inotes Newsletter from India's Leading Insurance Broking House
November 05

Summary

India Insure The risk managers

Message from the Editor

Dear Readers,

Over the last 3 months, we have seen a series of natural disasters - the Mumbai floods, Hurricane Katrina, Hurricane Rita, the Pakistan-Earthquake and now Hurricane Wilma. As we go to press, Bangalore and Chennai are being buffeted by torrential rainfall. Losses on account of life and property have been substantial.

On the domestic insurance front, there has been an important development. IRDA has laid down a detailed road map for de-tariffing - all insurance products are expected to be de-tariffed by December 2006 and insurers have been asked to build internal systems and capabilities in preparation for the same. India is also about to witness the birth of the first stand-alone Health insurance company (licence in pipeline).

Meanwhile, we at India Insure have expanded our foot-print to 2 more branches - **Coimbatore and Baroda** - thus taking our total to 8 branches.

In this issue of *inotes*, we touch briefly upon **A**lternative **R**isk **T**ransfer (ART) Mechanisms - an idea whose time has *"almost"* come. As the Indian market is detariffed and integrated with world markets, ART will become a reality sooner than we imagine. In the "Product" section, we discuss crime insurance, a cover whose time ***has*** come, what with more and more instances of employee dishonesty in corporates large and small.

To end on a celebratory note, we wish all our readers a Sparkling Diwali, followed by a Happy Ramzan and Merry Christmas.

V Ramakrishna
Editor - ***inotes*** & Managing Director, India Insure

Alternative Risk Transfer – The new kid on the block

INTRODUCTION

To most business people, insurance is an "off the shelf" product. It comes in various flavours, colours and shapes, but it is neither customized nor negotiated. What is most worrisome about it is that, every now and then, it simply becomes either unavailable, or startlingly expensive, and it seems there's nothing much the buyer can do about it, either. But insurance doesn't have to be a *"take-it-or-leave it"* proposition. Insurance for business, especially, can be tailored precisely to the needs and capabilities of the insured. An insured who is willing to consider customized insurance programs, and to think intelligently about what he actually needs from his insurance, can look forward to better terms, better prices, and more useful coverage.

Further, across the globe, financial services are undergoing a major restructuring. A quiet revolution is taking place in the (re) insurance industry. In this volatile environment forward thinkers want more solutions. They demand a combination of ***risk transfer*** and ***financial engineering*** which addresses both sides of the balance sheet. Corporations want to meet market expectations too. At the same time they want to reduce their risk financing and capital financing costs. In a market beset by terror threats, economic uncertainty, and insurer instability, clients who once relied exclusively on traditional carriers are now asking: ***"What's the alternative?"***

For a growing number of agents, brokers, and commercial insureds, the answer to that question is "the alternative market."

WHAT IS ALTERNATIVE RISK TRANSFER (A R T)?

Alternative Risk Transfer (or ART) combines ***financing*** with ***insurance and risk transfer*** to protect a company from all types of risks, not just those which are traditionally covered by insurance or reinsurance. In simpler words, anything outside of traditional insurance or some combination of "risk transfer and self-insured retentions" is called **A R T**.

Born in the times of severe capacity constriction (mid-1980s), the alternative market offered clients a way to escape the volatility of the underwriting cycle, enjoy stable protection, and participate in both underwriting and investment profits The alternative market continues to grow not only in volume but also in creativity and flexibility. ART allows a company to dedicate its capital to its core business as they target solutions that are applicable across the company's entire risk spectrum.

ART is used to manage complex or difficult risk exposures, which are often uninsurable economically in the mainstream insurance market, and tends to be most successful for large, financially strong companies with a sophisticated approach to the financing of risk.

TECHNIQUES OF A R T

The best ART structures, (i.e. those that deliver the maximum value at the best price) involve a combination of conventional (re)insurance and broader ART techniques so as to affect optimal risk transfer at optimal pricing.

In recent years, the insurance sector has evolved, aided by the tide of rising insurance costs combined with reduced capacity. This has led many organizations to consider customized risk financing strategies as an alternative to traditional risk transfer techniques to allow them to better manage their risk. Financial support for ART transactions can come not just from traditional insurance sources, but also from commercial banks, swap markets, credit markets and institutional investors.

