School of International and Public Affairs
Case Consortium @ Columbia
Columbia University

SIPA-21-0021.1

Target Cyber Attack:
A Columbia University Case Study

Executive Summary

In this case study, we examine the 2013 breach of American retailer Target, which led to the theft of personally identifiable information (PII) and credit card information belonging to over 70 million customers from Target's databases.

This case study will first consider Target's vulnerabilities to an external attack in 2013 and explain how the attackers stole the data. Second, this case study will discuss the importance of corporate responses to data breaches when they do happen, using Target as an example.

The case includes the following elements;

a) Video Intro and Discussions – Available Online

b) Written Case Study (This Document)

c) Annex A – Original Documents

This case was written by Sean Steinberg, Adam, Stepan, and Kyle Neary for the Picker Center Digital Education Group at Columbia's School of International and Public Affairs (SIPA). The faculty sponsors are Greg Rattray and Jason Healey.

Background

As long as companies have used online servers to store data, the benefits of greater convenience have had to be balanced against a higher degree of vulnerability to data breaches. Even in 1984, before the internet was widely used, the physical theft of a password allowed an attacker to access the personal financial information of 90 million American clients of a credit reporting company that would later become Experian.[1] Throughout the 2000s and 2010s, virtually all large companies' operations became reliant on storing sensitive data online.

Inevitably, increasingly large data breaches occurred as criminals became more skilled and companies used more online servers. In 2013 alone, the login credentials of 360 million MySpace users were stolen, and the personal information of a record 3 billion Yahoo users was compromised (though both attacks were not reported for years). Other large tech and internet companies such as Adobe and LinkedIn had also been breached before, but the Target data breach would show that companies in any sector were vulnerable to cyber-attacks.

In 2013, Target was the United States' third-largest retailer and a top 50 company in the Fortune 500, operating nearly 2,000 stores in the U.S. and Canada.[2,3] On December 19, in the middle of the holiday season, the company announced that its point-of-sale (POS) machines, by which customers pay in-store, had been compromised. As a result, the attackers made off with 70 million customers' Personally Identifiable Information (PII) and 40 million customers' credit card information.

Exemplifying the ever-growing sophistication of data breaches, the attackers used multiple types of malware, to harvest web application credentials and to scan POS machines for card information. However, they relied heavily on using nefarious legitimate IT applications nefariously, as well as a technique known as "Pass the Hash" to obtain administrator privileges.

A Chink in the Armor

In order to steal customer data, the attackers took advantage of Target's lack of network segmentation. Since company devices were highly connected to one another, the attackers' first step was to find a weak link – a less secure device – and from there spread to other devices, such as POS machines.[4] The attackers found their weak link in the computer systems of Fazio Mechanical Services, an HVAC contractor Target used, which in turn was using a free antimalware service and which had limited information security procedures in place.

Using phishing emails, the attackers infected Fazio's systems with Citadel, a popular malware that can steal login information stored in computers' web browsers.[5] This malware earned them access to credentials with which they signed into a contractor-facing portal hosted by Target. This portal was a web application where Fazio could upload legitimate documents such as invoices, but Target failed to block uploads of

[1] Newman, L.H. "The WIRED Guide to Data Breaches." *WIRED*. Dec. 7, 2018.

[2] "2013 Top 100 Retailers." *STORES Magazine*. Jul. 2013.

[3] "Fortune 500 2013." *FORTUNE*. 2013.

[4] Plachkinova, M., Maurer, C. (2018). "Teaching Case: Security Breach at Target." *Journal of Information Systems Education*, 29:1, 11-20.

[5] "The Untold Story of the Target Attack Step by Step." *Aorato Labs*. Aug. 2014.

executable files. Taking advantage of this access and the lack of controls on vendors' ability to interact with Target systems, the attackers uploaded a "web shell" named after a legitimate file. The web shell comprised a script with operating system commands that, once uploaded, gave the attackers remote access to Target's servers.

The attackers then located Target's secure servers, which contained credit card numbers and their holders' personal information. But first, the attackers would need the "holy grail" of access – Domain Admin privileges. Pass-the-hash methods provided an easy way of obtaining these privileges. The attackers took advantage of single sign-on, a common design that allows administrators to have to log in to their user account once and be automatically logged in for applications. Single sign-on relies on hashes, encoded output generated from passwords, remaining stored on servers as long as administrator accounts were logged in. Unfortunately, only the hashes, not cleartext passwords, were needed to log in as an administrator. Thus, the attackers harvested the hashes and gained administrator privileges.

