INFORMATION SECURITY

TARGET SECURITY BREACH DISCUSSION

BY: RAJDEEP SENGUPTA

SRN: PES1201800144

SECTION: C

Ques 1. What's your diagnosis of the breach at Target—was Target particularly vulnerable or simply unlucky?

Ans 1. According to me as a security analyst, I would state that all of this tragedy happened due to ignorance of the security team at Target. They should have fixed the bugs and loopholes immediately as the alerts came. The security team was ignorant about the repeated alerts by their own systems. This cost them a huge data leak and hence they lost millions of dollars during Thanksgiving and Christmas which also cost their reputation in the market.

Ques 2. What, if anything, might Target have done better to avoid being breached? What technical or organizational constraints might have prevented them from taking such actions?

Ans 2. Target security team should have taken the alerts seriously. This is the foremost job of the security team to analyse the alerts reported by their systems in the first place. There are many things that they should have done such as:

- **Appointed a Chief of Security with proper training to handle situations and to whom all these alerts were to be reported since the CEO cannot focus on every single thing**
- **Improved firewall rules**
- **Implemented POS management tool**
- **Improved logging and monitoring systems**
- **Hired a better and huge security team who can handle any situation at least during peak times like Thanksgiving, Christmas etc.**
- **Trained individuals in the security team**
- **Password rotation**
- **Two factor authentication**

Ques 3. What's your assessment of Target's post-breach response? What did Target do well? What did they do poorly?

Ans 3. In response to the breach, the way Target took some decisive actions which had both positives and negatives.

The positives:

- **Announced 10% discount before the Christmas**
- **Offered free credit monitoring for one year for affected users**
- **Post-analysis of their security systems**
- **Training of employees**
- **Announced that it will spend $100 million for advanced security**

The negatives:

- **The communication system in their company was poor(messages going from employees to CEO was very late)**
- **Spreading false news and providing false hope to their customers**

Ques 4. To what extent is Target's board of directors accountable for the breach and its consequences? As a member of the Target board, what would you do in the wake of the breach? What changes would you advocate?

Ans 4. The board of directors and CEO are the ones who take full responsibility for their company. At the end of the day, all the blame goes to them.

According to me, I strongly believe that the board of directors and the CEO are responsible even though not directly. I agree that the board of directors cannot attend to day-to-day faults and errors but they can hire someone as their Chief of Security who can do the same. Instead, they hired some inactive and ignorant staff as their security team who don't have the knowledge of categorizing situations as serious.

Ques 5. What lessons can you draw from this case for prevention and response to cyber breaches?

Ans 5. The basic lessons that this incident teaches everyone is to never ignore anything important. As the saying goes “Leave no stone unturned”, it means that we should never ignore any warning/alert. Also, when someone like a CEO should hire a good team with good management skills and proper training. Also, there should be a hierarchy in the company so that proper importance can be given to each issue.

Ques 6. How would you characterize your role as a director in relation to cybersecurity at your organization? What are some concrete things that you can do as a director to oversee this domain?

Ans 6. My role as a director, I would maintain a hierarchy in the company. I would hire a smart Chief of Security who would take care of the security team and I would take a daily update from the Chief of Security. Also, I would increase the standards in the hiring process for employees. Another solution to this would be hiring another company and giving them the responsibility of securing the database servers. In this case, the security company will be responsible for detecting vulnerabilities and bugs.

Ques 7. What do you think companies can do better today to protect themselves from cyber breaches and in their post-breach response?

Ans 7. Nowadays there are cybersecurity firms who specialize in securing big companies. They are under contract with these companies. In this case, the cybersecurity firms function with maximum security.