + **Incident Commander:** CTO (Chief Technology Officer) - Overall responsibility for incident management and decision-making.
  + **Technical Lead:** IT Security Manager - Leads technical analysis, containment, and recovery efforts.
  + **Legal Advisor:** General Counsel - Provides guidance on legal and compliance issues.
  + **Communication Lead:** PR Manager - Manages internal and external communications.
  + **Forensics Specialist:** Senior IT Security Analyst - Conducts investigation, evidence gathering, and analysis.
  + **Support Coordinator:** HR Manager - Ensures employee support and manages insider threats.
  + **Client Liaison:** Account Managers - Communicates with affected clients and manages expectations.

#### **3. Developing Step-by-Step Response Procedures**

* **Incident Detection:**
  + **Monitoring:** Utilize SIEM (Security Information and Event Management) tools to detect anomalies and alerts.
  + **Reporting:** Employees report suspicious activities via a designated incident reporting channel.
* **Containment:**
  + **Short-term:** Isolate affected systems, block suspicious network traffic, and disable compromised accounts.
  + **Long-term:** Apply patches, reconfigure firewalls, and enhance security controls to prevent reoccurrence.
* **Eradication:**
  + **Root Cause Analysis:** Identify and eliminate the root cause (e.g., malware removal, closing security loopholes).
  + **System Restoration:** Restore affected systems using clean backups and verify integrity.
* **Recovery:**
  + **Gradual Reintroduction:** Bring systems back online gradually, monitoring for signs of ongoing compromise.
  + **User Access:** Reinstate user access with enhanced security measures.
* **Communication:**
  + **Internal:** Keep employees informed about the incident and response efforts through secure channels.
  + **External:** Notify clients, regulatory bodies, and the public as necessary, ensuring transparency and compliance.
* **Documentation:**
  + **Incident Log:** Document all actions taken during the incident for post-incident review and reporting.
  + **Lessons Learned:** Conduct a post-incident review to identify lessons learned and areas for improvement.

#### **4. Conducting Training and Simulation Exercises**

* **Training:**
  + **Regular Workshops:** Hold quarterly workshops for the IRT on using tools, understanding roles, and following procedures.
  + **Awareness Programs:** Educate all employees on identifying potential security incidents and reporting procedures.
* **Simulations:**
  + **Tabletop Exercises:** Conduct tabletop simulations of different incident scenarios, such as a ransomware attack or phishing breach, to test the plan’s effectiveness.
  + **Live Drills:** Perform live drills in collaboration with IT and security teams to simulate real-world responses.
* **Evaluation:**
  + **Feedback:** Gather feedback from participants after each exercise to identify weaknesses and areas for improvement.
  + **Update Procedures:** Adjust the incident response plan based on the outcomes of simulations and feedback.

#### **5. Reviewing and Updating the Plan Regularly**

* **Scheduled Reviews:**
  + **Quarterly Review:** Conduct a comprehensive review of the IRP every quarter, focusing on updating threat scenarios, contact information, and technological changes.
  + **Post-Incident Review:** After each real incident or simulation, review the effectiveness of the response and make necessary updates.
* **Continuous Improvement:**
  + **Stay Informed:** Keep the plan aligned with the latest security best practices, emerging threats, and compliance requirements.
  + **Stakeholder Involvement:** Engage key stakeholders in the review process to ensure the plan remains relevant and effective.