

Security

Breach

at

Target

4375

A BST RA CT

This case study follows the security breach that affected Target at the end of 2013 and resulted in the loss of financial data for over 70 million customers. The case provides an overview of the company and describes the reasons that led to one of

management processes and the vulnerability at Fazio Mechanical Services that was among the main causes of the breach. Further, the case introduces the incident response plan implemented by Target and discusses the aftermath of the attack.

The lessons learned describe some of the steps the company took to mitigate risks in the future and to strengthen its security posture. While the breach had a significant impact on Target, the organization was able to fully recover from it and develop best practices that are now widely implemented by other retailers. The case is suitable for both undergraduate and graduate students enrolled in information security or information systems courses that discuss vendor management, security incident response, or general security program administration topics.

**Key words:** Information assurance & security, Cyber security, Case study, Teaching case, Experiential learning & education

1.

INTRODUCTION

There are numerous definitions of information security, but many of them revolve

2

around achieving confidentiality, integrity, and availability of the information and/or systems (Anderson, 2003; Dillon and Backhouse, 2000; Sumra, Hashbullah, and Ab Manan, 2015; Von Solms and Van Niekerk, 2013). These goals are important, as they provide trust and guarantee the safety of data in motion and data at rest.

Within the retail industry, information security is critical as it ensures that the organizations follow best practices and can protect their personal and financial information of the customers. As Greig, Renaud, and Flowerday (2015) point out,

Elloff, 2010). Security culture has the potential to play a significant role in this respect (Vroom and Von Solms, 2004). A strong and effective security culture is in place when every employee performs daily tasks in a secure manner and such

Demonstrating a strong security posture is especially important for retail companies because they rely on having positive brand recognition and gaining the

effect and potentially impact many other corporations in a negative way. Thus, understanding the critically important factors in building a strong security culture and following best practices is essential for any retail company.

2.

## MOTIVATION

In corporate real world examples into the cybersecurity curriculum. While it is important for students to master terminology and have solid foundational knowledge, the authors believe they should also be able to apply the knowledge to actual organizational settings where information security issues arise. There has been a myriad of breaches affecting a wide range of companies and individuals (Home Depot, J.P. Morgan Chase, Ashley Madison, the Office of Personnel and Management, eBay, Sony, and Hillary Clinton),

but there are relatively few case studies developed solely for use in the classroom with accompanying learning objectives and teaching notes. Thus, the authors wanted to explore the recent security breach at Target due to the abundance of information available and the various angles from which the students can approach the topic.

3.

## E VALU AT ION

A fter draftin g t he case tex t ,it was d ist ribu ted to stu d ent s i n an i nfo rmati on securit y  
p rin cip l es co u rs e at amedi um

-

si zed ,p riv ate univ ers it y i n th e US.T hi rty ei ght

u nd erg radu ate st ud ent s w erep res en t ed w ith th e cas e text an d refl ect ion qu esti ons

q uest ion s w ere col l ect ed as p art of ag rad ed ass ign ment and were ev al uat ed u si ng  
ru bri cs to d etermi n ew heth ers tud ents exceed ed ,met ,o rd id not meet ex pectatio ns  
acros s v ariou s learning ob jectiv es .Th e auth o rs al so prov id ed stu dent s wi th apap er  
s u rv ey th at in cl ud ed sev eral o p en

-

end ed ques tio ns .Th e au tho rs as k ed t h em to

d escrib ewh at t hey l ik ed and dis li ked abo ut th e cas e,wh et her any addi ti on al

i n fo rmati on s hou ld be pro vi ded ,w heth erth ey hav e an y su gg es ti ons for

i mprov ement ,and w hat sou rces th ey us ed whenp rep ari ng th ei ran al ys es .Ov erall ,

students provided very positive feedback on the casewrite

-

up. Students expressed

some concern over the discussion of vendor management processes, and therefore additional detail around the vendor management processes was added to the case.

In terms of performance against learning outcomes, the average grade students received on this assignment was 94%, which exceeds expectations. Moreover, specifically, 1 student did not meet the expectations (<65%), 9 students met the expectations (65

-

89%), and 28 students exceeded the expectations (>90%). These

results indicate that students were able to successfully perform the case study

analysis, understand and interpret the main issues, and provide feasible and

adequate solutions for improving the security practice Target Corp. The authors

statement with additional resources, readings, and integrate previous course

content in their analysis. The authors used Turn It In to avoid any plagiarism on the

Business recommended rubric for problem solving.

