Strategic alliances

Business

Strategic Alliances The Indian Department of Telecommunication (DoT) has issued warning over the involvement of private manpower in the development of the National Cyber Coordination Centre (NCCC), for the government of India (Aulakh, n. p.). While issuing this caution, the department of telecommunications observed that outsourcing manpower for the project would be risky. This is because, according to DoT, the establishment and development of such a sensitive installation does not deserve outsourced manpower, considering that outsourcing the manpower will open more avenues for the breach of the sensitive data for which the National Cyber Coordination Centre is meant to protect (Aulakh, n. p.). In this respect, the DoT has sought to be involved as part of the multi-agency taskforce committee meant to monitor the project, as one of the important stakeholders to the project.

This outsourcing caution resonates well with the outsourcing strategies provided under chapter 6, which requires that outsourcing can only make sense, where the outsourced services reduce the company’s risk exposure (Chapter 6, n. p.). Therefore, the caution issued by DoT to Department of Electronics and Information Technology (DIETY) of India, serves to meet this requirement as provided under the chapter. This is because, if the DIETY outsources manpower for the development of the NCCC, the private manpower will be aware of the possible security breaches that can be applied to bypass the security systems established by the project. This would be detrimental to the functionality and success of the project, considering that this project is meant to be applied for screening the entire web traffic on the internet within India, and then generate a security alert for the government recommending action, on the event that any cyber security

threat is discovered (Aulakh, n. p.).

According to the minister for information in India, the threat of Cyber security in India has been on the rise, with 24, 216 Indian sites being defaced in 2013, compared to 17, 306 sites that were defaced in 2011 (Aulakh, n. p.). In this respect, it is important that the government takes the necessary measure to curb the threat of cyber security attacks in the country, and that can only be achieved, if a foolproof system of scanning the threats is established. Nevertheless, the involvement of private manpower will be a higher risk to the project, than when the government enlists the services of its own manpower (Aulakh, n. p.). According to outsourcing strategies provided under chapter 6, outsourcing of services would only make strategic sense, if the services outsourced are not crucial to the competitiveness of the entity, and where such services do not affect the capabilities, know-how and the core competencies of the entity (Chapter 6, n. p.).

Thus, the outsourcing of the manpower to develop the NCCC project will not only affect the know-how in the public domain regarding the sensitive installation, but it will also affect the core-competencies of the project, considering that it will be much vulnerable to manipulation by the private expertise who helped in the development of the project. The country has been recording a high rate of malicious attacks and website intrusions, and the only way to address the problem is through establishing a secure, competent and protected system that will detect the threats and alert the government for action (Aulakh, n. p.). For this reason, outsourcing of private manpower is discouraged.

Works Cited

Aulakh, Gulveen. “ Department of Telecommunication cautions against

outsourcing manpower for internet scanning agency.” The Economic Times, February 26, 2014. Retrieved March 8, 2014 from http://articles. economictimes. indiatimes. com/2014-02-26/news/47705595_1_dot-cautions-national-cyber-security-policy-telecom-department

Chapter 6. outsourcing strategies: Narrowing the scope of operations, n. d.