ijcsm INTERNATIONAL JOURNAL OF CASE STUDIES IN MANAGEMENT

HEC130
Volume 14
Issue 1
March 2016

Autopsy of a Data Breach: The Target Case

Case[1, 2] prepared by **Line DUBÉ**[3]

On December 19, 2013, Target, the second-largest retailer in the United States, announced a breach involving the theft of data from over 40 million credit and debit cards used to make purchases in its U.S. stores between November 27 and December 18.[4]

On January 10, 2014, it reported that the cybercriminals had also stolen personal data, including the names, telephone numbers, home addresses and email addresses of up to 70 million additional customers.

The Discovery

As is often the case in such situations, Target learned of the data breach from law enforcement agencies. Indeed, on December 13, 2013, representatives from the U.S. Department of Justice notified Target's management of a large number of fraudulent debit and credit card transactions that all seemed to share a link to transactions made at Target. Following this meeting, Target hired a computer forensics firm to investigate the breach. The results confirmed its worst fears: cybercriminals had been hacking into Target's systems and stealing data from 40 million debit and credit cards used in its U.S. establishments since November 27. Target wasted no time eradicating all the software used by the cybercriminals, but despite the company's eagerness to stifle the news, word got out and reporters started asking questions.

On December 19, under growing pressure, Target announced the breach and theft of the data. Its website and call centre were quickly inundated with calls from worried consumers, creating a nightmare scenario for its customer service department. To make matters even worse, the breach

[1] Translation from the French by Andrea Neuhofer of case #9 65 2016 001, "Autopsie d'un vol de données : le cas Target."

[2] This case was written using public information sources and therefore reflects the facts, opinions and analyses published in the media. The blog by the investigative reporter Brian Krebs (krebsonsecurity.com), an expert in the field of computer security, was also a valuable source of information. See the list of publications used at the end of the case.

[3] Line Dubé is a full professor in HEC Montréal's Department of Information Technologies.

[4] This date varies between December 15 and 18, depending on the source. December 18 is used here because it is the date given by John Mulligan, Target's Executive Vice-President and Chief Financial Officer, in testimony before the U.S. Senate Committee on the Judiciary on February 4, 2014 (see http://www.judiciary.senate.gov/meetings/privacy-in-the-digital-age-preventing-data-breaches-and-combating-cybercrime).

The International Journal of Case Studies in Management is published on-line (http://www.hec.ca/en/case_centre/ijcsm/), ISSN 1911-2599.
This case is intended to be used as the framework for an educational discussion and does not imply any judgement on the administrative situation presented. Deposited under number 9 65 2016 001T with the HEC Montréal Case Centre, 3000, chemin de la Côte-Sainte-Catherine, Montréal (Québec) H3T 2A7 Canada.

occurred during the pre-Christmas shopping season, which included Black Friday, one of the busiest days of the year for “brick-and-mortar” retailers. The data breach affected approximately 10% of all debit and credit cards in circulation in the United States.

The financial institutions that had issued the cards from which data had been stolen reacted swiftly to Target’s announcement. Normally, in order to minimize losses, the banks would simply cancel the cards and issue new ones. However, because of the sheer number of cards affected and the massive costs involved, and because the holiday season is a very bad time to leave consumers unable to pay for purchases (without the possibility of paying by credit card or withdrawing cash from an ATM using a debit card), the banks sought alternative solutions. JP Morgan Chase, for example, which had at least two million affected customers, quickly placed strict limits on withdrawals ($100 in cash per day; $300 limit on card purchases) by its potentially affected customers until new cards could be issued. The banks, left alone to manage the breach, faced extraordinary financial and logistical challenges.

At the same time, Target launched a major public relations operation. It assured its customers that the technological component responsible for the breach had been found and destroyed and that they could continue to confidently shop in its stores. It also pledged that no one would be held liable for fraudulent transactions and offered a free subscription to a credit monitoring service. With the assistance of a specialized firm, Target continued its investigation of this major breach in an effort to get to the bottom of what had gone wrong. The U.S. Justice Department and Secret Service did the same.

So, What Did Happen?

