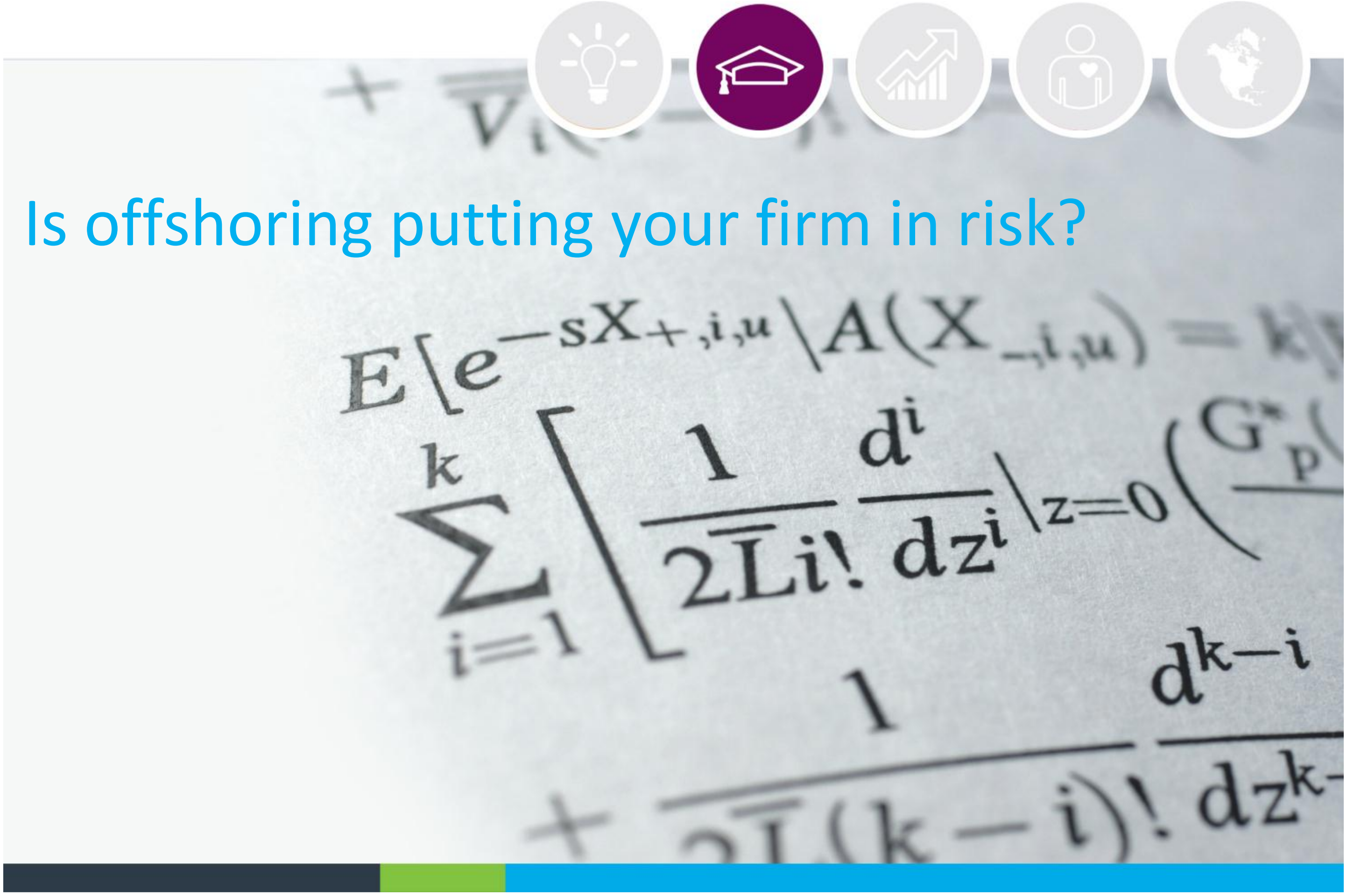
QA Consultants



Is offshoring putting your firm in risk?

Is offshoring putting your firm in risk?

The past 15 years has witnessed a stampede of IT services and business process outsourcing to Asia, particularly India. In many but not all[1] cases, North American and European companies have benefited from outsourcing large amounts of their back office operations to gain lower costs and quicker scalability. However, there have been nagging doubts around the security of their customer data and intellectual property (IP) given the geographic, legal and cultural divide separating Western and emerging countries. Are these worries justified?

