Executive Task Force - Summary Unit

What happened?

The attackers gained access to the central customer database by exploiting the vulnerability in the online payment portal 11 days before the detection of the attack, and about 2.3 million customer records were compromised which included: Full names, ID numbers, emails, addresses, phone numbers, and banking details.

What it means for the business(impact)?

Customers and investors lost trust in the company, resulting in the share price dropping by 8%. The customer loyalty programme that was supposed to take place in march was also compromised.

What the board must decide(action)?

The board must allocate a budget and prioritise fixing the vulnerability in the payment portal which was neglected four months back due to budget constraints. The board must also issue a public statement explaining the impact of this attack and try to regain the trust of customers and investors.