Experts agree that the attack was perpetrated by cybercriminals who used a well-known strategy and what are in fact fairly conventional technological tools. Between November 15 and 27, the hackers managed to penetrate Target’s point-of-sale network (most cash registers today are actually computers) and to install malware on the terminals. The malware resembled a widely known program called *BlackPOS*, which purportedly originated in Russia. Available for about $2,000 on the black market, this software is designed to be installed on point-of-sale terminals and to capture all the data stored on credit and debit cards that are swiped at the infected terminal. This type of malicious software, known as a memory scraper, makes a copy of the data at the point where they are the most vulnerable – that is, in the instant when the server processing the transaction has to store the raw data (unencrypted) in its random access memory for a few milliseconds. In this case, the copied data were immediately saved on one of Target’s web servers, which had been hacked. This type of malware is particularly dangerous because it is difficult for the generally used intrusion detection software to detect it. Moreover, malware is typically designed to delete any traces left behind, making it hard to assess the scope of the damage without an in-depth criminal investigation. Most of the time, organizations are not even aware they have been infected; in fact, studies show that it takes an average of 229 days for such a breach to be detected by the victimized company. As in Target’s case, the news is often delivered by law enforcement agencies acting on complaints from banks that notice an unusually high level of fraudulent transactions that all seem to lead back to the same retailer.

Thus, between November 15 and 27, the cybercriminals ran tests to make sure everything was working properly. A few days later, they installed the malware on all of Target's terminals (approximately 1,800 devices), which then began to make a copy of the numbers of all cards used. Each day, in order to avoid drawing attention, the cybercriminals took advantage of their remote access capability to retrieve a copy of the data amassed (over 11 gigabytes), working between 10:00 a.m. and 6:00 p.m. during the network's normal peak traffic periods. These data were then copied on three servers outside of Target, most likely without the knowledge of their owners; reportedly, there was one server in Miami, one in Brazil and another in the United States.[1] The investigation apparently uncovered a copy of the data carelessly dumped on one of these servers that had been used as temporary storage.

How Did the Cybercriminals Manage to Perpetrate This Theft?

Target was actually well protected against this type of attack, which is quite common. Target was considered a leader in cybersecurity in the retail industry, having invested massively in capital and resources to ensure the security of its IT infrastructure. It had multiple layers of protection in place, including segmentation, firewalls, malware detection software, intrusion detection software, prevention tools and plans to prevent data loss. Both internal experts and outside consultants regularly conducted tests and audits of all these security measures. In September 2013, Target was certified as being in compliance with the Payment Card Industry Data Security Standard (PCI DSS), an international standard that establishes the minimum levels of security that both small and large merchants must meet when storing, processing and transmitting credit card data.

However, none of these measures prevented the cybercriminals from finding and exploiting vulnerabilities in Target's IT infrastructure. One of its vendors, the HVAC firm Fazio Mechanical Services, based in Pennsylvania, had remote access to Target's network for the purposes of electronic billing, contract submission and project management. The investigation reportedly found that the cybercriminals obtained this firm's user code and password by sending a simple phishing email to which a Fazio employee responded. With this information in their possession, the cybercriminals were able to remotely penetrate Target's network and, by exploiting vulnerabilities in the security measures in place, managed to access the company's payment system network, which was linked to the point-of-sale terminal network. This cleared the path for them to install their malware.

But even with this unauthorized access, Target was, in theory at least, shielded against such attacks. Indeed, six months earlier, it had invested the tidy sum of $1.6 million to implement an anti-malware system called FireEye (customers include the defence industry, the CIA, the Pentagon and Bombardier Aerospace). FireEye is an advanced monitoring system for IT infrastructure. Based on the principle of prevention rather than detection, it works by creating virtual chambers into which hackers are drawn so that they can be detected before they succeed in actually penetrating the system under protection. A team of experts in Bangalore, working around the clock, monitored the results of these monitoring activities. If the team noticed any suspicious activity, it

[1] The geographic location of the servers used to house the stolen data varies depending on the source, but there appears to be a consensus that at least one server was located in the U.S. and another outside the country.

would alert the team in Target's security operations centre in Minneapolis (location of its headquarters), which would then spring into action or, in this case, choose to do nothing....

