

Capstone Project Root Cause Analysis

Root Cause Analysis

1. Lack of Verification Mechanisms:

- The primary failure was the absence of a multi-step verification process for validating vendor invoices.
- Employees trusted received invoices without independently confirming their legitimacy, exposing the organizations to fraud.

2. Effective Social Engineering:

- The attacker skillfully exploited human psychology, using realistic email communication and impersonation tactics.
- Employees were deceived into believing the fraudulent invoices were legitimate requests from a trusted partner.

Analysis Summary: The lack of internal invoice verification controls combined with sophisticated social engineering tactics created an environment where malicious activities went undetected for an extended period. Strengthening human and technological defenses is critical to prevent such breaches in the future.