

Good afternoon, Ladies and Gentleman. The organisation that I represent, the TT Club, is a specialist insurer of ports and terminals among other sectors – with Members around the world.

I am delighted to have the opportunity to talk to you this afternoon on the subject of risk and liability in the ports industry.

Initially, I had planned to talk about how and where your risks and liabilities might arise – but, you are all able to identify the majority of these issues without the help of me – so, I have decided to share with you instead a number of areas that the TT Club feel are becoming of increasing importance.

What I would like to talk about are the following subjects:

Firstly, the impact of Terrorism, Security Initiatives on Risk management and Loss Prevention;

Secondly, Natural Catastrophes – and the impact on the insurance market;

And finally, the importance of Emergency Planning.

Let's start with Security issues.

The first question, when considering Terminal Security, that any terminal operator must ask themselves, is "What level of loss is acceptable?"

If this presentation had been given pre 9/11 the emphasis would have been primarily, on minimizing the risk of theft or pilferage. At that time, the degree to which individual terminal operators would invest in security measures, risk management or loss prevention procedures was optional.

Unfortunately, security measures today are no longer just optional controls taken by a terminal operator in respect of the degree and quality of fencing, lighting, security guards, seal discipline, closed circuit TVs etc - but some are now mandatory. The risk of theft has been usurped by the potential risk of terrorists using the marine supply chain.

Immediately after the devastating World Trade Centre attacks in New York, governments around the world scrambled to assess their vulnerability to highly organised terrorist groups willing to sacrifice thousands of lives to achieve their aims. The risk of terrorism, via the use of a "dirty-bomb" hidden inside a shipping container, suddenly became a very real threat, and the maritime transport system loomed large in the eyes of security agencies worldwide as a prime target and/or vehicle for future attacks.

To date there has been noteworthy progress, including the development of the International Ship and Port Facility Security Code (ISPS Code), the 24-hour advance cargo manifest filing requirements, the Container Security Initiative agreements, and the Customs' Trade Partnership Against Terrorism (C-TPAT) program.

But even these programs are only beginning efforts that I am sure will continue to evolve, rather than completed projects.

Marine insurance generally excluded acts which were the result of intentional conduct, such as malicious acts or vandalism directed to promote some political objective, for example under the War, Strikes, Riots and Civil Commotion clauses common to marine insurance policies (however, often these covers could be "bought back").

Before the 9/11 attacks, insurers generally neither priced nor reserved for losses arising from a terrorist attack. Around the globe today there have been various insurance industry/government initiatives to find ways to combat the lack of coverage available, for example, the U.S. government responded by passing the Terrorism Risk Insurance Act, establishing a new program under which the federal government shares the risk of loss with the insurance industry, and mandates that coverage

be provided. Some insurers of Terminal Operators across the world are willing to provide Terrorism cover other insurers are not able.

Although 9/11 raised the consciousness of the spectre of terrorism for the American public, terrorism itself is not a new threat, especially in maritime commerce.

We all no doubt saw the horrific video images of the Hyundai Fortune ablaze in the Red Sea. Most of you will be aware of the rumours immediately after the news broke, that the initial cause of the fire was a terrorist attack. Whilst the consensus now seems to be focusing on dangerous cargo, I think that we are all aware that a terrorist attack would have resulted in a very similar tragedy. The mention here of dangerous cargo and the rather hap-hazard implementation of the IMDG Code could lead me off on a tangent – suffice to say, that this is also an area of major concern for the TT Club, but time does not allow me to say much more on this subject.....

Seafarers and ships have faced security threats ever since sea trade began. Protection by government against such maritime loss caused by terrorist attack is also not new. But the dualistic approach between government, as protector of public interests, and the insurance market, as a mechanism for reallocating private loss, may present an approach to combating and ensuring a safer and more secure maritime trading environment.

Estimating the costs of these investments is an extremely complicated task given the great variability of costs from port to port and from country to country. Hourly labour wages for security guards vary from just slightly higher than day-labourer levels in many areas to relatively high government pay levels. Costs for equipment (fencing, lighting, secured gates, locks, communications equipment, monitoring equipment, etc) also vary tremendously according to local construction and installation, related labour costs and port size and equipment needs. Finally, many ports, in order to reduce losses from cargo theft, have already invested heavily in security infrastructure and equipment (which may or may not need to be updated).

