Information Security: Target Cyber Breach

Name: Chandan N Bhat

PES1201701593

Section H

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

I strongly feel that Target was vulnerable in various aspects of security and is not just the case of being unlucky. But Target was unlucky in the fact that not all companies with vulnerabilities are victims of cyber-attacks.

- Firstly, information about Target's vendors was publicly available online.
- Target did not monitor the vendors security arrangements too. Faizo Mechanical Services, Targets external heating and ventilation provider's employee was using a free version software product to detect malware.
- Surprisingly, it is evident that target's security team identified several vulnerabilities in the firm's payment card systems and cash registers, but no follow up were undertaking regarding this issue which indicates overseeing on crucial aspects by Target.
- Another issue with Target is the absence of two-factor authentication to prevent intrusion. According to an analyst, Target has paid very little attention to vendors like Faizo, even without basic security assessment by Target.

Moreover, Target's network wasn't properly segmented and it had a route between a network from outside contractor and network payment data which was exploited by the attackers. Due to the poor network design, attackers could move within the network and also update the malware, as reports show that initially there were 3 variants of the malware which was further updated before the next wave of attack.

We observe that target initially ignored security warnings of malware intrusions assuming it to be a false positive. Even the further warning by FireEye was ignored by Target. Most surprising thing is that Target had turned off the feature that automatically deleted malware once detected.

Thus, a lot of issues, vulnerabilities and warnings were carelessly overseen and ignored by Target. We also need to consider that Target was unlucky too, as it is the first big hack.

Overall, Target was slightly UNLUCKY, moderately VULNERABLE and highly NEGLIGENT.

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?

Throughout this case we observer various situations were Target was careless about aspects of security of the organisation and its vendors. It also had a poor network design which was a major vulnerability.

According to me, few things that Target had to focus to prevent the breach are:

- A thorough security assessment on its vendor was necessary.
- Few vulnerabilities detected in payment card systems and card registers shouldn't have been ignored or emphasised.
- A proper network design preventing various vulnerabilities.
- Considering warnings from FireEye rather considering it a false positive as the consequence of it will be hard.
- The automatic malware detection and deletion feature was disabled. This could have prevented the breach if enabled but this isn't uncommon.

Some organisational and technical constraints could be:

- We observed that the automation tool to remove malware if detected was disabled. This could be because an organisation may not want a tool to achieve it instead have a person to make the decision rather the machine.
- There were many vulnerabilities and issues overseen which could have been due to certain organisational constraints in Target's work culture/environment.
- There could be failure in taking adequate controls in Target.
- With the upcoming busy season of thanksgiving and black Friday weekend, Target might have less prioritized the issues.
- Target being a large organisation with multiple chains throughout the world, and the huge volume of warnings, there could be a possibility that the cybersecurity team were constrained to address only few issues.

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

I feel Target's post-breach response was average, with few quick actions as well as few unclear actions.

- After discovering the breach few quick actions were taken. Targets executives got in contact with DOJ and Secret Service and also hired third-party forensics to investigate the breach.
- Target also started removing the malware from its systems gradually.
- Keeping in mind the Shopping Season, it managed to keep the stores up and execute the process without disruption in operations.
- It also managed preparing stores and call centres to answer customer's questions and the wait times were improved over months.
- Authorities and institutions were alerted about the unauthorised access.
- Target offered free credit and theft monitoring for affected customers for a year and reassured them that they would not be held liable for any fraudulent charges resulted from the breach.

But there were few things which were delayed and unclear

- Target took 1 week to announce the cyber breach that occurred. And the information propagated was minimal.
- Also the first public information about the breach reached the public through a blog and not Target which could impact the trust on the company and its reputation.
- Poor service when customers tried to gather more information about the breach and how they are affected by it.
- The means of communication about the breach was through its corporate website which wasn't frequently visited by customer and also was not easily navigable.
- Customers felt ill-equipped as few instruction from the CEO were ambiguous and unclear. Thus the customer sentiment towards this issue was against Target.

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?

With such an intense and huge data breach of 70 million customer's Personal information, Debit and Credit card the responsibility is more inclined towards the board of directors. It is evident that the board of directors are accountable for the data breach and also its consequences. The consequences include drop of stock price, fall in sales, trust on the brand and huge drop in the company reputation.

