The Rise in Payment System Breaches: The Target Case

Stephen J. Tipton, Young B. Choi[*]
Department of Business, Leadership, and Information Systems
College of Arts & Sciences
Regent University
1000 Regent University Drive
Virginia Beach, VA 23464
USA
[*]E-mail: ychoi {at} regent.edu

Abstract **— We investigate the recent Target Corporation payment system breach, in which an initial estimation of 40 million customers' credit card data was stolen in nearly a three-week span over the 2013 holiday shopping season. We examine exactly what happened, and who was primarily responsible for the attack. Furthermore, we explore the number of those affected by the data breach, which grew substantially after its initial disclosure. we then consider the reaction from the consumers primarily affected by the breach. We contemplate opportunities that Target Corporation et al. have in preventing the outcome of future attacks.**

Keywords-data; credit; breach; card; security; Target; consumers; payment; theft; systems

I. INTRODUCTION

You are a Security Analyst for a major retailer, and are preparing for the rollout of an update to payment terminals at retail outlets. Amid a bevy of recent memos from the federal government and private research firms regarding the emergence of evolving threats to payment terminals, you feel the need to highly recommend a thorough security review of your company's payment system. A critical period lies ahead with the tremendously competitive Black Friday weekend that would kick the holiday shopping season into high gear. The time is of the essence that these security warnings be addressed, as you have suggested. Unfortunately, your recommendation is brushed away initially; something that could be considered a critical misstep in the age in which such threats should be taken very seriously.

This scenario was recently revealed, as the security staff of Minneapolis-based retailer Target Corporation (subsequently referred to as "Target") raised concerns about such vulnerabilities to their payment systems at retail outlets as they were preparing for the release of an update to these systems. Based on memos from the federal government and private research firms, the warnings were in place for potential threats specifically targeted for retail payment systems. It was unclear whether the corporation followed through with the highly recommended review prior to the release of the updated payment systems coinciding with the impending holiday shopping season, or whether the major data breach that ensued was the result of simply allowing hackers to penetrate the system [1].

We will assess the major credit card security breach that ensued at Target, in which roughly 110 million customers' credit card and personal data was stolen during the peak of the 2013 holiday shopping season [2]. In the course of this investigation, we will examine the scope of exactly what occurred, as well as who was primarily to blame for the attack. Research will show that the number of those affected by the data breach grew substantially following its initial disclosure, in addition to findings that show similar companies being targeted as well. Furthermore, we consider the surprising reaction from consumers, in which a recent poll indicates, "Americans fear becoming victims of theft ... [y]et they are apathetic to try to protect their data [3]." As a positive outcome, we will analyze the opportunities that Target and other companies have in preventing future attacks; more importantly, we will shed light on what companies and their consumers can learn from such experiences.

While the major data breach suffered by Target, Michaels, and Neiman Marcus was a serious situation, consumer reaction in addition to lessons learned may actually prove to be a win for these companies.

II. OVERVIEW OF THE BREACH

A. Timing of the Attack

A few days prior to the start of the 2013 Christmas holiday, giant retailer Target acknowledged a massive data breach of credit card data from their in-store payment systems. The company confirmed that roughly 40 million credit and debit card accounts might have been impacted as a result during nearly a three-week window at the height of the holiday shopping season. Initial reports indicate, citing sources at two credit card issuers, that “the breach involved nearly all of Target's 1,797 stores in the United States [4].” Concerns of the vulnerability had been raised amid the release of information from the federal government and private research firms involving specific threats against retail payment systems.

B. Initial Impact

Security firm IntelCrawler reportedly placed the blame upon a Russian source in the creation and distribution of malware that infected Target’s payment system [2]. Additionally, this malware possibly compromised the systems of other retailers recently, such as Michael’s and Neiman Marcus. According to the report, the initial sample of the malware was created in March; more than 40 versions have since been distributed around the world, initially infecting retail systems in Australia, Canada, and the United States. Maksym Yastremsky, a noted Ukrainian credit card hacker who cost credit card companies over $11 million when he ripped off over 40 million cards from U.S.-based retailers in 2007, had collaborated with various hackers to accomplish the 2007 breach. Yastremsky noted that they would occasionally place malware directly on the networks at major retailers; resulting in the data theft at the instant the card is swiped [5].

