Direct and Indirect Cost of Privacy

The economics behind one of history's largest data breaches

Jason Lin, Jonathan Marin, Tanvi Arora, Muthu Palanisamy, and Stephen Merritt

Abstract— This article is a revised look into one of the most public and widespread data breaches of the last decade, the Target data breach of late 2013. Our focus of effort centered on the value that is placed on privacy by both consumers and those in the business to simultaneously protect and share our personal information. Our attempt was to highlight specific risk management decisions that must be weighed when considering the lengths to which companies will go to protect consumer data. Even more importantly, we take an in-depth look at a company's response following a large-scale breach. In the wake of the Target data breach, and every other similar large-scale event, it is said that the offending company's "brand" is severely damaged. This article looks to more clearly define just how much damage these companies sustain. Anecdotally, we also look at the growing trend of selling one's personal data for profit, which begs the question: Is the new cost/benefit analysis for data privacy shifting to the idea that one data point be the price a consumer would accept to sell their data and compare that to the amount they are willing to pay to protect it?

I. Introduction

In December 2013, it was announced that Target had suffered one of the most widespread data breaches in history. The most recent settlement with 47 different state governments in May, 2017 pushed the estimated loss to over $300M. [1] A host of employees, including the CEO and CIO were fired, and public trust was shaken. How shaken was the public's trust is certainly up for debate? A current CISO was recently quoted, saying "Let's be honest, a cyber-attack is not having life impact…. unless a breach really effects 'real' life, organizations don't care. Your data is my data – it's all virtual." [2] It should be noted that in year following the highly publicized data breach, Target enjoyed its most profitable year in the past five, with a gross profit of $19.24B. [3]

So, what are the true economic drivers behind the idea of data privacy? To answer these questions, it's important to provide definitions and context to the problem. Economics is the academic study of the production, distribution, and consumption of goods and services, while privacy is defined as the quality or state of being apart from company or observation, along with the freedom from unauthorized intrusion. [4]

Combining these definitions and looking at them through the prism of a large-scale data breach, the economics of privacy is loosely defined as the study of the processes and behaviors, both personal and corporate, that comprise the collection, protection, and disclosure of consumer data. The primary consideration here are the trade-offs that arise as the consequence of consumer data being disclosed or protected.

From a business perspective, CEOs and CFOs want a risk metric and value in terms of cost in order to understand their exact level of liability if a breach were to occur. Consumers want a feeling of security and a sense of trust that the companies they choose to invest their hard-earned resources in will take the necessary actions to ensure the privacy of their personal information remains intact. In the past twenty years, this give and take relationship between consumer and corporation has been under constant strain. "We live in a consumer data-driven and consumer data-focused commercial revolution, in which individuals are at the same time consumers and producers of a most valuable asset: their personal information." [5] Naturally there are two sides to the debate regarding the availability of information. On one side, in a theory, popularized by Chicago School economists, it is believed that the more privatized data is, the more social welfare is diminished. On the other, is the belief that all data must be protected.

To better understand these theories, we will take an in-depth look, through the lens of the Target data breach, at the balancing act of access and protection of consumer data. We'll investigate what Target and similar companies stand to lose in the event of a large-scale breach and look at the ways in which Target responded following the data breach, and perhaps, most importantly, we'll discuss measures to prevent large-scale data breaches from occurring. We will anecdotally delve into the topic of buying and selling one's personal data and conclude with holistic review of the Costs and Benefits to cyber security as they relate to Target.

II. Damage from breach

In the aftermath of a data breach, Business suffers in many ways like dealing with financial repercussion such as

1. Government imposed fines
2. Customer compensation
3. Legal expenses
4. Increase in E&O insurance cost
5. Stock value plunging
6. Additional IT spending to find

    a) Who are all affected? And to what extent?
    b) How to restore data integrity?
    c) Is there another business entity affected?
    d) Has the infiltration arrested?
    e) What is the contingency plan? & How to execute it?
    f) What is the time line?

