Case Study: First Horizon Corporation – Cybersecurity Breach

Introduction

SOX Section 404 is a provision that mandates how public companies must report on the effectiveness of their internal controls. This rule requires companies to establish, maintain, and annually assess an adequate internal control structure for their financial reporting processes, with the goal of increasing transparency and accountability in financial practices. **(Accounting Insights, n.d.).**

In view of that, the cybersecurity breach at First Horizon Bank demonstrates multiple failures in internal controls over financial reporting, which are required under SOX Section 404.

1. Stolen Login Credentials → Weak IT General Controls

- First Violation: First Horizon relied on simple usernames and passwords without MFA. This failure in preventive ITGCs meant unauthorized users could gain access, directly undermining financial data integrity.

  SOX 404 Principle: Companies must implement user access controls to ensure only authorized personnel can access systems impacting financial reporting.

2. Vendor Software Vulnerability → Weak Entity-Level Controls

- Violation: Attackers exploited a vendor software flaw, showing that First Horizon did not have effective vendor oversight and patch management. This is a breakdown in entity-level controls because management did not ensure vendors adhered to secure practices.
- SOX 404 Principle: Management must oversee and evaluate third-party risks that affect internal controls over financial reporting.

A table listing risks and corresponding internal controls

Risk	Condition	Proposed Internal Control
Compromised/Stolen login credentials	Weak authentication mechanisms allowed stolen login credentials to provide system access	Implementing Preventive Controls like the use of Multi-Factor (MFA) authentication, Biometric verifications, Passkeys or Tokens
Vendor software vulnerability	Failure to maintain adequate security and patch management in third-party applications created exploitable entry points into the system	Entity-Level Control for Vendor risk management program with patching, audits, and due diligence.
Insufficient Access Monitoring	No real time monitoring to detect unauthorized transactions that affect financial reporting integrity.	Application Controls could be established to log and monitor to detect suspicious activities and transaction patterns

Cybersecurity Remediation Plan Phase 1: Emergency (1-30 Days)

- Reset all passwords, install MFA on all systems
- Add biometric scanners for sensitive areas
- Deploy passkeys for key systems
- Limit access to essential employees only
- Patch all vendor software vulnerabilities

Phase 2: Defense (1-6 Months)

- Full MFA + biometric access for financial systems
- AI fraud detection with real-time blocking
- 24/7 security monitoring center
- Role-based access controls with monthly reviews

Phase 3: Maintenance (Monthly-Annually)

- Monthly security testing and quarterly training
- Annual vendor audits and continuous monitoring

Cloud-Based Access Control Structure

Basic Role: All employees get standard cloud access with MFA for business applications
Financial Role: Bank tellers and officers get cloud banking system access with MFA + biometrics (50-100 people)
Admin Role: IT staff and managers get privileged cloud access with MFA + biometrics + approval workflows (10-15 people)
Emergency Role: CEO and CTO get break-glass cloud access with full security controls + automatic logging (2-3 people).

Key Security Measures

Access Controls: MFA required for all logins, biometrics for financial systems, passkeys for customer accounts, strict role-based permissions
Vendor Management: Security certification required, continuous monitoring, quarterly audits, immediate patching requirements
Real-Time Monitoring: Suspicious detection monitoring, 24/7 SOC, automatic transaction blocking, instant customer alerts

Prepared by Grace A. N. Awuma