Security becomes key concern in global sourcing: Gartner

Gartner uses IT Security Summit to explain how to mitigate global sourcing risks.

Information security concerns surrounding global sourcing will gradually take centre stage alongside public concern over job losses, according to Gartner. As offshore outsourcing evolves from low value/low exposure projects to increasingly complex global projects involving core competencies, the cost and exposure of inadequate attention to security will increase significantly. Gartner urged enterprises and service providers to start an informed dialogue to address security early and to perform due diligence throughout the outsourcing life cycle. Although security issues will lengthen the sales cycles of global delivery, it will not stop enterprises from adopting global sourcing models.

Gartner presented its view on the real issues related to security, privacy and IP/confidentiality when going offshore at its recent IT Security Summit in London.

"The security exposure that both clients and service providers have to deal with, as global sourcing becomes more strategic and complex, increases by orders of magnitude," said Mr Partha Iyengar, research vice president, Gartner India. "Service providers are unable to provide standard security solutions because regulations, legislation and consequently risk vary vastly between industries and geographies."

Gartner said there is also tremendous hype and a lack of understanding of the issues surrounding security. The most significant security issues revolve around the protection of data in one manner or another. There are, however, other issues that are not well understood, vague and based on emotion rather than fact.

Said Iyengar, "One of the most frequently voiced concerns is related to call centres where consumers are alarmed when dealing with people with unfamiliar accents in unknown or foreign locations. This understandably raises questions around people's personal data, but may nevertheless not present a real risk."

"Service providers and users need to look jointly at risk and work together to create an information protection framework to identify and spell out each of the concerns, determine their validity and make educated decisions about the risk they may or may not pose," said Iyengar. "Companies also need to be more transparent and inform customers of the security steps they take when going global to alleviate fears and avoid hype."

Key asset protection issues in global sourcing

Understanding the relationship between business, security, IP and privacy is essential for enterprises in effectively managing business risks associated with corporate and individual privacy. Security deals with data, people and technology, privacy deals with data confidentiality and customers records, while IP concerns patents, copyrights and trade secrets.

"There is a significant 'cost of security', and it is not cost-effective to provide the same level of security to every aspect of a company's offshore exposure. Companies therefore need to understand which records and data they need to protect and why, and how much they should spend on this security," said Iyengar. "Diligence in understanding the actual risks involved will ensure that educated decisions can be made on the ROI around security expenses and investments. The most sensitive data can be found in personal, financial, medial, tax, employment and company financials records. Certain companies and vertical industries will have to classify data or determine the requirements for sharing data on project by project basis."

Iyengar highlighted that global delivery also includes a growing number of lines of service or application areas. These include applications development, IT infrastructure, contact centers and back-office BPO. Each of these could have vastly different requirements and exposure in terms of 'information protection' requirements and need to be understood and dealt with differently.

Regulations and country risk

The pace of new regulations is increasing for all industries and governments. The focus that countries have on privacy and data regulations is diverse and will evolve by country. "While the United States and Canada have strong regulations for personal data protection in the public sector and no comprehensive legislation for the private sector, the European Union, Japan and Brazil have data protection and privacy codes for the private sector," adds Iyengar. "Regulations will constrain or put additional requirements on the relationship between clients and service providers. At a minimum this could increase the cost of providing the services, and in the worst case it could prevent some work from being sent offshore. Enterprises need to understand all the nuances around these regulations to put an effective strategy in place."

To help enterprises evaluate the high-level risks posed by security regulations in global delivery Gartner has created a country status risk model:

Country risk status - security, privacy, IP and legal structure

Security risks: How strong are the country's laws around security, including the existence of standards around this? Equally (or more) important, what is the track record of the country and its people in the adherence/enforcement of these standards and laws.

Privacy protection: Is there an environment and inherent 'culture' that supports and promotes data and personal privacy. Is data security taken seriously and are adequate protection measures in placing in general that are followed. Is there sufficient awareness of the need to protect confidentiality in data?

Govt. interception risks: Issues like government interception of sensitive confidential information as well as guidelines for the use of or access to effective encryption algorithms in the country (some countries are restricted in this) are important.

IP risks: across IT and many other industries, protection of IP is taking centre-stage. Given the vast diversity in laws and regulations around this issue globally, one cannot assume that all countries provide the same level of protection, both from the perspective of existence of laws to their actual enforcement.

Employee/labour laws: how employer / employee friendly are the laws in each of these countries, and what are the ramifications from a labour perspective of doing business here.

Contractual/legal risks: at the end of the day, any non-conformance/breaches on any of these issues could end up in a contract dispute in a court of law. In some countries, justice is delayed to such an extent that it is truly denied. Understanding the risks of contractual and legal system maturity and speed (or lack thereof), can allow greater diligence during the contracting process.

"Generally, the maturity of legal frameworks, regulations and business approach mean that countries considered to be 'developed countries', such as Ireland, Canada and New Zealand provide a more secure environment," said Iyengar. "However, the trade-off is that companies will not be able to make the same cost savings as for example India or Russia. Recognising that the risk versus cost trade-off will increasingly drive sourcing location decisions, India is aggressively addressing issues around security. For example, the trade association, NASSCOM (National Association of Software & Services Companies) has launched specific security certification initiatives with the Indian government as well as its member companies."

The way forward

Gartner gave enterprises three key recommendations when addressing security issues in a global sourcing model:

1. Tackle security issues very directly and early in the sourcing strategy development phase. Then review throughout the life of the outsourcing deal through evaluation and selection, contract development and sourcing management, the three remaining phases of Gartner's sourcing life cycle.
2. Develop a detailed dialogue with your service provider and ensure you understand their approach and track record in delivering robust security. Do not cede overall control and responsibility for management of security onto the provider. This control should remain in-house, including responsibility of some of the auditing mechanisms.
3. Work with the service provider to create and deliver an information protection framework to identify and spell out each of the concerns, determine their validity and make educated decisions about the risk they may or may not pose, and how much should be spent on mitigating that particular risk.

By way of conclusion, Mr Iyengar stated, "It is imperative that security issues are addressed right from the start and throughout the life of the sourcing deal and this requires information security staff to be at the table in both operations and strategic planning functions."

www.gartner.com