The solutions that are generally being adopted include, *wholly owned captives, rent-a-captives, risk-retention groups* and *other risk financing arrangements* that employ elements of self-insurance, finite risk, financial reinsurance, loss portfolio transfers, risk-finality solutions, new products and new markets and other integrated risk strategies. All of these solutions are customized to the specific needs of an organization and can be highly complex. Commonly used methods of ART include :

Captives: An insurance company owned and operated by the corporation it insures. Captive insurers are founded by and insure a substantial portion of the loss exposures of one or more of its major insureds.

Self-Insurance: Self-insurance is the retention and payment of loss obligations as they become due by an individual, partnership or corporation that retains all or part of its risk in-house.

Contd... # 3

Crime Insurance

As businesses embrace new technological developments, they become inadvertent hosts to advanced exposures and an entire set of new risks. Fraud involving computers is fast becoming a problem in today's technologically enhanced society. Couple that with issues such as job insecurity and reduced company loyalty and we have an environment that increases the probability of an employee being dishonest.

Weaknesses in internal controls are the major contributing factor to the opportunity to commit crime in the workplace. Collusion between employees and third parties is the second most common element that allows fraud to thrive, followed by the type of industry involved. Retail and financial services sectors acknowledge that employee fraud is an inherent part of their business.

Whilst stringent internal controls and sound administrative and management practices help limit exposures, they can never eradicate the risk completely. Warning signs may be missed or not acted upon in time. Areas of greater risk may not be identified until too late. Contingency plans put in place to respond quickly to the discovery of fraud may not have been communicated effectively to all staff. Whilst internal "whistle-blowing" may be regarded as an effective tool in combating fraud, not every organization has a corresponding "no-blame" culture to promote this practice. The opportunity to commit fraud is there for everyone. Fraud and embezzlement in the workplace are on the rise, occurring in even the best work environments.

Companies are estimated to lose 1-2% of their revenues annually on an average on Fraud and the cost of fraud comes straight off from their bottom lines. The losses caused by fraud are on the rise and are more prevalent than ever before. These frauds can go on for years, and when discovered the ultimate impact can be enormous!

WHAT IS 'CRIME'?

Typical losses under a crime policy include

- **Theft by employees including direct theft of cash or any asset of the business** – eg: claiming false expenses or payroll fraud.
- **Collusion between employee and a third party** eg: receiving bribes or commissions from a supplier as a reward for awarding the contract to that supplier. Related party transactions such as the failure of an employee to disclose his/her financial interest in a transaction.
- **Computer Fraud** such as diverting funds from one bank account to another, stealing intellectual property, holding out to be legitimate business on the internet and obtaining payment for goods or services.

WHAT DOES CRIME INSURANCE COVER?

Fidelity or a wider form of Fidelity – Commercial Crime policies are now becoming increasingly popular amongst the Industry in view of 2 fold requirements – contractually imposed Insurance requirements by customers and the high cost and probability of indemnifying customers for consequential claims / losses.

What is typically covered?

- Employee Theft Coverage - Loss of Money, Securities or other property caused by Theft or forgery by any Employee of Insured acting alone or in collusion with others.
- Premises Coverage - Losses caused by the actual destruction, disappearance, wrongful abstraction or Computer Theft of Money or Securities within or from the Premises by third parties.
- Transit Coverage - Losses caused by the actual destruction, disappearance or wrongful abstraction of Money or Securities outside the Premises, while being conveyed by the Insured/ duly authorized Employee.
- Depositor's Forgery Coverage - Losses caused by forgery or alteration of, on or in any cheque etc, made or drawn by, or drawn upon the Insured or his agent.
- Computer Fraud Coverage - Losses caused by computer fraud committed by a third party
- Third Party Crime or Employee Dishonesty Cover – Losses caused to Third party due to acts of own employees.

COMMON EXCLUSIONS UNDER THE POLICY

- Losses caused or contributed to by the theft or fraud of the Insured's partner.
- Fees or expenses in prosecuting or defending any legal proceedings.
- Loss unless reported in accordance with the provision of the policy regarding notification of loss.
- Loss discovered prior to the inception date of the policy
- Consequential loss
- Fines and penalties and other uninsurable matters
- Non-payment of loan (financial institutions)
- Acts committed by Employees with known criminal record
- Loss of Intellectual Property

WHO WOULD REQUIRE CRIME INSURANCE?

