Chapter 29
Exploring Information Security Governance in Cloud Computing Organisation

Hemlata Gangwar
National Institute of Industrial Engineering (NITIE), India

Hema Date
National Institute of Industrial Engineering (NITIE), India

ABSTRACT

The paper reveals factors impacting information security governance within the cloud computing technology implementation in organizations. Case study methodology was used and 15 semi-structured interviews were conducted with directors and information security professionals from 5 different types of organizations. The main component that were identified as playing a significant role in information security governance were: information security strategy, security policies and procedure, risk management and assessment program, compliance and standard, monitoring and auditing, business continuity and disaster recovery, asset management and access control and identity management. The results show that awareness through education and training of employees needs to be given very particular attention in cloud computing security. The paper does not include any end-user perspective in interviews and this end-user context is missing. Companies need to focus upon awareness through education and training of employees. Moreover, management and employee support is the critical component of the effective information security governance framework implementation. Also, organisations should develop their information security using a very precise and detailed planning process that ensures the right cloud computing acceptance by the users. The proposed information security governance framework offers organisations a holistic perspective for governing information security, and minimizes risk and cultivates an acceptable level of information security culture.

DOI: 10.4018/978-1-5225-5634-3.ch029

1. INTRODUCTION

At present, information security is seen as an integral part of organisational strategies which emphasize upon adequate security of their information as a governance issue (Saint-Gemain, 2005).The mechanism of information security governance (ISG) ensures effective management of information security in organisations. It includes accountability to shareholders, compliance with legal requirements, setting of well-planned security policies, spearheading security awareness and education, defining roles and responsibilities within the organizational structure, contingency planning, and instituting best practice standards (Mears and von Solms, 2005).It is perceived as a business and governance challenge that involves adequate risk management, reporting, and accountability. Since effective information security requires the active involvement of executives, it is addressed at the highest levels of the organization to assess emerging threats and to effectively response to them. The implementation of information security governance practices not only reduces the risks, but also improves reputation, confidence, and trust from business partners. Organisations develop policies, procedures, records, people, governance structure, reporting, audit, and technical security measures to develop information security culture. It is further demanded implementation of the required information security components. In case of cloud computing, this becomes more important as cloud security is now placed as an important element in an organisation's overall information security program. Cloud computing faces many hurdles due to its privacy and security related issues. Although there are obvious cost benefits in the usage of cloud computing, a number of incidences in the past have raised questions on reliability of cloud computing in securing the outsourced data and information. It demands special considerations to security, governance, risk and compliance related issues which need to be formalized and streamlined. Further, a need is seen to come up with an information security governance approach for Cloud Computing to tackle these issues and provide a unified solution for cloud service providers and their customers. So, this paper develops an information security governance framework to arrive at a complete list of information security components and to compile a new comprehensive information security governance framework. The paper qualitatively examines the importance, implementation, and the main features of ISG in Indian organizations and introduces an integrated framework for ISG. It identifies and integrates the core components of ISG, and highlights the meaning, objectives, importance, procedures, and the expected benefits of implementing effective ISG.

2. CONCEPTUAL FRAMEWORK

ISG is defined as the organization's management responsibilities and practices that provide strategic vision, ensure objectives are achieved, manage risks appropriately, use organizational resources responsibly, and monitor the success or failure of the information security programs (Abu-Musa, 2010). Governance in information security is related to establishment and maintenance of the control environment that manages risks related to confidentiality, integrity and availability of information and its supporting processes and systems (Moulton and Cole, 2003).

This study introduces an integrated ISG framework (Figure 1) that would enable organizations to better understand, analyze, implement, and evaluate ISG practices to achieve business success. The proposed ISG framework has been developed based on the ISG conceptual framework proposed by D a Vega and E loff, 2007 and other ISG models and frameworks available in the literature (von Solms and