Assignment Cover Sheet



* The information on this coversheet will be included in Turnitin’s similarity analysis; however, your lecturers are aware of this and will disregard it.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Student Details | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Student Number | 1 | 0 | 4 | 9 | 8 | 7 | 4 | | 3 |  | |
|  | | | | | | | | | | | |
| Family Name | David Selvam | | | | | | | Given Name | | | Visahl Samson |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| UnitDetails | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Unit Code | CSI2102 | | | Unit Title | | Information Security | | | | | |
| Name of Lecturer | | | Dr Liau Vui Kieu | | | | Due Date | | | 24 June 2019 | |
| Topic of Assignment | | | A analysis of Target Data breach and lessons learned | | Groupor Tutorial(if applicable) | | |  | | | |
| Course | | Bachelors of Science in Cyber Security (FT) | | | | | | | Campus | | Singapore |
| I certify that the attached assignment is my own work and that any material drawn from other sources has been acknowledged. This work has not previously been submitted for assessment in any other unit or course.  Copyright in assignments remains my property .I grant permission to the University to make copies of assignments for assessment, review and/or record keeping purposes. I note that the University reserves the right to check my assignment for plagiarism .Should there production of all or part of an assignment be required by the University for any purpose other than those mentioned above, appropriate authorisation will be sought from me on the relevant form. | | | | | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ManualSubmission | | | | |
| If handing in an assignment in a paper or other physical form,sign here to indicate that you have read this form, filled it in completely and that you certify as above. | | | | |
| Signature |  | Date |  | ***Office Use Only*** |
| ElectronicSubmission | | | |
| **OR,**if submitting this paper electronically as per instructions for the unit, place an ‘X’ in the box below to indicate that you have read this form and filled it in completely and that you certify as above. Please include this page with your submission. Any responses to this submission will be sent to your ECU email address. | | | |
| Agreement | X☐select checkbox | Date | 23 June 2019 |
| For procedures and penalties on late assignments please refer to the [University Admission, Enrolment and Academic Progress](http://intranet.ecu.edu.au/__data/assets/pdf_file/0005/378320/Admission-Enrolment-and-Academic-Rules.pdf)  [Rules](http://intranet.ecu.edu.au/__data/assets/pdf_file/0005/378320/Admission-Enrolment-and-Academic-Rules.pdf)- rule 24, and the ECU Course and Unit Delivery and Assessment Policy | | | | |

Contents

[Assignment Cover Sheet 1](file:///D:\PSB\SEMESTER%201\IS\Davidselvam_Visahlsamson_10498743_CSI2102_Assignment_1.docx#_Toc12213184)

[Introduction 3](#_Toc12213185)

[Data breach background 3](#_Toc12213186)

[How it happened 3](#_Toc12213187)

[Mind Map 4](#_Toc12213188)

[CIA 5](#_Toc12213189)

[Protections 6](#_Toc12213190)

[In place 6](#_Toc12213191)

[Failed 6](#_Toc12213192)

[Respond from Target Corporation 7](#_Toc12213193)

[Legal and Ethical consequences 7](#_Toc12213194)

[Conclusion 8](#_Toc12213195)

[References 8](#_Toc12213196)

# Introduction

In this digital era information plays a vital role everywhere. Starts from small sized organisation to enterprise organisation everything relied on this information. This report contains the following, firstly the background which explains how the data breach took place. Then the report explains the threats have been faced in this breach. After it explains the CIA principles related it in this particular breach and it explains the protections were there and reason for failures. Then this report continues to the ethical and legal issues in this and ends with conclusion.

# Data breach background

Target Corporation is a well ranked store retailer in United States. The company operates almost 1844 stores all over the globe. The given case study explains about the data breach happened at Target Corporation in 2013. During this data breach over 70 million individual user details such as mailing addresses, names, email address, phone numbers, and credit and debit card account data were stolen. This data breach resulted in second largest credit card detail theft in United States. Credit card information includes Encrypted pins, Customer names, Credit card numbers, Credit card expiration date, embedded code on credit cards magnetic strip. This entire breach is a result of human error and failure of educating basic security practices required.