The answers to these questions typically take to time to realize, and in the interim, could lead to loss of business revenue, damage to the reputation, brand value and customer trust. If the stolen data has sensitive information like Personal Identifiable Information (PII), then the damage could be multifold and difficult to estimate since this opens up identity theft and long-term impact to the customers.

According to corporate IT Security Survey the Top 3 consequences of a breach are [6]

1. Loss of access to business-critical information
2. Damage to company reputation
3. Temporary loss of ability to trade

Top 3 most expensive types of security breach

1. Third-party failure
2. Fraud by employees
3. Cyber espionage

Before the Target episode, the cyber security initiatives were discussed within IT departments to focus the spotlight on root causes, technical fixes and required remedies. Unfortunately, these discussions rarely had any impact on executive team members. This all changed with the Target data breach which took a toll on the CEO who was 35-year employee of the company. Target also replaced their CIO who had a very strong background in information security. The company's board of directors was also under significant pressure. The message to the executive team and directors was clear, future security violations are the responsibility of the executive team. This means that C-level executives must understand the risks and gain in-depth knowledge on the technology concepts and applicable laws.

Companies experiencing data breaches often claim that they have state-of-the art, up-to-date security systems. In reality, hackers find gaps to get in and out with data. There could be a third-party vendor responsible for the gap. Vendors should also maintain high standards and be aware of the network & security concepts and technology. International Data Corporation predicted that a quarter of the world's population will be affected by a data breach by 2020. According to Breach Level Index, 7 Million [7] data are lost or stolen every day. That's a staggering 81 records per second.

For a fair estimation on the cost of the stolen records, we took the example of Equifax Data Breach that occurred in July, 2017. During this attack malicious agents infiltrated into Equifax systems by identifying a weak point in the credit agencies website software. This hack granted them access to sensitive files in the credit bureaus system from Mid-May to July 2017. The estimated amount of data stolen are around 147.7 million records of like, name date of birth, social security number and other personal information. From the 2017 Dream Market Darknet data published by the Arizona State University's Artificial Intelligence Lab [8], Full credit report of Equifax data is being sold in Dark Web for $50/record which translates to a whopping $7.385 billion USD.

Smaller breaches go unnoticed (or) not even reported, in some case these exposures are grossly underestimated. For example, the real depth of the Yahoo's 2013 & 2014 breaches came to light only last October. This revelation immediately wiped out $350M off of the Verizon acquisition deal.

For a more detailed look at the price of the Target data breach, please see the Cost-Benefit Analysis in section VI.

III. Company's Response to data breach

In the wake of the 2013 data breach at Target, critics have started to point out the many flaws and weaknesses concerning Target's network security and response. Target had systems in place to detect breaches in security; however, many did not know the significance or the correct response to the alert [9]. Therefore, the combinations of the given situations led way to the massive data breach at Target. Even though this was a tremendous blow to Target's profit and reputation, many lessons were learned from this event.

In the aftermath, Target made a multistate settlement, which in turn, was the beginning of data security standards across the nation. In this settlement, a standard was set to tighten Target's digital security and also security on Target's payment system. With respect to Target's digital security, the settlement required Target to implement the following:

1. Develop and maintain a comprehensive information security system
2. Install software and encryption programs on personal information
3. Segment out cardholder data from the corporate network
4. Control access to the network
5. Require Third Party vendor to assess security of their systems,
6. Hire an executive officer as security advisor the CEO [10].

This, in many eyes, is not considered a particularly advanced security standard. In many corporations, these points are considered a security industry standard that many have already implemented. However, by stating this in the settlement, it sets precedence in what is considered negligent activity in the eyes of the law when concerning data breaches.

The settlement has also stated standards that need to be implemented with respect to Target's payment systems and card holder data. The following are the main points listed in the settlement:

1. Whitelisting to detect and block unauthorized applications from executing,
2. file integrity monitoring,
3. change management, and logging and monitoring of devices connecting to the network [10].

