TABLETOP EXERCISE PLAN FOR PAYMENT CARD DATA BREACH IN A RETAIL CHAIN

1. Overview:

This tabletop exercise was done to simulate the detection and response to a payment card data breach within a retail chain, following the Payment Card Industry Data Security Standard (PCI DSS) incident response requirements. As a Regulatory and Corporate Compliance Officer at a retail chain, I conducted this exercise to guide the incident response team (IRT) through the stages of identification, containment, eradication, recovery, and lessons learned, while also focusing on communication protocols and the evaluation of the response plan.

2. Objectives:

- Simulate detection and response to a payment card data breach.
- Apply PCI DSS incident response requirements during the incident.
- Develop and refine communication protocols for notifying stakeholders.
- Evaluate the effectiveness of the incident response plan.
- Document lessons learned and updated the response plan.

3. Participants

- **Incident Response Team (IRT):** IT Security, Legal, Compliance, HR, PR, Customer Service.
- **Executive Team:** CEO, CIO, CISO.
- **External Parties:** Payment Card Issuers, Regulatory Authorities, Forensic Investigators.

4. Exercise Scenario

The exercise simulated a data breach where attackers have compromised the payment card information of customers at multiple retail locations. The breach was discovered when unusual transaction patterns were reported by the payment card issuers.

5. Timeline of Events

Phase 1: Detection & Identification

- **Trigger Event:** Payment card issuers report unusual transactions linked to multiple customer accounts. Customers begin to complain about unauthorized charges.
- **IRT Actions:**
  - Verify the report and assess whether it indicates a data breach.
  - Initiate the incident response plan.
  - Engage forensic investigators to identify the scope of the breach.

Phase 2: Containment

- **Trigger Event:** Forensic investigators confirm the breach.
- **IRT Actions:**

- Isolate affected systems to prevent further unauthorized access.
- Implement temporary controls to protect other systems.
- Ensure that affected payment processes are rerouted or secured.

Phase 3: Eradication

- ❖ **Trigger Event:** Containment measures are confirmed to be effective.
- ❖ **IRT Actions:**
  - Remove malicious code, close vulnerabilities, and eliminate any residual risk.
  - Ensure that no backdoors or unauthorized access points remain.
  - Coordinate with forensic investigators to confirm eradication.

Phase 4: Recovery

- ❖ **Trigger Event:** Systems are cleared of threats.
- ❖ **IRT Actions:**
  - Restore affected systems and ensure they are fully operational.
  - Monitor systems closely for any signs of compromise post-restoration.
  - Validate that payment card processes are functioning securely.

Phase 5: Communication Protocols

- ❖ **IRT Actions:**
  - Develop communication templates for notifying customers, payment card issuers, and regulators.
  - Coordinate with PR to manage media inquiries and public statements.
  - Ensure that legal and compliance teams review all communications.

Phase 6: Post-incident response and Lessons Learned

- ❖ **IRT Actions:**
  - Conduct a post-incident review with all stakeholders.
  - Identify gaps in the incident response plan and areas for improvement.
  - Document lessons learned and update the incident response plan accordingly.
  - Schedule additional training or resources if necessary.

6. Evaluation

- **Effectiveness:** Assess how well the team followed the incident response plan and PCI DSS requirements.

- **Communication:** Evaluate the clarity, timeliness, and effectiveness of internal and external communications.
- **Coordination:** Analyse how well the IRT collaborated with external parties (e.g., forensic teams, regulators).
- **Recovery:** Assess the speed and completeness of system recovery.

7. Documentation

- **Incident Report:** Detailed log of the incident, actions taken, and outcomes.
- **Post-Incident Review:** Summary of lessons learned, with specific recommendations for plan updates.
- **Updated Incident Response Plan:** Revised plan reflecting improvements identified during the exercise.

8. Conclusion

The exercise concluded with a debrief session, where participants discussed the outcomes, challenges, and insights gained. This debrief informed the final updates to the incident response plan, ensuring the organization was better prepared for future incidents.