Course

IFSC 76003-9U1 – Data Protection and Privacy

Submitted to

Prof Jennifer Davis

Prof Timothy Holthoff

Submitted by

Deepak Singla

Assignment 4

Data Breach Incident Response Plan
Quantum Leap, Inc

College

University of Arkansas Little Rock,

Little Rock, Arkansas

Data Breach Incident Response Plan
Quantum Leap, Inc.

Contents

Quantum Leap, Inc. – Data Breach Incident Response Plan

Section 1: Scope of the Plan

Applies to all data breach incidents involving subscriber, employee, or partner personal data (PII, PHI, financial, or proprietary information).

Section 2: Purpose and Objectives

This plan ensures Quantum Leap can respond swiftly and effectively to data breaches involving personal information. It supports regulatory compliance (e.g., GDPR, HIPAA, CCPA), protects subscriber trust, and minimizes financial and reputational damage across both conventional (EWS) and quantum (Q) computing platforms.

Section 3: Criteria to Activate the plan

Activate the DBIRP when:

- Subscriber data (e.g., contact, payment, medical billing) is accessed or exfiltrated without authorization
- Employee or vendor credentials are misused to access sensitive systems
- Physical devices (e.g., USB drives) containing personal data are lost or compromised
- Breach is suspected in either West Memphis or Paris data centers, or through remote access

Section 4: Response Team and Roles

Role	Responsibility
Chief Privacy Officer (CPO)	Lead response, coordinate investigation, regulatory reporting
Legal Counsel	Access legal obligations, draft notifications
Public Information Officer (PIO)	Manage public and subscriber communications

Role	Responsibility
Chief Data Officer (CDO)	Assess data types and impact
Chief Information Security Officer (CISO)	Support forensic analysis, containment
Human Resources Director	Coordinate internal communications and employee impact
Customer Support Director	Interface with affected subscribers
Vendor Representative	Coordinate with third-party vendors (e.g., HVAC, eVerifyMe)

Section 5: Phases of Incident Response

A. Detection and Initial Assessment

- Log and timestamp the breach report
- Identify breach source (e.g., HVAC credentials, USB device, support agent compromise)
- Identify affected systems: EWS subscriber database, Q billing engine, VPN tunnel
- Determine if personal data (PII, PHI, payment info) was accessed

B. Containment

- Disable compromised accounts or credentials (e.g., HVAC technician credentials)
- Isolate affected systems (e.g., subscriber database, VPN tunnel, billing engine)
- Suspend access to third-party systems if involved (e.g., Cool Computing, eVerifyMe)
- Preserve logs and evidence for forensic analysis

C. Investigation

- Coordinate with SOC and DOC teams in West Memphis and Paris

- Interview relevant staff (e.g., CFO, HVAC technician, support agents)
- Review access logs, badge records, and physical entry points
- Document timeline and breach vector (e.g., lateral movement from HVAC to subscriber database)

D. Impact Analysis

- Identify data types affected (e.g., payment info, medical records, subscriber contact data)
- Estimate number of affected individuals and jurisdictions
- Assess risk of harm (financial fraud, identity theft, reputational damage)

E. Notification and Reporting

- Notify affected subscribers with actionable guidance (e.g., fraud alerts, credit monitoring)
- Report to regulators (e.g., GDPR authorities, U.S. state agencies) within required timeframes
- Coordinate with law enforcement if criminal activity suspected (e.g., offshore transfers)
- Publish updates via EWS.com and subscriber portals

F. Remediation

- Offer credit monitoring or identity protection services to affected parties
- Update internal access controls and vendor onboarding procedures
- Review and revise data handling policies across EWS and Q
- Conduct staff training on breach prevention and physical data security

Section 6: Documentation and Notifications

- Maintain breach log with all actions, decisions, and communications
- Use Quantum Leap's standardized incident reporting form
- Prepare press releases and subscriber FAQs with PIO and Legal
- Ensure all communications are reviewed by Legal and approved by the CPO

Section 7: Post-Incident Review

- Conduct a “lessons learned” session with all stakeholders
- Update DBIRP based on findings and feedback
- Report outcomes to the C-Suite and board
- Track implementation of corrective actions across both data centers

Section 8: Appendix and Templates

- Quantum Leap Breach Notification Letter Template
- Subscriber Communication FAQ
- Regulator Contact List by Jurisdiction
- Vendor Breach Notification Checklist
- Incident Reporting Form (customized for EWS and Q)

References

1. Class Lecture discussion
2. 2025 IFSC 7360 Class Assignments and Final Project – Data Protection and Privacy
3. Copilot.microsoft.com
4. Prompt “Create sample Data Breach Incident response”
5. Quantum Leap Organizational Context (Internal Roles and responsibilities, Vendor relationship, subscriber data types and Infrastructure.
6. **GDPR – Article 33: Notification of a Personal Data Breach** https://gdpr-info.eu/art-33-gdpr/
7. **EDPB Guidelines on Breach Notification under GDPR** https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf
8. **CCPA Breach Reporting – California Attorney General** https://www.oag.ca.gov/privacy/databreach/reporting