C. Further Exposure of Personal Data

As the days since the initial acknowledgement of the breach moved forward, it became evident that the 40 million credit card accounts that may have been impacted were just a portion of the overall potential damage. While the amount of credit card data potentially impacted nearly eclipsed the largest credit card breach at a U.S. retailer reported previously, in which nearly 45.7 million payment cards were stolen over an 18 month period in an attack against TJX Cos, the parent of TJ Maxx and Marshalls, it was further revealed that at least 70 million additional consumer’s personal information was stolen as well, bringing the total amount of impact to roughly 110 million consumers [4]. This personal information “is believed to be selling in regional sets, after two men were found with 96 fraudulent credit cards at the Mexican border” used to make purchases from local South Texas retailers [6].

The resulting additional impact places a heavy potential upon the identity protection of these consumers. Criminals are further aided in developing far more sophisticated tactics in impersonating victims, or even leveraging social engineering to gain more sensitive information [7]. Warns Avivah Litan, a fraud and security analyst with Gartner: “These criminals are building up dossiers on individuals ... they’ve got [the consumer’s] e-mail, [the] name and [the] address, and now they have [the] credit card. So now she’s easier to target [7].” Since the discovery of the breach, which involved stolen vendor credentials in conjunction with the Russian-based malware, Target spokeswoman Molly Snyder has declared that the retailer has "taken extra precautions such as limiting or updating access to some of our platforms while the investigation continues [8]."

D. The Challenge of Mitigation

Both malicious code and compromising passwords are described as examples of attacks upon information systems. The malware, or malicious code, utilized in compromising the payment systems potentially could be an example of an active Web script, which is executed with the intent to destroy or steal information. Such malware is considered polymorphic, when it is constantly changing and uses multiple attack vectors. Polymorphic malware is more difficult to detect and intercept; when it uses multiple attack vectors, its complications in defense effort and cost are further increased [9]. SecureState CEO Ken Stasiak says, “One of the things the hackers do is take [ownership of] the malware as it's called. Once it's identified, then the security community can rally around it and put controls in place. But the problem is, the hackers know that. And they manipulate or mutate this malware, and then reuse it [2]."

Exactly how vendor credentials may have been compromised is unclear; however, a number of attacks that attempt to bypass access controls are achieved by guessing credentials [9]. The more common scenarios involve password cracking, brute force attacks, or dictionary attacks. It is unclear exactly what method was utilized to gain access to the passwords for the purpose of executing the malware, however.

III. CONSUMER REACTION

A recent poll indicates that Americans, although fearful of having their identity stolen, are passive when the idea of protecting their data is considered. A striking revelation shows that despite the compromise of 40 million credit and debit cards and personally identifiable information of up to 70 million others, Americans seem to be more laissez-faire in the scope of identity theft prevention [3]. A telling aspect of such a stoic reaction is evidenced by the four out of ten consumers that have had their identity stolen, whom mostly feel their respective credit card companies, banks, or even retailers will take responsibility.

Why does the American culture brush off critical issues in today’s world? Issues that invoke fear at the outset, prove to be too much of a burden to protect oneself from potential harm. The Ponemon Institute performed a study and found that the cost associated with customer loss post-data breach dropped by just over 33 percent. Furthermore, it was indicated that apathy and laziness are more reflected in the dismissal of the ensuing lawsuits that follow a data breach [10]. For example, the Heartland Payment Systems data breach was estimated to have had over 100 million accounts compromised, although actual numbers were never made public. However, the ensuing lawsuit was dismissed.

Carrying on with consumer assumption that credit card companies, banks, et al. will pick up the responsibility, it is suggested that the number one reason we’re losing the identity theft battle is due to consumers being convinced that there is nothing to lose, because there is zero liability. Such a notion was birthed “from a blend of federal law (the FACT Act or FACTA) and marketing savvy by financial institutions, to shift identity theft losses from consumers and victims to the financial industry and merchants [11].” It is true that the financial industry often consumes losses surrounding identity theft and fraud in the hopes of a positive and continued business relationship with customers; however, as a result, consumers have come to equate zero liability with zero responsibility.