Indeed, Target publicly acknowledged that escalating alerts (the last of which were level 1 alerts, the highest issued by the monitoring system) had been received starting on November 30 and that its local teams had analyzed them and deemed that no action was necessary. If the experts at Target had done a better job of assessing the alerts received, the attack against Target's infrastructure could have been thwarted, since the investigation shows that the first alert was issued before the first data were transferred. The security software itself would have been able to prevent the attack, as it has a feature similar to an anti-virus program that automatically eradicates software deemed to be "malicious" or "unauthorized." However, Target's experts had deactivated this feature because the system was new and they did not yet trust it completely. At the end of November, even Target's own anti-virus system had detected suspicious activities on the server protected by FireEye. This additional alert was also ignored.

Who Committed the Theft? Who Are the Suspects?

As is the case with physical thefts of high-value assets, large-scale data thefts like the attack against Target are usually the work of an organized team of cybercriminals, operating internationally, whose members have sophisticated and complementary skills (malware programming, network intrusion, server management, sale of stolen data, concealment of stolen goods, etc.). By tracking the data, it was found that, after being stored on three temporary servers, the data were ultimately transferred to a server in Moscow. A closer analysis of the malware code and the servers used revealed that all signs pointed to a group of hardened cybercriminals based in Russia and the Ukraine, two countries that, along with Romania, have formed a central hub for the theft and sale of data over the past 10 years. The ensuing international manhunt led to the identification of the main suspect and ringleader of the operation: a 22-year-old Ukrainian who had allegedly already been implicated in cases of data theft in his country. The same group was also believed to be linked to at least six other major data breaches over the previous two years and to a similar attack against Home Depot in the summer of 2014.

The data stolen from Target quickly wound up for sale on one of the most popular online stores for stolen data (rescator.so). This black market website offers the possibility to purchase data from either a single card or from batches of 1,000 cards, at a discount. Users can search by city, geographic region, bank, type of card, expiry date, etc. The price varies depending on the type of card: from $6 for a gift card to up to $200 for data from an American Express Platinum credit card. It appears that the Target cards were sold in batches of one million cards, with prices ranging from $20 to $100 per card. The site also offers impeccable customer service, allowing users to pay in bitcoin (or similar currencies) or via Western Union. It even offers a guarantee of validity in terms of the duration (for example, six hours) or the minimum amount on the card ($1,000, for example). Time is a crucial factor in this industry: crooks have to purchase the number and clone the card to make in-store purchases, but they can quickly use up the credit limit by shopping online. They often buy gift cards that have a longer expiry date. Eventually, either the bank's security system or the consumer detects suspicious transactions and the card is rapidly cancelled. Then the crooks start the process all over again with a new card.

Consequences of the Breach

Target's image took a severe beating following the announcement of the data breach – the largest in history at the time. The company was roundly criticized for its failure to act on the initial alerts, for its delay in making the breach public and for the inability of its customer service department to respond to customers. In late December 2013, for the first time, the Target brand scored negatively in all surveys of consumer perceptions. These negative sentiments were reflected in the company's fourth-quarter results. Indeed, Target announced a 46% decline in profits ($520 million compared to $961 million in the same period the previous year) and a 5.3% drop in revenue, which management attributed to fearful shoppers. The exodus of customers and the costs related to the breach affected not only the quarterly results, but also full-year results, which fell far short of Wall Street's targets. It should be noted, however, that the difficulties resulting from the company's expansion into Canada were a contributing factor in the missed targets.[1] On February 1, 2014, Target reported that it had spent $61 million responding to the breach, but that this amount would be offset by $100 million worth of cyber insurance held by Target.[2] However, experts speculate that, when all is said and done, the total cost of the breach will exceed $500 million, and may even approach the $1-billion mark. This amount includes the reimbursement of banks for card reissuing, all activities related to communication and customer management, fines for non-compliance with the PCI DSS standard due to the vulnerability of the external vendor's authentication method, the cost of credit monitoring for the tens of millions of customers affected by the breach and the huge legal costs for several years to come.

