TARGET CYBER BREACH

ASSIGNMENT - 1

Atmik Ajoy
PES1201800189

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

Target was definitely vulnerable and not just "unlucky". There are several facts and accounts to prove so. In short we can summarize the breach at target as just gross negligence and incorrect set up of network architecture. The following points below illustrate how target's cyber breach was clearly a consequence of their vulnerability:

- The far more secure and superious PCI standard being the 2-factor authentication was not enforced by target,which can only mean that for fazio as the industry analyst said in page2, they did not pay any attention nor did they consider that as a viable outlet for information leaks.
- Roping in the fact that Target's network infrastructure somehow allowed a hack in Fazio's system to access the payment data network is crazy in and of itself. While building the network infrastructure, being one of the biggest companies in the US at the time, Target should have taken more care to segment their network architecture correctly and make the payment data of customers inaccessible from any outside network like fazio's.
- Additionally, not only was the network infrastructure a joke, but fazio's security was also an even bigger joke! Considering that Fazio was associated with target as a ventilation provider, has access to target's mainframe network and even target data, the fact that they were using abysmal cybersecurity measures should have been a major redflag to target and should have done something about it.
- These gross negligence in security measures are not permissible as the target did have a chief information officer who should have overseen these details while they were being set up itself.
- This can further be seen reflected in targets negligence towards several warnings from the security firm based in bangalore (FireEye Inc) and targets own internal team. FireEye sent over 3 alerts to target signalling that there was something wrong going on with customer's payment data but targets internal team brushed it off without considering it seriously.
- Target had also turned off the function to automatically delete malware clearly indicating that they (the internal team) just did not pay attention/heed to any of the alerts and even indicating that the set up of targets whole cybersecurity system must have been in haste and not thought out properly.

For these reasons mentioned above, I believe that the breach at target was because target was highly vulnerable and not just because they were "unlucky"

Question 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?

Target could have done ONE simple act that would have prevented the breach and it wouldn't have even required human interaction. They could have just enabled the function that deletes malware. That way the hackers would not have been able to plant “citadel” and this whole fiasco could have been prevented.

In addition to the above act, they could have also paid more heed/importance to the alers coming on from the FIreEye team in india, that way they could have deleted the malware sooner. A constraint here though would have been that since it was november/december time which is their highest selling quarter, they would have been very busy and flooded with black friday, christmas stuff to prepare for and these alerts would have gotten lost in that fervour(not correct but reality).

They should have also implemented the new PCI standard with 2 factor authentication which could have also prevented the attack, along with segmenting their network neatly to prevent this sort of breach and lastly they should have had extensive security checks with the vendors they work with and made sure the vendors they work do not have abysmal security measures.

Question 3: What’s your assessment of Target’s post-breach response? What did Target do well? What did they do poorly?

Target discovered the breach quite late (18 days after it happened) and major damage was already done. It might have been salvageable but target's response to the situation sealed their fate in terms of being an overall poor response.

- Their first blunder occured with how they decided to break the news to the public. Not only was the news first published on Kreb’s for security blog but they decided to put it on their corporate website which is not even frequented by customers, making it difficult for customers to navigate. This faced huge backlash as customers found it very hard to find information about the breach since it was all the way over at their corporate website. This coupled with the fact that the news broke out from a blog did not go over well with consumers who had initially trusted Target.
- The second blunder so to say was that customers had to wait for hours to talk to customer care representatives about what was happening, and this made consumers even more angry. Consumers didn’t know what was even going on and they couldn't even access their target accounts to figure out what happened. This left consumers completely vulnerable themselves and scared as their privacy was completely breached, and voicing these concerns to the company was getting more and more difficult due to the waiting times.
- Thirdly, the blog Krebs on security found out that valuable information regarding credit cards and debit cards were being sold on the black market, and that there were fraudulent transactions being recorded in the same names. Yet, the consumers who owned these cards were not given any intimation that this may even happen and nothing was conveyed to them at al
- The overall “vibe” of target's response was dubbed , “disheartening” by consumers who had put their trust into target and were being betrayed like this with no information being properly relayed back to them.

But target also got some things right,

- They got the waiting time on customer care down to a max of 8 seconds which is commendable especially given the amount of calls they would be getting at a time like that
- The CEO was seen publicly giving out information and apologising multiple times which to some was seen as a good sign and hand holding gesture.

Question 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?