On the other side of the coin, the costs of inaction were and still are potentially tremendous. The maritime transport system *is* vulnerable to being targeted and/or exploited by terrorists. A large attack, especially a well co-ordinated one, could have the result of shutting down the entire system as governments scramble to put in place appropriate security measures. These may be drastic, such as the complete closure of ports, and inefficient, such as duplicative and lengthy cargo checks in both originating and receiving ports. The cost of such an attack would likely be measured in the tens if not hundreds of billions of dollars. It is precisely for these reasons that governments have sought to strengthen their security dispositions *vis-à-vis* maritime transport.

Ultimately, the cost of implementing new security systems and complying with the ISPS Code is not only prudent, but also necessary. Noncompliance for either terminal operators or owners is not likely to be a profitable venture.

In addition to possible delay, detention, refusal of entry, as well as fines for lack of compliance, there is yet another, less obvious potential downside for noncompliance. Insurance coverage may be voided by a marine insurer for failure by the terminal operator or shipowner to comply with the ISPS Code.

Under the law applicable to marine insurance, breach of an express warranty, such as a failure to comply with National or International regulations, for example, could give the insurer the possibility of rejecting a claim that has resulted directly from a failure to comply with the ISPS Code.

Even if not provided for as an express warranty in the policy itself, the doctrine of utmost good faith in revealing all material facts in placing coverage may also give rise to a defense of voiding a policy should an assured mislead an insurer about its compliance with the ISPS Code and inspection certificates.

The marine insurance marketplace, either for Terminal Operators, or for P&I, and to a lesser extent Hull & Machinery for the vessel operators had seen unprecedented premium increases in the immediate period after 9/11 - it did start to appear as if these increases were slowly leveling out – at least for top quality operators with good claims records.

A continued investment in quality operations, including adherence and maintenance of all new aspects of the ISPS code and transparency with insurers is a logical response by Terminal Operators seeking to hold their insurance costs down to the lowest levels in the marketplace.

We have looked at the maritime transport system's vulnerability to terrorism, and the current proposals to remedy the most flagrant gaps in security.

It should be stressed again, however, that many of the measures proposed have distinct *benefits* that are not related to their antiterrorism task. These benefits result from reduced delays, increased safety (less unauthorized people within the terminal), faster processing times, better asset control, decreased payroll (due to IT improvements), fewer losses due to theft and therefore, possible decreased insurance costs, etc.

These savings could be significant, and could therefore help to counter-balance the increased expenditure on security costs.

It would be fair to say, that as a rule, most security processes are allied to quality management programs which will have a very positive spin off in terms of liability exposures or at least the defence of same.

Whilst we have mentioned that some measures may slow trade, many others can in fact lower trade costs.

In an industry still largely dependent on paper and fax transmissions, it is not hard to see room for savings resulting from more integrated IT systems. Many large Manufacturers/shippers have already benefited from increased productivity due to IT improvements in their supply chain. If these were extended to all trading parties – small shippers, forwarders, land and sea carriers, customs authorities, port and terminal operators, etc. – the savings could be tremendous.

Vessel turn-around times could be shortened, customs clearing accelerated and costs associated with redundant data entry eliminated and cargo handling costs slashed.

In conclusion on security issues, we have seen ISPS compliance and adoption of other security initiatives being used as a marketing tool, we have further silver linings in Safety, Security and Efficiency.

We cannot promise that insurance costs will come down as a direct result of increased security costs – as we all know, unfortunately, accidents do still happen, berths do get blocked, fires do destroy warehouses, gantry cranes do drop containers, ships do still hit your cranes, and – perhaps most importantly and unpredictably, we should remember the power and impact of Natural Catastrophes.

This brings me onto my second subject.

Areas of the Philippines and other Asian regions are seen by insurers as major Catastrophe hot-spots, the impact of recent events especially those within the ports and terminal industry will have an effect not only on the cost of insurance that you as individual operators purchase – but also, to a certain degree, the availability of that insurance too.

Whilst 2006 was relatively quiet for catastrophe claims in the Ports industry, I would ask you to remember three significant events within your industry over recent years:

2003 – you will recall the devastating effect of Typhoon Maemi in the South Korean Port of Pusan;

2004 – the impact of the Indian Ocean Tsunami, which led to a number of Ports and Terminals in India, Sri Lanka, Malaysia, and Thailand suffering losses;

2005 – Hurricanes Katrina, Wilma and Rita in the US Gulf. Perhaps the largest of the three claims that I have mentioned in terms of insured losses in your industry (and certainly the largest claim that the TT Club has ever paid).

