*Based on the case discussions submit your individual written responses to all the seven questions as assignment in Edmodo. Your answers must be clearly typed in your own words.*

1. What’s your diagnosis of the breach at Target—was Target particularly vulnerable or simply unlucky?
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?
3. What’s your assessment of Target’s post-breach response? What did Target do well? What did they do poorly?
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?
5. What lessons can you draw from this case for prevention and response to cyber breaches?
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?
7. What do you think companies can do better today to protect themselves from cyber breaches and in their post-breach response?