The settlement also stated that Target also needs to comply with the Payment Card Industry (PCI) Data Security Standard (DSS) [10]. These safeguards are particularly important since customer payment information is considered highly sensitive and the highest security should be implemented for this particular type of data. The fact that all sensitive information must be encrypted is one of the standards set by PCI DSS shows that encryption is essential in security [10]. Many of the activities listed here are meant to prevent unauthorized users from entering the system and executing unauthorized applications, along with logging who has entered the environment. The explicit stating of these actions further iterates the importance that all companies should be following these standards.

Even though all these safeguards are explicitly stated, there are still some parts that need further clarification. Since the Target data breach came from a third-party vendor, there is vague explanation on what type of security standard corporations should hold third-party vendors to [9]. This makes sense because corporations need to know the network and data security standard third party vendors have in place. If the vendors have low quality security, it represents a serious vulnerability to the corporation. With this in mind, the corporation should not, in good consciousness, provide data to the vendor in fear there will be a data breach with the vendor. Therefore, further clarification needs to be made on the actions that need to be undertaken with third party vendors. The settlement also stated the need for penetration tests, however, it fails to explicitly state how often this needs to be completed. An important point, considering new vulnerabilities are constantly found and new attack programs are being developed [9]. Therefore, further clarification needs to be stated on how up to date software and security programs need to be made in order to be considered secure. The Target settlement had made great strides in clarifying the essential data and network security standards that corporations should follow, however, there is still work to be done to further protect our data as new attacks and new programs are being developed.

As shown here, Target had many deficiencies in its data security that led to today's predicament with the breach of many people's private information and accounts. This created a situation where people began to question if their information is being protected and seeing if other companies are as deficient as Target. Millions if not billions of dollars lost not only to the account holders, but also to Target. The reputation that Target gained through this event may have caused widespread shareholder sellout and probably loss of business and contracts with other companies that Target has dealings with it. Knowing how much direct and indirect cost of damage is important in knowing what is the cost of privacy in today's market.

IV. Prevention and Solution

Upon Target's failure to prevent a massive data breach, there were several measures of prevention and solutions to prevent a data breach from occurring have been suggested. Target needed solutions to combat:

1. Improper segmentation of the network
2. Securing point of sale (PoS) data
3. Improving warnings and not ignoring alerts provided by their network security system.

Hackers that stole consumer data were able to penetrate Target's network from the business sector of the network and gain easy access to the consumer data because of weak segmentation between non-sensitive and sensitive networks inside the company [11]. As the hackers gained access to the business division and then persistently infiltrated the entire network, segmenting their sensitive assets from normal network portions could have aided in the prevention of the data breach. Target's VLAN technique used for segmentation is reported as easy to get around [12]. Hackers were able to penetrate Target's network from vendor, Fazio Mechanical, that had access to Target's business sector and gained access of PoS terminals. [Fig. 1.] After CEO Gregg Steinhafel resigned, newly appointed CIO, Bob DeRodes, provided a solution to enhance security with 100 million dollars. DeRodes enhanced the network segmentation by reviewing and streamlining network firewall rules and developed a comprehensive firewall governance process [13].

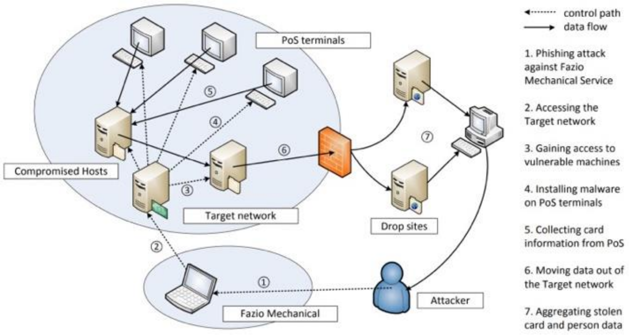
control path
data flow
PoS terminals
Compromised Hosts
Target network
Drop sites
Fazio Mechanical
Attacker
①
②
③
④
⑤
⑥
⑦
1. Phishing attack against Fazio Mechanical Service
2. Accessing the Target network
3. Gaining access to vulnerable machines
4. Installing malware on PoS terminals
5. Collecting card information from PoS
6. Moving data out of the Target network
7. Aggregating stolen card and person data

Fig 1. [15]

In result of the Target Breach, BlackPOS was installed onto the point of sale systems which left consumer data compromised. To correct this, Target enforced integrity of the PoS terminals by using digital signatures and certificates on the PoS systems [11]. The new workflow [Fig. 2.] demonstrates that only trusted executables can run on the point of sale machines.