It is difficult to predict the long-term financial impact of the data breach. Target is currently facing over 140 lawsuits, each seeking millions of dollars in damages. Several are class-action suits. The victims accuse Target of violating several laws, of negligence in its handling of customer data and of waiting too long to publicly disclose the breach, thereby increasing the vulnerability of its customers. On May 14, 2014, the court divided the lawsuits into three groups: financial institutions,[3] consumers and shareholders. The banks are at the heart of these suits (they alone account for 29 of them) and believe that Target should reimburse them for all costs arising from the breach, including the massive reissuing of cards, customer relations, refunds for fraudulent transactions, investigations, etc. Depending on the source, it is estimated to cost between $5 and $15 to reissue a card; between the announcement of the breach and February 2014, over 15.3 million debit and credit cards had to be replaced. Banks usually recover no more than a minuscule portion of the costs involved[4] because they are liable for these costs under the contract clauses established between merchants and credit card companies.

In addition to the effect on Target's bottom line, the breach also had a huge impact internally. On March 5, 2014, Target announced the "resignation" of its Chief Information Officer (CIO), who

[1] In January 2015, Target announced it was closing its 133 stores in Canada.

[2] In February 2015, Target reported total costs to date of $252 million, $90 million of which was offset by its insurance. However, in the fall of 2015, the fallout was far from over. Despite reaching settlements with a number of major card issuers related to Visa, several lawsuits were approved by the courts over the course of 2015 and will thus be heard in the coming years.

[3] In the summer of 2015, Visa and Target reached a settlement under which Target agreed to pay up to $67 million to card issuers (the banks) to cover a portion of the costs arising from the data breach. In May 2015, MasterCard card issuers rejected a similar settlement offer in the amount of $19 million.

[4] Approximately $2.50 per stolen card.

had held the position since 2008, in addition to the overhaul of its information security and compliance structure and practices. As a first step in this effort, the company also announced the creation of two key positions, to be recruited externally: Executive Vice-President and Chief Information Security Officer and Executive Vice-President and Chief Compliance Officer. The new security function would centralize all security management activities, which had previously been dispersed among different groups in the company. Finally, a few months later, in May 2014, Target's CEO was let go. There was speculation that the combination of the failed expansion into Canada and the massive data breach ultimately convinced the Board of Directors that Mr. Steinhafel, who had been with the company for 35 years and served as CEO since 2008, was no longer the right person to protect the firm's assets. Rumour also had it that these events forced a review of the presence of certain members of the Board themselves. Overall, the breach had significant repercussions on Target's leadership, as attested by the fact that most of the current players joined the company after this fateful event.[1]

The data breach also had an impact on Target's projects. For example, the company decided to move up its $100-million project to implement a chip card and personal identification number payment (chip-and-PIN) system by six months. This project, whose completion was planned for late 2015, involved the replacement of all point-of-sale terminals (as well as the supporting software) and all Target credit cards (REDcard) in circulation with a chip card. Chip-enabled cards have drastically reduced the number of cases of fraud in the countries where they are already widely used (Europe, Canada and Australia). It's important to note, however, that the chip-card payment system would not have prevented the type of theft committed against Target, although it would have made it much more difficult to clone the cards whose data had been stolen, making them much less useful and, hence, much less valuable.

While the Target fiasco no longer ranks as the largest data breach in history (this honour was claimed by Home Depot in early September 2014), it's unfortunate to note that, at the end of the day, it is always the customers who are the biggest losers when such incidents occur. A cardholder who detects a fraudulent transaction on his or her statement merely has to contact the bank and have the card cancelled, a routine operation that only takes a few moments. However, once the card is cancelled, if the cardholder has pending or recurrent transactions, he or she will have to contact every merchant involved. Card cancellation can also lead to further headaches, such as making it difficult to return merchandise paid for with a cancelled card. This is not to mention the serious and long-term consequences of thefts of personal data. In addition to the invasion of one's privacy, the resulting identity theft forces victims to embark on a long and arduous process to defend their identity and prove to various parties (merchants, lenders, government ministries, etc.) that they didn't commit any wrongdoing.