The history of insurance goes back many thousand years, back to the times of the old Greek Traders, then later the Romans (some even say as early as the Phoenicians) when marine traders used a system that allowed the ship-owner to borrow money on both his vessel and cargo – with the risk being shared by all involved, the cargo owners and the vessel owner.

In effect, risk is still shared today – but rather than individual cargo owners and ship owners sharing the risk, the global insurance industry either via primary insurers or through their reinsurers now shares the risk. The impact of an increase in any type of catastrophic insurance claims ultimately will affect all of us – regardless of the original geographic location of the claim.

The subject of developments in the insurance industry could provide enough topics for me to talk for a week – mergers, acquisitions, port development, environmental concerns, larger vessels, availability of handling equipment and consolidation of manufacturers etc. all have a significant impact upon what you do, how you do it and the costs of operating.

The mechanism of purchasing insurance cover by you, via your local insurance broker, into a local or international insurer, remains the same, but, the reinsurance costs of your primary insurer have undoubtedly gone up – and these increases in cost, will more often than not be passed back down the chain to you.

Rising property valuations, recalibration of catastrophe models and desire to mitigate earnings volatility has increased demand for reinsurance to the point that despite significant increases in reinsurance rates for cat exposed areas, demand for reinsurance cover is still outstripping supply.

Furthermore, initial indications are that 1 January 2007 programmes will further increase demand - having a knock-on effect on price increases and lack of capacity.

Reinsurance capacity has been severely constrained by the significantly higher capital requirements imposed by the rating agencies, and by a more conservative approach to aggregate management which limits reinsurer capacity in peak zones.

A further substantial catastrophe event or series of events in 2007 would almost certainly have an immediate 'shock' effect on pricing and capacity. Rating agencies also continue to exert increasing influence and their more cautious approach to catastrophe risk is likely to be reinforced if further substantial losses are incurred in 2007.

On a positive note, the markets were expecting an above average hurricane season, and resulting losses were built into market assumptions. Also the new cat models, based on the severity and frequency experienced in 2004 and 2005, included some forward looking factors for the first time.

So far, it would appear as if the hurricanes and typhoon seasons of 2006 have resulted in lower than anticipated insured losses – we must therefore hope that the volatility seen in insurance markets over recent years slowly begins to wane.

The final area that I would like to look at today is concerning emergency planning:

Despite the best risk management and risk control we cannot avoid accidents or claims all together – too many different influences come together and cause losses.

A fundamental business consideration, applicable to all threats to the company, whether from fire, flooding, hazardous materials spillage or loss of power, is the creation of an emergency plan.

The emergency plan should be based on a careful review of the threats to your business and include specific steps to minimise them.

The TT Club have created a booklet to assist in guidance on the creation and operation of such plans.

Whilst the Club's booklet is focussed primarily on the threat of windstorms – the background to creating a plan to deal with any emergency situation remains the same.

While many people may associate severe wind storms with these devastating occurrences in sub-tropical areas, gales and severe storms with winds gusting up to hurricane strength (force 12) also occur and cause damage in more southerly latitudes, particularly in the winter months. Please therefore do not think that, because you may not be operating in an area of tropical storms, this booklet is not for you: the advice it contains is still valid.

An emergency plan is also just that: something to be kept in reserve (but up-to-date) to be used when an emergency threatens. However there is often very little time to implement the plan in full. Simple good housekeeping practices round the clock and throughout the year can do much to reduce the volume of work that has to be done in that short period.

For example, if possible, keeping container stacks no more than four high means that you do not have to devote personnel and equipment to an emergency programme to remove high tiers if the wind increases in strength. Always locking down cranes when they are not being used guards against them being blown along the track in the event of sudden and unexpected squalls. Similarly, having a back-up computer facility off-site can protect the company's vital records.

Each facility's situation will be individual and specific. Because you have not yet suffered a disaster – man, or nature made, does not mean that you never will; nor should the fact that they have happened in the past necessarily mean that you are properly prepared for a future catastrophe.

Every port and every terminal has its own characteristics. The risk profile of any facility depends on factors such as design, construction, layout, location, the type and amount of equipment, the prevalence of wind storms and the wind speeds normally encountered; the other physical risks – earthquakes, floods etc: also importantly the impact of a disaster occurring at a neighbour's facility – significantly more problematic, if your neighbour is a chemical tank farm, rather than say a warehouse facility.

Good emergency planning can help ensure that an incident does not turn into a disaster, but when dealing with natural forces, not even the best plan can prevent unforeseen and disastrous damage occurring. A good plan will therefore also include measures to be taken to recover from a disaster.

