August 2017
Issue 122

FIRST ON
PROTECTION

J. B. BODA
MEDIAN

CONTENTS	PAGE NOS.

NEWS AT JBB

FICCI launched ATA Carnet Insurance Policy for StartUps & SMEs today at the Trident Hotel, Mumbai. Seen (L-R) – Mr. Nirankar Saxena, Assistant Secretary General, FICCI; Mr. Henk Wit, Deputy Chairman, World ATA Carnet Council (WATAC) ICC Paris; Mr. Vinay Mathur, Deputy Secretary General, FICCI; Mr. G Srinivasan, Chairman cum Managing Director, The New India Assurance Co. Limited; Mr. Atul D Boda, Chairman, JB Boda Group; Mr. P S Pruthi, Former Member Customs Excise & Service Tax Appellate Tribunal (CESTAT); and Mr. C R Vaidya, Senior Executive Director, JB Boda Reinsurance Brokers Pvt. Limited, Mumbai

J B Boda is currently passing through *74th glorious year* of its incorporation. The Group holds prestigious record to have been accredited as the 1st Indian Broker affiliated with Lloyds of London, the only insurance broker for ISRO Satellite Launch programme, leading correspondent for Protection & Indemnity Clubs in India and so on…

The year 2017 has awarded another feather in the cap. India's prestigious business body, Federation of Indian Chambers of Commerce & Industry (FICCI) expressed desire to have ATA Carnet Insurance cover for the Indian exporters, exhibitors & people engaged in Cinematography / Photography who visit abroad with their goods for a temporary period and comes back with material carried with them once their purpose is over. There is an international convention between World Custom Organisation (WCO) and World ATA Carnet Council under which the visiting person to other member country will not require to pay duty there if company / individual is holding ATA Carnet Certificate. FICCI is sole authorised Indian body to issue ATA Carnet Certificate. For obtaining ATA Carnet Certificate the overseas traveller needs to provide Bank Guarantee or Cash Deposit to FICCI to the extent of applicable duty in the visiting country. Out of 77 signatory countries for the WATAC Convention there are 36 countries where ATA Carnet Insurance is available. BG/CD requirement can be replaced by ATA Carnet Insurance.

ATA Carnet Insurance was not available in India till date. FICCI approached J B Boda in January 2015 for arranging ATA Carnet Insurance for the Indian market. We have been working with FICCI, J B Boda London office, Lloyds markets and Lloyds broker M/s. Besso Limited to introduce this product in India. After continuous negotiations, the product design and RI support was arranged and we approached India's flag insurance company The New India Assurance Co. Ltd. to issue the local policy with Reinsurance support arranged by J. B. Boda.

Finally the ***product was launched on 19th July, 2017 (cover effective from 1st August, 2017) by New India Chairman Mr. G Srinivasan and our Group Chairman Mr. Atul Boda in the presence of senior dignitaries*** from FICCI, New India, J B Boda and members from business community as listed above.

ON "WRITE" SIDE

PRA challenges firms on silent Cyber risk

Insurance firms need to act on cyber risk

The Prudential Regulation Authority (PRA) is proposing and a new supervisory statement (SS) setting out its expectations for the prudent management of cyber underwriting risk in a new consultation paper.

This is the result of thematic work undertaken by the PRA between October 2015 and June 2016 with firms across the insurance sector, including insurance and reinsurance firms, (re)insurance intermediaries, consultancies, catastrophe modelling vendors, cyber security and technology firms, and regulators.

The work focused on the underwriting risks emanating both from affirmative cyber insurance policies (eg data breach products), but significantly also across the cyber exposure within 'all risks' and other liability insurance policies that have not excluded cyber risk. The PRA's work found an almost universal exposure to cyber losses in what it terms as the 'silent cyber risk'.

The results show that firms do not currently have clear strategies and risk appetites for managing cyber risk, both affirmative and 'silent'. Despite cyber insurance being a key area of growth and risk, boards do not own the overall strategy around cyber risk and in a number of cases a clear strategy, supported by risk appetite statements, does not exist. This includes, but is not limited to, defining target industries to focus on, managing 'silent' cyber risk, specifying rules for line sizes, aggregate limits for geographies and industries and splits between direct and reinsurance.

