**Case Study1**

Target shoppers got an unwelcome holiday surprise in December 2013 when the news came out 40 million Target credit cards had been stolen (Krebs, 2013f) by accessing data on point of sale (POS) systems (Krebs, 2014b). Target later revised that number to include private data for 70 million customers (Target, 2014). The breach transpired between November 27 and December 15th 2014 (Clark, 2014). Over 11 GB of data was stolen (Poulin, 2014). Target missed internal alerts and found out about the breach when they were contacted by the Department of Justice (Elgin, 2014).

A series of steps were taken by the adversaries to obtain access to the credit card data and retrieve it from Target’s systems. A break down in detection further increased data loss. Sources suggest the breach transpired as follows:

1. Reconnaissance by attackers may have included a Google search that would have supplied a great deal of information about how Target interacts with vendors. Results would have revealed a vendor portal and a list of HVAC and refrigeration companies (Krebs, 2014g). This reconnaissance would have also revealed a detailed case study on the Microsoft web site that describes how Target uses Microsoft virtualization software, centralized name resolution and Microsoft System Center Configuration Manager (SCCM), to deploy security patches and system updates. The case study describes the Target technical infrastructure, including POS system information, in significant detail (Microsoft, 2011).
2. An email containing malware was sent to a refrigeration vendor, Fazio Mechanical, two months prior to the credit card breach. Malware installed on vendor machine may have been Citadel – a password-stealing bot program that is a derivative of the ZeuS banking trojan. The malware stole credentials to an online vendor portal (Krebs, 2014d).
3. Next the criminals accessed Target’s systems via Fazio Mechanical’s credentials via a vendor portal (Krebs, 2014d).
4. From this pivot point the attackers could have further infiltrated the network. The specific details are not available but we can speculate that the criminals used the used the attack cycle described in Mandiant’s APT1 report to look find vulnerabilities in the vendor portal move laterally through the network via back doors, reconnaissance and other vulnerable systems (Mandiant, 2014a). Common network tools were used to do reconnaissance once inside the network (iSight Partners, 2014).
5. Another Mandiant report on data breach trends describes how reconnaissance in a retail attack uncovered misconfigured systems. A vulnerable domain controller that could then be used to obtain access to POS systems. (Mandiant, 2014b). The Microsoft Target Case Study states *“*Except for centralized authentication, domain name resolution, and endpoint monitoring services, each retail store functions as an autonomous unit*”* (Microsoft, 2011) so the attacker would know to look for these pivot points.
6. Once access was obtained to the necessary systems, malware was installed on point of sale systems (Steinhafel, 2012). The number of POS machines that were compromised in a short amount of time indicates that the software was likely distributed to them via an automated update process. A Dell SecureWorks report explains how the malware was installled using SCCM (Jarvis & Milletary, 2014). The malware was custom software, undetectable by virus scanners (Krebs, 2014a).
7. The software gathered credit card information from memory as cards were swiped (Krebs, 2014b). The data was saved to a .dll file and stored in a temporary NetBios share over ports 139, 443 or 80 (iSight Partners, 2014).
8. Components used by attackers communicated via an ICMP tunnel (Warner, 2014). The ICMP traffic consisted of PING packets with custom text messages to indicate data movement from POS machines to compromised machine on the corporate LAN (iSight Partners, 2014).
9. Other customized components were used to send raw commands over the network that would not be discoverable by common network forensics tools and bypass network controls (iSight Partners, 2014).
10. Reports indicate data was retrieved using the default user name and password for BMC’s Performance Assurance for Microsoft Servers (Krebs, 2014e).
11. Data was moved to drop locations on hacked servers all over the world via FTP. Hackers retrieved the data from drop locations which hackers accessed to retrieve it (Krebs, 2014h).
12. While the attack was in progress, monitoring software (FireEye) alerted staff in Bangalore, India. They in turn notified Target staff in Minneapolis but no action was taken (Elgin, 2014).
13. Credit cards were then sold on the black market (Krebs, 2013c).

The cost of the breach was far reaching to both Target, customers, employees and banks. High-ranking employees lost their jobs including the CEO (Gonsalves, 2014) and CIO (Baldwin, 2014). Members of Target’s board of directors were threatened with removal (Lublin, 2014). Banks had to refund money stolen from customers via their credit cards and pay for replacement cards costing more than $200 million (D'Innocenzio, 2014). Banks refunded most funds stolen from credit and debit cards, but identity theft was at an all time high in the first half of 2014 due to large data breaches including Target (Murray, 2014). More than 140 lawsuits have been filed against Target (Webb, 2014). Banks sued Target’s PCI compliance auditor, Trustwave (Schwartz M. J., 2014). Target is dealing with investigations involving the Department of Justice (Hosenball, 2014), the FTC (Risen, 2014) and SEC (Michaels, 2014). Individual state laws may result in fines and legal proceedings over and above PCI compliance fines. States are passing even stricter laws as a result of recent breaches (Grande, 2014). Profits dropped 46% in the fourth quarter of 2013 during the critical holiday season (Ziobro, 2014). Customer visits dropped in the new year prolonging the losses (Halkias, 2014).

**Discuss the Security Strategy of this case study with respect to the following:**

1. **Risk Management**
   1. **Identification of Assets**
   2. **Encrypted and Unencrypted Data Flows**
   3. **Identification of Threats and Vulnerabilities**
   4. **Categorise them as High, Medium, Low**
   5. **Risk posed by each one of them and their prioritization**
2. **Defence in Depth**
   1. **Identification of weakest link**
   2. **Level of segregation**
   3. **Bypassing of segregation levels**
3. **Critical Controls**
   1. **Reconnaisance**
   2. **Email Attack**
   3. **Using Vendor credentials**
   4. **Exploiting Vendor Portal Vulnerabilities**
   5. **Network Infilteration and Communication**
   6. **Misconfigured Systems**



