Crisis Evaluation

Target Credit Card Hacking

Christy Brown, Elizabeth Earles, Maddie Hutt

Final Case Study

4-26-16

Target Misses the Mark

For more than 100 years, customers have shopped confidently at Target retail stores for affordable, reliable products. As a leading competitor in discount retail, Target emphasizes a focus on customer's privacy and satisfaction. However, on Nov. 27, 2013, Target's data security system was hacked, compromising customers' credit card information. Over this 18-day crisis, more than 40 million credit card numbers and 70 million addresses, phone numbers and other forms of personal information were leaked. In its handling of the crisis, Target exhibited poor communication with their key publics, and the incident is recognized as a public relations crisis management failure.

Target began in 1902 when George Draper Dayton took full ownership and became the first president of the Dayton's Department Store in Minneapolis, Minnesota. Dayton's leadership transformed the store into a mass-market discount store in 1960 that provided for "value-oriented shoppers seeking a higher-quality experience" ("Through the Years," 2016). The name "Target" evolved from the iconic bulls-eye logo, designed by Target's director of publicity, Stewart K. Widdess. "As a marksman's goal is to hit the center bulls-eye, the new store would do much the same in terms of retail goods, services, commitment to the community, price, value and overall experience," said Widdess ("Through the Years," 2016). On May 1, 1962, the Target retail store was born.

The Dayton Department Store's strong emphasis on customer relations and community involvement transferred to Target management. In 1970, management organized Earth Day volunteers to clean parks and plant trees in various states. After that, Target launched a "Take Charge of Education" campaign, became an active donor to St. Jude Children's Hospital and

received President Ronald Reagan's President's Committee on the Arts and Humanities Medal of Honor.

Target outlines environmental protection, political activities and lobbying and international trade in their “Community Outreach” chapter in their Code of Ethics (“Code of Ethics,” 2015). The company employs these initiatives by encouraging recycling and the use of sustainable energy, publicly advocating for gay marriage and supporting its "Wellness for All" campaign. Overall, Target strongly grasps community relations and actively gives back to the towns in which their stores are located.

The "Customer Relations" chapter of Target's Code of Ethics emphasizes five key points: credit and financial services, product and food safety, guest privacy, responsible advertising and fair competition. The "Guest Privacy" section states: "Guests expect (Target) to collect, use, share, retain and delete information appropriately." Repercussions for the improper handling of guest information are stated to "cause serious harm to (Target's) brand, reputation, and relationships and expose Target to legal consequences." It also states that Target depends on laws and regulations when working with customer’s financial products and requires all employees to take responsibility in keeping current with all new regulations (“Code of Ethics,” 2015).

Between Nov. 27 and Dec. 15, 2013, payment card information of 42 million Target customers was exposed to fraud (Clark, 2014). Personal information including names, phone numbers and mailing/email addresses, was stolen (Parks, 2015).

On Dec. 13 through 15, Target executives partnered with the U.S. Justice Department and Secret Service and hired a third-party forensics team to investigate the hack (Skogrand PR Solutions Blog, 2014). The team confirmed that criminals infiltrated the company's data security system, installed malware on its point-of-sale network (register technology) and stole guests' payment information. Upon discovery, Target removed the malware from its registers. The public remained unaware of any security breach (Clark, 2014).

Brian Krebs of KrebsOnSecurity, a security service company blog, reported the breach on Dec. 18 (Clark, 2014). The next day, Target acknowledged the report via Twitter with a link to a

press release that contained minimal details. "Target confirms unauthorized access to payment card data in U.S. stores. Issue identified and resolved." Target continued its usual holiday advertising via Twitter (Skogrand PR Solutions Blog, 2014). However, the story of the breach overpowered any attempt to promote shopping (Lee, 2013).

A Target spokesperson officially acknowledged the breach on Dec. 19. Concerned customers flooded service hotlines. To those customers, Target gave no indication that birth dates or Social Security numbers were accessed and promised that the theft of very few people's credit card information resulted in actual fraud (Clark, 2014).

On Dec. 20, Target issued a press release from Chief Executive Officer Gregg Steinhafel informing customers that the data security system breach had occurred three weeks prior. "The unauthorized access took place in U.S. Target stores between Nov. 27 and Dec. 15, 2013. Canadian stores and target.com were not affected," (Riley, 2014). Steinhafel issued a series of YouTube videos with quick tips for concerned customers. He also offered customers free credit monitoring and a 10 percent discount in-store purchases, a gesture which most customers found underwhelming (Lee, 2013). An apology video was never published.