In his letter to Insurance industry CEO's PRA Director, Chris Moulder announced that the PRA was taking action and set out the proposals for a new Supervisory Statement to detail the expectations of firms through a Consultation Paper (CP). Firms were asked to comment on the proposals by 14 February 2017.

Summary of PRA Concerns

1. 'Silent' cyber risk is material: The PRA's work found an almost universal acknowledgement of the loss potential of cyber exposures endemic in 'silent cyber'. However, most firms did not demonstrate robust methods for quantifying and managing 'silent' cyber risk.

2. 'Silent' cyber loss potential increases with time: The potential for a significant 'silent' cyber insurance loss is increasing with time. As both 'silent' cyber insurance awareness and the frequency of cyber-attacks grow, so does the loss potential from 'silent' cyber exposures. Insurance firms may find it increasingly challenging to argue that all risks or other liability policies did not intend to cover this type of risk given the publicity and awareness of the issue.

3. Casualty (direct and facultative) lines potentially significantly exposed to 'silent' cyber: Casualty lines are potentially significantly exposed to silent cyber losses. This is either due to the fact that exclusions are not widely used or because some policies cannot reasonably exclude cyber losses. An example of the latter is Directors and Officers (D&O) policies. There is wide acceptance in the market that these policies are potentially exposed and should therefore respond to cyber claims. This is due to the nature of the D&O products, covering the broad range of risks Directors and Officers are exposed to. The PRA's findings also suggest that professional indemnity (PI), financial institutions (FI) and general liability (GL) products are also likely to be exposed to various degrees to 'silent' risks due to a lack of use of effective exclusions.

4. Potential for 'silent' losses in marine, aviation, transport (MAT) and property lines: The PRA's thematic work showed that aviation underwriters are comfortable providing implicit cyber coverage (i.e. no exclusions are used currently) despite a background of continuous technological advances in aviation electronics, arguing that the risk is zero or minimal, which is concerning. The same holds true for motor despite the developments in autonomous vehicles and questions in relation to their cyber security. Property underwriters acknowledged the potential for cyber aggregation resulting for example from cyber-attacks on high-profile commercial or industrial targets, or from smart-house technology. Despite that, there are currently no widespread exclusions for cyber risk and the thinking around how to price or manage this risk does not appear to the PRA to have developed sufficiently.

5. The exposure and response of reinsurance contracts is uncertain: The PRA's work showed that reinsurers are aware of the potential aggregations resulting from 'silent' cyber and are looking to address this in future contracts. Currently, there is no widespread use of exclusion in either property or casualty reinsurance contracts. The PRA's work has not clearly demonstrated that this element is actively priced in to reinsurance contracts or managed otherwise. The PRA's discussions with key stakeholders suggest that where wordings exist to address the issue, these are bespoke and were introduced only recently. Given these wordings are not universally accepted and untested in time they may result in disputes should a cyber claim arise.

6. Most firms lack clear strategies and risk appetites: The PRA's work has shown that firms do not currently have clear strategies and risk appetites for managing cyber risk both affirmative and 'silent'. Despite cyber insurance being a key area of growth and risk, boards do not own the overall strategy around cyber risk and in a number of cases a clear strategy, supported by risk appetite statements, does not exist. This includes, but is not limited to, defining target industries to focus on, managing 'silent' cyber risk, specifying rules for line sizes, aggregate limits for geographies and industries and splits between direct and reinsurance.

7. Firm investment in developing cyber expertise is insufficient: There is currently insufficient investment from firms in developing their internal knowledge and expertise on both the affirmative and 'silent' cyber risk elements. This is due to a combination of: a) the early stage of development of their cyber offering; and b) the lack of supply of skilled professionals with cyber underwriting expertise. The PRA's work has also identified that growth aspirations in affirmative cyber are seldom accompanied by a commensurate investment in underlying expertise and talent.