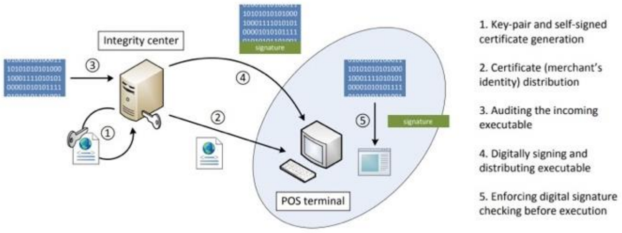
Integrity center
POS terminal
signature
①
②
③
④
⑤
1. Key-pair and self-signed certificate generation
2. Certificate (merchant's identity) distribution
3. Auditing the incoming executable
4. Digitally signing and distributing executable
5. Enforcing digital signature checking before execution

Fig 2. [11]

The executable verification techniques are suitable for dedicated environments such as point of sale systems since they are specifically designed to processes payment. This ensures that the software and programs on PoS terminals are bound and easily audited. Also, since PoS terminals are controlled by the merchant (Target), this warrants that the integrity center for auditing and signing of all executables that are created can be controlled as well. [11]

The PoS terminal is hardened by a policy that only binaries signed by the merchant can execute. The five step-protocol is:

1. The integrity center generates a public-private key and creates a self-signed certificate Cert
2. The integrity center distributes Cert to every PoS terminal in the company. Cert is placed in the root certificate list at each terminal.
3. The integrity center audits every binary that needs to be executed on PoS
4. The signed binary is sent over the merchant network to PoS terminals.
5. The PoS terminal checks the binary signature using Cert and executes only the ones correctly signed.

Target had been warned multiple times that malware was threatening their system by an application produced by FireEye, Inc., but these xml alerts were ignored by the warning team in Bangalore who took no action in response from these alerts [14]. Note that Target implemented the use of Fire Eye only 6 months prior to the data breach and it appears it was poorly implemented with little training provided to security analysts. The warning team turned off key functionality that would automatically remove the detected malware which could have halted the breach [11]. The nature of the alerts was also ambiguous and lacked detail with regards to the name of malware or the data being extracted. Since the BlackPOS software, which extracts and steals sensitive financial information, is regarded as a zero-day malware and few administrators have experience dealing with it, hence the alerts were ignored [15]. Turning on the features of to remove threats would be an obvious solution to improve security. Also, implementing adaptive warning strength may help security analysts take such alerts more seriously in the future such as continuing to alert security analysts and raising the severity until the threat is handled [11].

V. Price of Consumer Data

When the Target data breach occurred in 2013 we were most concerned about securing only PCI data, but today, privacy is a much broader subject. With the pervasiveness of the internet touching almost everything in our lives, individuals are no longer just consumers of information but public producers of often highly personal data. With the reduction in the cost of data collection, manipulation and use, this personal information is becoming highly valuable. These vast amounts of collected information have substantial economic value.

We are no longer just considering an Individuals' traits and attributes (such as their age, address, gender, income, preferences, and reservation prices), but now we also consider clickthrough's, comments posted online, photos uploaded to a social media site, etc. as highly valuable business assets. These can all be used to target services or offers, to provide relevant advertising, or to trade with other parties. In an effort to leverage the value inherent in personal data, new services (such as search engines and recommender systems), companies (such as social networking sites and blogging platforms), and even markets have emerged (such as markets for crowdsourcing" (Schenk and Guittard, 2011), or the complex online advertising ecosystem (Evans,2009). Existing services, such as travel agencies, record companies, and news media, have also been transformed [16].

