India struggles in privacy PR stakes

Keen to preserve its status as one of the world's top outsourcing destinations, India is pulling out all the stops to reassure businesses and governments that it is a (privacy) safe place to do business. But are events conspiring against it? By **Alan Pedersen**.

"Outsourcing costs UK cancer patient his medical history" read the headline that graced the pages of the *Times of India* earlier this month. The headline in question related to a story about a retired UK policeman suffering from cancer, whose medical reports - which had been outsourced to India for transcription - had somehow gone missing.

NASSCOM's 4E Framework for Trusted Sourcing

Earlier this year, the National Association for Software and Service Companies (NASSCOM) launched a 'trusted sourcing' initiative to promote more effective security and privacy controls in India. The 4E framework is based around four key principles:

1. Engagement
- Creation of Global and National Advisory Boards on Security.
- Meeting stakeholders in India and key markets.

2. Education
- Reports to NASSCOM members on model contracts, SLAs, security practices and standards, and key global privacy legislation.
- Seminars to educate members, lawmakers and judiciary
- Create intellectual capital for members and other stakeholders.

3. Enact
- Examine areas to strengthen the legal framework in India.
- Work with coalitions and regulators in key markets to identify relevant provisions.
- Establish best security practices in member companies.

4. Enforce
- Established Mumbai Cyber Labs (an initiative aimed at combating IT crime) - to be extended to other cities.
- Security audit of members, security certification for employees.

It must have made for some uncomfortable reading for India's outsourcing community, which is currently striving to reassure both businesses and consumers alike that they can be relied upon to protect people's privacy.

In truth, the incident could probably have occurred anywhere, but the huge growth in outsourcing to foreign destinations has put the spotlight on how medical data, credit card details and other personal information is protected once it leaves domestic shores.

To complicate matters further, privacy is increasingly being used by trade unions, politicians and other offshoring opponents who seek to limit jobs cuts and curb the loss of business to foreign service providers.

UK bank, Lloyds TSB, was recently on the receiving end of the outsourcing backlash (see p.6). In August, trade union representatives for the company's employees lobbied the UK Information Commissioner for an investigation into whether Lloyd's outsourcing practices breached the Data Protection Act's rules on data transfers. The story was widely covered by the global press, with some reports predicting dire consequences for the outsourcing sector should a breach be discovered. The union's argument, based on the false premise that you need customer consent in order to send data overseas, looks doomed to fail, but the publicity it attracted has perhaps dented consumer confidence.

Industry initiatives

Whether it is a serious problem or merely a smokescreen for protectionism, India's outsourcing industry needs to proactively tackle this issue. Which is why the National Association for Software and Service Companies (NASSCOM) has been developing self-regulatory initiatives such as the 4E security framework (see box, left) as well as the announcement in August of a new security auditing project (see p.5).

A report commissioned by NASSCOM this year suggests that data security in India is being taken seriously. The study, carried out by consultancy firm Evaluserve, benchmarked Indian IT companies against UK and US security practices, concluding that "India offers a secure environment for providing offshore services". The study points to range of measures used to ensure good data protection management. The vast majority of top providers studied have dedicated information security teams, while around half comply with the BS 7799 security standard.

Legal shortcomings

Effective self-regulation can go a long way to reassuring consumers, but the crux of the problem remains the fact that India is at a disadvantage to competing countries with more robust data protection laws. Offshoring opponents wishing to stir up consumer fears need only point to the fact that personal data is being outsourced to a country with inadequate privacy laws, regardless of whether the outsourcing relationship satisfies domestic legal requirements.

While the media could be accused of playing on consumer privacy fears, India can score a significant PR victory by acting on its pledge to strengthen data protection controls. But with government promises dating back well over a year now, the question has to be when will this take place?

AUTHOR:

Alan Pedersen, Editor, *PL&B International*.

FURTHER READING:

Evaluserve's security report: www.nasscom.org/artdisplay.asp?cat_id=660