# PES UNIVERSITY
# INFORMATION SECURITY ASSIGNMENT

*Aayush Kapoor PES2201800211*

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

Target was vulnerable as the main reason for the same :

- Ignorance of critical security alerts monitored by security specialist from FireEye
- The network architecture of Target had improper segmentation as they did not isolate the sensitive part of it from the easily accessible network sections.
- Target's point of sale was insecure by allowing unauthorized software installation and configuration and hence the use of POS attack by the attackers.
- Target's security team had turned off the automatic deletion of malware.

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?**

Yes, Target could have done better to avoid the breach. The following constraints might have prevented the breach :

- Multi-Factor authentication
- System integrity - such that only trusted software can be installed or executed on Point of Sale devices hence preventing POS attack.
- Adaptive security alerts that elevate the strength of warnings as the number of days passes by.
- Target could have built a better network architecture like Zero trust network as it not only protects from exterior attacks but also the insider attacks.
- Never turn off automatic deletion of malware functions.

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

The steps that Target took that did well were:

- Surveying the damage by hiring a third party forensic team and limiting the damage as they removed malware as soon as they could.

The steps Target took were poor:

- Notification on corporate the website instead of the most frequented customer website as the customers could have taken their own precaution to face the breach and also a week later.
- Target's poor call center management to answer more about breach and what steps to take to avoid loss of money but forwarded the customer to a site with a difficult interface and lack of information.

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?**

From my point of view, I would account for Target's board of directors' utmost accountability for the breach, but there are also few people who neglected the FireEye information regarding a malware intrusion that had not been activated yet. Board of directors of Target wasted huge financial resources for security, and later ignored their alert of an attack. They also made bad decisions post-breach that made customers think of an alternative to Target and hence the drop in sales.

If I were a member of the Target board, I would likely survey the damage and try to limit as much as possible till there is a sure way of stopping the attack. In the meantime notify those who were affected in this case all the customers and set up customer care service for the breach that might answer the questions of the customers like what precaution they can take and if they are affected by it pay them for the damage the company caused. Engage with law to identify the attackers, seek legal counsel and lastly document the breach like how was the company breached, what caused it, what did we do post-breach and so on.

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

- The company should check the security of their third-party as part of regular security checkup and inform them of the same and help them upgrade their security to a proper one so that it does not affect us.
- Later it was revealed that FireEye already had created an alert regarding some malware that had not been activated yet. This one tells us not to ignore any alert how small, instead keep an analytics for the monitoring that increases the level of severity of the alert as days pass by.
- Companies should share the information regarding the Cyber threat and what steps of precaution can be taken for the same, it can be held yearly twice as the rise in the cyber

threat is exponential. As long as there is data that is of high importance, the threat to the data will always be there.

- Network segmentation is inevitable as seen in this case. Never leave the open part of the network connected to a private network containing confidential data.
- Lastly, the above responses to an event in progress should not be a surprise, instead these reactions should be rehearsed components of an organization's Cyber Incident Response Plan. Without a plan, confusion ensues and costly mistakes will likely be made. Working a plan will show to law enforcement and the public that your intentions are good and will likely reduce fallout.

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 director in relation to cybersecurity is of utmost responsibility:

- Directors always have to keep the organisation safe by overseeing and approaching the cybersecurity risk not as a low level issue but an enterprise-wide risk management issue.
- Directors should understand the legal implications of the circumstance when facing such types of breaches.
- The organisation's Director must not only have knowledge related to the cybersecurity domain, but also discuss and give adequate time for cyber-risk management in the board meeting agenda.
- Directors should include the identification of which risks to avoid, accept or mitigate as well have a plan associated with the approach.
- Directors should always look at the reports related to security, if a new software is implemented and also regularly audit the policies.