The retail industry continues to accelerate rapidly, and with it, the need for businesses to find the best retail use cases for big data. New sources of data, from log files and transaction information, to sensor data and social media, present new opportunities for retail organizations to achieve competitive advantage [17]. It helps organizations make decisions based on data. There is an advent of people-tracking technology that offers new ways to analyze store behavior. Now, with the ability to make sense of the huge data collected, retailers can optimize merchandising tactics, personalize in-store experience via loyalty apps and drive timely offers to drive consumers to complete purchases with the end goal of increasing sales across all channels. By correlating customer purchase histories and profile information, numerous correlations can be generated that can reveal unexpected insights. This can be used to personalize the advertisements by placing ads and special promotions where they are more likely to get customers.

Data is the currency that makes free or near-free services possible. The only reason skype, Facebook and other similar services are free is due to data. Most consumers understand this conceptually but not specifically. Furthermore, consumers may be willing to accept the tradeoff between a value-added service and disclosure of information about them in a classic quid-pro-quo arrangement. However, the challenge is that all this information is buried in a 60-page privacy policy of which most consumers will never read, and if they did, they wouldn’t understand it. [18]

Valuing personal data is difficult. Even though consumer data — like age, gender, location, purchase history, and browsing behavior — has become an increasingly critical ingredient for the fast-growing digital advertising industry that now generates tens of billions of dollars annually, there still aren’t any high-volume marketplaces where personal data is transparently priced and traded. In other words, the average person doesn’t have any good way to determine the value of their own personal data. However, there are social media articles where people have tried to evaluate the price of consumer data. Below are few points from one such article by Wibson [19]. The average US consumer can make $240 per year monetizing their data for digital advertising. This was derived based on revenue generated through advertising products in 2016 in the US Digital Advertising industry ($83 Billion) with Facebook accounting for 19.7% of the total, paying approximately $47/year for the average user’s behavioral data in 2016 for an American Facebook user. Although this is a rough estimate using publicly available information and applying simplistic techniques, it provides a sense of the magnitude of the economic value of personal data. In all likelihood, the number is probably much higher when additional, high-value data-such as purchase history, location, app usage, communication patterns, financial information, among many others – are considered.

VI. Cost-Benefit Analysis

According to Target’s annual report from 2014, a third-party assessor found Target to be compliant with the Payment Card Industry Security Standards Council (PCI SSC) Data Security Standard (DSS) at the time of the Data Breach. So, how does one of the largest data breaches occur considering Target’s perceived strong security standing? Before this question is fully answered, a complete accounting of the data breach is necessary.

First, we need to examine the losses Target sustained in the months and years following the data breach and compare those losses to the investments the company made to ensure the data privacy of their customers. In the months immediately following the Data Breach, Target estimated expenses totaling $61M to cover the following:

1. Investigation costs
2. Credit monitoring and identity-theft protection services to affected customers
3. Increased call-center staffing
4. Procurement of legal and other professional services [20].

Over $44M of this amount would eventually be recovered by Target as a result of their comprehensive $100M Network-Security insurance coverage.

A second significant loss-related expense can be attributed to theft by cybercriminals who used the 2 million stolen Target charge cards while the investigation was still ongoing. Krebs on Security estimates a median charge amount of $18.00 - $37.50 per stolen card, leading to a total loss of $36M - $71M.[21] An even more significant expense incurred by the company was the $153.9M in litigation costs following claims by four major credit networks, individual class action lawsuits, and claims made by 47 individual state governments [1]. It should be noted here that contrary to what is listed above, a forensic investigator working for the credit card companies found Target not to be compliant with PCI SSC (DSS) at the time of the breach.

The most significant of the company's losses in the wake of the Data Breach became available with Target's 4th quarter, 2013 earnings report. The Company reported over $440M in losses that were directly attributed to customer loss of confidence in the final weeks of the quarter following the company's admission of the breach [20, 22]. One expense that should not be ignored was the $55M executive severance compensation package that Target provided the CEO and CIO who were fired amid the controversy. This brings Target's total bill for the Data Breach to a staggering $740M. While this figure represents less than 1% of the company's $72B in annual revenue, it is significant given the company's security posture.

