IT Risk Assessment: Capital One

Caleb Choo

Company Background

- Industry: Financial Services (Banking, Credit Cards, Loans)
- Employees: 50,000+
- Public Tech Stack:

  - AWS Cloud Infrastructure

  - Capital One Mobile App

  - Web Banking Platform

  - Third-Party Fintech APIs

Assessment Methodology

- Framework: NIST SP 800-30
- Risk = Likelihood × Impact (1–5 scale)
- Focused on 5 IT Assets: AWS S3, Mobile App, Admin Portal, Fintech API, Email System

IT Asset Inventory

1. AWS S3 Buckets
2. Capital One Mobile App
3. Internal Admin Portal
4. Fintech APIs (Mint, Plaid)
5. Email & Collaboration Systems

Risk Scores

- AWS S3 – Misconfigured bucket access – Risk Score: 20 (Critical)
- Mobile App – Weak MFA – Risk Score: 12 (Medium-High)
- Admin Portal – Insider threat – Risk Score: 15 (High)
- Fintech API – Insecure endpoints – Risk Score: 8 (Medium)
- Email System – Phishing – Risk Score: 12 (Medium-High)

Risk Score Formula

Risk Score = Likelihood x Impact

Likelihood (1 = Rare, 5 = Almost Certain)

Impact (1 = Negligible, 5 = Critical)

For example:

1. AWS S3 - Data Breach

- **Likelihood = 4 Based on breach in 2019 due to misconfigured S3 Access.**
- **Impact = 5 due to 100M+ exposed customer records**
- **Score = 4x5 = 20 (critical)**

Recommended Controls

- AWS S3: Least privilege, access logging, encryption
- Mobile App: Enforce MFA, device fingerprinting
- Admin Portal: Quarterly access reviews
- Fintech APIs: Secure APIs, authentication tokens
- Email System: Phishing simulations, SPF/DKIM/DMARC

Conclusion & Next Steps

- Highest Risk: Misconfigured cloud storage (AWS S3)
- Insider threat and phishing also significant
- Next Steps:
  - Prioritize high-score risks
  - Implement controls
  - Reassess post-control scores

Sources

https://cloudsecurityalliance.org/blog/2019/08/09/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach

https://www.securitymetrics.com/blog/securitymetrics-nist-800-30-risk-assessment

https://www.darkreading.com/cyberattacks-data-breaches/capital-one-attacker-exploited-misconfigured-aws-databases

https://cloudsecurityalliance.org/blog/2019/08/09/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach

https://cloudsecurityalliance.org/blog/2019/08/09/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach