Case Study Analysis on 2013 Target Data Breach and 2020 SolarWinds Data Breach

Introduction:

This is an analysis of the Case Study of the 2013 Target Data Breach and the , integrating risk identification, control assessment, similarities and differences, lessons learned, audit tasks, and the application of RPO/RTO concepts, based on both the case study scenarios and key focus areas

Summary of 2013 Target Data Breach

In November–December 2013, hackers stole 40 million payment card numbers and 70 million customer records from Target during the holiday shopping season. Attackers didn't break directly into Target's systems. They first compromised a third-party HVAC vendor (Fazio Mechanical) and stole its credentials, then used those to infiltrate Target's internal network. Once inside, they moved laterally and planted malware on point-of-sale (POS) registers nationwide to capture card data in real time.

Timeline & Detection Initial Infiltration: ~November 15, 2013 Malware deployed to POS systems: by November 27 (Black Friday) Target noticed suspicious activity mid-December after an alert from a third party. Public disclosure: December 19, 2013 (about 20 days after the breach began, but only four days after Target internally confirmed it).

Summary of SolarWinds Data Breach

In **2020**, hackers compromised **SolarWinds' Orion software build system**, inserting malware into legitimate updates. Thousands of organizations who use Orion, including U.S. government agencies, installed the backdoored updates, giving attackers broad access were affected. The Malware introduced around March–June 2020; remained undetected for months; publicly disclosed in December 2020.

Risk Identification for both

Risk Identification for Target Data Breach	Risk Identification for SolarWinds Data Breach
Inadequate access controls management based on the principle of least privilege	A supply-chain breach that compromised the software production and update process;
Vendor risk management – this is being the main risk that led to the breach	Malware introduced into reliable updates
Insufficient network segmentation	Poor traffic monitoring
Stolen third-party credentials	Gaps in patch management

Shared and Unique Risks

Shared Risk	Unique to Target	Unique to SolarWinds
Lack of robust controls over privileged access	Risk through third-party /vendor access to credentials	Compromised backdoor software system update
Inadequate monitoring and anomaly detection		
Weak supply chain, vendor, and third-party security		

2. Control Assessment

IT General Controls (ITGC) Effectiveness Analysis:

Target Breach ITGC Failures:

- **Logical Access Controls:** Network segmentation and vendor access restrictions were not properly enforced.
- **Change Management:** Controls over vendor access modifications and privilege escalation were insufficient.
- **IT Operations:** Detection and response to incidents were inadequate.

Proposed Controls:

- **Enhanced Vendor Security Assessment:** Conduct thorough security questionnaires and on-site audits for all third-party vendors with network access.
- **Network Segmentation Controls:** Implement a zero-trust architecture with micro-segmentation to isolate vendor access from critical systems.
- **Privileged Access Management (PAM):** Introduce just-in-time access controls with multi-factor authentication for all vendor connections.

Failures and Proposed Controls

SolarWinds Attack ITGC Failures:

- **Change Management:** Software development and release processes were compromised.
- **Backup and Recovery:** Verification of software integrity prior to distribution was insufficient.
- **IT Operations:** Monitoring of software supply chain security was lacking.

Proposed Controls:

- **Software Supply Chain Security:** Apply comprehensive code signing, integrity checks, and secure software development lifecycle (SDLC) practices.
- **Enhanced Monitoring and Detection:** Use advanced threat detection systems with behavioral analytics to identify unusual software activity.
- **Patch Management Validation:** Implement strict testing and validation procedures for all software updates before deployment.

- **3. Similarities and Differences**
  Similarities in Both:
- **Inadequate Third-Party Risk Management:** Both organizations did not sufficiently evaluate and monitor security risks linked to external entities in their supply chain.
- **Insufficient Real-Time Monitoring:** Both breaches went undetected for extended periods due to weak security monitoring and incident detection capabilities

Differences in Both:

1. **Complexity of the Attack Approach**: Target involved relatively straightforward credential theft and lateral movement, while SolarWinds required a complex smart method to attack the software development build process.
2. **Scope of Impact**: Target primarily affected one organization's customers, while SolarWinds created a widespread supply chain compromise affecting thousands of organizations globally including government agencies like homeland security.

Three Critical Lessons:

Early Detection and Rapid Response Capabilities: Organizations must invest in advanced real-time monitoring, threat detection, and incident response capabilities to minimize damage through early identification and immediate action. Both the Target and SolarWinds breaches demonstrated that prolonged undetected access leads to exponentially greater damage - Target's breach continued for approximately 20 days undetected, while SolarWinds remained compromised for 8-9 months. Early detection systems with automated alerting, combined with practiced incident response procedures, can significantly reduce the scope of data exposure, financial losses, and reputational damage. This includes implementing Security Operations Centers (SOCs) with 24/7 monitoring, User and Entity Behavior Analytics (UEBA) for anomaly detection, and pre-established incident response playbooks with clear escalation procedures.

Comprehensive Third-Party Risk Management: Organizations must implement effective vendor risk programs with security requirements, regular audits, and continuous monitoring across the entire supply chain. Third-party access should be restricted and closely monitored.

