Mini Mock – Suggested Answers

Strategic Case Study – May 2023 / August 2023

Section 1

Financial Analysts' Comment

According to the financial analyst, implementing this strategy will lead to higher net operating cash flows in the future, resulting in increased profitability. Although the initial cost of introducing autonomous vehicles to our fleet may be significant, operational efficiencies and the elimination of driver salaries will eventually lead to cost savings.

Adopting autonomous vehicles will open new revenue streams as well, since environmentally conscious customers will prefer to use Daistruk's services. However, Daistruk needs to closely monitor any additional operating costs that will be incurred due to this venture.

The increased cashflows would mean that Daistruk will be able to pay higher dividends, which would satisfy its shareholders. Further, the existence of additional revenue will increase profits, which would further increase the share price, thereby strengthening investor confidence.

The increased beta implies that the volatility of Daistruk's shares would increase. The current beta of the company stands at 1.27, which is higher than 1.00. This indicates that Daistruk's stock is relatively risky, when considered as part of a diversified portfolio.

The increased beta (post diversification), will make our shares riskier, imposing a downward pressure on Daistruk's share price. The higher beta will also increase the cost of equity. This might discourage the board from seeking equity when pursuing expansion imperatives.

However, the additional risk will not be a major problem, given the probability for enhanced revenues and profitability in the future.

Note that Daistruk's systematic risk will be combined with the specific risk when carrying out day-to-day operations, after including autonomous vehicles within its fleet and these need to be monitored and controlled appropriately.

Director's Salaries

It is legitimate that directors seek for additional remuneration. Yet, the directors should not have a final say in the decision to increase their own salaries. Any conflict of interest will be avoided when directors' salaries are determined by the Remuneration Committee of Daistruk, which comprises of Non-Executive Directors.

Alternatively, the board members might feel that they are overburdened with work. Including autonomous vehicles within its fleet increases the business risks and this may have made board responsibilities more complex and challenging.

Thus, the Remuneration Committee should compare salaries with other comparable 3PLs to establish the best rate of pay.

It should also be noted that remuneration paid to executive directors should encourage strategic success of Daistruk. To attract and retain executive directors who are skilled and competent, Daistruk needs to make sure that they are well remunerated.

However, the salaries should not be excessive, which could lead to shareholders seeing the directors as greedy individuals, operating out of mere self-interest.

If the directors feel that their workload has increased significantly, the Nomination Committee should consider a board restructuring. If the board members cannot cope with their responsibilities, then at least an additional board appointment should be made.

Further, increasing salaries in relation to increased workload could come to a point where the board members are overstretched and they will not be willing to do anything about it, since they might fear a salary reduction when their workloads are reduced to original limits.

Strategy: Reducing the impact of Carbon laws

As a starting point, Daistruk should aim to identify the stakeholders whom it will have to deal with to address this criticism.

Daistruk should consider how best to deal with the environmentalists, who have a high interest in sustainability issues but relatively little power of their own. They could, however, harness the power of other powerful stakeholders such as the government.

There is little point in negotiating directly with the environmentalists themselves because they are unlikely to withdraw their complaints about the industry under any circumstances. Indeed, any direct engagement with environmentalists or any of the other lobbyists could simply generate additional adverse publicity.

Daistruk should aim to engage with these environmentalists through media. Dasitruk should aim to offer its own perspective of any point raised by environmentalists to ensure that the public recognize that Daistruk is not necessarily as guilty as suggested, with regards to harming the environment.

Daistruk should also engage directly with the government. The government has a great deal of power, and it appears that their level of interest is high in this instance as per the information which appears on the article and their Net Zero goals.

The law would clearly not apply to Daistruk alone; many others in the industry would be left in a position where they would face disruption in business activities which would inevitably affect business operations adversely. Thus, costs will rise, at the same time, harming the relationship between us and clients.

Daistruk could potentially make changes that would convince the government that the proposed change in the law is unnecessary. This would allow the government to claim that it has taken steps to address the issue and avoid losing the support of citizens who would be negatively affected by the change.

Daistruk should aim to work with its multiple stakeholders (such as shipping companies & airlines), with a view to reduce emissions in transportation. At the very least, Daistruk should be able to count on support from its connected stakeholders, who would lose sales if the law is imposed.

Care should be taken to ensure that the tone of any lobbying is managed carefully to avoid creating the impression that the government is being bullied. The focus should be on protecting the livelihoods of employees and the investment of shareholders.

Daistruk should also work with its closest competitor, Carree which will inevitably display a high level of interest in the matter. If both entities can work together, it will result in creating some power to resist the proposed law.

Additionally, Daistruk can leverage the political connections of Mabalemi Maleka, who serves as the company's Non-Executive Chair, to its advantage.