8. Affirmative cover risks are not well understood: The PRA's work suggests that firms do not understand sufficiently the aggregation and tail potential of affirmative cyber cover. The advent of the cloud and the continuous evolving nature of the cyber landscape create significant challenges that potentially are unique to this line of business. Firms are limited by a lack of expertise and an insufficient length of claims data. Moreover, using past claims data to estimate future cyber losses may not be appropriate due to data being non-stationary.

9. Risk management's ability to challenge is limited: Risk management teams are often not adequately equipped - in terms of skills and expertise - to provide effective challenge to the business. In most cases, risk management input is limited to either developing simple deterministic scenarios or reviewing and adapting widely publicised work on the topic. This is concerning given the continuously developing nature of cyber risk and the importance of risk management as the second line of defence.

10. Third-party vendor models at early stages of development: The main catastrophe modelling vendors have expressed their commitment to developing fully probabilistic cyber catastrophe models. However, development is at an early stage and it may take a few years before the first versions are available. Catastrophe modelling vendors have developed small sets of deterministic cyber scenarios to assist their clients in managing aggregation, and data schemas have been developed for categorising cyber exposures. Although these are helpful steps, it is the PRA's view that the market has much work to do before it can capture and manage cyber exposures effectively.

11. EU Data Directive will increase affirmative cyber exposures: The implementation of the new Data Protection Directive in 2018 will strengthen the European regulatory framework on personal data. So far, firms have expanded their affirmative cyber coverage portfolios mainly in the United States. However, the forthcoming introduction of the Directive has seen a number of firms looking to expand their offering to Europe as well. Any perceived geographic diversification benefits for insurers could be offset by an increase in cyber risk aggregation potential.

NATIONAL

IBM's research lab may help farm sector in India with Watson cognitive technology

IBM's India research lab is looking at ways of using its Watson cognitive technology to help farmers determine potential crop yields and protect against pests, an effort that could increase the use of such data in farmer loans and insurance. The India research lab counts agri-business as one of the three industries it focuses on in India. The technology — part of a solution called Precision Agriculture — involves the use of a few strategically placed sensors and remote sensing data from satellites to answer questions about the state of the soil, moisture content, weather data and susceptibility to pests. "Blanketing a farm with sensors is extremely expensive and hard to manage. But data from a small amount of local sensors and data from satellites can be married using cognitive technologies — a process called cognitive fusion. We can answer those questions in a cost-effective way," director of India Research Labs, said. Cost is of great importance in a country like India, where farms are small and organised farming of large plots of land is still rare. IBM is looking at large agri-businesses and financial institutions as its potential market.

Agri-businesses has the ability to invest in technology and have an interest in increasing productivity even if the farms are run by individual farmers. The other model is to look at financial institutions. There has been a lot of issues with agri insurance and credit and while there are definite non-technology issues to be solved, there is an opportunity for technology to help provide better visibility to financial institutions. With the technology, the financial products issued in the agri space need not be driven just by the credit history of a farmer, which may not be a viable model, but can be driven by knowledge of the farm and focus on health on the farm which will increase risk awareness. The company is also using its cognitive technology to help farmers identify pest infestation earlier and in working out supply chains and grain storage.

Importance of home insurance today

Home insurance is an under-purchased product in India. This is in spite of the fact that there has been a significant surge in the number of home buyers in the country over the past few years. There is an apprehension that home insurance policy comes with high premiums and complex processes. However the reality is that people lack sufficient information about the product. Given the uncertain times we live in, home insurance is the need of the hour.

Here are several reasons why purchasing a home insurance policy is a must

To recover from natural and man-made disasters : A home insurance policy provides financial protection in case your house is damaged due to natural or man-made calamities like floods, earthquakes, fires or vandalism. For instance, floods in Chennai, cyclone in Andhra Pradesh and cloudburst in Uttarakhand caused massive destruction. This should serve as a warning sign for the need to have adequate safeguards for your house.

Compensates for the loss/ damage to your assets and personal belongings : Home insurance covers not just the structure of your house but also the personal belongings. This includes jewellery, electronic appliances, furniture, luxury and antique items etc. Thus in case of burglary or accidental damage, you can rest assured that you have a back-up plan.

