****

**Target Breach Case Study**

**Executive Summary**

Xian Sun

Assistant Professor in Finance

Carey Business School

Johns Hopkins University

To cap things off, we found out that Target was the victim of cybercrooks. Between Black Friday and December 15, hackers collected credit card details on about 40 million people who had shopped in person at the popular retail chain.

In 2013, Target Corporation’s (Target) security and payment system was breached, compromising 40 million credit and debit card numbers, along with 70 million addresses, phone numbers and other personal information [1]. Target was made aware of this situation in mid-December when the U.S. Department of Justice informed the company that their system was being attacked [2]. Target had received notifications prior to this date, but had failed to act.

What happened?

Timeline:

|  |  |  |
| --- | --- | --- |
|  |  |  |
| * May 2013 | FireEye (anti-malware system - $1.6 million) installed but the feature of eradicating  the malware was turned off as mistrusted by Target security personnel |  |
| * 11/27/13 | Breach started. |  |
| * 11/30/13 | FireEye captured the first malware code and issued an alert that was ignored |  |
| * 12/2/13 | Hackers started downloading the collected data to Russia through US servers |  |
|  |  |  |
| * 12/12/13 | Contacted by Dept of Justice and aware of the breach |  |
| * 12/13/13 | Target executives meet with US. Justice Department |  |
| * 12/14/13 | Target hires a third-party forensics team to investigate the hack |  |
| * 12/15/13 | Learned the criminals hacked the system to gain guest credit and debit and card  information including names, mailing and email address, phone numbers. | |
|  |  |  |
| * 12/15/13 | Closed access point and uncovered the problem and had informed authorities and  financial institutions |  |
| * 12/18/13 | First time published the breach by a blogger |  |
| * 12/19/13 | Target publicly announced and emailed shoppers |  |
| * 12/20/13 | Gregg Steinhafel, a message from CEO Gregg Steinhafel about Target's payment  card issues. |  |
| * 12/21/13 | JPMorgan Chase & Co. (NYSE:JPM) places daily limits on spending and withdrawals  for its debit card customers affected by the Target breach, begins reissuing cards  and opens some branches on a Sunday to help Target customers. |  |
| * 12/22/13 | Transactions at Target fell 3 percent to 4 percent compared to the year earlier on  The last weekend of holiday shopping before Christmas. Other retailers report  strong results. |  |
| * 12/23/13 | Press release, Target data security media update |  |
| * Days later | Hired security expert at Verizon to probe its network for weakness |  |
| * 12/27/13 | An ongoing investigation by a third-party forensics unit finds that encrypted debit  card PIN information was accessed during the breach, but Target says it believes  PIN numbers remain secure. |  |
| * 1/10/13 | Target says an additional 70 million customers had personal information stolen  during the breach, including emails. The company lowered its forecast for its  fourth quarter, saying sales were meaningfully weaker than expected after news  of the breach. |  |
| * 1/12/14 | CEO confirmed that malware (RAM scraping) installed on POS terminals at  US based stores enabling the theft of financial information. |  |
| * 1/22/14 | Target lays off 475 employees at its headquarters in Minneapolis and worldwide  and leaves another 700 positions unfilled. |  |
| * 2/4/14 | Target CFO John Mulligan testifies before the U.S. Senate Judiciary Committee,  mentioning the ongoing investigation but offering no new information on who might  have hacked the data. Mulligan says Target has invested hundreds of millions in  data security and rejects claims that its systems weren’t up to par. Other witnesses  discuss the benefits of chip-and- PIN technology, used widely in Europe but not in  the U.S., where banks and retailers have balked at the expense.. |  |
| * A few weeks later | Second batch of information compromised, personal information of 70 million people,  Overlap of at least 12 million people in two groups. |  |
| * 2/18/14 | Costs associated with the data breach topped $200 million, a report from the Consumer  Bankers Association and Credit Union National Association finds. |  |
|  |  |  |
| * 3/7/14 | Target lets its employees wear jeans and polos to work in an effort to boost morale  after layoffs and the sales-killing data breach. |  |
| * 4/30/14 | Target says it has committed $100 million to update technology and will introduce  chip-and-PIN technology for its debit and credit cards by early 2015. |  |
| * 5/5/14 | Bob DeRodes, a former tech adviser in several federal government agencies, takes  over as Target’s chief information officer. Target CEO Gregg Steinhafel resigns. |  |