With these privileges, they could create their own separate Domain Admin account, which could maintain their network access even after the original account's password was inevitably reset. To avoid suspicion, they even named this new account after a legitimate IT application.

After mapping their targets, the attackers then used a series of connected servers as a "tunnel" to bypass security measures and infiltrate the database. When they arrived, however, they found no credit card information awaiting them. This was because Target complied with Payment Card Industry (PCI) Security Standards, which among other things required merchants to dispose of card numbers after purchases, rather than storing them in a database.[6]

Though slowed down, the attackers turned instead to the memory on POS machines. On about 40,000 out of Target's 60,000 POS machines, they installed Kaptoxa, a type of malware that can disguise itself as legitimate antivirus software and break POS machine's firewalls.[7,8] Kaptoxa then stored customers' credit card information in machine memory as transactions were made; ultimately, the credit card information of 40 million customers was exfiltrated to an attacker-controlled server.

A Harsh Dose of Reality

The operation affected customers who shopped at Target between November 27 and December 15. Target did not notify customers of the breach until December 19, four days after identifying it. In his first interview after the breach, Gregg Steinhafel, who served as Chairman, President, and CEO, justified the delay. He explained that the first day "was about making our environment safe and secure. We worked very hard on that. And by 6:00 at night, our environment was safe and secure. We eliminated the malware and the access points. And, so, we were very confident that coming into Monday, guests could come to Target and shop with confidence with no risk."[9] However, the drive to enable customers to continue shopping during the holiday season would prove shortsighted, as even after Target removed the immediate cyberthreat, many customers' confidence in the company would be slow to rebound.

[6] "The Prioritized Approach to Pursue PCI DSS Compliance." PCI Security Standards Council. May 2016.
[7] Kitten, T. "Target Breach: What Happened?" *BankInfoSecurity*. Dec. 20, 2013.
[8] Prabhakaran, K.P. "Beware of 'BlackPOS' malware in data breaches." *Fraud Magazine*. Nov./Dec. 2015.
[9] "CNBC Exclusive: CNBC Transcript: Target Chairman & CEO Gregg Steinhafel Speaks with Becky Quick Today on CNBC." CNBC News Releases. Jan. 13, 2014.

Target itself did not become aware of the breach through its own detection systems, but through credit card companies, who realized an attack had occurred after noticing a surge in fraudulent transactions. Target had invested in a virus detection service, which flagged malware from the attack on November 30. However, Target's security operations team did not fully investigate this particular alert and respond in time to prevent the attackers from moving within the network and escalate privileges.[10] This oversight highlights the challenges of effective monitoring in detecting suspicious activity. Additionally, the value of controls such as routine checks for new Domain Administrators and tighter controls on who could access what parts of the Target network would have gone a long way in preventing the attackers from successfully exfiltrating data.

For Target, after understanding it had suffered a cyber breach, "day two was really about initiating the investigation work and the forensic work … Day three was about preparation. We wanted to make sure our stores and our call centers could be as prepared as possible. And day four was notification. So, throughout that four-day process, to some people it probably felt longer than that, we worked around the clock to try and do the right thing," according to Steinhafel. Clearly, to Target executives, four days qualified as a speedy response, and indeed, Target was much quicker than other major companies have been to reveal breaches, with some waiting months.[11] Nonetheless, Target appeared to lack transparency due not only to their relatively slow response, but also the fact that news of the breach broke before Target revealed it. To repair the public relations fallout from these mistakes, Target had to offer more generous sales and even offered victims a free year of credit monitoring and identity theft protection.[12]

For many Americans, the scope and prominence of the Target attack brought cyber risk out of the realm of abstraction and made it a concrete reality. Previously, major corporations were largely trusted by the public with safeguarding their most sensitive information. If America's third largest retailer could be hacked, cybersecurity could no longer be taken for granted. In 2014, a study found that 45% of shoppers did not trust retailers to securely store their personal information.[13] The attack's scale of impact should not be understated – as expressed by the security blog *WeLiveSecurity*: "The odds are very good that if you lived in the US in 2013, even if you yourself were not affected [by the attack], you probably know plenty of people who were."[14] In the worlds of business and information security, the Target attack also served as a wakeup call to the dangers of interconnectedness: that your network is only as secure as your least secure business associate.

