INFO 7374 - Cybersecurity Audit and Compliance
Week 3 Assignment

Name: Krisha Lakhani
NUID: 002334794

1. Risk Identification

Target Data Breach (2013):

- Risks:
    - Weak vendor risk management.
    - Insufficient access controls for third-party vendors.
    - Lack of network segmentation between vendor systems and sensitive payment data.
    - Use of stolen credentials from a third-party HVAC vendor.

SolarWinds Cyberattack (2020):

- Risks:
    - Compromised supply chain via malicious software updates.
    - Lack of software integrity checks.
    - Insufficient monitoring of software updates.
    - Delayed detection of the attack due to sophisticated evasion techniques.
    - Presence of malware in legitimate software updates.

Shared Risks:

- Third-party/vendor vulnerabilities.
- Inadequate monitoring and detection mechanisms.

Unique Risks:

- **Target:** Weak access controls and lack of network segmentation and reliance on vendor systems without proper oversight.
- **SolarWinds:** Malware inserted through a software update and poor supply chain security practices.

INFO 7374 - Cybersecurity Audit and Compliance
Week 3 Assignment

Name: Krisha Lakhani
NUID: 002334794

2. Control Assessment

Effectiveness of IT General Controls (ITGC):

Target: Poor IT general controls related to monitoring vendor activity and access, along with poor network segmentation, have provided attackers with the ability to gain access and laterally move within the network. This constitutes a serious weakness in the management of vendor risk and access controls.

SolarWinds: The weakness in ITGCs-in terms of patch management, controls were lacking that would have detected and prevented malicious updates-allowed attackers to compromise the supply chain of the software. This depicts critical vulnerabilities in the security of the supply chain and how the inability of ITGCs was not able to protect such an attack. Like Target, SolarWinds suffered from weaknesses in access controls, although the vector differed-the compromised build process versus vendor access.

Proposed Controls:

For Target:

1. Implement multi-factor authentication (MFA) for third-party access.
2. Enforce strict network segmentation to isolate vendor systems from sensitive data.
3. Regularly audit and assess third-party vendor security practices.

For SolarWinds:

1. Integrity checks for software updates using cryptographic signatures.
2. Conduct regular vulnerability assessments of supply chain components.
3. Regular security audits for anomalous behaviors in third-party software.

INFO 7374 - Cybersecurity Audit and Compliance
Week 3 Assignment

Name: Krisha Lakhani
NUID: 002334794

3. Similarities and Differences

Similarities:

- Both breaches exploited third-party vulnerabilities, highlighting a systemic weakness in managing external dependencies.
- Ineffective detection mechanisms in both cases allowed attackers extended access and time to operate before discovery, demonstrating a failure in timely threat detection.
- Both incidents revealed insufficient vendor oversight and risk management practices, indicating a common root cause.
- Weak monitoring and detection mechanisms for anomalous activities were present in both breaches, contributing to the prolonged attack lifecycle.

Differences:

- **Mode of Attack:** Target's breach stemmed from stolen vendor credentials, granting access to the network. SolarWinds, conversely, was compromised through the insertion of malware into a legitimate software update, poisoning the supply chain.
- **Scale:** The Target breach primarily impacted customer payment data, affecting approximately 40 million customers. The SolarWinds attack had a broader and more systemic impact, affecting numerous organizations globally, including government entities, demonstrating a difference in the scope of compromise.

INFO 7374 - Cybersecurity Audit and Compliance
Week 3 Assignment

Name: Krisha Lakhani
NUID: 002334794

4. Lessons Learned

Lessons:

1. **Proactive Vendor Risk Management:** The organization should always identify and monitor third-party risks through stringent management and oversight of vendors.
2. **Importance of Network Segmentation:** Segregating sensitive systems limits the impact of breaches, containing lateral movement and preventing widespread compromise.
3. **Improved Patch Management:** Rigorous integrity checks ensure safe software updates, including stringent validation of software updates in the supply chain. This monitoring needs to be continuous in order to identify anomalies as quickly as possible.

Actionable Recommendations:

1. **Vendor Risk Management:** Establish an effective vendor risk management policy. Establish strong frameworks with regular audits to understand and mitigate third-party risks.
2. **Threat Detection and Response:** Intrusion detection systems and endpoint detection and response solutions will be implemented to provide advanced threat detection using AI/ML in the identification of anomalies.
3. **Security Awareness and Secure Development:** Cybersecurity best practices inculcation among employees and vendors, enforcement of secure development with code reviews and integrity checks in all software updates.

INFO 7374 - Cybersecurity Audit and Compliance
Week 3 Assignment

Name: Krisha Lakhani
NUID: 002334794

5. Key Audit Tasks Creation

Vendor Risk Management (Target):

1. Review the cybersecurity risks associated with vendor selection and onboarding.
2. Review the contracts of vendors for security requirements and compliance clauses.
3. Review access controls and permissions granted to third-party vendors.
4. Assess the implementation of MFA and other access control mechanisms for vendors.
5. Assess network segmentation practices and verify network segmentation policies by testing their effectiveness in isolating sensitive systems.

Supply Chain Security (SolarWinds):

1. Software update integrity check by cryptographic methods, integrity verification process of the software update to be examined, including code-signing.
2. Audit supply chain security practices will be performed; the audit should include third-party providers of software. Audit supply chain risk management policy, including evaluation and certification of vendors.
3. Log monitoring and analysis shall be performed for software installation activities pertaining to anomaly.
4. Testing of monitoring systems for the capability of detecting malicious activities in third-party software.