Homework: 1
Name: Anusha Balasubramanian
Email: ab19533n@pace.edu

Paper: Cyber Attacks on U.S. Companies in 2014 - *Riley Walters (pdf)*

Case 1:Target (retail) :

In January, Target announced an additional 70 million individuals' contact information was taken during the December 2013 breach, in which 40 million customer's credit and debit card information was stolen**.**

As per the analysis , the hackers have stolen 70 million of contact informations and out of which 40 million customers credit and debit card information was also stolen. Based on the information given and along with few research this cyber attack falls under **high level impact of loss of confidentiality.**

Firstly, the reason for this attack to fall under confidentiality category is; contact, credit and debit card information are **private and sensitive informations** that has values which needs to be protected from disclosure to unauthorized parties.

Secondly, hackers could use customer names, credit or debit card numbers, expiration dates and CVVs datas to make **card replicas** and can either withdraw money from ATM or use it for any other purchases. Few reports have been made by customers regarding unauthorized access to their account.

Also gaining access to contact informations gives hacker a way to get the customers phone number, email, address and zipcode details which is again a sensitive/private information.With phone numbers hacker can track the location and snoop on to phone calls and texts . When email id is compromised, the hacker can perform **"email account takeover"**, **"targeted phishing attack"** by posing as one of a businesses you deal with and try to steal even more information from you.

Finally the zip code ,is tied up with lots of credit card account, stealing both the informations helps hacker to perform credit card transactions from your account.
Thus considering the above mentioned facts i strongly feel that the Target(retail) cyber attack was high impact loss of confidentiality.

Case 2: Feedly (communications)

Feedly's 15 million users were temporarily affected by three distributed denial-of-service attacks.

As per the analysis this cyber attack seems to be a **low level impact of loss of availability** as the feedly website was under DDoS(Distributed Denial of Service) attack and was unavailable to the users till the time it was recovered.

Though the website was under attack, it is stated that none of the customer informations was stolen and hence there was **no loss of confidentiality.** Also it is considered to be low impact because , the unavailability of website didn't harm any customers as Feedly is a news aggregator application for various web browsers and mobile devices , and hence people had alternate options to read news feeds.

It was also stated in a blog that "the attacker is trying to extort us money to make it stop, and ,We refused to give in,". The feebly along with making changes to its infrastructure also teamed up with network providers to bring the service back.

Thus considering the above mentioned facts i strongly feel that this cyber attack was a low level of the loss of availability as it didn't cause any catastrophic harm or financial loss to customer nor to the organization.