**Target Data Breach 2013:**

**3MTT Training Mini Project**

**Introduction**

During the final months of 2013, Target, the well-known American retailer experienced a large-scale security breach. The Target data breach led to several point-of-sale systems being compromised by malware, giving cybercriminals access to millions of customers’ personal and financial data.

**Overview of the Breach**

The Cybercriminals utilized an email-based phishing scam to trick an employee from Fazio Mechanical—an HVAC contractor and one of Target’s third-party vendors into providing their credentials. From there, the cybercriminals used these stolen credentials to infiltrate Target’s network and install malware on a number of point-of-sale systems on November 15th.

**Impact of the Target Data Breach**

Recovery Cost

* Obtaining assistance from a third-party forensics firm to investigate the breach
* Offering customers one year of free credit monitoring,

Legal expenses

* The company was involved in over 140 lawsuits throughout the country regarding the incident.
* Target finally reached an $18.5 million settlement spanning 47 states

Reputational damages

* Reduced customer confidence
* Distrust in senior leadership

**Lessons Learned from the Target Data Breach**

* Investing in cybersecurity measures is worth it
* An effective cyber incident response plan is critical
* Third-party exposures must be considered
* Proper coverage can make all the difference

**ShieldGuard's Takeaway**

Shieldguard should robust cyber security practice by investment in cyber security measures is worth it.

**My Recommendation**

To guard against possible scams:

1. Never share the information with anyone over the phone, text message or email even if they claim to be someone you know or do business with. Instead ask for a call back number
2. Delete text immediately from numbers or names you don't recognize
3. Be wary of email that ask for money or send you to suspicious websites.