In November and December 2013, cyber thieves executed a successful cyber attack against Target, one of the largest retail companies in the United States. The attackers surreptitiously gained access to Target’s computer network, stole the financial and personal information of as many as 110 million Target customers, and then removed this sensitive information from Target’s network to a server in Eastern Europe.

In December 2013, just days after a data breach exposed 40 million customer debit and credit card accounts, Target Corp. hired security experts at Verizon to probe its networks for weaknesses. The results of that confidential investigation — until now never publicly revealed — confirm what pundits have long suspected: Once inside Target’s network, there was nothing to stop attackers from gaining direct and complete access to every single cash register in every Target store.

Target spokesperson Molly Snyder would neither confirm nor deny the authenticity of the documents referenced in this report, but she maintained that Target has made great strides and is now an industry leader on cybersecurity.

“We’ve brought in new leaders, built teams, and opened a state-of-the-art cyber fusion center,” Snyder said. “We are proud of where we stand as a company and will be absolutely committed to being a leader on cybersecurity going forward.”

The American retailing company was a target (no pun intended) for a cyberattack back in 2013, and it has ended up costing the company $162 million (slightly more than £104 million).

Reason:

He cited the 2013 Target Corp. data breach, which eventually was discovered to have come from a computer of a heating and air-conditioning firm under contract to the retailer. "It's any vendor, providing any service, that has a link to that firm's data.[2]

Development of the breach [5]

* Target gave network access to a third-party vendor, a small Pennsylvania HVAC company, which did not appear to follow broadly accepted information security practices. The vendor’s weak security allowed the attackers to gain a foothold in Target’s network.
* Target appears to have failed to respond to multiple automated warnings from the company’s anti-intrusion software that the attackers were installing malware on Target’s system.
* Attackers who infiltrated Target’s network with a vendor credential appear to have successfully moved from less sensitive areas of Target’s network to areas storing consumer data, suggesting that Target failed to properly isolate its most sensitive network assets.
* Target appears to have failed to respond to multiple warnings from the company’s anti-intrusion software regarding the escape routes the attackers planned to use to exfiltrate data from Target’s network.

The "hows" and the "whys"[9]

Malware was installed on Target’s payment and security system on November 15, 2013. Access to the system came from network credentials that were stolen from an HVAC provider based in Sharpsburg, Penn. Initial speculation was that this vendor was monitoring HVAC systems installed at Target facilities remotely via network connection and that this was the way hackers gained entry into Targets internal network. As it turned out, this was not the case [3]. The compromised data connection was being used for “electronic billing, contract submissions and project management” [4], not monitoring of equipment. The network credentials were, in

fact, gathered after the HVAC contractor's employee fell victim to a phishing scheme attack and clicked on a malicious email [5].

Target was not unprepared for the breach. Earlier that year, the company had installed malware detection software by computer security firm FireEye (high-profile FireEye customers include the CIA and Pentagon). The FireEye team in Bangalore, India monitored Target’s system around the clock, and reported the activity to Target’s security team based in Minneapolis, Minn. [6].

Exfiltration malware was installed on November 30, 2013 to move the stolen information out of the Target servers. These drop points were first staged around the U.S., then to computers in Russia. It was at this point that the Bangalore team became aware that something was wrong and notified the Target security team in Minneapolis. For reasons that are unclear,

Target's Minneapolis team failed to act on the alert, allowing customer information to be compromised [7].