Supply Chain Security Validation: Organizations must implement pre-deployment verification processes for all software, updates, and third-party components before installation. This includes digital signature verification, hash validation, and software composition analysis to detect malicious code or unauthorized modifications. Companies should never automatically trust vendor updates and must establish independent validation procedures using tools like code signing verification utilities, binary analysis platforms, and software bill of materials (SBOM) scanners. Implementation should include mandatory security testing in isolated environments, automated integrity checks through tools like Veracode or Snyk, and approval workflows that require security team validation before any software deployment to production systems.

Actionable Recommendations:

- **Vendor Management:** Require SOC 2 Type II reports, use Audit Board for continuous vendor risk monitoring, deploy Nessus for vulnerability scans, and conduct quarterly vendor security assessments with risk registers.
- **Change Management:** Use automated change tracking with Splunk, enforce formal approval workflows, maintain change logs, require UAT, implement rollback procedures, and conduct ITGC-aligned reviews.
- **Logical Access:** Enforce RBAC with least privilege, implement MFA, conduct periodic automated access reviews, monitor failed logins via Splunk, and deploy PAM solutions.
- **Supply Chain Security:** Validate software with digital signatures and SBOM scans, test in isolated environments before deployment, and track all software changes.
- **Real-Time Monitoring**: Centralize log monitoring in Splunk, establish 24/7 SOC operations, deploy UEBA for anomaly detection, and define incident response escalation protocols.
- **ITGC Framework**: Strengthen Change Management, Access Controls, Backup/Recovery, and IT Operations with incident runbooks, monitoring dashboards, and automated backups with restoration testing.
- **Compliance & Governance:** Apply COBIT for IT governance, ISO 27001 for security management, NIST CSF for risk management, and use Audit Board for compliance oversight and reporting.
- **Business Continuity:** Define RTOs/RPOs, perform annual disaster recovery tests, and ensure automated daily offsite/cloud backups.

Key Audit Tasks Creation

Vendor Risk Management Audit (Target-focused)

Phase	Strategy
1 - Risk Management and Assessment	Document and evaluate IT risk management frameworks using ISO 31000 standards Assess risk identification processes for third-party vendor relationships Review risk prioritization matrices and mitigation strategies

	Test risk response adequacy for vendor access controls using Audit Board risk registers **Timeline – (1-3 days)**
2 – Data Integrity and Security Controls	Evaluate encryption controls for payment card data (PCI DSS compliance) Test data classification processes and handling procedures for sensitive customer information Assess backup and recovery procedures for critical payment systems Validate data access logging and monitoring controls using Splunk analytics Review data manipulation prevention controls and database security measures **Timeline – (1-4 days)**
3 - Access Control and Identity Management (4 days)	Test multi-factor authentication implementation across all systems Evaluate role-based access control (RBAC) and principle of least privilege enforcement Review user provisioning, deprovisioning, and access change procedures Assess privileged access management for administrative accounts Validate regular access reviews and certification processes
4 - Vendor Risk Management and Third-Party Controls	Review vendor security assessment and due diligence procedures

	Test network segmentation between vendor and internal systems using Nessus scanning Evaluate vendor contract security requirements and SLA compliance Assess ongoing vendor monitoring and risk reassessment processes

SolarWinds Attack - Multi-Domain Audit Approach

Phases	Strategy
1 - Risk Management and Assessment (3 days)	• **Evaluate supply chain risk management frameworks aligned with NIST SP 800-161** • **Assess risk identification processes for software development and acquisition** • **Review third-party software component risk assessment procedures** • **Test risk communication and escalation processes for supply chain threats**
2: Data Integrity and Security Controls (4 days)	Test software integrity verification using digital signatures and hash validation Evaluate code signing processes and certificate management controls Assess source code protection and development environment security Review Software Bill of Materials (SBOM) tracking and vulnerability management

	Test data protection controls for development and build systems
3 - IT General Controls (ITGC) - Change Management Focus (4 days)	Evaluate change management procedures for software development lifecycle Test approval workflows for software updates and patches Assess testing procedures before production deployment (UAT implementation) Review rollback procedures and change monitoring controls Validate change documentation and audit trail requirements
• 4 - Supply Chain Security and Compliance (4 days)	Test software acquisition validation procedures and vendor security assessments Evaluate patch management processes using automated deployment tools (WSUS/SCCM) Assess threat intelligence integration for supply chain security monitoring Review incident response procedures for supply chain compromise scenarios Test business continuity and disaster recovery controls (RTO/RPO validation)

Technology-Enhanced Audit Procedures:

- **Splunk log analysis for security event correlation across all domains**
- **Nessus vulnerability scanning for network and system assessments**
- **Automated evidence collection and documentation management**
- **Jira workflow coordination for audit team task management and progress tracking**

Implementation Timeline

- **Preparation: 2 weeks (scope definition, tool configuration, stakeholder alignment)**
- **Target Audit Execution: 2 weeks (covering all four audit phases systematically)**
- **SolarWinds Audit Execution: 2 weeks (parallel or sequential based on resource availability)**
- **Documentation and Reporting: 1 week (consolidated findings and recommendations)**
- **Follow-up and Monitoring: Quarterly reviews with automated compliance tracking**

Written by Grace Aku Nutifafa Awuma