# Target Corporation Data Breach (2013): Phishing Attack via Third-Party Vendor

**21CSC308T – SECURITY RISK MANAGEMENT PRINCIPLES**

*Submitted by*

**Hardik Jindal – [RA2311030010221]**
**Shubham Jha – [RA2311030010230]**
**Ananya Dahiya – [RA2311030010236]**


**DEPARTMENT OF NETWORKING AND COMMUNICATIONS**

**FACULTY OF ENGINEERING AND TECHNOLOGY**

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**
**KATTANKULATHUR – 603 203 NOVEMBER**
**2025**

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY KATTANKULATHUR – 603 203

# BONAFIDE CERTIFICATE

This is to certify that the Case Study Report titled **"Target Corporation Data Breach (2013): Phishing Attack via Third-Party Vendor"** is a bonafide record of work carried out by the following students **HARDIK JINDAL [RA2311030010221], SHUBHAM JHA [RA2311030010230], ANANYA DAHIYA [RA2311030010236]**, as part of the course **21CSC308T - Security Risk Management Principles**, during the academic year **2025–2026**. This report has been submitted in partial fulfillment of the requirements for the successful completion of the course and has not been submitted elsewhere for any academic or non-academic purpose. The work is found to be satisfactory and is hereby accepted.

Submitted by:

| **Register Number** | Name of Students |
|---|---|
| Hardik Jindal | RA2311030010221 |
| Shubham Jha | RA2311030010230 |
| Ananya Dahiya | RA2311030010236 |

Date of Submission:

**Faculty Signature**

Mrs. R. Abirami
Assistant Professor
Dept of Networking and Communications

**HoD/NWC**

Dr.M.Lakshmi
Professor & Head
Dept of Networking and Communications

**Case Title**

# Target Corporation Data Breach (2013): Phishing Attack via ThirdParty Vendor

# Introduction

## Organization Description:

Target Corporation is one of the largest retail companies in the United States, operating over 1,800 stores nationwide. The organization maintains a vast amount of sensitive customer data, including payment card details, personally identifiable information (PII), and internal corporate data. Its operations heavily depend on interconnected IT systems, third-party vendors, and digital payment infrastructures.

## Scope of Risk Identification and Control:

This report focuses on the information technology and supply chain risks that contributed to the 2013 Target data breach. The incident began when attackers compromised a third party HVAC vendor through a phishing email.

Using the stolen vendor credentials, the attackers gained unauthorized access to Target's internal network, eventually deploying malware on the Point-of-Sale (POS) systems to steal millions of customer payment records.

The purpose of this report is to identify and analyze the assets, threats, vulnerabilities, and risks involved in the attack and to recommend effective risk control measures to prevent similar incidents.

# Asset Identification

Asset Identification is the process of recognizing and documenting all valuable assets within an organization, including hardware, software, data, and personnel.

| Asset ID | Asset Description | Owner/Department | Importance |
|---|---|---|---|
| A1 | Customer payment card data (credit/debit card information of customers) | IT & Payment Systems | High |
| A2 | Point-of-Sale (POS) systems handling realtime transactions | IT Infrastructure | High |
| A3 | Vendor access credentials for third-party HVAC maintenance company | Supply Chain / Vendor Management | High |
| A4 | Internal corporate network and connected servers | IT Operations | High |

The assets involved in the Target breach include critical customer data, POS systems, and vendor credentials that serve as gateways to Target's internal network.

# Risk Identification

Risk Identification is the process of detecting and documenting potential threats that could negatively impact an organization's assets or operations.

## 1.Threat Identification

Multiple threats were exploited by attackers to infiltrate Target's network. The primary threat vector was phishing, which initiated credential theft. Once credentials were obtained, attackers deployed malware, moved laterally within the internal network, and exfiltrated sensitive data to remote servers.

| Threat ID | Threat Description | Source | Potential Impact | Likelihood |
|---|---|---|---|---|
| T1 | Phishing emails targeting vendor employees: Deceptive emails tricked employees at the vendor company into downloading malware, enabling attackers to capture valid Target network credentials. | NIST-SP 800-30 | Credential theft and unauthorized network access | High |
| T2 | Malware installation on POS systems: Once access was obtained, attackers deployed memory-scraping malware to collect payment card data from POS terminals. | ENISA Threat Landscape 2023 | Theft of millions of credit/debit card records | High |
| T3 | Lateral movement within Target's internal network: Attackers leveraged stolen credentials and poor segmentation to move from the vendor zone to Target's core payment systems. | ISO 27005 | Privilege escalation and full network compromise | Medium |

| | | | | |
|---|---|---|---|---|
| T4 | Data exfiltration to attackercontrolled servers: Stolen customer data was transmitted to external servers using encrypted channels, bypassing detection mechanisms. | NIST-SP 800-61 | Large-scale data breach, financial penalties. | High |