Customer impact:

* Up to 70 million individuals affected
* 40 million debit and credit card numbers
* 110 million Target customers
* The retailer last year was the No. 7 best- perceived brand among consumers, but not only did it fall off the top 10 list, it plummeted all the way down to No. 21. [7]
* Impact on bank customers: Members stated that the Target breach caused a major inconvenience to cardholders, right amid the busy holiday shopping season. Many bank customers only have a debit card and no longer use checks, so it was a very significant inconvenience to them.[13]

Financial impact:

* Fourth quarter and full-year 2013 net expense related to the data breach was $17m (£11m), reflecting $61m (£39m) of gross expense partially offset by the recognition of a $44m (£28.3m) insurance receivable.”
* 2013 fourth-quarter profits were down 46% compared with the same period the year before. During that quarter, the company said, it spent $61 million on breach-related expenses, and executives said they expected the costs to continue.[6]
* Breach-related expenses of $4m (£2.5m) in fourth quarter 2014 and full-year net expense of $145m (£93.4m), which reflects $191m (£123m) of gross expense partially offset by the recognition of a $46m (£30m) insurance receivable,” the company said.
* It has ended up costing the company $162 million (slightly more than £104 million).
* Target Corp. has reached a preliminary settlement with banks affected by the retailer's 2013 breach, agreeing to pay out $39.4 million to the financial institutions.
* Under the terms of the settlement, filed in a St. Paul, Minn., court Wednesday, banks and credit unions would get about $20.25 million while another $19.11 million would be put toward reimbursing those who issued MasterCards, according to a report by Reuters.
* Target has reached a $67m agreement with Visa over a massive breach of customers' payment data during the 2013 holiday shopping season that tarnished its reputation and raised serious questions about the company's data security systems.
* Target’s much-publicized data breach cost the company more than the $400-$450 million that’s been estimated. [7]
* The Company incurred breach-related expenses of $4 million in fourth quarter 2014 and full-year net expense of $145 million, which reflects $191 million of gross expense partially offset by the recognition of a $46 million insurance receivable. Fourth quarter and full-year 2013 net expense related to the data breach was $17 million, reflecting $61 million of gross expense partially offset by the recognition of a $44 million insurance receivable.[10]
* To sum the math up, Target's gross expenses totaled $252 million, insurance compensation brought that down to $162 million, and further tax deductions yield a final $105 million. [10]

Target reaction:

* Hired security expert at Verizon days after announcement
* Resignation of its CIO, a restructuring of its security and IT organization and

the eventual ouster of the company's CEO

* Will spend $100 million switching to the new system including changing its branded credit and debit Redcards and cost of installing new payment terminals.

Market reaction:

* JPMorgan Chase said in Feb 2014 it would begin issuing some chip- and-PIN-enabled credit cards this year after the breach. [6]
* Several financial institutions serving central Ohio are contacting their debit- and credit-card customers who have been affected by the major information breach that recently struck Target. [8]
* Most of the banks are monitoring customer accounts for fraudulent activity and telling customers to do the same. [8]
* Some banks also are limiting per- day purchases and ATM withdrawals with the cards, or simply reissuing the cards to prevent future fraud. [8]

**Costs**

Direct cost:

* Investment in systems:
* invest chip-enabled technology in stores and on Target REDcards by early 2015, six months ahead of the previous plan.
* Will spend $100 million switching to the new system including changing its branded credit and debit Redcards and cost of installing new payment terminals.
* Training employees:

- Hired security expert at Verizon days after breach announcement

* Outsourcing:

Indirect cost:

* Legal penalties
* pay out $39.4 million to mastercard and related banks and credit unions
* pay out $67m agreement with Visa
* Loss of customers
* The retailer in 2013 was the No. 7 best- perceived brand among consumers, but not only did it fall off the top 10 list, it plummeted all the way down to No. 21.
* Customers stopped using credit card or cancelled it.
* Loss of partnerships/suppliers
* The breach resulted in longer turnaround time for card reissuance due to volume of requests. Card vendors were reportedly behind for weeks because of the vast number of cards they needed to produce. One bank experienced delay for replacement cards up to three months; delay for normal expired cards not involved in the breach up to two months.
* Impact on bank customers: Members stated that the Target breach caused a major inconvenience to cardholders, right amid the busy holiday shopping season. Many bank customers only have a debit card and no longer use checks, so it was a very significant inconvenience to them. [13]
* Impact on bank operations: The breach caused a major disruption to employees’ daily duties at the bank. [13]
* Impact on bank revenue: Members cited loss of spend on reissued portfolio and some accounts lost due to failure of customer to activate new card, reducing spend and revenue. Members also experienced loss of revenue due to legitimate point of sale declines related to heightened fraud strategies. [13]
* Other costs to bank: In addition to the costs of reissuing cards, survey participants cited expenses for inbound and outbound phone calls, staff time spent on implementing heightened fraud strategies, fraud monitoring, claims processing, and responding to customer inquiries. [13]
* Impair firm reputation and stock value slides
* Since 2011, Target's CSR score -- a measure of the enterprise dimensions of reputation that include 'workplace,' 'governance,' and 'citizenship' -- fell dramatically, the largest drop among any U.S. retail company in the same time frame.[11]
* Target was hit with over 90 lawsuits related to the massive data breach, and spent over $61 million as of February 1 responding to the attack. [12]
* The stock experienced a 10% drop in price in the aftermath of the security breach
* Spillover effects that impacts the future prospect of the whole industry

Target’s much-publicized data breach cost the company more than the $400-$450 million that’s been estimated. [7]

**Benefits:**

Direct benefits:

* Stability of the operating system and avoid loss from system downtime

Indirect benefits:

* Stronger partnership with suppliers
* Attach more customers
* Increase the value of the whole value chain
* More sympathy from shareholders at the event of a cybersecurity attack
* by the end February 2014, Target had experienced the highest percentage stock price regain in five years.
* Shareholders only react to breach news when it has direct impact on business operations, such as litigation charges (for example, in the case of Target) or results in immediate changes to a company’s expected profitability.

Summary

Attackers targeted the major US retailer via a phishing campaign on one of its third-party vendors. The vendor downloaded a file containing a virus which was designed to collect all of the data entered within the system. From here the attackers were able to obtain the vendor's login credentials to the retailer's systems.

With these stolen credentials the attackers gained access to the retailer's system and were able to move about freely within the network unnoticed over a two week period. Whilst there they installed malware to attack the POS system enabling them to enter the system again and again to steal information about the 110 million people who shopped at the retailer in late December 2013.

Target's CEO resigned as a result of the breach and the associated financial costs reportedly exceeded USD$300 million.

In March 2022, U.S. District Court in St. Paul ruled that Target's general liability policy covered some of the data breach losses after nearly a decade of dispute between the company and their insurance company.( https://www.cybersecuritycasestudies.com/library/target-customer-credit-debit-card-details-stolen)

**Reference**

[1]: Target reaches preliminary $39.4M settlement with banks. SC magazine (US)

[2]: Asset owners demand info on cybersecurity processes. Pensions & Investments

[3]: Bankers group threatens suit over Volcker rule. Washington Post

[4]: Target to pay $67m over Visa data breach. Financial times

[5]: A “Kill Chain” Analysis of the 2013 Target Data Breach. US Senate. Committee on commerce, science, and transportation

[6]: After data breach target plans to issue more secure chip-and-pin cards. New York times.

[7]: Amazon Has the Best Consumer Perception of Any Brand. Adweek

[8]: Banks react decisively to Target data breach. The Columbus Dispatch. Dec 27, 2013

[9]: Cyber Security: Target's 2013 Data Breach. Melesio Munoz. Cupertinon Electric Inc. Sep 21, 2015

[10]: How much do data breaches cost big companies? Shockingly little. Robert Hackett. Mar 27, 2015. <http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/>

[11]: How do Home Depot and Target save their reputation after data breach? The street. Jason Notte. Sep 27, 2014.

[12]: It turns out Target could have easily prevented its massive security breach. Chris Smith. Mar 13, 2014.

[13]: Target Breach Impact Survey. American Bankers Associations. Jul 2014.