**Target Data Breach (2013) – Summary**

**Organization Involved:**  
Target Corporation, one of the largest U.S. retailers, suffered a massive cyberattack compromising millions of customer records. The breach highlighted weaknesses in third-party security and payment systems.

**Timeline of the Breach:**

* **September 2013:** Hackers gain access through third-party HVAC vendor’s stolen credentials.
* **November 15, 2013:** Malware is installed on Target’s point-of-sale (POS) systems.
* **November 27, 2013:** Data collection begins during Black Friday shopping.
* **December 12, 2013:** Security firm FireEye detects the breach, but warnings are ignored.
* **December 15, 2013:** U.S. Department of Justice alerts Target.
* **December 19, 2013:** Target announces the breach, impacting 40 million credit/debit card records.
* **January 10, 2014:** Additional 70 million customer records (emails, addresses, phone numbers) found compromised.
* **April 2014:** CEO Gregg Steinhauer resigns.

**How the Breach Occurred:**  
Hackers used stolen credentials from a vendor to infiltrate Target’s network. They moved laterally through the system, installing RAM-scraping malware on POS terminals, capturing unencrypted card data during transactions, and exfiltrating the stolen data to external servers.

**Vulnerabilities Exploited:**

* Weak third-party security (vendor had excessive access).
* Poor network segmentation (POS system was not isolated).
* Ignored security alerts (warnings from FireEye went unaddressed).
* Lack of multi-factor authentication (MFA) for privileged accounts.

**Preventive Measures That Could Have Been Taken:**

* Enforcing **stricter third-party security policies** and limiting vendor access.
* Implementing **network segmentation** to isolate critical systems.
* Deploying **MFA** to reduce unauthorized access risks.
* Acting promptly on **security alerts** to detect intrusions earlier.

**Post-Breach Security Improvements:**

* **$100 million investment** in cybersecurity enhancements.
* Hiring a **Chief Information Security Officer (CISO)** to oversee security strategy.
* Strengthening **vendor security policies** and access controls.
* Full deployment of **EMV chip technology** for safer transactions.
* Improved **incident response protocols** for faster threat mitigation.

The breach served as a wake-up call for retailers and businesses, leading to stronger cybersecurity measures industry-wide.

 Strengthen **Vendor Security** – Limit third-party access, enforce strict security policies, and monitor vendor activities.

 Improve **Network Controls** – Segment critical systems, enforce role-based access, and regularly test security measures.

 Enhance **Threat Response** – Act on security alerts promptly, train staff on cybersecurity, and conduct incident response drills.