The Case Study

Data Mule Marketing & Analytics Ltd

Data Mule Marketing & Analytics Ltd (known from now as simply 'Data Mule') are an Australian marketing and advisory company providing data collection and analytical services primarily to the medical industry. Their chief clients tend to be pharmaceutical and health insurance companies requiring expert marketing data analysis and forecasting expertise as part of their product development strategies of existing and future customers that meet public demand.

Since marketing and data analytics is a specialist area and potentially spans key sales-related areas of the modern organisation, Data Mule's main value proposition is the benefit of relieving their clients from the burden of recruiting and maintaining the specialist data collection and analysis staff needed to support the business that drive their sales.

Background

Since its formation 4½ years ago, Data Mule orchestrates online surveys and data collection schemes for companies and institutions via its online 'Data Mule' smart app. This easy and free to use app enables companies to offer this app to their clients on almost any subject they choose. The data is then collected and stored by Data Mule and released at cost to the client. The app can also carry advertisement for other companies partnering with Data Mule's primary clients. There have been no instances of cyber attack received by Data Mule so far, thus no review of practices has been made so far (given the relatively short time the business has been running.)

Data Mule manages its own information and client data using free cloud-based storage and, occasionally, via a collection of locally stored files (in electronic format only) which has grown steadily over this period to the point that continuation of this practice represents real risk to the organisation. During the recent COVID-19 pandemic, there is research to support the dramatic increase in public online activity (e.g. increased online TV/Movie subscriptions, data from wearable devices from their manufacturer, etc.), meaning there is much data collection and opportunity for analysis which a variety of company types (e.g. health insurance, financial institutions, etc.) would find interesting in terms of marketing opportunities.

Data Mule's main revenue stream is the sale of participant data in order for these companies to build direct marketing schemes online to individual users. Participants are informed of their data being used by 'partners of Data Mule' during surveys when asked to tick a box describing an incentive: that they stand to win a new smart tablet by their participation. From a risk management perspective, Data Mule is expected – some would say have a duty - to maintain the confidentiality of data collections, much of which contains recipient details. The main concern here is perhaps that there is no evidence the leadership or staff of Data Mule are aware of their legal obligations in relation to the security of client identity and data.

The issue

In the face of this sudden growth of business, Data Mule is in the process of drafting their strategic plan for 2024-2033 and is aiming to finalise by July 31, 2023, setting out all its commercial ambitions over this period. This strategic plan not only outlines their plan for expansion but also addresses some of the organisational issues that present existing barriers to this expansion.

One other key theme of these challenges is the increase of information that has accompanied Data Mule's growth, along with the lack of management and security of client data and their liaison with third party business partners. One practical example from this issue emerged during a recent migration project for one of their larger medical clients, where cloud backups of client data were rendered unusable when restored at the time needed for the data analysis.

Never Plagiarise !

Cont.

This set back the project by many weeks, though revealed crucial frailties within the Data Mule's management of information of client data, including suppliers and other professionals (e.g. GP Doctors, Pharmacists, Allied Health professionals, etc.) This single issue represents a threat to Data Mule's reputation as a responsible provider of solutions and the management of confidential data of its existing and future clients.

In the same year, another incident occurred when Data Mule's free Dropbox account was infiltrated by a Ransom ware attack, resulting in all client data (files and databases) being encrypted until the ransom was paid. Since Data Mule have no real firewall apparatus to protect the internal network from the untrusted outside world, the ransom was duly paid and all data was accessible after the attacker released the encryption key on receiving payment. The fact that crucial student and client data was accessed and possibly being used by other unauthorised third parties has so far not been discussed, and no changes to ICT personnel or processes have been put into effect since this incident whilst Data Mule consider their options to prevent a recurrence of such an event. Anecdotally, this inactivity has not gone unnoticed by some of the senior members of the organisation who wonder if there is a lack of leadership at the root of these and other issues.

Following an informal internal review of these two incidents, there is a strong indication that key legislation relating to intellectual property and privacy of client data is at risk of infringement, since Data Mule have no formal information management system or a set of policies and procedures in place to govern such practices. There is no internal role within Data Mule responsible for supervising this area, and no general education program informing staff of their responsibilities. Therefore, it could be said that Data Mule could be breaking the law relating to the management of client data, potentially caused by ignorance of its legal and ethical obligations. The review concluded that a solution needs to be found to address this major issue.

Summary and intended outcomes

Data Mule's rapid growth, lack of general education awareness around IP and Privacy of client data and a lack of internal governance and information management strategies represents clear risks to the business. There are also secondary issues, such as reputation damage through resulting from continual concerns from staff and clients. Thus, the leadership and staff of Data Mule suspect that some systemic, possibly cultural disjoint may lie at the root of these issues and should be addressed through a purposeful and planned approach. Therefore, Data Mule management team have asked your team to investigate this from an ICT perspective with the following general outcomes in mind:

- Attempt to identify the probable root cause(s) of these that associate strongly with ethical organisational behaviour that takes greater responsibility for the rights of client privacy, identity and data protection
- Plan and conduct identification and risk assessment of the key challenges faced by Data Mule.
  NOTE: You are not required to suggest any solutions at this stage
- List all relevant legislation – state and federal – relating to Data Mule's duty of care to its clients and protection of their Intellectual Property and Privacy rights
- Communicate the identified issues, along with recommendations to mitigate or eliminate these issues in the form of a video presentation to Data Mule directors within an accessible format
- List any other actions recommendations that aim to add value to the organisation's projected growth in a sustainable and responsible manner conducive to the recommendations made by your consultancy.

<End>

Never Plagiarise!