Following the attack, Target faced numerous lawsuits from different parties. Target announced in 2015 that the breach cost the company $162 million in expenses related to the breach. It paid $18.5 million to settle a multi-state lawsuit, $10 million to settle a federal class-action lawsuit, $39 million in response to a separate class-action lawsuit brought by several U.S. banks, and $67 million to Visa alone. One analyst expected to see Target's merchant fee increase by "a few basis points" as a result of the failure to secure their data. In the immediate wake of the attack announcement, Target's share price fell 2.2%, while the S&P-500 fell

[10] Riley, M., Elgin, B., Lawrence, D., Matlack, C. "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." *Bloomberg*. Mar. 17, 2014.

[11] Burg, N. "Five Lessons For Every Business From Target's Data Breach." *Forbes*. Jan. 17, 2014.

[12] Petru, A. "Can Companies Restore Consumer Confidence After a Data Breach?" *TriplePundit*. Jul. 8, 2014.

[13] "Retail's Reality: Shopping Behavior After Security Breaches." Interactions, Jun. 2014.

[14] Meyers, L. "Target targeted: Five years on from a breach that shook the cybersecurity industry." *WeLiveSecurity*. Dec. 18, 2018.

0.06%. Overall, Target was estimated to have lost $1 billion from the attack, only a small fraction of which cyberattack insurance covered.[15]

In the wake of the data breach, both CEO Gregg Steinhafel and Beth Jacob, the company's Chief Information Officer, resigned. "Just going through the motions, like buying security products and getting your security tested, was not going to cut it: you need to architect for security, skill up for security, and train for security," said cybersecurity expert Stephen Cobb.[16] "If the C-suite is not making security a priority for all departments and all employees, you are at higher risk than your competitors that *do* prioritize security." The Target case increased attention to cyber vulnerability and risk as an essential element of corporate governance and highlighted the exposure of corporate leadership to mismanagement of these risks.

The Target breach became a primary driver of two key expectations with cyber risk management. First was that cybersecurity programs must include understanding and minimizing vulnerabilities posed by network and data access by vendors and the greater supply chain, not just the protection of the corporate network and data itself. Additionally, along with a number of other high profile data breaches in 2013 and 2014, this case led to acknowledgement that corporate crisis management programs must stress response and recovery as key elements, including the ability to effectively communicate with a wide range of external stakeholders such as press, regulators, and law enforcement.

Additionally, many analysts believe the Target attack had an even greater impact within the financial system by galvanizing the push for the widespread adoption of credit card chips & PINs. For example, shortly after the data breach, one fraud analyst argued "it's time for the U.S. card industry to move to chip/smart cards and stop expecting retailers to patch an insecure payment card system," referring to magnetic stripe cards.[17] Within months of the breach, President Obama went so far as to sign an executive order to speed up the transition to chip and PIN credit cards.

Summary

The December 2013 attack on Target is notable for its role both in heightening public concern about data breaches and in expanding the significance of cybersecurity in corporate responsibility. Target was the United States' third largest retailer and one of its most ubiquitous companies. Further, on the whole Target did not have particularly poor IT or payment practices. Nonetheless, all it took to compromise the majority of their POS machines was a contractor with less effective antimalware and an exposed web portal on Target's end.

Key takeaways include the necessity of companies with large amounts of sensitive to data to go beyond industry standards in securing their information and the benefits of segmentation in company networks for reducing risk. In the twenty-first century, corporations must constantly be aware of evolving threats and routinely check for vulnerabilities at all levels in their computer systems. Further, they must understand and limit supply chain cyber risks. After all, it is clear that attackers are only becoming more sophisticated from the Target attack, which used phishing, deployed multiple types of malware, impersonated legitimate programs, and combined manual hacking with automatic scraping of card

[15] Perlroth, N., Harris, E. "Cyberattack Insurance a Challenge for Business." *New York Times*. Jun. 8, 2014.
[16] Id.
[17] Litan, A. "What can we learn from the Target Breach." Gartner. Dec. 19, 2013.

information. While more secure computer systems and checking the security posture and access of vendors does place greater operational costs on companies, corporate leaders must ensure they analyze the potential value of avoiding a wide range of costs such as those suffered by Target in this case: multiple lawsuits, higher credit card processing fees, and lost customer confidence, all of which decreased revenues. In the Target case, accountability for the effective risk management, slow crisis response and, reputational damage suffered went all the way to the top of the corporate leadership.

