Mitigation of Business Risk around IT Universe

Introduction

Now a days many companies are facing rapid pace of change and unprecedented uncertainty as the pandemic has destabilized operations, disrupted supply & demand, and destabilized previously sound business models to such an extent that very few would have imagined earlier. However, with proactive steps from governments and natural recovery out of the pandemic, the economy is beginning to show promising recovery following the deepest global recession, however challenges such as supply chain issues, inflation risks, data protection are still some of the areas which are adversely impacting the businesses. Digitization of Economy has happened at much faster pace than ever in the past which along with advantages, is also bringing some of the pitfalls such as cyber security concerns, data protection etc

Businesses are changing the working models from “Work at Office” to “Work from home” and the use of IT tools, online E-platforms, chatbots, data storage tools, cloud technologies, remote access are becoming part of day-to-day business work. Now due to the market recovery after pandemic, companies are again looking out to employ more human capital to manage the business operations. As per industry statistics, once a company employs more than a dozen people, it naturally tend to lose track of devices and data. Without having proper polices & procedures in place, company’s information gets stored at odd places such as some of the information in the cloud and some in the personal devices. This is hardly perceived as a problem / risk until something goes wrong and the management realize that they are losing track of all the data and losing control over their intellectual property which can very well sneak out to the competitors in an unauthorized manner. All such events can lead to reputational and financial issues to the Company.

Statistical trends suggest that companies are spending more efforts in securing against the cyber and malwares risks then making their internal IT data management and infrastructure controls more stronger. From our experience in working with companies from different industries, we have noted that having a strong internal audit process can help develop robust internal controls that protect the company against internal and external risks while also guiding when things are going off the radar from business plans perceived by the management. Below are the key insights that can help improve the internal control environment

1 Maintain an Asset Register

There are a number of businesses that do not keep real information on list of IT assets held by them. It's not just about the laptops but IT asset goes beyond that which includes computers, phones, servers, routers, USB devises, specialized business IT tools, Software subscriptions, Cloud devices, IT infrastructure etc.

Controls to be placed

To ensure that all the IT equipment, especially the one's holding key company data should be kept in proper control. One person should be given the ultimate responsibility to control such asset register and verify it periodically depending on the importance attached to such an equipment. Also it is always better to draft a policy around this for proper control. Where possible, such assets should be tagged with bar codes or RFIDs so that its verification and tracking becomes easier

2 Develop Data Pipeline

Due to the use of multiple devices, some companies lack visibility of what data they keep, and where it is saved/archived. In the modern era business information spread across multiple locations, servers, cloud and mobile devices. This can create compliance issues especially with new laws in place such as Data Protection Law, customer protection rights

Controls to be placed

It's advisable that Companies must map the existing data in such a way that it is easy to find where different types of data is stored, how such databases are connected and how it can be retrieved in the event of a need. Such data maps should be reviewed and updated after proper interval to avoid any risk exposures. Developing proper policies around this can help better the control environment

3 Manage Data Access Rights

In the mid-size organizations, it's not uncommon that most of the company staff would have access to everything on the corporate network. Such open-ended access exposes the organization to the risk of intellectual property theft.

Controls to be placed

Companies should develop a Matrix for Data Access Rights where access should only be given to the authorized user with required rights such as view, edit, delete and copy. All the confidential documents placed over the network showed have special view/edit rights to individuals and should not be allowed to be copied to an external device without the approval of authorized person.

4 Align Data Management Mandate with HR

Data management is normally considered the child of IT department. But when it comes to incidents such as intellectual property theft, the issue really lies with human resources. So, it's important that policies of appropriate data management are well catered in the employee contracts, trainings and induction processes.

Controls to be placed

New and existing staff should be made aware about the company IT and Data Management policies. HR department must get the non-disclosure agreements signed from the employees for the protection of the data. Finally, a culture to use the personal devices, emails and storage spaces should be discouraged and all the company related data shall be retained with the company sponsored IT equipment's.

5 Perform Exit Checks for Employees Leaving the Company

Normally business show a lot of care while recruiting a new employee to ensure that the person brings new skill set to the organization. Whereas, less attention usually paid to the departing employees with respect to the data and information which employee may carry out with them when they leave.

Control to be placed

Companies should put in place the Data Protection policies for the outgoing employees. It's always appropriate that Exit Interviews shall be carried out and NDAs signed with the employees should be restated and enforced. Employees leaving the organization should be asked to give an assurance that they are not in possession of company devices or information.

6 Bring Fresh Pair of Eyes

Wordy policies can be developed and controls can relatively be straightforward to implement but when it comes to enforcement and monitoring of the same, most of the companies face challenges.

Control to be placed

It's recommended that companies shall bring independent experts for regular monitoring and review of controls which can be easily achieved by outsourcing the the Internal Audit to an expert for unbiased opinion. By having an in-depth Internal Audit, companies can benefit by having a detailed risk assessment of their existing process and controls along with best industry benchmarked recommendations to mitigate the business risks.

How Premier Brains Can Help

Premier Brains has a team of specialized internal auditors with lot of experience of working on IT audits as well. Having long experience of more than 10 years, the team is well placed in identifying key business risks and advise on various practices that can help mitigate its ill-effects

Subject matter experts at Premier Brains are always there to see that your business grows smoothly with proper systems in place manage business risks

Prepared: Moin Ibrahim