# How it happened

The beginning of this data breach starts with Phishing attack. In Phishing attack the intruder/hacker will send a fake email/message which looks like from an official source. The main motive of this phishing attack is to steal sensitive data from the user (Security, n.d.). By using this same method the intruders/hackers targeted a third party air-conditioning firm vendor Fazio Mechanical Services. Due to poor security practices this third party vendor fell in this phishing attack and certainly installed the malware called Citadel which is a password stealing bot program. Using this malware the intruders/hackers gained access to Target Cooperation’s network.

Once, they gained access to the network they exploited poor segmentation of target cooperation’s network which had no separate segmented network for the sensitive information. This poor network management made the work easy. Once they exploited this vulnerability they have installed another PoS (Point of Service) malware called BlackPOS. By using this malware intruders/hackers were able to take the information whenever customers use their credit card in the POS. After collecting the data it was stored in .dll file and stored in a temporary NetBIOS and shared over ports 139, 443 or 80. Reports indicate that almost 11GB of data had stolen and posted for sale in dark market (Dark web) ("Case Study — Target Security BREACH - Cruisecoders - Medium", 2017)

This entire breach could have been avoided if the organization would have educated its employees about basic security practices. If the target corporation would have segmented its separate network to VLAN to store the sensitive information this data breach could have been avoided. Also, ignored the warnings given by security software is a biggest mistake committed by the employees.

# Mind Map

# 

Screenshot Information threats faced by Target Corporation

Firstly, as mentioned in the case study the beginning of this data breach is human errors here includes Phishing attack which occurred due to inefficient security and malware Citadel had been installed, inefficient network configurations, ignored the warnings given by Target’s FireEye monitoring system. These are very basic things that an organization should educate its employees failure results in data breach.

Secondly, the software attacks. In this scenario the POS malware BlackPOS installed on the POS machines. Though FireEye provides warning to the Target corporation it doesn’t provide clear information such as malware name, type, so, the Target cooperation ignored the warnings.

After these 3 threats now the Targets Corporation’s customer data faces other threat which is Espionage/ Trespass which is unauthorised collection of Target Corporation’s customer data. Then other major threats theft and information extortion comes along. Theft includes stealing of customer data and Information extortion includes information disclosure of about 70 million customer details.

So, these are the information threats faced by Target Corporation during the data breach in 2013.

# CIA

CIA stands for Confidentiality, Integrity and Availability. It’s a model used to evaluate the information security. Failure/attacks on CIA lead to data breaches.

Here in Target Corporation’s data breach though the end result is theft of customer data which comes under confidentiality breach but the root cause comes from integrity breach. (Ruubel, 2014)

Basically, using malwares, viruses in data breaches are comes under integrity attack. Here in Target data breach the hacker/intruders used malware which caused the data breach so, here the attack is on integrity model. The installed malware has compromised the integrity of the system. Once it affected the integrity it directly affects the confidentiality.

Here the confidentiality breach followed by integrity compromise resulted in theft of 70 million user data and making the data breach as 2nd largest credit card data breach in United States.

# Protections

## In place

* Target Corporation had several layers of security measures which includes FireEye. FireEye which is a well-known network security system offer all the levels of security required to protect the network ("FireEye Security Bundle for Mid-Market Enterprises | FireEye", n.d.). The main feature of this FireEye is it can automatically detect the threat and remove it without requiring manual help.
* Also, Target Corporation had Symantec antivirus for endpoint protection which is a well-known security software used by all over the world.

