

# COVERING IT RISKS IN AN OUTSOURCED MILIEU

By: K C Mishra, Director

National Insurance academy, India

*Internationally, there are branded insurance products for customers exposed to IT data risk*

There is a natural warning to organisations which outsource their IT systems that they are increasing their potential vulnerability to security breaches, causing possible long-term damage to their business.

The Economist Intelligence Unit (EIU) has uncovered a lack of awareness among many European businesses of the increasing risks which outsourcing poses to their networks. EIU is also aware that there is a degree of uncertainty among many businesses, as far as the level of protection given to their computer systems and the cover provided by existing insurance policies are concerned. Businesses are not only dealing with their own employees but with those of a third party, often in another country. While technology is part of the solution, it alone cannot guarantee network security, particularly in an outsourced environment. Businesses must look at alternatives, including transferring the risks to insurers, in order to reduce the impact of technology failure, human error or criminal activity.

More than half of the European companies surveyed for information technology losses had suffered significant financial damage as a result of IT system failure or damage or misuse of systems by staff or contractors.

Outsourcing computer operations increases the risk of security breaches as the responsibility for protecting the system cannot be outsourced.

The National Outsourcing Association (NOA) of the US made allegations that staff in an Indian call centre had sold data on UK financial services customers. While the NOA said it was unaware of any trends in security flaws in this type of outsourcing practice, it did point out that security should be of concern to any company and that they must ensure that offshore operations are managed particularly carefully.

Internationally, there are branded insurance products for customers exposed to IT data risk. ACE insurance company is one of the

brand leaders in this field.

Dataguard Outsourcing Insurance has been specifically designed for companies, which outsource their IT systems.

It aims to fill the insurance gap, offering comprehensive protection against financial losses arising from malicious or accidental incidents to computer networks and telecommunications systems.

India is in a high growth league. Insurance needs are on the rise, but still the projections are miniscule compared to the top 14 OECD countries even for mid-term future. This is because Indian insurance has lagged behind the country's economy, though presently there is a catching-up effect. India must diversify its products in the areas signaling high growth and high risk. India is a favoured destination for business process outsourcing (BPO), so it can as well be a brand leader in 'Dataguard Outsourcing Insurance' type products.

There are three components to risk, as seen by insurers while assessing outsourcing risk of companies

1. Operational risk: Propensity of a process to break down in delivery or transfer
2. Strategic risk: Losses that result when the third-party behaves opportunistically.
3. Composite risk: Risk arising over time from a combination of factors like erosion of competence and loss of flexibility.

Insurers' product range will replicate the range of possibilities and risks sought to be covered within the possibilities. Indian insurers have started issuing sample products to cover sporadic IT risks, but such BPO risk products are yet to be marketed. Looking at global developments, inward reinsurance through the retrocession route may be a better route to gain initial experience by Indian insurers. It makes good business sense to harness the barometric opportunity of growth in BPO sector in India as also insurance required to cover BPO risks.