The Black Swan: The Unexpected in Ports and Terminals

Ports and terminals play a critical part in infrastructure in a country or region. While operators may be aware of many of the complex risks they are susceptible to and employ best practice to mitigate them, they may not be fully prepared for the potentially devastating impact from a low-probability, high-impact event. Such a rare event, whether a natural hazard, an act of terrorism or war, or even a major cyber-attack, which cannot be fully predicted or mitigated is known as a "black swan".

BLACK SWANS AND PORTS AND TERMINALS

Natural hazards impacting ports and terminals are not entirely unexpected and can, to varying degrees, be mitigated. However, less frequent, more extreme events – also known as black swan events – are much harder to predict and consequently manage. Significant natural disasters such as earthquake, volcanic activity, windstorm, flooding, or tsunami can cause devastating damage to ports and terminals. In addition, a large-scale terrorism or cyber-attack could produce a black swan event.

Risk identification, best practice controls, and emergency responsiveness are nothing new to port and terminal owners and operators, but a black swan event may not be one that is typically planned for. The need for robust risk management is compounded by the fact that ports and terminals are typically nationally or regionally critical infrastructure, whose operations are essential for economic as well as political stability.

A black swan event may or may not directly damage the infrastructure of a port business, but it could catastrophically damage the delivery of operations for key customers. In doing so, the event has the potential to impact investor confidence and/or destroy reputations.

SPOTLIGHT

What is a black swan?

As Nassim Nicholas Taleb wrote in his 2007 book, *The Black Swan*[1], such extreme events have three key characteristics:

1. Their probability is low, based on past knowledge and experience.
2. Although probability is low, when it happens it has a devastating impact and the shock caused is profound.
3. It is impossible to predict the exact nature of the event, but they are retrospectively defined as an event of obvious concern and should or could have been better understood and, to some degree, forecast as a potential risk.

Furthermore, black swans could be compounded by the simultaneous occurrence of risk events, perhaps due to undetermined or flawed assumptions.

[1] Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable,* New York: Random House, 2007.

PORTS AND TERMINALS PRESENT UNIQUE RISK PROFILES

Ports and terminals are exposed to a complex range of risks when handling, storing, and managing the secure onwards journey of cargo and, in some cases, passengers.

In addition to risks to the safety of assets and passengers passing through, a port can be at risk of business interruption and a corresponding drop in revenue from a wide variety of factors outside its control. This could include denial of access to the port if a key access route by sea, road, or rail is blocked or broken, or damage to a key partner's facility such as a mine, factory, warehouse, or port. It could also include the consequences from a failure of essential utilities or a cyber-attack.

Given the risk of business interruption, the impact of a black swan event on ports and terminals could be severe, and needs to be considered more carefully as part of operators' risk management.