## Failed

Though Target Corporation had several security measures this data breach happened. The main reasons for the data breach listed here,

* Firstly, from the beginning the human error played a significant role in this data breach. Here the warnings given by Fireeye and Symantec tools were ignored (Chiacu, 2014). Also the automatic function of deleting the malware by off fireeye was disabled. So if the security team would have checked on the warnings it would have been helped. Also effective security audits should be conducted to ensure the security.
* Secondly, Target provided their network access to a third party. Since the third party have no required security practices they trapped by phishing attack. So poor security practices are main reason. In this case the organization should ensure the company which going to handle their services have enough knowledge in security practices.
* Thirdly, Target Corporation failed to segment their network and kept everything under one same network. So, it made easy to the intruders/hackers to take control of customer information. If Target Corporation would have segment their network to store sensitive information the data breach would haven’t happened (Chiacu, 2014). I would recommend using VLAN segmentation since, it’s a better way to keep the network secure.
* Fourthly, less secured POS machines which allowed the installation of Malware to steal the data. This is another major reason if the POS machine software would been secured it this breach would have been prevented

# Respond from Target Corporation

As a response, Target Corporation announced that it deleted all the malware from its computers. Also it updated its security policies and arrangements. They are follows, (Corporate, 2014)

* Enhancing the monitoring and logging
* A new application that white lists the POS systems.
* An Effective network segmentation to keep the sensitive information safe.
* Limited and effective vendor access to its network with effective auditing.
* Enhanced security for customer accounts to keep their information safe.

These updates clearly show that Target Corporation is learned the importance of security after the data breach. Also, all these updates check the vulnerable parts that the hacker/intruder used in data breach. So, if these updates would have been implemented before itself the data breach would have been avoided.

# Legal and Ethical consequences

In legal side almost 90 lawsuits were filed and expected to pay 3.6 Billion USD as compensation to the affected customers. Also, following this incident Target’s CEO Gregg resigned his job and the company created a new security position which is Chief Information Officer. (Abrams, 2017)

In market wise, Target Corporation’s profit falls 46%. The reasons include the settlement to the customers affected in the data breach, card reissuance costs and additional legal expenses. (McGrath, 2014)

Following the data breach Target announced that its going to invest US$5 million in cyber security education for stakeholders. Furthermore Target did offer a free year of service making sure customer’s credit hadn’t been affected and some kind of ID theft protection. (Gallagher, 2015)

Here in Target data breach the remedies taken by the target corporation are appreciated. Also, the decision of investment in cyber security education is should be viewed as good choice. Because by seeing this response other organizations will come forward to do the same in their organizations.

# Conclusion

In this particular case a simple phishing attack caused all the issues. Also, it’s clearly shows that basic information security practices are crucial. These practices can be followed by providing basic trainings and educating. Also, Target’s data breach shows the importance of effective information security practices required. The decisions/actions by target network corporation after the data breach shows their statics to overcome from this issue.

# References

Security, E. What Is a Phishing Attack? Definition and Types. Retrieved from <https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html>

Case Study — Target Security BREACH - Cruisecoders - Medium. (2017). Retrieved from <https://medium.com/@hypatiaacademy/case-study-target-security-breach-3803d2182c91>

Ruubel, M. (2014). Target: A Confidentiality or Integrity Breach ? — Guardtime. Retrieved from <https://guardtime.com/blog/target-a-confidentiality-or-integrity-breach>

FireEye Security Bundle for Mid-Market Enterprises | FireEye. Retrieved from <https://www.fireeye.com/solutions/security-suite.html>

Chiacu, D. (2014). Target missed many warning signs leading to breach: U.S. Senate report. Retrieved from <https://www.reuters.com/article/us-target-breach-senate/target-missed-many-warning-signs-leading-to-breach-u-s-senate-report-idUSBREA2O1VA20140325>

Corporate, T. (2014). updates on Target’s security and technology enhancements. Retrieved from <https://corporate.target.com/article/2014/04/updates-on-target-s-security-and-technology-enhanc>

Abrams, R. (2017). Target to Pay $18.5 Million to 47 States in Security Breach Settlement. Retrieved from <https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html>

McGrath, M. (2014). Target Profit Falls 46% On Credit Card Breach And The Hits Could Keep On Coming. Retrieved from <https://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/#172b2ce47326>

Gallagher, C. (2015). Target Data Breach. Retrieved from <https://www.chuckgallagher.com/2015/03/21/target-data-breach-ethically-where-from-here/>

Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the Target: An Analysis of Target Data Breach and Lessons Learned. IEEE, 1-10 <https://arxiv.org/pdf/1701.04940>