# Security Risk Assessment Report for Social Media Organization

## Executive Summary

Following a recent data breach compromising customer personal information, our security assessment identified four critical vulnerabilities that require immediate remediation. This report outlines hardening measures to address password sharing, default credentials, inadequate firewall rules, and lack of multi-factor authentication.

## Part 1: Hardening Tools and Methods to Implement

### **1. Multi-Factor Authentication (MFA) Implementation**

**Implementation Plan:**

* Deploy MFA solution requiring employees to authenticate via:
  + Primary method: Strong password
  + Secondary method: Mobile authenticator app (e.g., Google Authenticator, Microsoft Authenticator)
  + Fallback method: SMS-based verification (for accessibility)
* Enforce MFA for all internal systems, especially database admin access
* Conduct employee training on MFA setup and use

### **2. Comprehensive Password Policy Enforcement**

**Implementation Plan:**

* Establish policy requiring:
  + Minimum 12-character passwords
  + Mandatory mix of uppercase, lowercase, numbers, and special characters
  + Password changes every 90 days with no reuse of last 5 passwords
  + Account lockout after 5 failed attempts (30-minute lockout duration)
* Replace all default credentials immediately, especially database admin passwords
* Implement enterprise password manager to reduce password sharing

### **3. Firewall Rule Configuration and Maintenance**

**Implementation Plan:**

* Establish baseline firewall rules to:
  + Block all inbound traffic by default (whitelist only necessary services)
  + Filter outbound traffic to prevent data exfiltration
  + Implement geo-blocking for high-risk regions
* Create maintenance schedule:
  + Weekly review of firewall logs
  + Monthly rule audits
  + Immediate updates following security incidents

### **4. Employee Security Awareness Program**

**Implementation Plan:**

* Monthly security training sessions covering:
  + Risks of password sharing
  + Phishing identification
  + Proper credential management
* Simulated phishing exercises quarterly
* Clear disciplinary policy for policy violations

## **Part 2: Recommendations and Justification**

### **Multi-Factor Authentication**

MFA implementation addresses both the immediate lack of MFA and helps mitigate password sharing by making shared credentials insufficient for access. Our recommendation goes beyond basic MFA by:

Using authenticator apps as primary 2FA method (more secure than SMS)

Including mandatory MFA for database admin access

Reducing breach impact through layered authentication

### **Password Policy Enhancements**

The proposed password policies directly address:

* + Default credential vulnerability through immediate credential rotation
  + Password sharing through complexity requirements and monitoring
  + Brute force protection via account lockout mechanisms

The addition of an enterprise password manager reduces the temptation to share passwords while maintaining usability.

### **Firewall Management**

Regular firewall maintenance with strict default-deny posture will:

* + Prevent unauthorized access attempts
  + Limit potential attack surfaces
  + Provide logging for incident investigation
  + Block suspicious traffic patterns associated with data exfiltration

### **Security Awareness Training**

Employee education is critical because:

* Human factors often undermine technical security measures
* Training reduces risky behaviors like password sharing
* Awareness helps identify social engineering attempts

## **Implementation Timeline**

|  |  |  |  |
| --- | --- | --- | --- |
| **Priority** | **Measure** | **Timeline** | **Owner** |
| Critical | Default password replacement | 24 hours | Infrastructure Team |
| High | MFA implementation | 1 weeks | Security Team |
| High | Firewall rule baseline | 1 week | Network Team |
| Medium | Password policy enforcement | 2 weeks | HR & Security |
| Ongoing | Security awareness training | Monthly | Training Team |

## **Conclusion**

By systematically implementing these hardening measures, the organization can significantly reduce the risk of future breaches. The combination of technical controls and employee education addresses both technological vulnerabilities and human factors that contributed to the recent incident. Regular audits and updates will ensure these measures remain effective against evolving threats.