CASE STUDIES

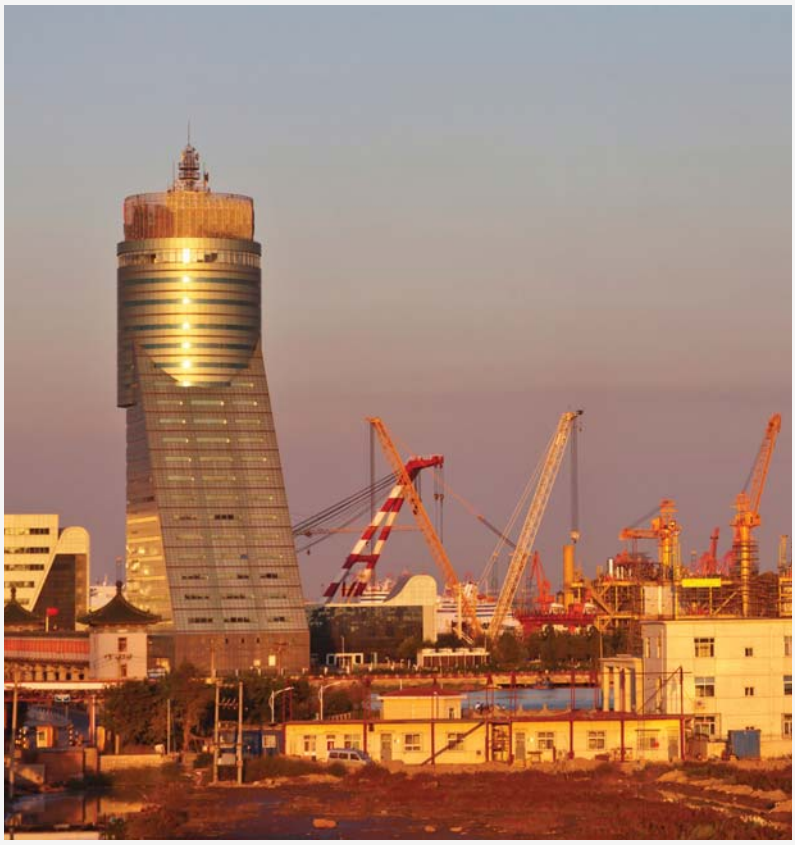
Tianjin Port Explosion

On August 12, 2015, the port at Tianjin, China was rocked by an explosion, which sent a fireball and shockwave through the site, blasting shipping containers and vehicles in the port and on a nearby highway overpass. It destroyed warehouses, production facilities, and dormitories, hit the nearby Donghai Road railway station, and blew out windows within residential structures for several kilometers.

The event, impacting the world's 10th largest port, has since become one of the largest and most complex man-made losses in recent history. The impact was felt far beyond the port, disrupting supply chains across the globe, including a severe impact on the automotive industry. The effect the explosion has had on supply chains is expected to be a long-term one.

Reports have emerged that the explosion had been caused by hazardous chemicals being stored in one of the warehouses. However, while it could be argued this could have been mitigated against, the sheer scale of this event is expected to have caused losses approaching US$1 billion. This, coupled with the complexities of modern supply chains, mean it has unpredictable results for the marine industry.

According to Guy Carpenter, the final insured losses from Tianjin are likely to come in at around US$874 million. This includes substantial losses for automotive industries and multi-million dollar cargo losses.



THE NEED FOR HORIZON SCANNING AND STAKEHOLDER COORDINATION

Although accurately predicting the impact of a black swan event on ports and terminals is impossible, horizon scanning and assumption testing is critical. As with all risks, internal and external lenses should be applied in order to ensure there are no unexplored assumptions, weaknesses, or threats. For instance, while a physical phenomenon such as the 2010 Eyjafjallajökull volcanic eruption and resulting ash cloud could be argued to be a known risk, the huge impact to global travel was neither foreseen or planned for.

In the case of ports and terminals, while natural disaster risks are to be expected, some catastrophes can have unexpectedly severe consequences.

One such black swan event was typhoon Maemi, which hit South Korea in 2003. The multi-billion dollar loss event caused signficant damage to the port of Busan, damaging infrastructure and ships.

While South Korea is prone to typhoons, it was a combination of Maemi's strength, direct hit on the port, and that it hit at high tide, which resulted in a high amount of losses.

Other large-scale threats could include the failure of critical infrastructure within the port environment, for which neither business impact analysis nor planning has been undertaken. Port and terminal operators should be aware of their key assets, but how many have tested their assumptions around continuity, or considered their dependencies on assets not owned by the business?

The result of a cyber-attack could be catastrophic for a port or terminal operator. Until around 2010, the majority of cyber-attacks were driven by an attempt to obtain personal or financially sensitive data. Today, the nature of the threat is changing, and companies across all business sectors have begun to experience highly sophisticated and complex attacks that attempt to inflict damage to property and operations by seeking to take control of industrial control systems.