Target purchased full-page newspaper ads in the nation's top 50 markets and sent a mass email from Steinhafel reiterating the points from his videos (Skogrand PR Solutions Blog, 2014). The company posted daily news briefings on its online newsletter, "A Bull's-Eye View," that featured flurries of photos with captions designed to show employees aggressively responding to the crisis (Lee, 2013). "Thousands of Target team members, including our most senior leaders, have been working around the clock to help make this right for our guests. From call centers to our financial services team to technology teams throughout the company, we will not rest until every guest's need is met," (Lee, 2013).

Allowing five days of silence after the first breach announcement cost Target some credibility with customers (Lee, 2013). "Any time you are not controlling the release of information, you lose the opportunity to cast yourself in the role of hero rather than the villain," said Jack Maloni, head of data security and privacy for Levick Strategic Communications (Lee,

2013). It was clear that Target had no predetermined crisis communication plan for a data security breach (Skogrand PR Solutions Blog, 2014).

By Dec. 22, company records showed that transactions fell 3 to 4 percent compared to the concluding week of holiday shopping the previous year. Stocks dropped significantly after the breach was announced, hurting Target's holiday season revenues (Clark, 2014).

An investigative forensic unit also discovered that encrypted debit information was accessed during the breach, but Target assured customers that PIN numbers remained secure (Clark, 2014). The company tweeted a guide to setting up REDcard alerts for monitoring one's bank account, posted instructions for reaching the customer support center and released an article about the crisis on its website (Parks, 2015).

The article, however, was poorly formatted. Customers wanted to know if it was safe to use their credit and debit cards in Target stores. Target vaguely answered this question fourth on the list of Frequently Asked Questions (Kosner, 2013). The answer read, "Has the issue been resolved? Yes, Target moved swiftly to address this issue so guests can shop with confidence. We have identified and resolved the issue of unauthorized access to payment card data. The issue occurred between Nov. 27 and Dec. 15, and guests should continue to monitor their accounts." The vague implications of the answer left customers to believe that because Dec. 15 had passed, the source of the breach was identified and the crisis was resolved (Kosner, 2013).

By Jan. 10, 2014, the toll of customers affected by payment or personal information theft increased by an additional 70 million. Target's executive board lowered the company's profit forecast for the fourth quarter and reported that sales were meaningfully lower than expected after the news of the data security breach (Clark, 2014). This breach affected Target's relations with their employees. Target's Minneapolis headquarters released 475 employees, and another 700 employee positions in the U.S. were left unfilled (Clark, 2014). In Canada, all 133 stores closed and the company released more than 17,000 employees (Parks, 2015).

The Consumer Bankers Association and Credit Union National Association reported that costs associated with the data security breach topped $200 million (Clark, 2014). Target

committed $100 million to update security technology and announced Chip-and-PIN register technology for credit and debit cards to be introduced by early 2015 (Clark, 2014).

The company also agreed to pay $10 million to settle a lawsuit for invasion of privacy, distributing nearly $10,000 to each victim of identity fraud. For victims to receive the remedial payments, they must have experienced at least one of the following: Unauthorized reimbursed charges on their payment card, time spent addressing unauthorized charges, fees spent to hire someone to correct a credit report, higher interest rates or fees on their bank account, credit related costs such as purchasing credit reports or costs to replace their ID, Social Security number or phone number. The settlement also required Target headquarters to make changes to its security policies within 10 business days. Changes included appointing a new chief information security officer, keeping a written log of information security program activity and offering security training to relevant workers (Parks, 2015).

On May 5, CEO Gregg Steinhafel resigned, and Brian Cornell, the former CEO of PepsiCo Americas Food, took the position in July (Parks, 2015). Bob DeRodes, the former technology advisor to several federal government agencies, became the new chief information officer (Clark, 2014).

Target's lack of preparedness and timely communication classifies this crisis as smoldering. Known for their secure systems, Target did nothing after receiving a notification of a security breach in their credit card system. Target's leadership first thought the notification of a data security breach was unreliable, assuming big corporations often receive similar messages ("Missed Alarms," 2014). Target should have carried out a practiced crisis management plan after receiving the initial notification. However, Target reacted defensively and was not equipped to handle the breach. It was clear that they did not anticipate this crisis even though a breach of this magnitude was possible.

Investors were never addressed. There is no written evidence of Target ever making a formal announcement to its investors about the breach. Because of this, Target overlooked a major public and lost sight of reaching their key stakeholders. There could have been a closed-

door interaction between the two, but if that was the case, that information should have been released to the rest of its publics to demonstrate full disclosure.

After the public was notified about the crisis, Target practiced poor public relations by burying the lead in a badly formatted press release. "We have identified and resolved the issue of unauthorized access to payment card data," (Kosner, 2013). Customers were forced to read the entirety of the release in order to find this sentence at the end of the statement. This important information should have been listed first to allay the fears of the customers. Within their release, Target said, “We deeply regret the inconvenience this may have caused,” (“A Message from CEO Gregg Steinhafel,” 2013). This insincere phrase shies away from a direct apology to those affected.