Covers temporary living expenses : Your home insurance policy will take care of the expenses if you need to rent another house or move into a hotel temporarily, until your home is repaired/ rebuilt. This will help you to be independent and recover from any eventuality.

Provides aid in availing home loan from financial institutions : Some banks have a pre-requisite of providing home loan only if your house is insured. In fact, home insurance is a preliminary requirement to be eligible for a home loan in a lot of cases.

Premiums for home insurance for a sum assured of Rs 10 lakh for 10 years could be as low as Rs 2,400 for a structure only cover. Depending on the items in the house that are covered premiums will slightly vary.

To conclude, home insurance is an important precautionary measure that you should definitely invest in. Make sure that you are not under insured, by declaring the value of assets accurately so as to derive the right sum insured figure.

Also it is important to understand the terms and conditions of a home insurance policy and ensure that you check the policy every three to five years as the cost of reconstructing a house is bound to appreciate, due to inflation. If you keep these points in mind, you will not think twice before opting for your home insurance policy.

48% of parents fund schooling from insurance/savings

Around half (48%) of Indian parents fund their child's education from general savings, investments or insurance, says a report. More than half (59%) of Indian parents fund their child's schooling from day-to-day income, and almost a third (30%) get the money through a specific education savings or investment plan.

About 89% of Indians fund their child's education. They are spending an average of US$18,909 on their child's education. The parents make an average spending of $8,552 on elementary education, $4,264 on secondary education and $6,093 on university undergraduate education, says the report.

Many parents are making financial sacrifices, with 89% willing to do so. Sacrifices include reducing spending on leisure activities, working extra hours in jobs and contributing less to their own long-term savings.

Over nine in 10 (94%) parents want their children to undertake postgraduate studies, and of this number, 79% expect to contribute towards funding that too.

Impact of Major Cyber-attacks Across the Globe

Cyber-attacks have become a lucrative money-making business for criminals, inviting smarter, more sophisticated hackers to launch advanced and complex attacks on organizations. Modern times demand that almost all of companies' information, be it financial, process-related, customer or intellectual property, stored digitally on their network and be accessible from various locations. This makes the security of this data, vulnerable. In certain cases, all this information is stored on a cloud which is outside organization's firewall thereby adding higher risk to crucial data.

With advancements in cyber-attacks, the associated costs, which include direct losses and cost of recuperating from an attack, have also grown exponentially. To gauge the scale of losses let us look at some of the recent attacks and their impact on the organizations.

Titan Rain: The attack on U.S military networks including those of NASA and Lockheed Martin, led to the theft of classified data and weapons research data. While it's hard to quantify the effect, but the impact of this theft on national security is huge.

TJ Maxx: TJ Maxx, a retailing company was a victim of a cyber-attack in 2006. The cyber criminals breached the network and stole 45 million credit and debit card information. The total damages were to the tune of 250 million dollars.

Heartland Payment System: In 2008, this company's payment network was injected with a spyware and millions of credit and debit card details were stolen. This attack cost the company about 140 million dollars in damages.

Bangladesh Bank Hacks: In February 2016, a bank officer's computer was used to siphon off 81 million dollars of Bank's money. The interesting thing here was that it was a single computer inside the bank's network that was hacked to siphon off the money.

Ashley Madison: In 2015, Ashley Madison, a dating website, was hacked and data of millions of users from many countries was stolen. The company faced a 560 million USD class action lawsuit from its users. But the real cost in terms of lost credibility and humiliation of its users (and two unconfirmed suicides linked to this hack) cannot be measured in dollars.

Talk Talk Hack: In 2015, the British telecommunications company Talk Talk lost more than 100,000 customers and 60 million British Pounds (About 90 million USD at that time) as a result of this hack. This ransomware attack is still fresh and businesses are still recouping and assessing its impact. It was one of the largest global cyber-attacks, affecting more than 150 countries simultaneously. The total cost of this attack is estimated to reach 4 billion USD.

