Simulated Cardholder Data Breach (PCI DSS 12.10 Incident Response)

Scenario Introduction

> Our SIEM flagged suspicious outbound traffic from multiple point-of-sale (POS) terminals across four stores. After investigation, we suspected malware designed to extract and exfiltrate payment card data. We treated this as a real-time exercise to validate our PCI DSS incident response readiness.

Phase 1: Identification

I said to the team

"The security team detects anomalies in data flow from POS systems at Store 104, 117, 121, and 129. What steps do we take to verify if this is a legitimate breach of cardholder data?"

Expected Actions:

- Pull logs from SIEM and endpoint detection systems
- Check for memory scraping malware or unauthorized remote sessions
- Determine if PAN, CVV, or track data may have been accessed

Phase 2: Containment

"Assuming we have confirmed a cardholder data breach, how do we isolate affected systems without disrupting business across all stores?"

My Plan :

- Immediately isolate POS terminals in affected locations (disable internet, revoke credentials)
- Notify store managers via the incident bridge
- Implement temporary offline payment fallback systems

- Ensure no further spread to central systems or HQ network

Phase 3: Eradication

"Now that we've contained the incident, we must eliminate the root cause."

Steps (PCI DSS-aligned and tailored to your chain):

- Conduct full forensic scans on compromised devices
- Wipe and reimage POS systems from trusted backups
- Patch any vulnerabilities (e.g., outdated RDP services or OS)
- Enforce password resets for affected service accounts

Phase 4: Recovery

I asked
"Before we bring systems back online, what validation do we require?"

Recovery Plan :

- Restore systems with validated clean images
- Monitor real-time logs for abnormal behavior
- Reconnect POS terminals under strict change control
- Notify internal teams and card brands that affected systems are secure

Phase 5: Communication Protocols

As IR Lead I say:

> "We now need to execute our notification responsibilities. Timing and clarity are critical."

Audience	**Message content**	**Sent By**	**Timing**
Customers	Notice of	Cusomer	Within 48-

	breach, how to monitor accounts, offer credit monitoring	service lead	72 hours
Card brands	Initial report of breach, ongoing updates per Visa/MC rules	Compliance manager	Within 24 hours
Acquiring Bank	Notify to assist with chargeback monitoring	CFO or controller	Immediately
Regulators	Depending on local laws (e.g.GDPR, CCPA etc)	Legal counsel	Within required timeframes
Internal staff	Instructions, talking points and data access freeze notices	IT and HR	Same day
Public/Media	Statement prepared (if needed)	Marketing + legal	Only if required

After-Action Review

I asked my team post-exercise:

"Did we meet the response timelines expected under PCI DSS?"

"Were any communication paths unclear or slow?"

"What slowed containment or eradication?"

Key Issues Noted:

- Delay in escalation from SIEM alert to human analyst

- Confusion over who notifies card brands
- Store staff uncertain about whom to call for POS isolation
- No current list of PCI Forensic Investigators (PFIs) on file

Update to Incident Response Plan

Final Recommendations i Presented to Leadership:

- Add a 24/7 escalation playbook with named contacts and timeframes
- Create store-level breach protocols (who to call, what to shut down)
- Pre-arrange contract with a certified PCI Forensic Investigator (PFI)
- Update communication templates for customers and banks
- Schedule quarterly IR training with rotating team leads

My Final Summary to Leadership

> This exercise demonstrated that our team is committed but needs better escalation processes, clearer communication lines, and real-time readiness. With these updates, the organization will not only meet PCI DSS standards, but be prepared to protect our brand, our customers, and our reputation.