In our view, yes. Take India as an example. A 2012 Ernst & Young India report said there has been a significant increase in the incidence of fraud in the technology services industry over the past decade. Crooks are getting past the multiple safeguards and verification processes of even the largest companies, compromising consumer data, aiding terrorist organizations and enabling improper trading.

To wit, there have been numerous examples of fraud and security breaches in the press over the past 12 months. While many are likely covered up, three significant lapses hit the international media, with serious financial, regulatory and reputational implications for the companies involved:

- According to a joint probe by Swiss and British regulators, key controls for “detection of suspicious trading activity” failed at an Indian outsourcer, contributing to a 2.3 billion dollar trading loss by a rogue UBS trader.
- The US Senate’s Permanent Committee on Investigations found major lapses in the work of HSBC’s India staff compromising consumer data.
- A probe of Britain-based Standard Chartered bank by New York State regulators found deficient money laundering controls by the bank’s Indian outsourcer. Poor controls significantly contributed to the movement of hundreds of millions of dollars through the bank to Iran, in violation of U.S. law. Standard Chartered eventually settled the allegations by paying a 150 million dollar fine.

These security lapses trace to many factors. One major cause is the low ethical standards of many Indian employees. According to CIO Insights magazine, an estimated 20% of all Indian job seekers overstate his/her academic qualification, work experience and salary history. Given the cultural, social and economic dimensions of this problem, it is unlikely that any organization in the short term could significantly reduce this risk to North American levels.

Low employee skill levels also contribute to poor security management. In every company, many Indian workers suffer from important gaps in language, knowledge and business practices that complicate efforts to quickly and fully leverage the latest risk management technologies and processes. One telling statistic from The Wall Street Journal indicates that 75% of India's technical graduates are unemployable by their IT sector.

Another culprit is the rapid pace of change experienced by most of the Indian outsourcing industry. The perils from criminal behavior and incompetent worker performance increases significantly when companies are growing at historical rates of 25-35% per annum. The reality is that many rapidly growing firms dispense with background checks in order to on-board people as quickly as possible. Further complicating the risk management effort is high levels of employee turnover. In some IT functions in some firms, as many as 80% of the workers have to be replaced each year due to poor performance or poaching by other firms.

While detection is improving in many companies, most cheats continue to go undetected. There is no national, comprehensive and accurate database for tracking job seekers. The competition for people is so fierce that companies are reluctant to share former employee details like salaries and performance reviews. When a cheater is caught, they are usually just terminated; the police rarely get involved. Even if the police agree to prosecute, India's plodding legal system hampers the likelihood of a quick trial and conviction. Once exposed, the employee –emboldened by the lack of exposure and punishment – merely moves on to his/her next opportunity.

This situation is unlikely to change in the short term. The appeal of well-paid outsourcing jobs and high demand continues to be a strong magnet for millions of Indians, particularly recent graduates with high student debt and lofty ambitions. This perfect storm creates significant incentives to cheat or not fully comply with all risk management procedures. While every North American firm outsourcing to India faces some risk, some industries are especially vulnerable. These would include sectors that process consumer information (e.g, banks, insurance) market premium brands (e.g, luxury goods, retail) or generates IP (e.g, pharmaceuticals, software).

To be fair, North America is not a risk-free geography. Similar crimes and security breaches have taken place in North America over the same period. And, there is no reason to believe any local company and operations (except the most vigilant) will be immune to the most sophisticated attacks.

However, when it comes to dealing with breaches India and the U.S. are totally different jurisdictions. India continues to look and act like an emerging economy, no matter how modern the Bangalore or Pune development center appears. The considerable physical, linguistic and cultural separation naturally triggers high levels of management anxiety, defies easy communications, confounds information gathering and dramatically drives up the cost of risk mitigation. Finally, should serious fraud occur it is far more difficult and expensive easier to investigate, prosecute crimes and seek damages in India than North America.

As long as the economics make sense (though this gap is shrinking), Asia will always be a major center for outsourcing operations that require high numbers of employees with minimal or low skills. However, managers should make outsourcing decisions with their eyes wide open. Specifically, they need to ask two vital questions: How likely will something go wrong? And, what are the financial, regulatory and brand image implications of a major security breach. Where the benefits of offshoring are shrinking and the potential risks are growing, managers would be wise to consider repatriating key operations back to Canada or the United States.[2]

For further information please contact:

Harry France
Sr. VP Sales
(519) 575-0314
hfrance@qaconsultants.ca

[1] For an analysis of the problems with offshoring, see the QA Consultant white paper, “The Perils of Offshoring Software Testing”

[2] For a review of the benefits of in-shoring, see the QA Consultants white paper “In-shoring’s growing appeal