Capstone Project Key Findings

Key Findings

1. **Root Causes:**
    - *Lack of Verification Mechanisms:* Insufficient invoice authentication protocols allowed fraudulent payment requests to bypass detection.
    - *Effective Social Engineering:* The attacker leveraged sophisticated phishing emails and spoofed communications to manipulate trusted processes.
2. **Actions Taken:**
    - *Detection and Investigation:* Internal audits were launched to trace unauthorized payments.
    - *Collaboration with Authorities:* Facebook and Google cooperated with law enforcement agencies, leading to the arrest of the perpetrator and partial fund recovery.
3. **Effectiveness and Timeliness:**
    - Initial detection was delayed by nearly two years, showing a need for stronger real-time monitoring.
    - After detection, response efforts were swift, efficient, and led to successful legal action.
4. **Successes, Gaps, and Failures:**
    - *Success:* Effective collaboration with international law enforcement.
    - *Gap:* Lack of invoice verification procedures.
    - *Failure:* Absence of employee training on recognizing phishing scams.

These findings offer crucial insights for bolstering organizational cybersecurity frameworks.