Data Security Incident Analysis & Remediation Project

Executive Summary
I conducted a detailed security incident analysis for an educational technology company following a data leak of confidential business plans. This project demonstrates my ability to analyze security incidents, evaluate control effectiveness, and provide actionable recommendations based on NIST frameworks.

Business Context
- **Industry**: Educational Technology
- **Product**: Automated Assignment Grading Application
- **Data Types**: Academic institution data, instructor information, parent records, student data
- **Incident**: Unauthorized disclosure of internal business plans via social media

Incident Analysis

Root Cause Investigation
Through careful analysis of the incident, I identified several critical security control failures:
- Excessive sharing of sensitive internal folders during sales meetings
- Lack of access revocation procedures after temporary sharing
- Insufficient segregation between promotional and confidential materials
- Inadequate controls on external sharing capabilities

Control Framework Assessment
I evaluated the existing security controls against NIST SP 800-53: AC-6 (Least Privilege) requirements:

Current State Assessment:
- No automatic access expiration for temporary shares
- Mixed storage of materials with different sensitivity levels
- Inadequate role-based access controls
- Limited audit trail of access grants and usage

Recommended Security Improvements

Technical Controls
1. **Implement Time-Based Access Revocation**
   - Automatic expiration of shared access
   - Configurable timeframes based on business needs
   - System notifications for access expiration

2. **Enhanced Role-Based Access Control (RBAC)**
   - Granular permission sets based on job functions
   - Separate repositories for different sensitivity levels

  - Structured approval workflow for access elevation

Operational Controls
1. **Access Review Procedures**
   - Regular audit of active shares
   - Quarterly privilege reviews
   - Documentation of access justifications

2. **Data Classification Guidelines**
   - Clear marking of internal vs external documents
   - Separate storage locations based on sensitivity
   - Automated classification tools integration

Implementation Impact Analysis

Security Benefits
- Reduced risk of accidental data exposure
- Improved audit capability
- Enhanced compliance with NIST guidelines
- Better visibility into information access patterns

Business Benefits
- Streamlined sharing workflows
- Reduced manual security oversight
- Improved partner collaboration processes
- Enhanced protection of intellectual property

Skills Demonstrated
- Security incident analysis
- NIST framework implementation
- Control evaluation and design
- Risk assessment
- Technical documentation
- Business impact analysis

Tools & Technologies Used
- NIST Cybersecurity Framework
- NIST SP 800-53 Controls
- Access Control Systems
- Security Audit Tools

Metrics & Success Criteria
- Implementation of automatic access expiration
- Completion of initial access review

- Development of role-based access matrices
- Zero critical findings in follow-up security audit

Lessons Learned
This incident highlighted the importance of:
- Proactive access management
- Clear data classification
- Automated security controls
- Regular security reviews

Project Deliverables
1. Incident analysis report
2. Control improvement recommendations
3. Implementation roadmap
4. Security metrics dashboard
5. Updated security policies

This project showcases my ability to:
- Analyze complex security incidents
- Apply industry frameworks
- Develop practical security solutions
- Balance security with business needs
- Create professional technical documentation

Note: This case study has been anonymized to protect confidential information while preserving the demonstration of security analysis capabilities.