4.

## CASE SYNOPSIS

At the end of 2013, amid the holiday shopping season, Target became a victim of a

security breach affecting over 70 million customers. Their personal and financial

Fazio

Mechanical Services. The breach was first reported by the security journalist Brian

able to regain the customer

After the attack, Target implemented several steps to mitigate any future breaches.

The company created a Cyber Fusion Center, provided free credit card monitoring

for its customers, and implemented POS terminals with chip readers. These steps

4

demonstrate

future.

breach (including vendor management and incident response), the investigation, the fallout, and lessons learned.

5.

## CASE TEXT

5.1

### Company Profile

With its first store opening in Roseville, Minnesota, on May 1, 1962, Target aimed to differentiate itself by providing many features of traditional department stores but providing lower prices typically associated with discount retailers. The name Target was chosen purposefully as Stewart Widdess (Director of Publicity) states

-

they thought the store would do much

the same in terms of retail goods, services, commitment to the community, price,

across the country. Through various acquisitions and expansions into new areas of the country, Target has become the second

-

largest discount retailer in the United



States (behind Walmart). As of February 1, 2014, Target operated 1,793 retail stores to retail locations in the United States, employed approximately 360,000 employees, and had annual revenues of \$72.6 billion (Statista, 2015).

providing great value to its customers while maintaining an exceptional shopping

experience for both customers and employees is to always behave ethically and with integrity. Their efforts to be a responsible corporate citizen have earned

(Target, 2017).

While Target has worked diligently to position itself as a leading retailer in the United States with prominent charitable values, they have certainly experienced hardships throughout their long history. Notably, in 2013, they suffered a massive data breach that exposed sensitive financial information for millions of customers.

recovered and has learned many valuable lessons on the importance of protecting sensitive information.

## 5.2

### Before the Breach

Like many corporations, Target employed a staff of dedicated security professionals to implement safeguards to protect sensitive data. As part of their ongoing security efforts, Target successfully passed a compliance audit for the Payment Card Industry Data Security Standard (PCI

-

DSS) in September of 2013

(Riley et al., 2014). PCI audits involve a review of critical security controls and systems configurations to verify that best practices for protecting payment card information on computer systems is maintained. Target also completed the implementation of a \$1.6 million malware detection tool developed by the cybersecurity company FireEye in 2013 (Riley et al., 2014). Their security operations center, with

teams of personnel in Minneapolis, Minnesota, and Bangalore, India, provided round

-

the

-

clock monitoring of cybersecurity threats on the network. While there is no method for ensuring complete protection against cybersecurity threats, Target appeared to be following industry best practices and had reasonable security controls in place.

### 5.3

#### Breach Notification and Initial Response

On November 30, 2013, security operations personnel in Bangalore, India, received notification from their malware detection software that some potential all-y-malicious activity was recorded on the network. The alert was shared with security personnel in Minneapolis, but no further action was taken. Another alert was raised on December 2, 2013, but again no action was taken (Riley et al., 2014). It was not until December 12, 2013, when the U.S. Department of Justice contacted Target about a possible breach of their network, that Target began investigating the issue in earnest. The Federal Bureau of Investigation (FBI) and the Secret Service joined the investigation as well. While no public disclosure was made at the time, the independent security researcher and blogger, Brian Krebs, posted information regarding a possible breach of the Target network on December 18, 2013. On December 19, 2013, Target issued the following public statement on the matter:

Target today confirmed it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Target is working closely with law enforcement and financial institutions, and has identified and resolved the issue.

Swiftly to address this issue, so guests can shop with confidence. We regret any

Approximately 40 million credit and debit card accounts may have been impacted

6

between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions immediately after it was made aware of unauthorized access, and is putting all appropriate resources behind these efforts. Among other actions, Target is partnering with leading third

-

party forensic firm to conduct thorough investigation of the incident.

Initially, Target denied that debit card PIN numbers had been stolen, but reports confirmed that encrypted PIN numbers had indeed been stolen (Finke and Henry, 2013). Another update (Target, 2014) on the breach was provided by the company a month later, on January 10, 2014, outlining the fact that personal information (names, addresses, phone numbers, and email addresses) were also taken in this breach. While there were some critiques about the fact that the company delayed its response after initially identifying the breach, Target Chairman and CEO Gregg Steinhafel defended the decision:

Sunday (Dec.15) was really day one. That was the day we confirmed the address and so our membership priority was ... making our environment safe and

eliminated the malware in the access point, we were very confident that coming into Monday guests could come to Target and shop with confidence and no risk.