- The prime concern for the board of directors is obviously to safeguard personal information and more importantly their financial information if any.
- Moreover, it is the responsibility of the f=directors to inform the stakeholders, especially the customers had to be informed about the breach immediately which didn't happen in case of Target.
- Also the analysis of the situation by Target and the Board of directors was very clear. In addition to the delay in information told to customers, the information propagated was also unclear. First they claimed that sensitive information, PIN etc were not compromised. But about a week later they announced that sensitive info was also compromised. This made the situation worse as people would have reacted accordingly if mentioned clearly earlier. Also it was too late for many customers to regain access to their accounts and money.
- Also the board of directors failed to manage the post breach situation as lot of customers had issues in reaching out to customer care etc to understand the situation.

But we cannot make the board of directors completely responsible and accountable as various important warnings and vulnerabilities were ignored, overseen by the technical and cybersecurity team of target and they are also accountable for the cause.

Assuming myself in that situation, my priority first would have been towards the customers rather than escaping from the criticism on company or propagating that the scope of the attack was not so huge and not any sensitive info had been compromised.

- I would first make the entire situation very clear so that customers do not panic. Call centre management would be improved to ensure unambiguity.
- The current findings about the case and the possibilities that could happen would also be made clear so that customers were monitoring the activities much carefully which would have reduced the damage.
- Warnings and vulnerabilities wouldn't have been ignored carelessly and would be prioritized higher as even the most updated and latest technology isn't of use with poor management.

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

Target case study is a great example to realise three main aspects which could shatter a Business.

- Manageability
- Negligence (of warnings and risks)
- Technology and Network Design
- Treat Response
- Response to customers after the attack

1. Firstly, Negligence towards the indicated risks and warnings on vulnerabilities should never bee overseen. The negative consequence of it is drastic than the positive side when the company is lucky and attack doesn't happen. We have many instances where warnings were directly ignored and never iterated in spite of the risk involved.

2. In times of crisis and having your customers at risk, it is better to think about their well-being and their perceptions on how you are handling things, rather than trying to save the company. If not, we will lose their business, which in turn puts you out of business.

3. Upgrading risk analysis and technology to meet changing threats. Keeping the technology, especially security up to date is very essential. Having a segmented network design and certain principles such as Defence-in-depth, separating payment network from the company network etc.

4. Operationalize your incident risk assessment and breach response processes and understand how quickly an attack can spread through a system if delayed to be noticed.

5. Protect the organization's reputation with quick and accurate assessment.

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?

- Board of directors should have considerable access to cybersecurity expertise and cyber risk management should be given regular checks. Discussions on the same during the meetings can elevate the awareness among them. More awareness implies less chances of falling for the attacks.

- More focus must be provided towards identification of risks, mitigation and plans to approach them. Managing cyber security risk requires an understanding of the significance of the assets to estimate their exposure to risks.

- Directors should understand the legal and regulatory implications of cyber risks as they relate to their company's specific circumstances. With responsibility comes accountability. Executive management and board members are being held accountable for many high-profile breaches, and in many cases losing their positions.

- Directors must understand cybersecurity as enterprise risk management issue. Even though most of the reporting structures come up through the IT department, it can't be the central focus because the impacts are organization-wide. The skill-sets needed to manage the risks and deal with issues are organization-wide.

- Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.

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

Target case can be used as a very good example for various companies to ensure that they are safe from breaches and how to react to one if occurred.

1. Third party vendors must comply with security guidelines. Companies rely on various 3rd party vendors for services. Security assessments on vendors is also essential.
2. Ensure that employee of the organisation follow the security guidelines and make them aware of security attacks such as phishing etc.
3. Update software, technology products, security policies etc regularly. Have a segmented network design to ensure that hackers can't easily access important sections of the network.
4. Along with technological advancements, ensure that the organizations management is not careless and negligible, especially in terms of security.
5. Develop a cyber-breach response plan. Ensure accurate breach assessment and updated risk assessment and analysis.

6. Reassure the customers. In critical situations like these ensure that the customers and stakeholders are clearly communicated with situation and possibilities of future risks. Having a point person for response would improve the situation.
7. Never prioritize the companies reputation and escaping the criticism than the customers which might eventually lead to lose the Business.

THANK YOU

References:

https://drive.google.com/file/d/1bidY_1zsDkBbWSy3mgg39deIqDhcUgQ_/view?ts=5f5cd27f

https://drive.google.com/file/d/165Xzn3EMA_-2B_JInrlcW4COqPxFVnZC/view

https://hbr.org/2014/03/could-target-have-prevented-its-security-breach

https://medium.com/@cruisecoders./case-study-target-security-breach-3803d2182c91

https://www.idexpertscorp.com/knowledge-center/single/six-lessons-we-can-learn-from-the-target-data-breach

https://www.techsupportofmn.com/6-ways-to-prevent-cybersecurity-breaches