## 2.Vulnerability Identification

Several vulnerabilities across Target's IT environment and third-party management system facilitated the breach. These vulnerabilities include technical flaws such as weak network segmentation and organizational weaknesses like inadequate training and lack of multi-factor authentication.

| Vulnerability ID | Vulnerability Description | Asset Linked | Source Document | Severity |
|---|---|---|---|---|
| V1 | Lack of MultiFactor Authentication (MFA): Vendor employees could access Target's systems using only username and password credentials, which attackers easily exploited. | A3 | NIST-SP 800-171 | High |

| | | | | |
|---|---|---|---|---|
| V2 | Inadequate network segmentation: The vendor portal was not isolated from Target's internal POS and payment networks, allowing attackers | A2, A4 | ISO 27001 Annex A | High |
| V3 | Ineffective intrusion detection and alert management: Target's security systems detected suspicious behavior but alerts were ignored or not prioritized. | A4 | ENISA Security Monitoring Guidelines | Medium |
| V4 | Lack of phishing awareness and user training: Vendor employees were not trained to identify malicious emails, resulting in initial compromise. | A3 | NIST-SP 800-50 | High |

## 3. Threat–Vulnerability Pairing

Each threat exploited specific vulnerabilities, leading to cascading impacts across critical assets. Mapping these relationships helps understand the attack chain and the consequences.

| Pair ID | Threat | Vulnerability | Asset Affected | Possible Consequence |
|---|---|---|---|---|
| P1 | T1 – Phishing attack on vendor | V4 – Lack of phishing awareness | A3 Vendor credentials | Vendor credentials stolen; unauthorized access to Target's network |
| P2 | T3 – Lateral network movement | V2 – Weak network segmentation | A2, A4 POS and corporate network | Attackers moved from vendor systems to internal POS systems |
| P3 | T2 – Malware deployment | V2 Inadequate segmentation | A2 – POS terminals | Malware harvested card data from POS memory |
| P4 | T4 – Data exfiltration | V3 Ineffective detection systems | A1, A5 Customer data | Massive data exfiltration and privacy breach |

# Risk Analysis

Risk Analysis is the process of evaluating identified risks to determine their potential impact and likelihood of occurrence.

## Risk Rating Matrix

The following matrix evaluates the likelihood and impact of each risk using a 1–5 scale (1 = Low, 5 = Very High). Risk Score = *Likelihood* × *Impact*.

| Risk ID | Threat Vulnerability Pair | Likelihood (1–5) | Impact (1–5) | Risk Score | Risk Level |
|---|---|---|---|---|---|
| R1 | P1 Phishing and credential theft | 5 | 5 | 25 | High |
| R2 | P2 – Lateral movement and privilege escalation | 4 | 5 | 20 | High |
| R3 | P3 – POS malware and card data theft | 4 | 5 | 20 | High |

| | | | | | |
|---|---|---|---|---|---|
| R4 | P4 – Data exfiltration and breach | 4 | 5 | 25 | High |

# Risk Control

**Risk Control is the process of implementing measures to reduce or eliminate identified risks.**

## 1. Control Options

### Preventive Controls:

- Enforce Multi-Factor Authentication (MFA) for all vendor access accounts.
- Implement strict network segmentation between vendor systems, corporate network, and POS systems.
- Conduct phishing simulation and awareness training for both employees and third-party partners.

### Detective Controls:

- Deploy Endpoint Detection and Response (EDR) tools and Security Information and Event Management (SIEM) solutions.
- Use Intrusion Detection/Prevention Systems (IDS/IPS) with automated alert escalation mechanisms.
- Enable real-time log correlation to detect unusual data movement or exfiltration activity.

### Corrective Controls:

- Establish a comprehensive Incident Response (IR) plan covering vendorrelated breaches.
- Maintain customer notification and credit card reissuance protocols to limit damage after exposure.
- Perform forensic analysis and patch management after any incident to restore system integrity.

## 2. Risk Control Table

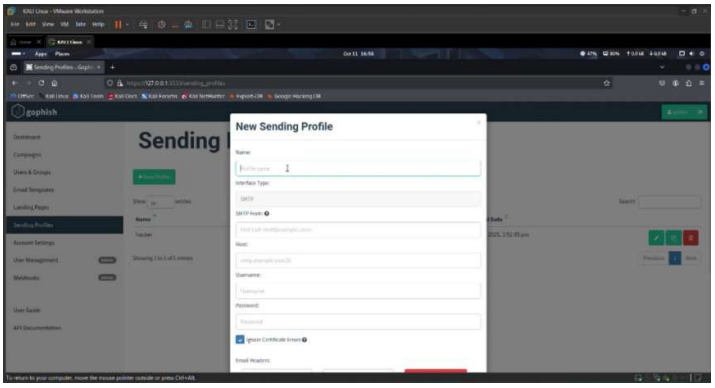
| Risk ID | Proposed Control | Control Type | Responsible Team | Expected Effective |
|---|---|---|---|---|
| R1 | Implement MFA for all vendor access | Preventive | IT Security Team | High |
| R2 | Enforce strict network segmentation and least-privilege access | Preventive | Network Administration Team | High |
| R3 | Deploy EDR and continuous SOC monitoring | Detective | SOC Cybersecurity Operations Team | High |
| R4 | Establish incident response plan and customer communication strategy | Corrective | Incident Response & Legal Teams | Medium–High |