Target's board is completely accountable for the breach and its consequences. Even if it is a mistake committed by a third party employee, at the end of the day they need to know what's going on in the company, the daily operations, its vulnerabilities. And rightfully so there were fingers being pointed at the board and questions being raised questioning the board , especially the CEO and how he did not know about this at all, and more so on how it took them 18 days to even notice the breach. Mainly the CFO and the CIO were the main people along with the CEO who were held accountable as the CIO and CFO were in charge of information security and should have made sure an attack like this shouldn't have been possible in the first place. They are liable to the extent of lawsuits being filed against them for failing to perform their duties effectively and expecting resignations from all of them. The idea here is not that "since it has happened once it will not happen again" but rather that if something unexpected like this were to happen again, these individuals would not be equipped to deal with it. Creating a foolproof system is something they failed to do and not only that, they also failed to respond effectively and even notice the breach fast enough. It is quite clear that they do not have enough control over what is happening in the company in their respective domains hence all the public outrage/lawsuits/resignations is expected, and rightfully so.

If i was a member of the target board, first thing as CIO would be to regularly check alerts coming in regarding security of the system. The moment fireEYE sent an alert, it would be handled. No alert would be lost in translation/ in the haystack. Additionally regular updates regarding company working, the network infrastructure would be done and finding an ideal moment to zhuzh up the network infrastructure to segment it would be ideal. In the wake of the breach, giving out as much information as we can, holding the customers hand through this scary process of having their private information leaked to the unknown and understanding the breach of trust with the consumer would be a top priority. Being completely transparent and trying our best to get as many benefits as we can to retain as many customers as we can, revamp the security system and give consumers updates on such would be a major step to be taken if I was in that place.

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

The salient points we can take away from this cyber breach for prevention would be:

- While designing network infrastructure, it must be highly segmented and separated efficiently so as to prevent unregulated access throughout the network
- ALWAYS implement 2-factor authentication (PCI standard 2.0)
- As a large company with millions of customers dependent on you and giving their information to you, make sure all the vendors you work with have adequate security measures implemented and verify their credentials before access to certain information (for example, a

person from fazio should not have the power to access payment data of customers as ventilation system is not remotely related to that)
- Pay heed to cybersecurity alerts in specific as they can be quite detrimental if left unattended.

In terms of response:

- As outlined in the previous answer about “What i would do as a member of the board of directors” , we can learn that being transparent is the best way to go as it gives the customer a better picture of what's really going on and lets them at least deal with vulnerabilities caused by the companies screw up
- Having customer care lines set up with very low waiting time is very helpful to customers
- Giving customer benefits in light of the breach would be a good way to sort of patch things up , or at least an attempt to
- Majorly, the target response regarding the directors is something to take away from that is, we shouldn't run away from taking responsibility like the directors did based on what the lawyers defended in court.

At the end of the day, its all about the customers and what we can do for their best experience.

Question 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?

The role of a director in relation to cybersecurity is a complex role which requires the following traits:

- The ability to understand that security is an enterprise-wide risk management issue and not just an IT issue
- The ability to understand the legal and regulatory implications of cyber risks and how their company is going to get affected by these risks if they happen
- Cyber security MUST be a regular item on the agenda for a board meeting and must be given adequate time to be discussed on. They must also bring in experts to discuss how to make it better
- They should have constant discussions on identifying what risks to avoid.accept,transfer through insurance and what each approach entails and its consequences
- Constantly review the cybersecurity policies that are in place at the company and try to make them better constantly
- Educate the staff on how to be more vigilant and prevent such attacks from happening (like not to click on malicious links through email phishing attacks)

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

Companies can::

- Segment their network efficiently to prevent this sort of unauthorised access to happen again.
- Be more vigilant with the vendors they deal with
- Conduct employee security awareness training
- Update their software regularly
- Introduce a business continuity plan with cybersecurity integration

- Have a clearly defined CIO role which would include the responsibilities mentioned above in question6

In terms of response :

- They would first have to survey the damage to see how many people were affected, how were they effected, the scale of the attack
- Next would be to limit the additional damage by reducing the attack from spreading like rerouting network traffic, blocking traffic and isolating parts of network with very sensitive data
- They would then have to get details of the attack like the affected systems, the compromised data, the data/network affected by the attach and the amount of damage done
- Once the gather those details is when they can go to law enforcement agencies to take action
- Notify the customers affected and give them very regular updates as to what is happening and why it happened, how to combat it , and most importantly Reassure the customer as they are the most valuable asset to the company.
- And then last but not the least learn from the breach