# RA 3 assignment Avinash Pentyala

RMA GROUP

RISK ASSESSMENT ANALYSIS


## Introduction

RMA group is an organization of risk managers, whereas risk management is a domain that undergoes certain transformations by adapting Conceptual logic to intervene in conditions of business operations and expectations of stakeholders. By implementing risk management in an organization there is an unquestionable competitive advantage added which creates value for stakeholders and potential effectiveness. Nowadays Uncertainty is becoming a significant factor and risk which adds to the areas to be of interest by managerial staff due to damages that might cause to an organization such as by reputation, finances, and personnel. The method of making decisions is overlapping with the uncertainty and risk that are forced to be embedded into the efficient areas of managers and are

divided.

Organizations that generally decide independently to implement the risk management function that needs to be handled by the top management or any special position in the form of risk manager will be created. Some believe that a special position for the risk manager is not required as it should be inculcated with the general management system which should not be isolated from the other functional operations.

Identifying and assessing risk

When the data is shared among people to read and, access is not given then it is known as a data breach. Once through the source, if they can read the data, it can be taken and altered frequently. This leads to the violation, i.e., disclosure of private information, which is the theft of intellectual property and legal obligations to warn and possibly recompense people impacted, depending on the type of data involved.

Some threats which target the data come from their own employees of an organization who have the access to the network and from different individuals who lay outside the organization. By gaining access to your data such as personal information, emails, and accounts through devices and to your cloud. Regular protection doesn't allow you to keep your data safe from threats. In these kinds of scenarios, organizations must identify the consequences of these data breaches and there is an absolute need to find solutions to reduce the risks.

Objectives

The main objective of this risk assessment is to identify the possible successful losses caused by the data breach and sometimes it might

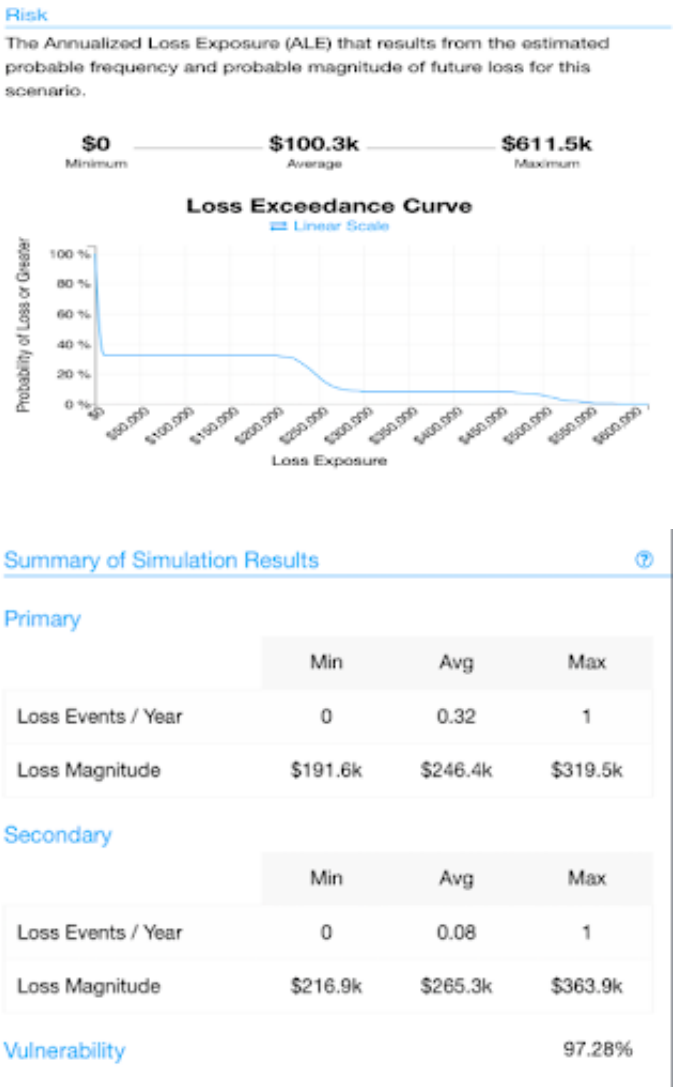
occur within your organization which might lead to a lot more than expected damage. We are analyzing the two companies and their risk management system, what could possibly go wrong and how they can be identified within the range and avoid additional losses. The RMA group which provides risk managers to many potential leading organizations, by leaking the details of the managers can cause damage with respect to financials, reputation etc.