The largest cost for identity theft victims is long-term emotional harm. Despite zero liability and the feeling of zero responsibility, the truth is, from the victim’s point of view, that if a thief has your identifiable information, the fight could last for years [12]. Furthermore, worry, lack of trust, betrayal, and impact on credit-worthiness and employment to list a few, seem to linger in the back of consumer’s minds after suffering identity theft.

Since the Target breach, nearly half of Americans surveyed feel a deep concern about their personal data when shopping in stores. Sixty-one percent state they have concerns shopping online, while 62 percent have similar concerns shopping from their mobile devices. However, a mere 37 percent have decided to make their purchases with cash rather than a credit card; and only 41 percent have even followed through with checking their credit report. Even more alarming is that much fewer consumers are reacting by changing their passwords, or even signing up for credit monitoring [3].

We can see with this evidence that consumers are clearly apathetic when it comes to any further personal responsibility following a data breach. While this is good for the affected businesses in continuing a long-term consumer relationship, it goes to show that America follows a lackluster attitude when it comes to preventing the side effects of a business-level crisis such as the Target data breach. However, from the business aspect, it does offer opportunities for the future. Lessons learned in such crises can be a valuable result, a mere reflection of the good that comes from harm. These opportunities are what will be focused on in the next section.

IV. FUTURE OPPORTUNITIES

Closing the last section, it was contemplated that a crisis such as dealing with the fallout of a major credit card data breach could reveal valuable lessons to be learned; therefore, the opportunities that lay ahead for companies dealing with the magnitude of such events are a mere reflection of ultimate good that is revealed through the intention of harm. This section considers several opportunities Target should leverage, some of which have already been addressed. The first two are actions that Target has already acted upon; the latter two, are imminent opportunities on the national level.

A. Preventative Opportunities

In the immediate aftermath of the acknowledgement of the breach, Target began a public relations venture in apologizing for the mishap; more importantly, the company began to embrace the opportunities that lay ahead in preventing future data thefts. The National Retail Federation suggests there be a discussion regarding the need for tougher security standards that could bring higher spending within the industry, banks and business partners. Changes imminent involve the new wave of passion for higher-security cards, known as “Chip-and-PIN” payment cards, which contain computer chips and additionally require consumers to enter a PIN number for authorization [13]. Furthermore, the National Retail Federation is encouraging its members, which include Target, Wal-Mart, and other retail outlets, to upgrade to the higher-security cards despite the higher cost relative to the existing magnetic stripe system.

B. Security Education, Training, and Awareness

Through the implementation of security education, training, and awareness (SETA), organizations will accomplish the improvement in the awareness of the need to protect system resources; the development of skills and knowledge so consumers and employees are able to consider security enhancements; and, knowledge enhancements in effectively operating security programs within the organization and its utilized systems [9]. Likewise, Target has announced a partnership with three trusted organizations--the National Cyber-Forensics and Training Alliance (NCFTA), National Cyber Security Alliance (NCSA), and the Better Business Bureau, Inc. (BBB)--to advance public education surrounding the need for cyber security. As a result, Target will gain expert knowledge from organizations that best understand the complex and growing challenges associated with cyber security. More importantly, the company will be able to effectively educate consumers “in trusted, accessible and understandable ways [14].” Moreover, such a collaborative effort can only be achieved through sharing responsibility and working together effectively, says Michael Kaiser, executive officer of the National Cyber Security Alliance.