The overall objectives of emergency planning are:

- to contain and control emergency incidents;
- to safeguard people in the operational area and neighbouring areas;
- to mitigate the effects and minimise damage to property and the environment;
- to enable business to be resumed at the earliest opportunity.

Plans will be concerned with three factors:

- the hazard and nature and extent of the threat;
- the risk and the probability of occurrence;
- the consequences and the possible effect on people, the environment and the business.

The preparation of an emergency plan cannot normally be carried out in isolation. Local authorities and emergency services may well have their own developed plans; your facility may be very close to another industrial plant, or it may fall within the jurisdiction of a port authority. There may be other organisations working in, or with involvement in your facility, for instance stevedores, warehouse operators, engineers and repairers, other terminal operators, customs, railway operators, forwarders,

ship's agents and so on; each should, in turn, have its own detailed plan. Alternatively, employees of such organisations should be included in your own plan.

If you regularly use workers from outside agencies (for instance, a port labour pool) you should involve that agency in your plans.

The key to success lies in the harmonisation of all these plans, and in drawing clear lines of responsibility for control according to the nature and severity of the particular emergency. Once developed and agreed, emergency plans should be published, tested and revised at regular intervals.

Timing

The plan should be realistic about the time needed to undertake some of the tasks. For example you should monitor how long it takes to complete the tie-down of a crane (including moving it from its operational position to an anchor point), and then factor in an increase of at least 25% to allow for the difficulties of undertaking the manoeuvre in high winds, to work out how much time will be required to tie down all the cranes in the facility.

In doing these calculations, you should remember that personnel may understandably be concerned or preoccupied with the safety of their own homes and families and may therefore want to leave early or may simply stay away from work at times of storm threat. The local authority or police may also order people to evacuate danger areas, or may stop people travelling into coastal areas under threat. You may therefore need to calculate that you will have a reduced workforce available for some of the shutdown tasks

Decision-making

The plan should include a hierarchy of decision-making. For instance, it is probably inappropriate for a single crane driver to decide that the whole facility should be closed because the conditions on his/her crane are too dangerous to work in. Whether you would wish to allow the berth supervisor to make the decision to cease work on that particular berth is a matter for your organisation. It would probably be better for the decision to be made by an incident controller, who should be guided by the experience of the operating personnel concerned.

Testing the plan

Once agreed, the overall plan should be published and copies made available to all personnel. It should be tested regularly by drills or practices, and any lessons learned should be incorporated in the plan. Everybody involved should be made aware of any revision and appropriately revised instructions and plans made available.

Emergency plans need to be tested when first devised and rehearsed at suitable intervals thereafter. Rehearsals or exercises are important because they:

- familiarise personnel with their roles, equipment and the details of the emergency plan;
- allow the professional emergency services to test their parts of the plan, the co-ordination of their activities and the compatibility of communication equipment;
- familiarise the professional emergency services with the special hazards;
- prove the current accuracy of details of the plan, e.g. telephone numbers, the availability of special equipment such as fire and rescue equipment, etc.;
- give experience to and build confidence in team members. In the initial shock and confusion of a real incident the ability to fall back on well-rehearsed actions will be invaluable;
- can identify any unforeseen weaknesses of the plan.

Implementing the plan

If an emergency is declared, your emergency coordinator should automatically become the incident controller, with responsibility for implementing the plan. He or she should be vested by the board of directors with full authority to take whatever decisions that may be necessary to protect the business. The coordinator/controller should have at least one deputy with the same level of authority, to cover for absences. The controller should be supported by an emergency operations team, with people drawn from a number of different departments and specialisms. The incident controller, or his deputy, together with an emergency team and nominated key personnel should always be available to carry out immediate response. As they may be called out at any time, ideally none of the team should live too far away from the facility.

Emergency operations room

The incident controller and his/her team must have access to an operations room housed in a substantial building that is storm-proof and unlikely to be affected by the emergency itself, including flooding or the effects of the storm on cranes, box stacks or any other equipment. It should be located, designed and equipped to remain operational throughout an emergency

Arrangements should be made to ensure that all staff not required as part of the emergency plan, are safely away from the danger area.

Operators, in conjunction with the appropriate authorities, should regularly test their emergency plans and ensure that all employees receive refresher training. Such exercises should test each part of the emergency plan in each part of the area, or each berth, stage by stage starting with the first immediate action. Emergency shut down, securing of equipment and evacuation should be rehearsed. Where appropriate this may be by simulation. Familiarisation visits by the emergency services should be encouraged.

Thank you for your attention.