Scenario: 1- Credit Suisse

The organization chosen for this scenario is Credit Suisse, which is a leading financial services company that provides advice to its clients in all the different aspects of finances across the globe. There are many reputed people who are invested and have been part of this. To increase the exponential rate of Greensill which is a financial technology startup to support its high valuation, some high-risk and questionable business practices are being made. Veteran bank officials who are not aware of this practice may be chosen to ignore this. This Situation created a big risk and collapsed the Greensill, the bank paid a high amount as a price for overlooking this issue in terms of reputational damage. The case has been filed about how the bank's top official's negligence while chasing the quick money caused a risk and disobeying risk management and due diligence regulations.

These types of scandals stand out as an example to improve risk management practices which ultimately accelerates sustainable and minimum improvement to its procedures.

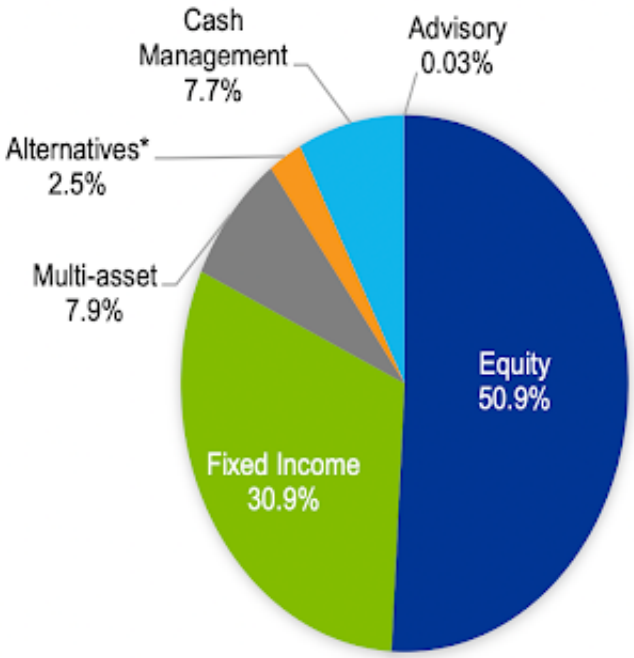
Using FAIR analysis: Scenario - 1



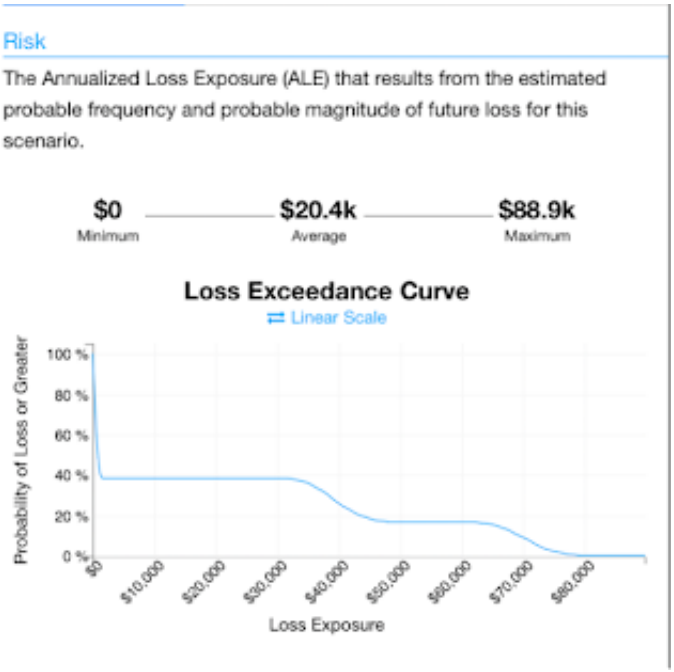

Scenario:2- BlackRock

BlackRock which is a financial firm, developed from a start-up to a market leader. It also remained committed to managing assets on behalf of its clients and offering advisory and risk management services throughout. Many individuals' servers from all around the world in mutual funds, individual savers, wealth funds, and banks are among the clients. One of the most significant efforts is made to dissuade asset managers and banks from taking these aspects to make financial choices. Financial institutions which support political parties etc. are being targeted to use the data against. The value of customers' assets while acting in their best long term will engage the firms. Reputation stands at the utmost edge point which could cause

a high risk of a data breach.




Using FAIR analysis: Scenario - 2



Summary of Simulation Results

Primary

| | Min | Avg | Max |
|---|---|---|---|
| Loss Events / Year | 0 | 0.38 | 1 |
| Loss Magnitude | $29.6k | $39.6k | $55.6k |

Secondary

| | Min | Avg | Max |
|---|---|---|---|
| Loss Events / Year | 0 | 0.17 | 1 |
| Loss Magnitude | $25.5k | $30.9k | $37.4k |

Vulnerability 100%

Conclusion

In this paper, we discuss two different scenarios by two companies and the possible risk that is occurring by the data breach. By using the FAIR tool, a risk assessment analysis has been run for two different scenarios at two different ranges.