C. Congressional Action

From a national standpoint, the data breach could force Congress to act on long-awaited legislation that would better protect credit and debit card information. Congressional gridlock could finally be lifted after years of circular legislative efforts to summarize data protection and disclosure of information theft [15]. Such efforts have withered due to disagreements on potentially far-reaching regulations. However, even a bitterly partisan Congress may see the sense of urgency, at last. Efforts may involve a potential three-fold approach. First, such an effort would require technology improvements that force enhanced security surrounding credit and debit cards; second, it would provide enhanced penalties on data theft; and third, it would enforce stricter regulations involving the reporting of security breaches. Of any potential legislation, the Senate has four data security proposals that could effectively "be combined into a single bill that would win approval and go to the House [15]." Alternatively, the House has several cyber security bills, in addition to one breach notification bill. With these opportunities, the congressional gridlock may finally thin out, after nearly a decade of frustration.

D. Emerging Technologies

"It is interesting that the Target breach happened as discussions about payment security are becoming more intense, driven by the migration in the U.S. to EMV," states James Wester, Research Director for IDC Financial Insights [16]. Even more interesting with this statement is the parallelization it has to the reflection of ultimate benefit that is revealed through the intention of harm. Other opportunities that credit card companies in the United States have involve migrating to EMV, or what may be known as "Europay, MasterCard, and Visa [16]." While Wester notes potentially heated discussions are still to occur on how to successfully implement a transition to EMV within the U.S., as well as how the technology standard would be carried out at the point of sale, this transition may be on the rise. It is important to note, therefore, that EMV would not have prevented the breach. Rather, it would have merely limited the value of any stolen data. Randy Vanderhoof, executive director of the Smart Card Alliance further advocating for the benefits of EMV, considers that it would make an organization "a less likely target for a data breach if the data stored in their system were less valuable to criminals [16]." Similar to the "Chip-and-PIN" potential discussed earlier, EMV entails the use of a small chip on the credit card that validates with a transaction. Most U.S.-based credit cards still function with the magnetic stripe that can unfortunately be captured and copied with relative ease. The chip-based solution, on the contrary, utilizes cryptography and other multi-layered defenses against fraud. In combination with a PIN, security is considerably heightened. As one of the remaining countries to migrate to EMV, according to the Smart Card Alliance, American Express, Discover, MasterCard, and Visa have all made the intention of being the first major credit card companies to transition to an EMV-based infrastructure in the U.S.

V. CONCLUSION

John Mulligan, Executive VP and CFO for Target believes that the chip-based smart cards discussed in the previous section are the wave of the future for American businesses [17]. For Target, this has been in the works for a number of years; as a result of the breach, however, this effort is being accelerated. Mulligan points to a $100 million investment to implement chip-enabled technology for Target point of sale systems. The goal, Mulligan says, is to carry out this technology in Target stores and on the retailer's proprietary REDcards by early 2015, more than six months ahead of the company's previous plan. The importance of this effort being relayed to consumers lies in the simple fact that while the current magnetic-stripe system is highly prone to theft and further compromise of customer identity, the theft of a chip-based card number would be rendered useless to the attacker without the chip.

Countering the chip-based explorations, the effectiveness of mobile payments against any use of a physical card is considered. Mobile payments, mobile ticketing and mobile transactions "will be central to our lives in the future." Most people throughout the world will be in a situation in which mobile will be the only avenue of electronic payment. Backing such a statement up are the 4.6 billion mobile phones currently in use, in addition to the 1.2 billion mobile web users in the world and 3 billion active SMS users; all encompassing the support of a $100 billion business and an infrastructure forging ahead as "the world's foremost transaction platform [18]."

These are all very relevant opportunities to leverage in the wake of such a massive data breach. Most evident in these situations is the collective good that is becoming a result of the harm the attackers intended to infuse upon consumers and the various targeted companies. Through the investigation of the major credit card security breach that occurred at Target, involving the credit card data theft of roughly 40 million customers, research has shown that the number of those affected by the data breach grew substantially following its initial disclosure. Additionally, research has shown that not only other retailers, such as Michael's and Neiman Marcus, were also targets. Considerations were discussed involving the reaction of customers regarding the likelihood of taking necessary steps to prevent identity theft. It was determined that much of the country is increasingly apathetic to the responsibility of ensuring protection of their identity. Lastly, an extensive focus on the opportunities ahead for the affected retailers--and credit card companies in the United States as a whole--was detailed clearly showing that not every evil plan in the world has to result in long-term pain. In fact, it may be a considerably valid statement to make that despite the major data breach suffered by Target et al. was a serious situation, the valuable lessons learned may actually prove to be a win for retailers, credit card companies, banks, and consumers in the long term.