ANNEX A: Original Documents

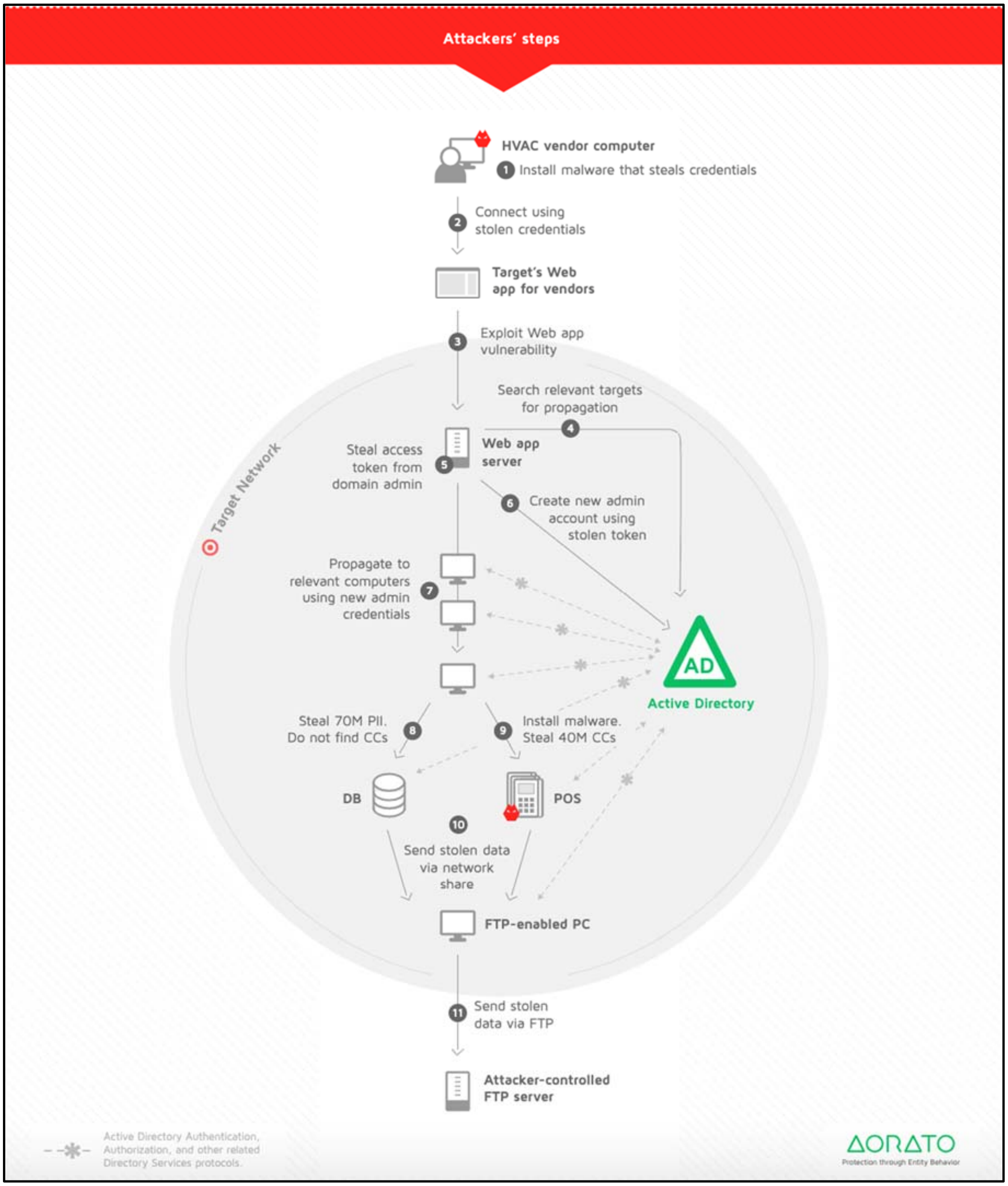
Annex A-1: Flowchart of the Target data breach

