**PCRE-2 by Rithu Anand Krishnan**

For this assignment, I would like to use the data breach incident faced by AirAsia in November 2022. Here is a link to their 10K filing for the year 2021-22 and attack article: <http://www.airasiax.com/misc/ar/ar2021.pdf> <https://techwireasia.com/2022/11/following-data-breach-reports-what-does-airasia-do-with-customer-data>

After going through the documents above, here's what I found. They have a risk management committee that identifies significant risks and implements systems to manage overall risk. They have a structured format with three lines of defence, all these details nicely tie up with the **Identify** component of the NIST CSF framework: -

1. The first line of defence is provided by management by identifying and evaluating risks under their respective departments.
2. The second line of defence is by the risk management department and risk management committee. They are responsible for monitoring risks.
3. The third line of defence is the internal Audit department which provides details regarding the effectiveness of the company's enterprise risk management framework.

We should look closely at the risk management department's tasks for the **Protect** component of the NIST CSF framework. They are responsible for reviewing and updating the risk management methodologies. But they do not provide details regarding the precise controls they will execute to protect their data.

They also come up with risk profiles and mitigation plans for every department. They identify and inform the committee regarding critical issues faced by groups. As well as Monitoring action plans for managing these issues. The Internal Audit department is responsible for regularly reviewing system controls and their effectiveness. But the exact frequency of these intervals are not provided. We are unsure if they are done in a timely manner to detect the intrusion at the earliest. However, they see risks and satisfy some requirements of **Detect** component from the CSF framework.

AirAsia has a list of risk management initiatives where they have a list of risks that the committee closely tracks and has brief information regarding its mitigation plan. Here, under cyber threats, we can see that their primary focus is online sales channels, guest feedback, help channels, and other digital solutions. The mitigation plan is to assign a group that acts as a dedicated information security team. Their primary focus would be to detect, contain, and remediate these cyber threats. This fulfils a few aspects of the **Respond** functions of the CSF framework but not in depth. The group adopts the ISO/IEC 27002, the international code for information security control, into the company's processes, procedures, and systems; this serves as the informative references mentioned in the framework's core structure.

The mitigation procedure also includes running regular security assessments and penetration testing, where they try to break into their system to test its durability. Source code reviews on the system are performed daily to ensure cyber resilience. Furthermore, they constantly find new technologies and tools to implement that can help them mitigate emerging cyber threats. Very little to minimum information is provided regarding their data storage strategy. Evidently the poor data storage caused the attack by the Daixin hacker team.

Violation of data privacy laws and regulations is also treated with high importance. Data security and privacy take care of monitoring the loss of customer confidence due to data breaches. However, there is not enough information regarding how they will **Recover** from an attack and its timeline. These issues could have led to the cause of the episode in November 2022 when a ransom attack compromised the personal information of 5 million customers and employees.