Technological advances have drastically altered the speed with which financial transactions and fraud can occur. This is more so now with the increased reliance on computers.

The recent spate of frauds or reports of alleged frauds in BPO companies is compelling one to re-look at their Internal controls and vulnerability to employee frauds. Coupled with this is the insistence of customers for maintaining adequate Insurance covers to address these problems and thereby include employee wrong doings within their Insurance program.

Any business employer needs to be concerned with Employee Dishonesty or any business handling cash or securities needs protection from robbery or theft will need Fidelity/Crime Insurance. As Cyber-crime is becoming an increasing concern it would be advisable for Software / BPO industries to opt for this cover.

HOW ARE CRIME POLICIES MARKETED IN INDIA?

Commercial Crime covers are now being offered by few Private players based on International forms. These covers are much wider than the Indian Market Agreement Fidelity Guarantee Cover. Various kinds of covers are offered by companies. To these, covers like Employee Dishonesty or Third Party Crime extension is to be added to provide seamless protection for all First and Third party losses caused by employee frauds.

Contd... # 3

Alternative Risk Transfer..... Contd. from # 01

Risk Retention / Purchasing Group : A Risk Retention Group (RRG) is a corporation or other limited liability association, functioning as a captive insurance company and organized for the primary purpose of assuming and spreading the liability risk exposure of its group members. A Purchasing Group (PG) is an organization which purchases liability insurance on a group basis from an insurance company or from an RRG for its member.

Pools : Pools are arrangements between corporations or insurers to mobilize sufficient capacity for very large risks. Pools are typically organized on a national basis to cover a specific risk class.

Capital Market : Alternate risk management via capital markets is the concept of buying insurance protection directly from capital markets.

New Products: These products are designed specifically to meet the needs of the customers, they are typically multiyear contracts that assist the customer in reducing their cost of capital via earnings. Finite risk products are long-term solutions that, by their nature, reduce the year-to-year volatility normally associated with a commercial insurance policy.

Insurance-Linked Securities (Cat Bonds): These products were developed specifically to offset the decrease in insurance capacity. They are designed to assist insurers and corporations in transferring catastrophic risks (wind, flood and earthquake) to the capital market via a bond issue. Typically, these products come about as a result of a bond being issued, and the proceeds being invested. Bondholders then receive interest payments and the principal repayment over the life of the bond. However, should the issuer suffer a catastrophic loss, both the interest and principal could be used to pay the loss. While many believed that the hard market would accelerate the use of CAT bonds, utilization has been modest over the past few years. However, as the transactional costs decline and the acceptance of these products increases, usage is expected to grow.

Weather Derivatives: Energy companies needed to find ways to mitigate the significant earnings volatility that was usually associated with changes in weather. Weather derivatives, introduced in 1997, have since expanded beyond the energy industry.

Credit Securitization: Typically, these products involve a portfolio of loans, bonds, or other credit assets. By bundling these assets together, they can be structured as a single portfolio with many layers, each with its own credit rating. The major advantage of these products is that bundling these risks diversifies the credit risk across single companies, industries and geographic locations, thereby becoming more attractive to the capital markets.

'A R T' IN THE WEST vis-à-vis ASIAN/ INDIAN MARKET

While ART has taken root pretty strongly in the US etc, where it is estimated that about 50% of commercial property/casualty premium volume now resides in the alternative market; in Asia, however, it is still is in its infancy, except, possibly, Japan where some ART products have been successfully issued, including Tokio Marine's EQ bonds, Yasuda's typhoon bonds, Mitsui's earthquake swaps and Tokyo's Disneyland earthquake bonds.

Inadequate understanding of ART and lack of professional ART underwriting expertise could be the key inhibitive factors to growth of ART in Asia. Some of the countries in the region (eg: Singapore), have taken steps to create a favorable regime for ART. In India, the absence of facilitating regulation and the lack of expertise have prevented the growth of ART.