Annex A-2: Graph of the Target data breach’s costs

Annex A-3: Email sent by Target notifying customers of breach

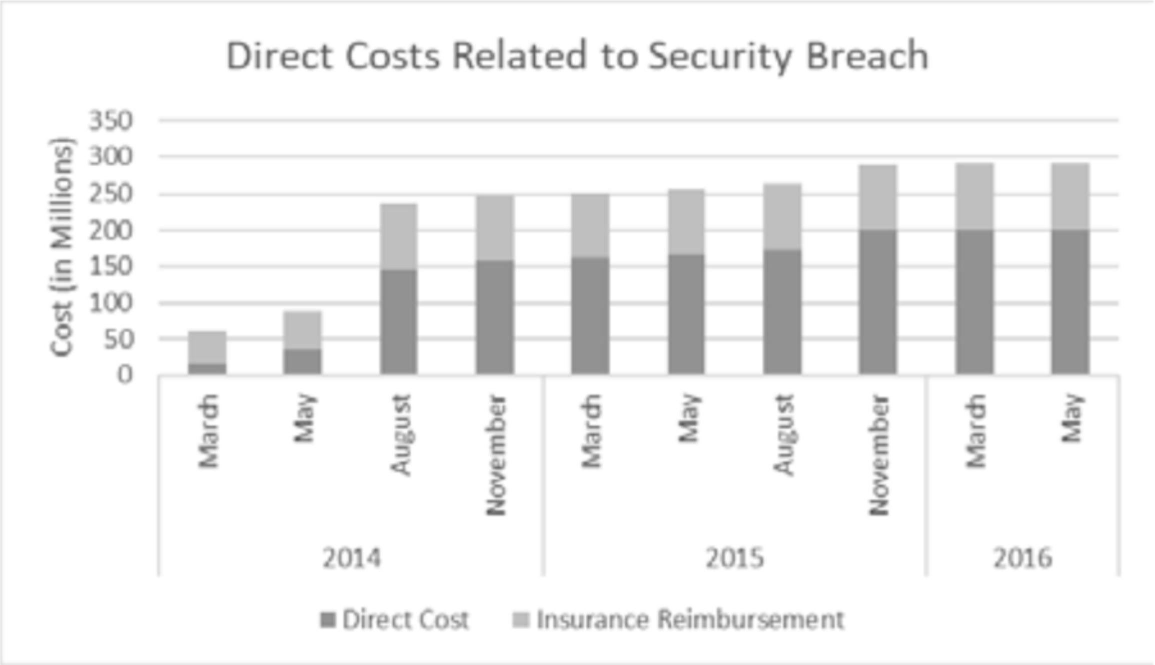
Annex A-1

Flowchart detailing how attackers stole 70 million PII's and 40 million credit cards from Target. Available from Arato Labs here.


Attackers' steps
HVAC vendor computer
1 Install malware that steals credentials
2 Connect using stolen credentials
Target's Web app for vendors
3 Exploit Web app vulnerability
Search relevant targets for propagation 4
Web app server
Steal access token from domain admin 5
6 Create new admin account using stolen token
Target Network
Propagate to relevant computers using new admin credentials 7
AD
Active Directory
Steal 70M PII. Do not find CCs 8
9 Install malware. Steal 40M CCs
DB
POS
10 Send stolen data via network share
FTP-enabled PC
11 Send stolen data via FTP
Attacker-controlled FTP server
Active Directory Authentication, Authorization, and other related Directory Services protocols.
AORATO
Protection through Entity Behavior