Although it is estimated that the Target data theft alone will ultimately cost financial institutions over $200 million, industry stakeholders (financial institutions, the IT industry, and merchants) continue to pass the buck by failing to put in place the necessary measures to protect consumers. Why? Mainly because the investments required are huge: the entire technological infrastructure (payment terminals and all data storage and processing software) must be replaced, along with all the cards in circulation. The string of major data thefts in the United States has legislative

[1] See Target's leadership team: https://corporate.target.com/press/leadership?_ga=1.74193618.1913530050.1448163247

authorities there extremely worried. On February 4, 2014, the U.S. Senate Committee on the Judiciary held hearings on "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime," before which the Executive Vice-President and Chief Financial Officer (CFO) of Target was called to testify. The aim of the hearings was to determine how laws could be amended to ensure better data protection. Some people even called for laws at the national level that would force the different industry stakeholders to work together to prevent data violations. To avoid this, Visa and MasterCard launched concrete initiatives to force the hand of all players in the industry. To cite just one example, on October 15, 2015, a new rule was implemented governing credit card liability in the event of fraudulent purchases. The rule shifted fraud liability from card issuers onto the weakest link in the chain – that is, either the retailer or the bank – with the weakest link being defined as the party that has not yet upgraded its equipment, software and cards to allow the use of chip technology. Despite this ultimatum, stakeholders have been slow to make the necessary investments, and it is estimated that the switch to chip-enabled cards in the U.S. will not be complete until the end of 2017. At the international level, the government is looking at ways to strengthen international collaboration and to sign and enforce extradition agreements, given that most of the cybercriminals are based outside of the country.

Overall, it is increasingly clear that cybercrime is still in its infancy and that we still have a very long way to go to combat it effectively. One thing that's certain, however, is that it's always the end consumer who gets stuck with the bill, no matter how big it is. To be continued...

NOTE:

Detailed research was conducted in an effort to locate, analyze and corroborate the information available in order to provide as accurate a picture as possible of the situation described. However, it is clear that Target and the law enforcement agencies have in their possession additional, highly relevant information that to date remains secret. This limitation should be kept in mind when reading and interpreting this case.

The following is a list of the main publications consulted:

ASSOCIATED PRESS (March 5, 2014). "Target CIO resigns as security revamped over data breach – Company's 4th-quarter profits take a hit following hacking incident", CBC News.

BASU, Eric (June 15, 2014). "Target CEO fired – Can you be fired if your company is hacked?" *Forbes*.

CBC NEWS (January 10, 2014). "Target data hack affected 70 million people – Stock drops as retailer reveals more customers affected and names and addresses leaked."

CLARK, Meagan (May 5, 2014). "Timeline of Target's data breach and aftermath: How cybertheft snowballed for the giant retailer", *International Business Times*.

CONTE, Andrew (February 7, 2014). "Hackers likely hit Target "lottery" through Sharpsburg firm's remote link", *TRIBLIVE News*.

HELLER, Laura (March 14, 2014). "Target failed to act on security warnings", *FierceRetail*.

HELLER, Laura (February 16, 2014). "Target: Timeline of a data breach", *FierceRetail*.

HESSELDAHL, Arik (May 27, 2015). "Target CEO loves Apple pay, but wants chip-and-PIN cards first" (video), *recode.net*.

KITTEN, Tracy (August 18, 2015). "Target, Visa reach breach settlement", *Bankinfo Security*.

KOSSMAN, Sienna (2015). "8 FAQs about EMV credit cards", *Creditcards.com*.

LOEB, Walter (January 15, 2015). "Target's new CEO makes a bold decision to leave Canada", *Forbes*.

MELTON, Nicole Marie (December 20, 2013). "Target sued over data breach as customer backlash causes PR nightmare", *FierceRetail*.

PAYMENTS LEADER (2015). "Will retailers be ready for EMV by Oct 2015?"

RILEY, Micahel, Ben ELGIN, Dune LAWRENCE and Carol MATLACK (March 13, 2014). "Missed alarms and 40 million stolen credit card numbers: How Target blew it", *BusinessWeek*.

ROMAN, Jeffrey (February 25, 2015). "Target breach costs: $162 million", *Data Breach Today*.

SIDEL, Robin (August 18, 2015). "Target to settle over data breach", *The Wall Street Journal*.

SMITH, C. (March 13, 2014). "It turns out Target could have easily prevented its massive security breach", *BGR*.

SMITH, Chris (January 16, 2014). "Expert who first revealed massive Target hack tells us how it happened", *BGR*.

TARGET (n.d.). Press releases related to the data breach: https://corporate.target.com/about/payment-card-issue.

2016-05-12