Further, Daistruk should attempt to address the root cause of the criticism. Ideally, it should carry out its own internal investigation to figure out whether the facts which appeared on the magazine is true.

If that is the case, Daistruk should accept their fault publicly, and inform customers of the steps it will take to reduce the emissions, waste, and pollution in the future. The information should be publicized on Daistruk's website as well.

I hope that this information would satisfy your need. Please contact me if you need any further explanations.

Best Regards,

Senior Finance Manger

Section 2

Strategic Options: Data Breach

Daistruk could do nothing at this early stage. It may be that the concerns expressed by the Head of IT security are unfounded. The report by the Head of IT Security raises some alarming possibilities, but there is no direct evidence that the attempt to compromise users had been effective.

Doing nothing could create the strategic advantage of avoiding an unnecessary controversy over Daistruk's online security. For example, the main target for a thief would be the three-digit security number and it would be extremely reckless for clients to have provided that information.

Daistruk could contact the major credit card companies and warn them that some of their clients' card details could have been hacked. That would have the strategic advantage of demonstrating a proactive response to the threat, while minimizing public exposure.

Unfortunately, data protection rules would prevent Daistruk from releasing the identities of the clients whose accounts have been reviewed since this scare began. Daistruk will have to seek permission of users to share data with designated third parties in response to security threats. Ideally, that should be part of the company's standard terms of business so that permission do not have to be sought.

Daistruk could suspend all services until IT Security has had the opportunity to investigate and resolve the events that it is investigating. The strategic advantage is that this would be a decisive response that would have the added benefit of preventing any further losses of data until the threat of hacks can be evaluated and eliminated.

Clients might be impressed that Daistruk is prepared to lose revenue even though there is no way of knowing whether the attack could ever be repeated. The downtime would also make it easier to upgrade the defenses against the repetition of such cyberattacks.

However, implementing such a measure would cause significant disruption to Daistruk's entire business operations, and a wide range of clients and stakeholders would be negatively impacted, including those who were not affected by the data breach.

Such disruptions to services could have a negative impact on Daistruk's reputation and competitiveness within the market. Furthermore, it goes against the company's core values, which is to deliver excellent service at all times.

Daistruk could make a public admission that warns users that their accounts might have been compromised. This is a strategic decision due to the impact that such an admission might have on Daitruks reputation and the attitude of its clients.

To be effective, Daistruk would have to issue a full press release and make an explicit post on social media, because the hackers could have interfered with the emails, mobile phone numbers and other important information in Daistruk's data files. Also, time is very much of the essence if the hackers are planning to abuse client' credit cards.

The recommended option should fulfil two objectives: it should be an immediate and effective response to the threat of losses, and it should maintain Dasitruk's reputation. The public admission will achieve both of those objectives.

Further, it will minimize future losses by alerting users to contact their card providers immediately. It will also serve as a warning to all users that they should be suspicious of any requests for such details that they may receive in the future.

A public admission could also be phrased in such a way as to imply that Dasitruk is concerned about the welfare of its clients and that it is acting to address problems.

Objectives

The Head of IT should be asked to reach a tentative conclusion about the cause of this incident by early afternoon so that the Board can decide what action to take, if any, over the services to be offered during the evening rush hour.

It should be made clear that this is a crucial deadline and should indicate the questions to which the Board requires answers. The Head of IT should also be given a clear indication of whether the Board would prefer a tentative answer to no response if a question cannot be answered with certainty.

The Board also needs to know how long it will take for IT Security to identify the users who have been targeted and the specific data that has been compromised. Users will wish to know immediately whether they need to take action to prevent losses, such as cancelling their credit cards.

If that information cannot be released immediately, then the next best option for the Board is to make an announcement as to when the facts will be made available. The Head of IT Security will then have to ensure that Dasitruk's credibility is not further affected by failing to meet any such deadline.

The Head of IT should be asked to prepare a credible report highlighting the nature of the attack and the methods used by the perpetrators. Specific criteria should be set for the standard of evidence that the Head of IT Security should meet in collating and interpreting the facts.

Ideally, the report should be supported by evidence that meets the standards required for criminal prosecutions in case the perpetrators are ever caught and brought to trial.

Finally, the Head of IT Security should be tasked with preparing a plan for preventing a recurrence that stands up to scrutiny by an independent expert or consultant. The quality of the plan will be evaluated based on its ability to offer a proportionate and cost-effective response to each of the weaknesses.

The Head of IT Security should be prepared to accept responsibility for the plan, even if he delegates elements of its preparation to members of his staff.

I hope that this information would satisfy your need. Please contact me if you need any further explanations.