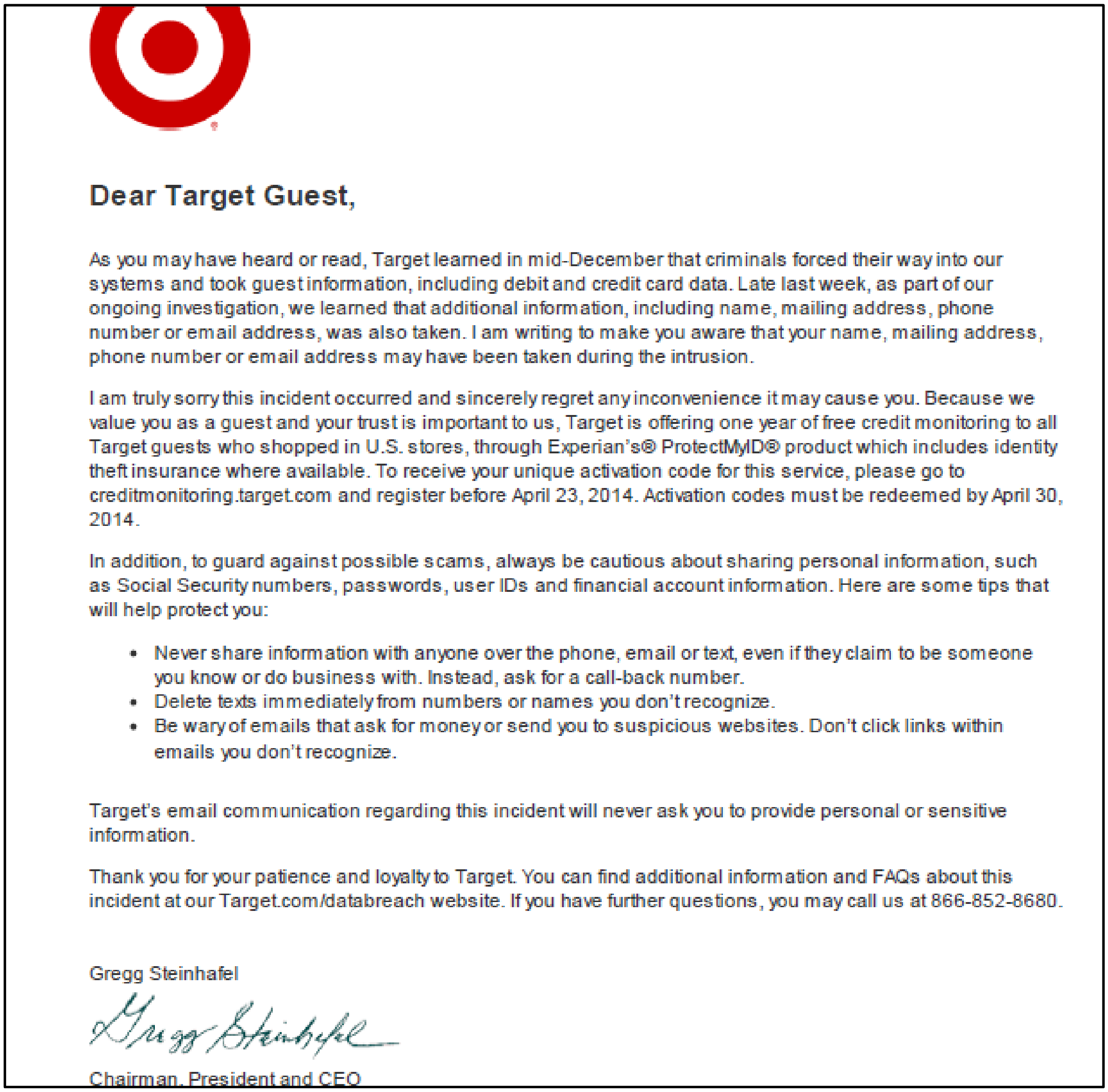
Annex A-2

Graph of the December 2013 Target data breach's costs by (cumulative by quarter). Available from the Journal of Information Systems Education here.



Annex A-3

The email sent out by Target on December 19, 2013, to notify customers of the data breach. The email was sent four days after Target discovered the breach and one day after journalist Brian Krebs broke the news to the public. Available from ZDNet here.



Dear Target Guest,

As you may have heard or read, Target learned in mid-December that criminals forced their way into our systems and took guest information, including debit and credit card data. Late last week, as part of our ongoing investigation, we learned that additional information, including name, mailing address, phone number or email address, was also taken. I am writing to make you aware that your name, mailing address, phone number or email address may have been taken during the intrusion.

I am truly sorry this incident occurred and sincerely regret any inconvenience it may cause you. Because we value you as a guest and your trust is important to us, Target is offering one year of free credit monitoring to all Target guests who shopped in U.S. stores, through Experian's® ProtectMyID® product which includes identity theft insurance where available. To receive your unique activation code for this service, please go to creditmonitoring.target.com and register before April 23, 2014. Activation codes must be redeemed by April 30, 2014.

In addition, to guard against possible scams, always be cautious about sharing personal information, such as Social Security numbers, passwords, user IDs and financial account information. Here are some tips that will help protect you:

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

Target's email communication regarding this incident will never ask you to provide personal or sensitive information.

Thank you for your patience and loyalty to Target. You can find additional information and FAQs about this incident at our Target.com/databreach website. If you have further questions, you may call us at 866-852-8680.

Gregg Steinhafel

Gregg Steinhafel

Chairman, President and CEO