SCOPE FOR 'A R T' IN THE INDIAN MARKET

Frankly, the issue is not 'whether' there is scope for ART in the Indian market, but 'when' will we see the growth of ART in India. We may not realise it, but ART is already in operation in India in a big way. The 'Terrorism Pool' created by GIC post- 9/11 is one such example. Large chunks of Government property and business (Railways, Postal, Defence etc) use the ART technique of 'Self-Insurance'.

Where there are large corporations with hefty premium bills and favourable loss ratios (ideal for '**Captives**' or '**Self-insurance**'), or homogeneous groups of companies sharing a similar risk profile (ideal for starting a "**Risk retention group**"), or a well-informed investing public with surplus-cash ready to share the risks (for **C A T Bonds** and the like), ART products are expected to have a market. India has all of the above and more.

Perhaps, if regulations permit and give it a bit of thrust, we will see an active ART market in India soon. After all who would have believed, just 3 years ago, that the Derivatives market would grow so strongly and the pink papers would devote a full-page to F&O quotes every day?

So, remember, the next time you hear the word "ART", don't automatically assume it is MF Husain being discussed – there's a different ART coming soon to your neighbourhood.

Crime Insurance ..... Contd. from # 02

SOME EXAMPLES OF CLAIMS:

- Two employees are accused of issuing cheques payable to vendors and diverting them. The employees then gave the cheques to a senior vice president of a local bank, who caused them to be fraudulently endorsed. The funds were then distributed to the conspirators through a dummy bank account. The loss was approximately $1,000,000.
- Two ticket agents in one of the Insured's regional offices were accused of causing the Insured to sustain a loss through a variety of schemes, including: converting funds paid by passengers for tickets, issuing fraudulent frequent flyer tickets, and exchanging tickets and converting the resulting fees for their own benefit. The claim amount exceeded $2,000,000.
- Four employees of a construction contractor conspired with three non-employees to submit fake invoices for goods and services not supplied to the Insured. The amount of the claim is approximately $600,000.

A WORD OF CAUTION

The policy is presently marketed by various Insurers. However, the coverages vary to a great extent between each insurer and would require be discussed before the final placement is made.

Risk Management - *E-mail Liability*

Most businesses today have some electronic mail (e-mail) capability; and most find it to be an extremely efficient way to communicate. However, users and managers should be aware of potential risk management issues concerning the use, storage, and deletion of electronic mail messages and other forms of electronic communications. Electronic communications are of concern in the areas of employment practices, personal privacy, and many forms of litigation.

Legitimate Reasons for Monitoring Electronic Communications

Employers have legitimate reasons for monitoring electronic communications, including:

- Monitoring employee performance
- Detecting employee misconduct
- Reducing liability arising from employee acts

Monitoring Employee Performance

Employers may monitor employee performance to determine productivity, quality of work, and customer satisfaction. For example, if you call your bank to inquire about your balance, you may hear a message that states that the call may be recorded for quality control purposes.

Detecting Employee Misconduct

Employers may monitor electronic communication to detect employee misconduct such as gambling or improper disclosure of company information. If the employer were not permitted to monitor electronic communications for this purpose, employees could share company secrets simply by sending e-mail.

Reducing Liability Arising From Employee Acts

Employees can place the company at risk from liability in a number of ways such as downloading illegal or sexually offensive materials from the Internet, making inaccurate or untrue products claims, or engaging in illegal activities via a computer or other electronic communication devices.

Policies for Business Use of Electronic Communications

Policies that cover employee use of e-mail, voice mail, the Internet, and other forms of electronic communications should include, but not necessarily be limited to, the following:

1. The policy should include statements that indicate that:
   - Employees' use of e-mail, voice mail, Internet access, and other forms of electronic communication are subject to management review. This will reduce employees' expectation of privacy with regard to electronic communications.
   - Employees' use of electronic communications is limited solely to legitimate business purposes.
   - Although the company may provide for individual passwords, the passwords can and may be overridden by the company and its authorized personnel.
   - Employees who violate the company policies and procedures related to electronic communications are subject to disciplinary action, up to and including termination of employment.
2. The policy should include statements that prohibit:
   - The use of electronic communications that is contrary to state/ federal/local laws.
   - Inappropriate messages and information. This would include telling offensive jokes and the distribution of other offensive materials, pictures, etc.
   - Any use of electronic communications that could damage the company's/organization's reputation or put it at risk for legal action.
   - Distribution via electronic communications of company proprietary information.
   - The use of others' passwords or the accessing others' messages, except by authorized personnel for legitimate business purposes.
3. The policy should be published as part of the company policies and procedures and in employee handbooks.
4. Employees should be required to sign off that they have read and understood the policy. Sign off statements should be kept on file.