A few years ago, Wall Street reported that the total cost of cyber-crimes in the US alone was over 100 billion USD. In 2015, A British insurance company Lloyd's estimated that the cost of cyber-attacks to business was nearly 400 billion USD. The cyber-crimes are increasing at such a staggering pace that Juniper Research estimates that by 2019, cyber-crimes would cost businesses more than ***2 Trillion USD.***

It is observed that even big companies with huge IT and security budgets are not safe from cyber-attacks. Cyber security is not just a matter of installing firewalls and antivirus anymore. Every endpoint in the organization, be it an open network port or a computer and a USB drive on a laptop that can be used to access data needs to be secured and protected. Full access to the data must be limited to the authorized users only. The data can be transferred (via email, or FTP or any other mode of transfer) only if the user is authorized to transfer and that too by using a particular mode.

IRDAI issues new norms for mediclaim policies

Many customers only realise at the time of making a claim that their health insurance policy does not cover certain medical conditions or ailment. Policy holders usually depend on what has been told to them by their insurance agents, who sometimes overstate the coverage. To prevent such cases, the Insurance Regulatory and Development Authority of India (IRDAI) has asked insurers to group together all policy exclusions upfront in the policy document. Misselling is a huge problem for the insurance industry as, of 1.72 lakh complaints in 2016-17, about 50% related to unfair business practices, according to IRDAI's consumer booklet 2016-17. Many a times, exclusions are lost in a maze of fine print. But the IRDAI has now said that the terms and conditions for claims, renewals have to be bifurcated. So that customers exactly know the coverage limits of their policy. Another change with the new regulation is the introduction of penal interest. If customer is not paid the claim within 90 days of reporting, the insurer has to pay the bank rate + 2% interest for every day of further delay.

INTERNATIONAL

GCC: Insurers warming up to debt instruments

Debt instruments have slowly been gaining acceptance in the Middle East insurance sector which has traditionally been underweight in debt since a significant portion of the investment portfolio consists of high-risk high-growth assets such as real estate and equities.

Underpinning the appeal of the debt market for insurers are the high-grade instruments now available but which the region lacked before the oil price decline that began in 2014.

Several market participants are predicting a spike in bond issuances — both conventional and sukuk (*Islamic bonds, structured in such a way as to generate returns to investors without infringing Islamic law – prohibiting interest*), as regional governments seek financing to reduce fiscal deficits. For instance, Saudi Arabia alone raised a total of $26 billion through the international sale of conventional bonds and sukuk in the past nine months. As the region rolls out ambitious plans to wean the economies off their dependence on oil, other GCC states such as the UAE, Kuwait and Oman have all issued sovereign bonds in the past few months.

Currently valued at approximately $300 billion, according to a recent report, the GCC bond market will continue to evolve and attract investors, primarily driven by the high yields these bonds offer.

Providing further cause for optimism is the regulatory environment, particularly in the UAE, that has evolved in the past couple of years, encouraging insurers to improve exposure to the debt market. The regulations that enforce limitations on exposure to a single asset class would undoubtedly benefit both insurers and consumers in the longer term. More specifically, these regulations are widely expected to bolster governance, compliance and risk management, simplified product structures, and international-standard regulations, among others.

Australia: Reinsurance pool eyes cyber terrorism cover

Cyber terrorism will be on the agenda of the government terrorism reinsurance agency, the Australian Reinsurance Pool Corporation (ARPC), as part of its tri-annual review.

Cyber terrorism has been in discussion in the market. But it is something that’s not currently covered by the scheme.

ARPC, the statutory government body dealing with terrorism-related insurance claims and protection, says cyber terrorism is the biggest black hole in the insurer’s framework, and it is an increasing threat.

ARPC provides back-up insurance coverage that cover major commercial and infrastructure assets in Australia. The companies must have deductibles of between A$100,000 and A$10 million per insurance contract before they can turn to the ARPC for back-up insurance for claims above these levels if an event is declared a terrorist event under the legislation.