Day two was really about initiating the investigation work and the forensic work ... that has been ongoing. Day three was about preparation. We wanted to make sure ours to respond our call centers could be as prepared as possible, and day four was about notification. (Quick, 2014)

In addition to the public response, Target sent out an email to its customers (Appendix A) on January 16, 2014, offering one year of free credit monitoring. The company provided them with information about protecting themselves and staying safe. However, the email was sent to many individuals who never had conducted business with Target, which raised speculation as to how the retailer obtained the data. One possible explanation is that perhaps the email addresses were from Amazon, a remnant from the old Amazon

-

Target partners hip. However,

when consumers asked where Target obtained email addresses for people who are not now and have never been customers of the retailer, the spokeswoman simply

trust with the offered incentives, Target opened another door for speculation on its processes for collecting and handling customer data.

## 5.4

### The Investigation

As part of the incident response process, Target commissioned security

## 7

professionals at Verizon to assist in the investigation into how the breach occurred.

A detailed security audit was performed from December 21, 2013, to March 1, 2014, and served two primary purposes: 1) identify the root cause of the breach

While the report issued by Verizon has remained confidential, various media outlets claimed to have received information stemming directly from the report.

The findings presented below have not been confirmed by Target, but have been reported by several reputable security researchers and media outlets.

The initial point of entry appears to have stemmed from hijacked credentials stolen from Fazio Mechanical Services, a third-party service provider. Fazio, a supplier of

refrigeration devices and services, began working with Target to support the expansion of fresh food offerings across stores in the United States. As with many

Services, 2014).

cyber

-

malware that can be used to steal login credentials from computer systems.

been alleged that Fazio relied on the free, non

-

commercial version of

Malwarebytes Anti

-

Malware software, which does not provide real

-

time

protection. It is not clear whether Target enforced any ongoing security reviews of

its vendors to ensure compliance with security best practices.

While this attack did not appear to have an immediate impact on Fazio, it is likely that account credentials for accessing Target systems were stolen during the Fazio

attackers to access customer data, however, so additional vulnerabilities in side the Target network must have allowed attackers to escalate their account privileges, traversed the network, and obtained over 40 million customer card numbers.

Further investigation revealed that there were no major obstacles to access in point of sale (POS) terminals across the entire network on behalf of the internal Target network. This lack of network segmentation could allow any malicious user the ability to traverse the network and attempt to access various devices ranging from point of sale terminals to mission critical back-

end systems. To illustrate the lack

of segmentation, the Verizon audit team supposedly accessed a cash register after they compromised

an electronic scale that was located in a different store (Krebs,



The audit team also found significant problems with enforcement of password policies. Target maintained a password policy that included industry -

standard

practices, however, investigators found multiple files stored on Target servers that included login credentials for various systems. According to Brian Krebs, the audit report revealed that

The Verizon security consultants identified several systems that were using misconfigured services, such as several Microsoft SQL servers that had a weak administrator password, and Apache Tomcat servers using the default administrator password. Through these weaknesses, the Verizon consultants were able to gain initial access to the corporate network and to eventually gain domain administrator access. (Krebs, 2015)

The use of weak passwords was apparently rampant within the Target infrastructure, and the security investigation team was able to crack over 500,000 passwords, representing 86% of identified accounts, to various internal Target systems.

Investigators also identified significant issues related to the maintenance and patching of systems. Again, Brian Krebs claims:

For example, the Verizon consultants found systems missing critical Microsoft patches, or running outdated [web server] software such as Apache, IBM

Web Sp here, and PHP.These services were hosted on web servers, databases, and other critical infrastructure. These services have many known

vulnerabilities associated with them. In several of these instances where Verizon is covered these outdated services or unpatched systems, they were able to gain access to the affected systems without needing to know any authentication credentials. Verizon and the Target Red Team exploited several vulnerabilities on the internal network, from an unauthenticated standpoint. The consultants were able to use this initial access to compromise additional systems. Information on these additional systems eventually led to Verizon gaining full access to the network

and all sensitive data stored at on network shares

through adomain

administrator account. (Krebs, 2015)

Given the previously stated vulnerabilities, the attackers were able to access points of sale terminals and install malware directly on all machines across the network.

-

malware software installed

November and early December, it is likely that the malware was installed on the terminals at this time.

