



STUDYDADDY

**Get Homework Help
From Expert Tutor**

Get Help

Description of Adverse Event

You are the Chief Risk Officer (CRO) of LIFT, a global ride sharing service. At 9:00 AM, you read in today's newspaper that your main competitive rival, U-Beer has just been hit with a cyber breach. The root cause of the incident was employee misconduct and the inappropriate misuse by that employee of company funds to pay off hackers who had breached security parameters and gained access to customer sensitive data including (names, address and social security #'s). The employee failed to escalate or notify anyone in internal management of the breach until the event was made public. U-Beer has since removed their Chief Information Security Officer (CISO) and is in full-blown crisis management mode as public concern around the situation has escalated. The CEO of U-Beer has also been under tremendous pressure by the media and customers to resign off the back of the incident.

At 10:00 AM, you get a call from the CEO of LIFT, your boss, asking for more details on the situation at U-Beer and whether this type of incident could occur at LIFT. You commit to do an analysis of the situation and report back by 5:00 PM to the CEO and he wants answers to the questions to follow.

Please Answer the Following Questions. You are encouraged to make assumption(s) about the current control environment, known internal gaps, key risks previously identified and known issues from Internal Audit or other areas of the firm in formulating your response. Be creative and think out of the box!!! Use and state assumptions where facts are not available.

Your risk response must include the following short sections in the form of a Risk Response to Adverse Events - Executive Summary: (No more than 1 ½ to 2 pages in total, list references if any)

The Executive Summary must cover the following section(s):

Part one: Individual responses

- I. Short summary of key factors that led to the adverse event at U-Beer
- II. Impacts to the U-Beer business caused by the adverse event
- III. Mitigation efforts needed at Lift to prevent a similar event from occurring
- IV. Draft a high level crisis response plan for Lift to respond to a similar breach should one occur

Part two - Target Project Firm

- I. Cybersecurity is a risk for all firms with access to the internet (via laptops, cellphones, or other devices) describe what key risk factors your target project firm(GrubHub) must consider with respect to cyber risks? (examples include social

media, web-surfing at work and IoT devices, etc.) Short paragraph answers are expected - no more than 5-7 sentences.

- II. What do you think the impact would be if your firm (GrubHub) experienced a data breach or ransomware?
- III. As a chief risk officer, what steps should be taken to mitigate the risk of a data breach? (please consider business impacts, customer impacts, vendor impacts, market impacts and regulatory response such as legal impacts) Short paragraph answers are expected - no more than 5-7 sentences
- IV. Draft a high level crisis response plan for your target project firm (GrubHub) to respond to a similar breach should one occur. Short paragraph answers are expected - no more than 5-7 sentences



STUDYDADDY

**Get Homework Help
From Expert Tutor**

Get Help