Risk assessments of dealing with Third Parties

Today a business cannot be done in silos, the parties who becomes part of the business also plays an important role in overall growth of business. Presently, most of the business wants to focus on their core activities and wants to outsource the other ancillary activities to various other parties. On analyzing the overall risk of organization, specifically during due diligence, merger, or acquisition, it becomes important not only to understand the risk environment of the organization but also the third parties which are involved with the organization. With most of the services rendered through online mode, the security risk plays a very crucial role when the product or service is outsourced to a third party. The risk assessment typically involves establishing risk criteria and performing onboarding and screening for third-party partners and vendors.

What is it?

The third-party risk assessment which is also generally known as the supplier risk assessment as most of the risk assessment are done for the associated supplier. The third-party risk assessment is a process of quantifying the risk associated with the parties. During the risk assessment cyber risk assessment plays an important consideration. If the cyber security of the third party is compromised, there are chances that the security of the organization with whom company is dealing may also be compromised.

Reason for conducting third - party risk assessment

1. Understand the risk undertaken by dealing with the vendor: Third party risk assessment helps to analyze how much risk you are taking by engaging with a

particular vendor. This process forms part of the vendor evaluation and helps to understand whether to continue the relationship with the vendor.

2. Preparedness for cyber security:

When you allow your vendors / or any other third party to get into your network, you are allowing a potential cybercriminal to access your network. It is important for an organization to understand whether the party you are dealing with takes cyber security seriously as you do for your own organization.

3. Improving compliances: There is a growing number of regulations which a company must go through. In certain cases, the non-compliance of such regulations may attract penal clause and may be detrimental to the business. Now if your company is dealing with a third party who does not take the compliance aspect seriously, it could be detrimental for your business as well.

4. Branding:

To create a brand, the trust of customer is very

important. The reputation of the company in the market plays an important role for the company to stay in the market. It maintains the brand it is important that not only the company but also their extended arms like the vendors maintains proper security of the customer data.

Steps involved:

1. Identification, evaluation, and selection: Third party risk assessment may be essential process but let us understand that third party risk assessment comes with cost in terms of man hours involved and the cash outflow. It will not be practical for the organization to conduct the third-party risk assessment on each vendor the company is dealing with. The company needs to identify the

third parties which that may have unique risk in terms of the geographical location or the political conditions. It is important to identify the third parties based on the criticality tiers.

2. Establishing the risk criteria: This process involves the risks of the third parties which are most detrimental to the

organization. The clients which handle sensitive data must have very specific requirements with respect to security risk in the vendor risk criteria. Establishing the risk criteria will affect your organization's actions and policies, techniques the will be used to assess the third parties.

3. Third party on boarding and screening:

Maintaining a detailed diagrams outlining the relationship with the third party or the supplier helps to anticipate and avoid possible risks. It would be imperative to build a third-party risk management program using a specific framework that standardizes all third-party on boarding and screening. A well-designed risk management program framework is beneficial to both the parties. It saves time and provides insightful risk assessment.

4. Risk mitigation: After conducting a third-party on boarding and screening, risks can be calculated and mitigation can begin. Common risk mitigation workflows include the following stages:

a) Flagging of the risk and assigning score to the

risk

b) Evaluation of risk against your organization's risk appetite

C) Treatment and control validation in the scope of your desired residual risk level

d) Continual monitoring for increased risk levels whether there are any data breaches.

5. Ongoing monitoring: Ongoing monitoring throughout the life of third-party relationship is critical. The engagement of third party may not be one time affair for the organization. In the absence of ongoing monitoring, new risk of new issues like the breaches and sanctions arising may not be effectively monitored.

What does Third party security risk assessment template consist of?

a. Identify and describe the threats / risk

b. Assess the possible consequences of the threats / risks

C. Quantify each threat / risk

D. Recommendations / security measures risk

e. Streamline the existing process

f. Opportunities of ongoing improvements

Conclusion:

Third party risk assessment is a method of risk assessment to prevent expensive damages while dealing with the business associates / third party. When the risk like the cyber security risks is known upfront, it is appropriate to evaluate and implement appropriate controls. Regular assessment of third party ensures that third party risks are evaluated and taken care of on a regular basis.

Measuring third party assessment and mitigating associated risks gain more importance in the present world where bogus/ fake entities or fly by night operators are having increasing trajectory/ graph; causing huge revenue losses, tax mismatches and demands by the authorities.

The cost and efforts incurred on the third party assessments will be lesser and minimal as compared to the future revenue gains from such assessments.