9

The malware contained memory

-

scraping functionality that allowed the attackers

to intercept cardholder information before it was sent for processing by payment processor. The PCI

-

Council, 2016). However, the configuration of point of sale terminals at Target did not provide the ability to immediately encrypt cardholder data upon registering a card swipe. Because of this, card data remained in plain text within the POS

external card processing systems (as required under PCI

-

DSS). Since the malware

was installed directly on POS terminals and allowed the ability to scrape data from memory of these machines, the attackers were able to intercept unencrypted

cardholder data for all card swipes registered in Target's to res.

5.5

The Fallout

Target has claimed that up to 70 million individuals may have been impacted by this data breach (Target, 2015a). At the time, this was one of the top ten largest data breaches recorded (Quick et al., 2016). In the aftermath of the breach, consumer confidence in Target was impaired significantly. According to Kantar Retail, a consulting group researching consumer spending behaviors, the percentage of U.S. households shopping at Target in January 2014 was 33%. This was down from 43% for the same month the preceding year (Malcolm, 2014). In

We believe the Data Breach adversely affected our fourth quarter U.S. Segment sales. Prior to our December 19, 2013, announcement of the Data Breach, our U.S. Segment fourth quarter comparable sales were positive, followed by meaningfully negative comparable sales results following the announcement. Comparable sales began to recover in January 2014. The collective interaction of year

-

over

-

year

changes in the retail calendar (e.g., the number of

days between Thanksgiving and

Christmas), combined with the broad array of competitive, consumer behavioral

and weather factors makes any quantification of the precise impact of the Data

Breach on sales infeasible. (United States Securities and Exchange Commission, 2014)

financials, the company experienced a 1% decrease in revenues from 2012 to 2013,

and its net income decreased 34.3% in the same time period. The large impact to

net income was largely attributable to the additional costs associated with

investigating and remediating the security breach.

The financial impacts were not limited to the few months following the breach,

however. Over the course of the next two years, Target continued to incur costs

10

-

Q and 10

-

K filings

with the SEC, the company has incurred \$2.91 billion in cumulative expenses related to this breach. Of this, approximately \$90 million was offset by insurance coverage, leaving Target with total direct costs of just over \$200 million (United States Securities and Exchange Commission, 2016). The breakdown of costs reported by Target for each quarter from the announcement of the breach to May 2015 are displayed in Figure 1:

Figure 1: Cumulative Costs Related to Security Breach, by Quarter

5.6

## Lessons Learned

Even though Target experienced one of the biggest data breaches in history, it is still accessible to billions with almost 1,800 stores in North America in 2015 (Target, 2016). While the attack did impact the company, there are some key

loyalty is something that builds over time and even such massive security flaws could be overlooked by the most devoted and dedicated individuals who associate themselves with the company. Some of them even perceived Target as a victim of the attackers and sympathized with the company during the hard times it was experiencing.

operations, and in 2015 created the first Cyber Fusion Center, which is dedicated to preventing similar attacks from happening again. Brian Cornell, chairman and

CEO of the company, said:

Data security is a top priority at Target, so we continue to invest heavily in top talent, as well as technology, and focus on continually evaluating and evolving our plans to invest in technology and supply chain this year. (Target, 2015b)

mix of human intelligence, analytics and state

-

of

-

the

-

art technology to detect,

investigate and contain threats to our business. Much of the work they do takes place in our newly opened Cyber Fusion Center (CFC). (Target, 2015b)

Another improvement that Target made was adding chip readers with PIN codes for customers. In fact, Target became the first major U.S. issuer to use chip and

PIN credit cards in 2015 (Digangi, 2015), even as most card issuers in the United States were issuing less secure chips and signature cards. The addition of an EMV

11

chip makes a card more difficult and more expensive to counterfeit. However, adding a PIN code on top of the EMV chip makes it even less likely that card information can be stolen and used to make unauthorized purchases.

35

-  
year employee of the company with the last 6 at the helm, resigned in May 2014. The CIO was also replaced with Bob DeRodes, an executive with a very strong background in information security. The Target board of directors was also undersignedificant pressure. A proxy firm, Institutional Shareholder Services, had recommended that investors oust seven board members. The firm said the board failed to protect the company from the data breach. The board members were able to convince shareholders to re-

-  
elect them, however, although the message to them was clear that future data security breaches were considered to be their responsibility (Basu, 2014). The full press release from Target regarding the



man ag eri al chang es is avail ab l ei n Ap pendi x B.