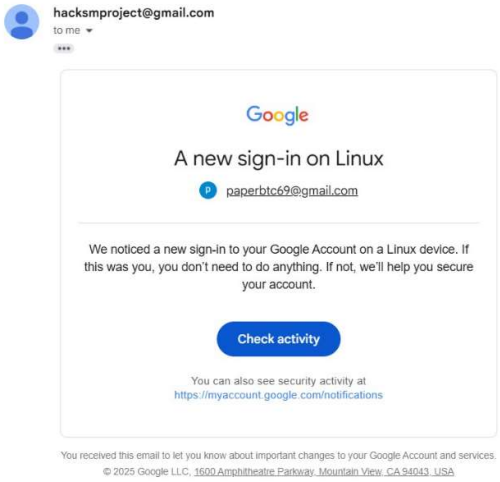
# Residual Risk Evaluation

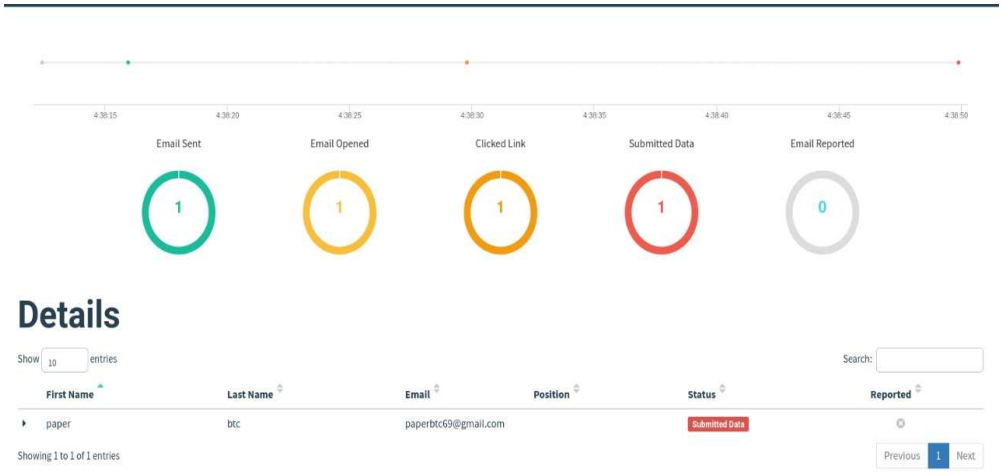
Residual Risk Evaluation is the process of assessing the remaining level of risk after implementing control measures. After applying appropriate controls, the residual risks are significantly reduced. Continuous evaluation and monitoring are necessary to ensure risks remain within acceptable levels.

| Risk ID | Initial Risk Level | Control Implemented | Residual Risk Level | Acceptable ? |
|---|---|---|---|---|
| R1 | High | MFA, employee/vendor training | Low | **Yes** |
| R2 | High | Network segmentation, monitoring | Medium | **Yes** |
| R3 | High | EDR, SOC monitoring | Medium | **Yes** |
| R4 | High | IR plan, policy enforcement | Medium | **Yes** |