July renewals see continued downward pricing

The reinsurance market has maintained the downward pricing trends seen at the January and April 2017 renewals, despite first quarter deterioration for many reinsurers' results. The report found that the continued softening has been driven by the realization that, for the global reinsurance industry, the June and July renewal seasons were said to be the last realistic chance for underwriters to meet their 2017 premium targets.

It was clearly seen in the Florida renewals, the report said, where, in the face of flat demand, a larger than anticipated influx of capacity, particularly from Insurance Linked Securities (ILS) markets, led to not only a further drop in pricing from the 2016 renewals but at a greater pace, albeit slight, than the reductions seen on U.S. property catastrophe programs earlier this year.

Rate reductions across most lines in international markets followed the improving trend seen in January and April renewals with a strong demand from ILS investors, the report said, where ILS markets' pricing is now matching or, in a few selected cases, more competitive than traditional reinsurers.

The report said underlying loss and expense ratios for many reinsurers are showing a worrying trend, with combined ratios for many classes now looking unattractive, according to the report.

Underlying loss and expense ratios for many reinsurers are showing a disturbing trend, the report said, with combined ratios for many classes now looking unattractive.
Cost control measures are being applied widely and more aggressively across the entire reinsurance chain as a result stubbornly soft pricing, the report said.

Market initiatives to contain and reduce costs, such as the London market Placing Platform Limited (PPL) initiative, are seeing increased impetus and support as the importance of the promise of greater efficiency is recognized.

Yet again, the weakening position in the global reinsurance industry's performance has not reached an unacceptable level. Reinsurers across the board do not yet feel compelled to take a stronger stance over conceding further modest rate reductions and walking away from clients. Much now will depend on loss activity in the traditionally more active third and fourth quarters and on any instability in investment returns.

The report said the recent WannaCry cyber-attack, which reportedly infected more than 230,000 computers in over 150 countries, shined a bright light on the future potential for the cyber reinsurance market but the longstanding puzzle of understanding and managing systemic cyber risk accumulation remains unsolved, despite the substantial ongoing efforts by many market participants.

The goal of developing the cyber reinsurance market to sufficient scale so that it can help absorb the excess capital currently supporting the reinsurance industry remains some way off but, with an appropriate understanding of risk, it is ultimately achievable, the report said.

Japan: Sales of cyber policies more than triple

Three major nonlife insurance companies saw sales of cyberattack policies more than triple to over 1,000 clients combined in the financial year ended March 2017 (FY2016). Demand for cyberattack insurance, which covers losses caused by damaged computer systems, is surging as cybersecurity concerns spread to small and midsize firms, reported Kyodo News Agency.

The Japan Network Security Association said the cyberattack insurance market is expected to grow to JPY15.6 billion in the year ending next March. Nonlife insurers saw interest swell after a ransomware attack struck companies in at least 150 countries in mid-May, the Tokyo-based association said.

Tokio Marine & Nichido Fire Insurance, which in February 2015 became the first Japanese insurer to launch a financial product for cyberattacks, saw new policyholders leap around threefold in FY2016.

The company provides consulting services for those worried about malware infections and provides cost estimates for potential cyberattacks.

Sompo Japan Nipponkoa Insurance released a product last October for small and midsize companies that charges relatively low premiums. New contracts for its cyberattack insurance products jumped fivefold in the six months to March compared with the same period a year ago.

MS&AD Insurance Group Holdings saw cyberattack insurance contracts surge about 3.7 times in FY2016. It instructs customers, mainly employees at small and midsize companies, on how to prevent targeted attacks sent by electronic mail.

Ruling leaves insurers exposed to environmental claims

A 1989 settlement that released insurers, including a Liberty Mutual Holding Co. Inc. subsidiary, from any future claims arising from environmental contamination at five facilities did not include a New Jersey storage battery facility because it was not specifically named, says a federal appeals court in a divided opinion that overturns a lower court ruling.

The ruling in the case means the policyholder is not barred from seeking insurance coverage for subsequent environmental claims by the U.S. Environmental Protection Agency.