A lth oug h T arg et never shared di rectl y any lessons learned ,t h e ex amp les abo v e

p rot ecti on fo r it s cus to mers .T aki ng res pons ib ili ty for th e breach at th e hig hest  
l evel w as so met hin g th at i s s til l u ncommon in o rgani zat ion s o f su ch scal e.O v erall ,  
t h e breach en fo rced many new ru les and pract ices wi th reg ards to in fo rmat ion  
s ecu rity ,as b oth retail ers and cu st omers were no w aw are of th e con s equ en ces of  
s u ch an att ack .

6.

## CON CL U SION

Wh il e th es ecu rity breach at Targ et i mp acted asin gl e co rp o rati on ,i t is imp ort ant to  
n ot et h at su ch breaches hav eno w b eco mep art of o ur everyd ay li v es .It i s no t a  
matt er of if,b ut wh en ab reach w il l o ccu r.T hus ,th e auth ors b eliev et h at

th e

l esso ns learn ed fro mT arg et arevali d and can be gen erali zed to o th ero rg ani zati ons  
as well .Fo ri nst ance,t h e breach s ti mu lat ed other ret ai l ers s uch as Wal

-

Mart and

H ome Depot to in st all chip read ers on th ei r POS t ermin al s .Su ch best pract i ces  
s how th at ot h ers realize th e impo rtance o f s t reng th eni ng th ei r secu ri ty pos tu re and  
p rovi din g b et t er pro tect ion again st ind ivi dual s wi th mal i cio us inten ts .Furth er,

Target demonstrated that they have the capacity to recover from such serious events due to having up

-

to

-

date disaster recovery/business continuity plans. These

best practices should be followed by others who want to prepare themselves for the inevitable.

In conclusion, this case study provides an objective view of the events surrounding the 2013 Target breach and outlines both the adequate and inadequate actions

how major organizations are impacted by such attacks, what can be done to limit

12

these breaches in the future, and how to be better prepared to respond when they happen. The case study adds value to the cybersecurity curriculum as it requires students to put into practice the knowledge they gained from the classroom and apply it to a real world scenario. The case study reveals the complexity of the security breach and its impact on the business processes and customer trust

factors that any business professional should understand before going to the

industry.

7.

## ACKNOWLEDGEMENTS

Research reported in this publication was supported by the Sykes College of Business Faculty Collaboration Grant at the University of Tampa for the 2016-2017 academic year.

8.

## REFERENCES

Anderson, J.M. (2003). Why We Need a New Definition of Information Security. Computers & Security, 22, 308-313.

Basu, E. (2014). Target CEO Fired

Can you

be fired if your

Company is Hacked? Retrieved October 29, 2017, from

https://www.fores.com/sites/ericbasu/2014/06/15/target

-

ceo

-

fired

-

can

-

you

-

be

-

fired

-

if

-

your

-

company

-

is

-

hacked/#709e3f37c9fa.

Daveiga,A.&Elloff,J.H.(2010).A Framework and Assessment Instrument for

Information Security Culture.Computers &Security,29,196

-

207.

Dhillon,G.&Backhouse,J.(2000).Technical Opinion: Information System

Security Management in theNew Millennium.Communications of ACM,43,125

-

128.

Digangi,C.(2015).Target Becomes First Major U.S.Issueto Use Chip & PIN

Credit Cards.Retrieved January 31,2017,from

<http://blog.credit.com/2015/10/target>

-

becomes

-

first

-

major

-

u

-

s

-

issuer

-

to

-

us e

-

chi p

-

p in

-

credi t

-

card s

-

127 55 1/ .

Fazio Mech an ical Serv i ces .(2 014 ).St at emen t on Targ et dat ab reach .Ret ri ev ed  
J anu ary 3 1 ,2 017 ,from [http :// fazio mechani cal .com/T arg et](http://fazio-mechanical.com/Targ-et)

-

Breach

-

St at emen t .pd f.

Fi nkl e,J .&H enry ,D.(2 01 3).Ex clus iv e: Targ et Hackers Sto l eEn cry pt ed Ban k  
PINs

So u rce.Ret riev ed J anu ary 31 ,20 17,fro m

[h tt p://ww w .reut ers .com/ art icl e/u s](http://www.reuters.com/article/us)

-

target

-

data breach

-

id USBRE9BN0 L22 013 122 5 .