VI. REFERENCES

[1] D. Yadron; P. Ziobro; and D. Barrett. "Target Warned of Vulnerabilities Before Data Breach." February 14, 2014. http://www.marketwatch.com/story/target-had-warnings-before-breach-2014-02-14-134493028

[2] M-L. Gumuchian; and D. Goldman. "Security firm traces Target malware to Russia." January 21, 2014. http://www.cnn.com/2014/01/20/us/money-target-breach/

[3] A. D'Innocenzio. "Poll: Target security breaches not changing people's habits." January 27, 2014. http://www.northjersey.com/news/Poll_Target_security_breaches_not_changing_peoples_habits.html

[4] "Target confirms massive credit, debit card data breach." CBS/Reuters. December 19, 2013. http://www.cbsnews.com/news/target-confirms-massive-credit-debit-card-data-breach/

[5] S. Hargreaves; and K. Johnston. "Busting a credit card hacker." February 5, 2014. http://money.cnn.com/2014/02/05/technology/security/credit-cards-hacker/index.html?hpt=hp_t1

[6] D. Lynch. "Michaels, Target, and More: The Biggest and Most Sensitive Data Breaches in Recent History." January 25, 2014. http://www.ibtimes.com/michaels-target-more-biggest-most-sensitive-data-breaches-recent-history-1548033

[7] J-L. Yang; and A. Jayakumar. "Target says up to 70 million more customers were hit by December data breach." January 10, 2014. http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html

[8] G. Wallace. "Stolen credentials blamed in Target breach." January 29, 2014. http://money.cnn.com/2014/01/29/news/companies/target-breach-password/index.html?iid=EL

[9] M. E. Whitman; H. J. Mattord; and A. Green. *Guide to Firewalls & VPNs.* 3rd ed. Boston, MA: Course Technology, 2012.

[10] J. Stroup. "Data Breaches Slip Through The Cracks." n.d. http://idtheft.about.com/od/Commentary/a/Data-Breaches-Slip-Through-The-Cracks.htm

[11] N. O'Farrell. "12 Reasons Why We're Losing the Battle Against Identity Theft." 2013. http://www.idt911blog.com/2013/08/12-reasons-why-were-losing-the-battle-against-identity-theft/

[12] N. O'Farrell. "The Top 10 Most Common Identity Theft Myths." 2013. http://www.nealofarrell.com/20131221151/identity-theft/the-top-10-most-common-identity-theft-myths.html

[13] R. Kerber; P. Wahba; and J. Finkle. "Target apologizes for data breach, retailers embrace security upgrade." January 13, 2014. http://news.yahoo.com/target-apologizes-data-breach-retailers-embrace-security-upgrade-172658839--sector.html

[14] "Target to invest $5 million in cybersecurity coalition." Target Corporation. January 13, 2014. https://corporate.target.com/discover/article/Target-to-invest-5-million-in-cybersecurity-coalit

[15] J. Spencer. "Target data breach fuels drive for new laws." January 26, 2014. http://www.startribune.com/business/241992041.html

[16] T. Groenfeldt. "American Credit Cards Improving Security With EMV, At Last." January 28, 2014. http://www.forbes.com/sites/tomgroenfeldt/2014/01/28/american-credit-cards-improving-security-with-emv-at-last/

[17] J. Mulligan. "Time for smartcards." February 4, 2014. https://corporate.target.com/discover/article/time-for-smartcards

[18] D. Birch; and N. Livingston. "Mobile Payments - Safer than Cards?" *Inside Revenue Management Issue 30*. https://www.tmforum.org/ArticleMobilePayments/8745/home.html

[19] S. Tipton and Y. Choi. "The Target Security Breach: A Case Study," CyberSecurity 2014, Stanford University, Stanford, California, USA, May 27-31, 2014.