Now, we'll examine the investments Target has made in information security. Target invested $1.6M annually into the same Malware detection system employed by the CIA and Department of Defense. The aforementioned system from FireEye, Inc. is capable of correlating alerts from networks and endpoint security to manage alert volume and false positives to avoid overtaxing Information security employees with too many alerts. This system was online at the time of the breach, and actually notified Target employees of the anomaly caused by the BlackPOS Malware[23] that affected Target's Point of Sale (POS) systems. Had Target employees reacted to the system's alerts, this alone would have prevented the breach. By the numbers, Target had the system in place and operating properly for less 0.2% of the data breach's total cost. It should be noted that Target's security logs have not been made available to the public, so it is unknown how many false positive security events Target's employees were exposed to in the months leading up to the breach. One telling fact is that the share prices for FireEye, Inc. have more than doubled in the years following the data breach hinting at the system's effectiveness and positive reputation.

A second significant investment Target has made to protect customer data is $100M to update their registers and other PoS systems to allow for chip enabled card transactions. While Target had already invested in the system, they were not rolled out until after the breach had occurred. While seen as an effective deterrent, according to Krebs on Security, the chip enabled registers would not have been effective in stopping the theft of card information because they require end-to-end encryption. These chip-enabled technologies are still susceptible during online purchases. This $100M acquisition can be annualized to $20M per year, which brings the annual data privacy costs to $21.6M, or still just 3% of the total data breach costs.

The most difficult cost to analyze is for the event that doesn't happen. Daily security logs are full of these "non-events", and any one of them could potentially end in a massive breach. While most incidents don't ever culminate in the sizeable costs endured by Target Inc., investing in systems that cost less than 3% of the worst-case scenario losses a company can endure is easily worth the investment. This is the constant battle CISOs must face when aiming to convince Executive teams of the need to continually evolve the security posture of their business. The data we now have in the wake of the Target breach does provide a compelling case study for security professionals to dissect and deliver concrete evidence as to worst-case scenario costs, and just how little capital in comparison is a necessary investment to keep customer information safe.

VII. Conclusion

It is well worth mentioning that despite all the publicity, these very preventable large-scale breaches continue to occur at regular intervals. In one of the few cases where the U.S. Court of Appeals actually found a Company at fault for failing to protect customer data, Wyndham Worldwide was found negligent primarily due to the fact they did not require users to change their default passwords.[24] This was two years after the Target breach! As we discussed above, it is extremely difficult to put a price on privacy, or loss of privacy, which in turn makes it harder to use legal or regulatory means as way to punish companies who allow the breaches to occur.

Many feel that GDPR will go a long way in solving the regulatory issue, however, the penalties proposed for bad actors are so steep as to almost not be feasible to enforce. Is the EU going to alienate companies such as Facebook, and possibly lose jobs in the process to impose stiff penalties for a loss of privacy that is difficult to quantify? In the U.S., the opposite is occurring, with the legal system shying away from thoroughly investigating many of these breaches. Until these systems are remedied, it will fall to the individual consumer, and coincidentally, data generator to decide how much their privacy is worth. Just as in any free market, they can then vote with their wallets as to which companies deserve the public's trust.

[1] Vincent Lynch, (May, 2016), TheSSLStore, *Cost of 2013 Target Data Breach Nears $300 Million* Available: https://www.thesslstore.com/blog/2013-target-data-breach-settled

[2] Doug Drinkwater, (Jan, 2016), CSOOnline, *Does a data breach really affect your firm's reputation?* Available: https://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html

[3] Market Watch (Sep, 2018), Available: https://www.marketwatch.com/investing/stock/tgt/financials

[4] Merriam-Webster, Available: https://www.merriam-webster.com/dictionary

[5] Alessandro Acuisti, (December, 2010), OECD.org, *The Economics of Data and Privacy,* Available: https://www.oecd.org/sti/ieconomy/46968784.pdf