Greig, A., Renaud, K., & Flowerday, S. (2015). An Ethnographic Study to Assess the Effectiveness of Information Security Culture in a Retail Store. In International Security (World CIS), 2015 World Congress (61

-

66).

Krebs, B. (2015). Inside Target Corp., Days After 2013 Breach. Retrieved January 31, 2017, from <http://krebsonsecurity.com/2015/09/inside>

-

target

-

corp

-

days

-

after

-

2013

-

breach / .

Malcolm, H. (2014). Target Sees Drop in Customer Visits after Breach. Retrieved

January 31, 2017, from

<http://www.usatoday.com/story/money/business/2014/03/11>

/target

-

customer

-

traffic/6262059/.

Quick, B. (2014). Target CEO Defends 4

-

day Wait to Disclose Massive Data

Hack. Retrieved January 31, 2017, from <http://www.cnbc.com/2014/01/12/target>

-

ceo

-



d efend s

-

4

-

d ay

-

wai t

-

to

-

d is cl os e

-

mass iv e

-

d ata

-

h ack .ht ml .

Q ui ck ,M., Ho llo wood ,E ., Mil es ,C., &H amps on ,D .(2 016 ).Wo rld 's Bigg est

D at a Breach es .Ret riev ed Janu ary 31 ,20 17,

fro m

h tt p:/ /ww w .in fo rmat io nis b eaut iful .net/ vis ual izatio ns /wo rl ds

-

biggest

-

data

-

breaches

-

hacks/.

Quirk,M.B.(2014).Non

-

Target Customers Wondering how Target got Contact

Info to Send Email about Hack.Retrieved

January

31,

2017,

from

<https://consumerist.com/2014/01/17/non>

-

target

-

customers

-

wondering

-

how

-

target

-

got

-

contact

-

info

-

to

-

send

-

email

-

about

-

hack/.

Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014). Missed Alarms and 40

Million Stolen Credit Card Numbers: How Target Blew It. Bloomberg

Businessweek, 13.

Security Standards Council.(2016).PCIDSSQuick ReferenceGuide.Retrieved  
January 31,2017,from [http://www.pcisecuritystandards.org/documents/PCIDSS\\_](http://www.pcisecuritystandards.org/documents/PCIDSS_QRG_v3_2.pdf?agreement=true&time=1476207333578)  
[QRG\\_v3\\_2.pdf?agreement=true&time=1476207333578](http://www.pcisecuritystandards.org/documents/PCIDSS_QRG_v3_2.pdf?agreement=true&time=1476207333578).

Statista.(2016).Total Number ofTarget Stores in North America from2006 to  
2015.Retrieved January 31,2017,from

<https://www.statista.com/statistics/255965/total>

-

number

-

of

-

target

-

stores

-

in

-

north

-

america/.

Sumra,I.A., Hasbulah,H.B., &Abmanan,J.B.(2015).Attacks on Security

Goals (Confidentiality,Integrity,Availability) in VANET: A Survey.In Vehicular

Ad

-

How Net works for Smart Cities (51

-

61): Springer, Singapore.

Target.(2014).Target Provides Update on Data Breach and Financial

Performance.Retrieved January 31,2017,from

<https://corporate.target.com/press/releases/2014/01/target>

-

provides

-

update

-

on

-

data

-

breach

-

and

-

financial.

Target.(2015a).Data Breach FAQ.Retrieved January 31,2017,from

<https://corporate.target.com/about/shopping>

-

ex p eri en ce/p ay men t

-

card

-

iss u e

-

FAQ .

J anu ary

31,

2 017 ,

fro m

h tt ps: // co rp o rat e.t arget .co m/arti cl e/20 15/ 07 / cyb er

-

fus ion

-

cen t er.

T arg et .(20 16 ).T arg et th roug h th e Years .Ret ri ev ed J an uary 31 ,

2 017 ,

fro m

[h t t p s : // c o r p o r a t e . t a r g e t . c o m / a b o u t / h i s t o r y / T a r g e t](https://corporate.target.com/about/history/Target)

-

th ro ugh

-

th e

-

years .

14

T a r g e t . ( 2 0 1 7 ) . A w a r d s a n d R e c o g n i t i o n . R e t r i e v e d J a n u a r y 3 1 , 2 0 1 7 , f r o m

[h t t p s : // c o r p o r a t e . t a r g e t . c o m / a b o u t / a w a r d s](https://corporate.target.com/about/awards)

-

r e c o g n i t i o n .