The complex litigation has a long history. In the 1950s, the McGraw-Edison Co. owned a plot of land in Bloomfield, New Jersey, where it operated two battery factories, the Primary Battery plant and the Storage Battery plant, according to the June 30 ruling by the 6th U.S. Circuit Court of Appeals in Cincinnati in *Employers Insurance of Wausau et al. v. McGraw-Edison Co.*

McGraw sold the Storage Battery plant in 1960 and later transferred the Primary Battery plant to a subsidiary called Battery Products Inc., according to the ruling.

After Waukesha, Wisconsin-based Cooper Industries acquired McGraw-Edison, it discovered that several of McGraw's factories, including the Primary Battery plant, had potentially contaminated the environment.

Cooper asked its insurers, which included Employers Insurance of Wausau, a unit of Boston-based Liberty Mutual, to cover its liabilities for the cleanup, and in response the insurers filed suit seeking a declaration the contamination was not covered by their policies.

That suit was settled in 1989. The settlement agreement released insurers from future claims arising from contamination at five facilities, including one identified as the McGraw-Edison Battery Products Battery Products Plant facility.

Twenty years later, the EPA notified Cooper that the entire McGraw Bloomfield property, including both the Primary Battery plant and the Storage Battery plant, might have contributed to pollution in the Passaic River.

Cooper's insurers then returned to federal court in 2014, arguing the 1989 settlement agreement barred Cooper from seeking insurance coverage for the EPA claims. (Cooper Industries was acquired by Cleveland-based Eaton Corp. in 2012.)

The U.S. District Court in Grand Rapids, Michigan, ruled in the insurers' favor, holding the 1989 settlement agreement included the Storage Battery plant.

The 6th Circuit overturned that ruling in its 2-1 decision. "According to Cooper, the term 'Battery Products Plant facility' refers to only the Primary Battery plant — the factory that McGraw transferred to its wholly owned subsidiary, Battery Products Inc., in 1985. The settlement agreement supports this position," said the majority ruling, in holding the agreement did not apply to the Storage Battery plant.

In the settlement agreement, "Each facility is named after the entity or division operating it, with names including the 'Service Division Facility,' the 'Bussman Facility,' and the former 'Toastmaster' and 'Worthington' facilities," said the ruling.

"These names show that the contracting parties had a convention for identifying the facilities in the agreement based on the entities that operated them.

"Under that convention, the Battery Products Plant facility refers to the Primary Battery plant, which Battery Products Inc. operated, and which does not include the Storage Battery plant," said the ruling, in reversing the lower court's ruling.

The dissenting opinion says, "I conclude that the settlement agreement is ambiguous and I would vacate the District Court's judgment and remand for an evidentiary hearing."

J. B. BODA GROUP

- **J. B. BODA - First on Protection – 70 Years of Transformation.**
  Service with Commitment – Third Generation & Moving on …
- **24 Offices in India & 5 Offices Overseas in U.K., Singapore, Dubai, Nepal, Kenya.**
- **Employs 1,000 + personnel.**

S E R V I C E S

- **Insurance & Risk Management Consultants, Life Valuation, Life & Employee Benefit Schemes.**
- **Actuarial Valuations.**
- **Training Academy.**
- **Valuation of Land, Building, Plant & Machinery.**
- **Protection & Indemnity Insurance Services.**
- **Fire, Engineering, Miscellaneous Accident Surveyors & Loss Assessors.**
  Marine Cargo Surveyors, Loss Assessors, Superintendents.
  Container Surveyors, Tank Calibrators, Samplers & Analysts.
- **International Reinsurance Brokers (Non-Life & Life).**
- **Direct Insurance Brokers (Non-Life & Life).**

Head Office :

Maker Bhavan No. 1, Sir Vithaldas Thackersey Marg, Mumbai 400 020 (INDIA)

Telephone : + 91 22 6631 4949 / 6631 4917 * Telefax : + 91 22 22623747 / 22625112

E-Mail : jbbmbi@jbbodamail.com * Web : http://www.jbboda.net

For previous issues click on www.jbboda.net/news.php

We value feedback at median@jbbodagroup.com

Follow us on

DISCLAIMER