[6] Kapersky Lab, *Damage Control: The Cost of Security Breaches,* Available: https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

[7] Data Breach Statistics, *Data Records Stolen Since 2013*, Available: https://breachlevelindex.com

[8] AZSecure, *Intelligence and Security Informatics Data Sets*, Available: https://www.azsecure-data.org/dark-net-markets.html

[9] Fahmida Rashid, (May, 2017) The Target Data Breach Settlement sets a Low Bar for Industry Standards. Available: https://www.csoonline.com/article/3199064/security/the-target-data-breach-settlement-sets-a-low-bar-for-industry-security-standards.html

[10] Attorney General of the State of New York Bureau of Internet and Technology: Target Corporation Settlement Available: https://ag.ny.gov/sites/default/files/nyag_target_settlement.pdf

[11] Xiaokui Shu, Ke Tian*, Andrew Ciambrone and Daphne Yao, (Jan, 2017), Breaking the Target: An Analysis of Target Data Breach and Lessons Learned, Available: https://arxiv.org/pdf/1701.04940.pdf

[12] Forrester Research, "Developing a framework to improve critical infrastructure cybersecurity," NIST, April 2013, in Response to: RFI# 130208119-3119-01. https://www.nist.gov/sites/default/files/documents/2017/06/01/040513_cgi.pdf

[13] "Target appoints new chief information officer, outlines updates on security enhancements," April 2014. Available: https://corporate.target.com/press/releases/2014/04/target-appoints-new-chief-information-officer-outl

[14] M. Riley, B. Elgin, D. Lawrence, and C. Matlack, "Missed alarms and 40 million stolen credit card numbers: How Target blew it," March 2014. Available: https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data

[15] J. Finkle and S. Heavey, "Target says it declined to act on early alert of cyber breach," March 2014. Available: https://www.reuters.com/article/us-target-breach/target-says-it-declined-to-act-on-early-alert-of-cyber-breach-idUSBREA2C14F20140313

[16] Allessandro Acquisti , Curtis Taylor and Liad Wagman ,The Economics of Privacy , DRAFT Conditionally accepted at the Journal of Economic Literature, Available: https://www.law.berkeley.edu/wp-content/uploads/2015/11/The-Economics-of-Privacy.pdf

[17] Erin Hitchcock, Datameer Blog Post on "Five Big Data use Cases for Retail", Available: https://www.datameer.com/blog/five-big-data-use-cases-retail/

[18] Keith Johnson , Forbes CommunityVoice, " What Is Consumer Data Privacy, And Where Is It Headed?, Available: https://www.forbes.com/sites/forbestechcouncil/2018/07/09/what-is-consumer-data-privacy-and-where-is-it-headed/#538cb51d1bc1

[19] Wibson , "How Much Is Your Data Worth? At Least $240 per year. Likely much more", Available: https://medium.com/wibson/how-much-is-your-data-worth-at-least-240-per-year-likely-much-more-984e250c2ffa

[20] Target 4th Quarter Earnings Report (Feb 2014), Available: https://corporate.target.com/press/releases/2014/02/target-reports-fourth-quarter-and-full-year-2013-e

[21] Krebs on Security, "Target Breach by the numbers (2014)", Available: https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

[22] 2014 Target Annual report, Available: https://corporate.target.com/_media/TargetCorp/annualreports/2014/pdf/Target-2014-Annual-Report.pdf?ext=.pdf

[23] Assion Folivi, (2016), *Don't Be the Next Target,* Available: https://www.amazon.com/Dont-Next-Target-Diligence-Negligence-ebook/dp/B01LWY7A2F/ref=sr_1_1_sspa?ie=UTF8&qid=1538256903&sr=8-1-spons&keywords=don%27t+be+the+next+target&psc=1

[24] Josephine Wolf (2018), *Why It's So Hard to Punish Companies for Data Breaches*, Available: https://www.nytimes.com/2018/10/16/opinion/facebook-data-breach-regulation.html