# Screenshot of Implementation

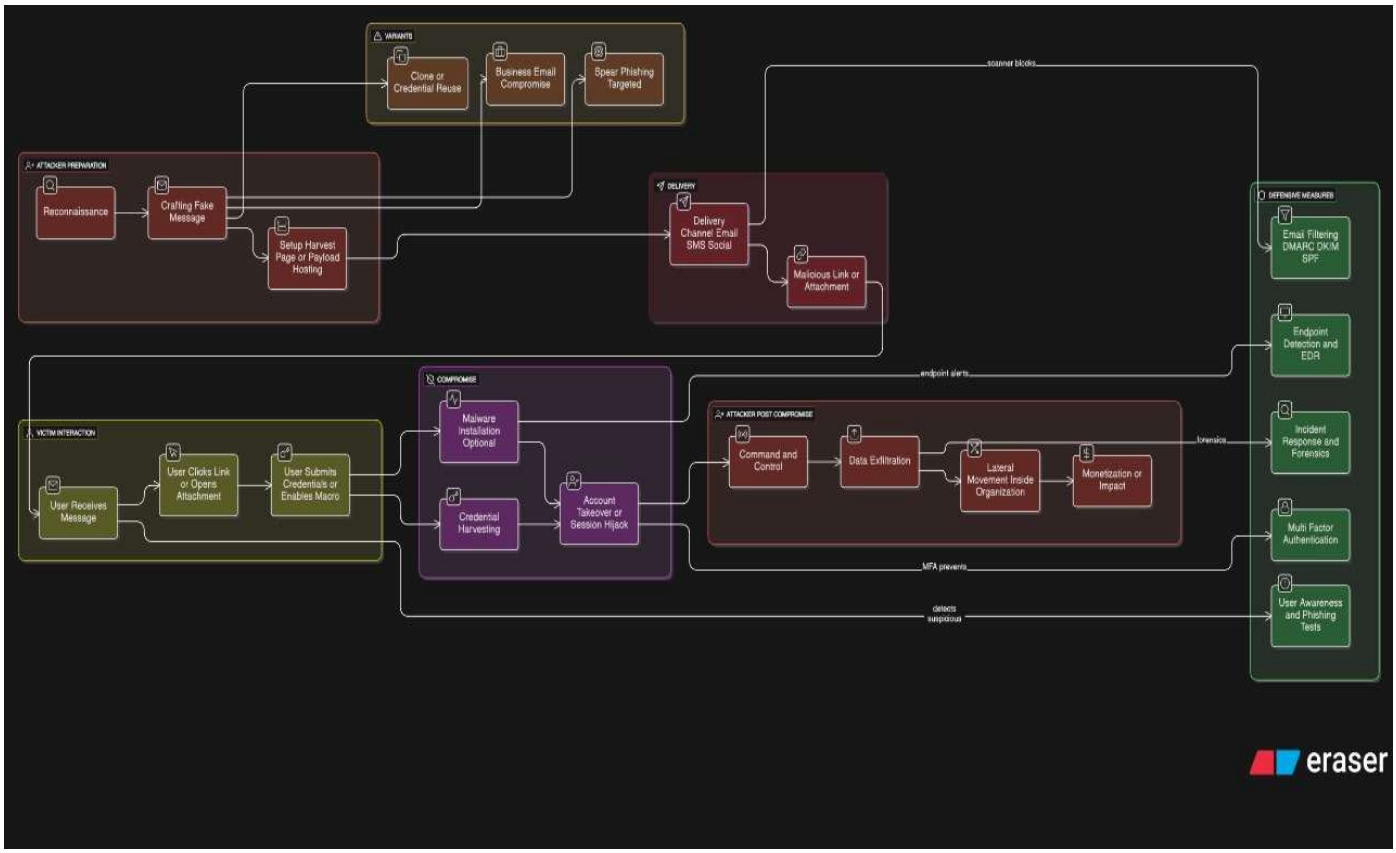



| Parameter | Value(s) |
|---|---|
| Email | paperbtc69@gmail.com |
| GALX | SJLCkfgaqoM |
| PersistentCookie | yes |
| _utf8 | ☃ |
| bgresponse | js_disabled |
| checkConnection | |
| checkedDomains | youtube |
| continue | https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hlcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX |
| dnConn | |
| dsh | -7381887106725792428 |
| password | SRMpassword1! |
| pstMsg | 1 |
| service | lso |
| signIn | Sign in |

# System Architecture



# Conclusion

The 2013 Target data breach serves as a landmark example of how a phishing attack targeting a third-party vendor can escalate into a catastrophic data compromise. The event revealed systemic weaknesses in vendor risk management, network design, and employee awareness.

The risk assessment identified critical vulnerabilities such as the lack of MFA, poor network segmentation, and inadequate detection capabilities, all of which contributed to the scale of the breach. Implementing preventive controls like multifactor authentication, network isolation, and continuous security awareness programs can significantly lower the likelihood of recurrence.

Furthermore, the deployment of real-time monitoring tools, incident response frameworks, and vendor compliance audits ensures a proactive and resilient defense Posture.

Ultimately, organizations must adopt a risk-based security approach aligned with frameworks such as NIST SP 800-30 and ISO/IEC 27005, treating vendors as extensions of their security boundary.

# References


- NIST SP 800-30: *Guide for Conducting Risk Assessments*
- ISO/IEC 27005: *Information Security Risk Management*
- **ENISA Threat Landscape Report 2023*
- Krebs on Security (2014): *Email Attack on Vendor Set Up Breach at Target*
- U.S. Senate Committee on Commerce (2014): *A "Kill Chain" Analysis of the 2013 Target Data Breach*
- Target Corporation (2014): *Press Release – Update on Data Breach and Financial Performance*