Tips to Stay Out of Trouble

Legally archived or deleted messages can be acquired by a court of law or government agency in regard to antitrust, discrimination, termination, or copyright infringement investigations.

- E-mail is not the place for discussing sensitive issues, such as suspicions, employee performance, hiring, or firing. If you do use this venue for such issues, always consider it a formal and permanent form of communication.
- Stating a negative opinion or feeling about an employee while using e-mail lends merit in a legal proceeding related to discrimination or termination.
- Prosecuting attorneys count on the fact that your e-mail archives will be ripe with incriminating information. They want you to be careless with your e-mail; disappoint them.
- Certain comments, suggestions and even graphics delivered by e-mail to others can give merit to a harassment claim.
- Be careful what you write about others. You can't control who will read your documents.
- Downloading and viewing graphics that are personal in nature are not appropriate at work.
- Common sense will usually tell you what you should or should not do. If you even wonder if something is inappropriate - don't do it.

Conclusion

Employers must develop programs to address the liability risks associated with electronic communications. Employers have legitimate reasons for monitoring electronic communications, including monitoring employee performance, detecting employee misconduct, and reducing the potential liability arising from employee acts. Such monitoring is permitted as long as employees give prior consent and there is no expectation of privacy. The program should be disseminated to all employees. Training should be provided, with appropriate employee sign-off Legal review of the program policies and procedures and periodic updating is critically important to reduce the exposures in this area.

Disclaimer

Contact us

India Insure Risk Management Services Pvt. Ltd.

Bangalore
13, 3rd Floor, Mother Theresa Road,1st Stage, Austin Town,
Bangalore - 560047. Phone: 080 - 51128056 - 58 Fax: 080 - 51128597
Contact: Mr. Anurag Bishnoi email: anurag.bishnoi@indiainsure.com

Baroda
315, Race Course Tower, Nr. Natubhai Circle, opp. Citi Bank, Gotri Road.
Baroda - 390007. Tele Fax : 0265-2352031, Mobile : 09898566579
Contact : Mr. Deepak Kwatra email : deepak.kwatra@indiainsure.com

Chennai
Sri Valli Griha, Flat GA, Ground Floor, New # 34, (Old # 26), Raman Street ,
T Nagar, Chennai-600 017. Ph: 044-5202 3797/98 Fax: 044-52023799
Contact: Mr. Vippin Chandra email: vippin.chandra@indiainsure.com

Coimbatore
58/1, 2nd Floor, Dr. D R Karunanidhi's Building, Sengupta Street, Ramnagar,
Coimbatore - 641 009. Ph : 0422-5380939, Fax : 0422-5380539
Contact : Mr. Roy Maller email: roy.maller@indiainsure.com

Hyderabad
405, Archana Arcade, St John's Road, Secunderabad - 500025
Ph: 040-27822989/90/91, Fax: 040-27822993
Contact: Mr. M. Vijay Chowdary email: vijay.chowdary@indiainsure.com

Mumbai
Branch & Corporate Office : # 427/428 Chintamani Plaza Chakala, Andheri-Kurla Road,
Andheri (East) Mumbai - 400 093. Ph: 022-56791416-20, Fax: 022-56791421
Contact: Mr. V. Ramakrishna email: ramakrishna.v@indiainsure.com

New Delhi
A-70, Sector-2, Noida NCR, Dist. : Gautam Budh Nagar (UP) - 201 301
Ph : 011-51520666, Fax : 011-51520667
Contact: Mr. Anuraag Kaul email: anuraag.kaul@indiainsure.com

Pune
101, Premium Point, Opp. Modern High School, J.M. Road,
Shivajinagar, Pune - 411005, Tele Fax: 020-56030713
Contact: Ms. Deepali.A.Rao email : deepali.rao@indiainsure.com