Data Privacy in Business Process Management organizations.

Business Process Management (BPM) organizations that conduct outsourcing and transformation business in a transnational environment face a multitude of challenges related to the privacy and protection of their client's confidential and sensitive information. Globalization of data through cross border data flows, enablement of multi-shore data processing through interconnected networks and virtual technology architectures, diverse global geographies environments and cultures, industry specific regulations and stringent contractual requirements; all continue to influence the usage and protection of individual's Personal Information (PI) in this global business environment.

Global BPM organizations are required to maintain compliance across all the three dimensions: with the laws of the land across the geographies in which they operate globally such as UK DPA & Indian IT Act, with the industry specific regulations, such as GLBA, HIPAA, HITECH that they operate in and with client's legal binding contractual obligations.

There is an increasing need therefore for these organizations to have a comprehensive Information Security Management System (ISMS) and Data Privacy (DP) Framework to adequately protect various forms of personal and confidential data that is part of their multi-shore business operations. A robust Information Security and Data Privacy program should address the information lifecycle phases in its entirety (collection, use, sharing, disclosure, retention and disposal) in its entirety.

Some of the most important factors in driving such programs successfully are to establish cross-functional & multi-disciplinary teams, establish senior management sponsorship, periodic governance with the internal stakeholders & with the clients counterparts and promote the awareness of the program by embedding it culturally into the organization's core fabric.

To start with, the organization will need to perform an as-is assessment of their existing information security maturity and data privacy practices vis-a-vis the prevailing regulations, contracts and obligations, which happens to be one of the best methods to establish a realistic baseline.

It is essential to gain an in-depth understanding of the business processes, data flows therein and assess the applicability of various data privacy laws and regulations through development of an inventory of one's clients' contractual & legal obligations and a current-state gap analysis on compliance on these will help prioritize the areas of focus and investments.

Using Generally Accepted Privacy Principles (GAPP) is one of the simplest, yet most effective approaches to devise the foundational charter of the program. In order to understand the applicability of GAPP for each client areas & business processes, organizations should perform Privacy Impact Assessment (PIA) that will aid the development and maintenance of a risk-compliance profile for all their clients and the underlying business processes therein.

Progressive maturity can be driven in the program by taking on one regulation at a time in depth, as it

may be applicable in the respective industry verticals or domains of the business operations such as Banking, Insurance, Healthcare, F&A and address their stipulations as bolt-on on top of the foundational framework.

It is also essential to provide an architectural treatment for implementation of the policy and processes. This can be achieved through investment in security and privacy tools such as Data Leakage Protection (DLP), Security Operations Center (SOC), Data Classification, Encryption (end points, portable devices), Rights Management System (RMS) and Privacy Dashboards that will aid the efficiency and ongoing operational manageability of the program.

For this program to operate effectively and be adopted well, organizations need to demonstrate high standards of security and privacy work practices. The best way to achieve this is by developing and implementing robust, enterprise-wide evangelization and training program to promote awareness and bringing everyone together in the organization on this important business discipline.

Robust security and privacy work practices help organizations build client confidence through trusted outsourcing and also mitigate any incidents, breaches, penalties and loss of reputation with their stakeholders. This is pivotal for an organization's success, and to cultivate and maintain a reputation of a security and privacy conscious service provider in the industry.

Author

Mr. Baljinder Singh, Global Head of Technology, InfoSec and BCP, EXL Service.com Pvt. Ltd