According to the press release, the data security system breach took place between Nov. 27 and Dec. 15 of 2013. However, Steinhafel did not address the crisis until Dec. 20 (“A Message from CEO Gregg Steinhafel,” 2013). The breach occurred for a month before Target disclosed any information. Many customers suspected that Target withheld the information from the public to not damage sales potential during the holiday shopping season. The company sacrificed credibility with its customers. Target should have notified customers immediately after receiving intelligence of the breach, then kept publics updated as more information became known.

Target did keep a commendable presence on Facebook during the crisis by making several posts about the breach. The press release posted to Target's website displayed both positive and negative Facebook comments from customers, allowing for transparency and open communication with publics ("Twitter Activity Around Target's," 2013).

However, most of Target's posts included blanket statements such as, "We're listening to your tweets about the data breach in our U.S. stores and have six answers to questions ("Twitter Activity Around Target's," 2013)." Target should have replied personally to the tweets and Facebook comments of concerned customers to address specific questions. Target did not display the ability to be in tune with customer needs in a personable manner.

Target's call center was also not adequately prepared to handle such a crisis. Lines quickly backed up and customers were required to wait a long time to speak to a Target employee ("A Message from CEO Gregg Steinhafel," 2013). From the beginning, multiple call centers and a higher number of employees available should have been established ("Twitter Activity Around Target's," 2013). Eventually, Target tripled its call support after receiving negative feedback on social media from customers.

An outside forensics team investigated the hack (Newman, 2013). Doing so proved that Target accepted the seriousness of the data security system breach and sought to discover the source of the problem and provide a meaningful solution. It showed that Target was willing to accept the consequences of failure to protect its customers' information. Target should have continuously released the information found by the investigative team. This lack of constant communication led customers to believe that though Target's intentions in hiring the investigative team may have been genuine, it was not willing to admit the nature of its mistakes to its publics.

Although Target took a dive in stock after this crisis, it was able to rebound quickly. Target takes responsibility for the hack and includes it in their history on their website timeline named “Through the Years” as an example of a lesson learned. Today, their stocks are continuing to increase and they rely heavily on their Code of Ethics to ensure this won’t happen again.

The 2013 Target data security system breach serves as a lesson to all major corporations about the importance of having a plan, especially for incidents that can escalate into a nationwide crisis. Though Target spoke with one clear voice, it should have spoken louder and more often to protect and inform its customers. Target launched a defense against the breach by being reactive and was ultimately not prepared for the crisis.

Works Cited

1. Clark, Meagan. (2014, May 5). Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed For The Giant Retailer. Retrieved April 20, 2016, from http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056

2. Kosner, A. (2013, December 20). Target's Biggest PR Mistake With Credit Card Security Breach. Retrieved April 03, 2016, from http://www.forbes.com/sites/anthonykosner/2013/12/20/targets-biggest-pr-mistake-with-credit-card-security-breach/#324ab2a439b4

3. Lee, Thomas. (2013, December 25). Target strives to patch its image after huge data security breach. Retrieved April 20, 2016, from http://www.startribune.com/target-strives-to-patch-its-image-after-huge-data-security-breach/237207491/

4. Newman, J. (2013, December 19). The Target Credit Card Breach: What You Should Know | TIME.com. Retrieved April 03, 2016, from http://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know/

5. Parks, Miles. (2015, March 19). Target Offers $10 Million Settlement In Data Breach Lawsuit. Retrieved April 20, 2016, from http://www.npr.org/sections/thetwo-way/2015/03/19/394039055/target-offers-10-million-settlement-in-data-breach-lawsuit

6. Public relations case study: Target data breach. (2014, February 5). Skogrand PR Solutions Blog. Retrieved April 20, 2016, from http://skograndpr.blogspot.com/2014/02/public-relations-case-study-target-data.html

7. Riley, Michael. (2014, March 17). Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It. Retrieved April 25, 2016, from http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data

8. Target. (2013, December 20). A message from CEO Gregg Steinhafel about Target's payment card issues. Retrieved April 25, 2016, from https://corporate.target.com/article/2013/12/important-notice-unauthorized-access-to-payment-ca

9. Target. (2015, September 9). Target Code of Ethics. Retrieved April 24, 2016, from file:///Users/christybrown/Downloads/business_conduct_guide (2).pdf

10. Target. (n.d.). Target through the years. Retrieved April 25, 2016, from https://corporate.target.com/about/history/Target-through-the-years

11. Twitter Activity Around Target's Credit Card Breach [STATS]. (2013, December 30). Retrieved April 03, 2016, from http://www.adweek.com/socialtimes/twitter-target-credit-card-breach/494889