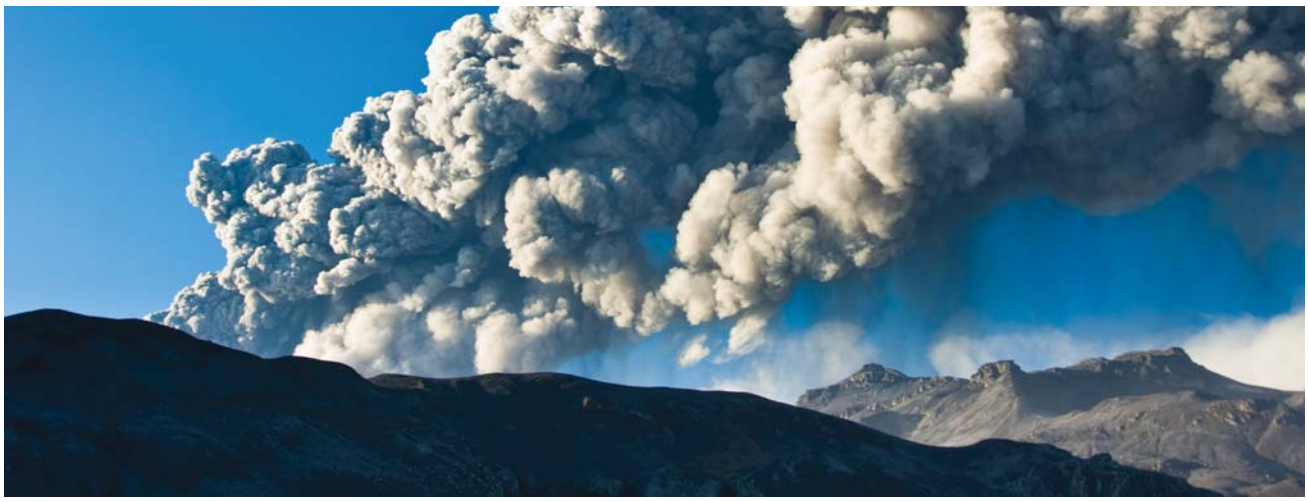
Port assets and infrastructure may also be exposed to politically-motivated violence from strikes, riots, civil commotion, terrorism, or sabotage. The threat from those events may be well understood, but risks are changing.

Consider, for example, the threat of a nuclear device/dirty bomb/ conventional bomb being hidden inside a container. Even if there was no weapon, the threat alone could result in the port being shut down during a laborious search through thousands of containers.

Port and terminal operators should develop contingency plans against the risk of terrorists or a nation state hacking into and disrupting the electronic navigation systems that enable access to the port with the intention of bringing trade to the country/region to a halt.

Clearly, these types of events could have significant, if not catastrophic, ramifications for ports and terminals, and operators should consider the possibility of extreme events and the effects these could have on their interests, both internally and externally.

Where possible, a multi-stakeholder approach is recommended in order to understand the joint risk landscape, causes of risks, and shared accountability for controls.



Withstanding a major catastrophe necessitates tailored, multi-stakeholder crisis management, business continuity management, and risk management. The glue that holds all of this together is leadership, management, and staff effectiveness.

HOW CAN BLACK SWAN EVENTS BE MANAGED?

Black swans are long-tail events which cannot be precisely identified, and it can be difficult to put controls in place to mitigate the level to one deemed as low as reasonably possible. Therefore, there is a need for port and terminal operators to be sufficiently resilient to manage the unexpected. Resilience can be defined as the ability of an organization to withstand unplanned disruptions, originating from any cause, that have the potential to impact its strategy or mission-critical (strategically important) activities, whether asset-people-or process-related.

Withstanding a major catastrophe necessitates tailored, multi-stakeholder crisis management, business continuity management, and risk management. The glue that holds all of this together is leadership, management, and staff effectiveness. Understanding, communication, and motivation are prerequisites for high-level performance during a crisis.

Mission-critical activities should be reviewed on a regular basis, and business continuity and crisis plans should be joined up and exercised at strategic and tactical levels to ensure resilience and agility to respond. It would be a mistake to assume that resilience equals business continuity, which is dealt with at an operational level. If an extreme event were to occur, its implications would be felt all the way through the port operating company, and senior leadership actions would be scrutinized and reported 24/7 through multimedia channels.

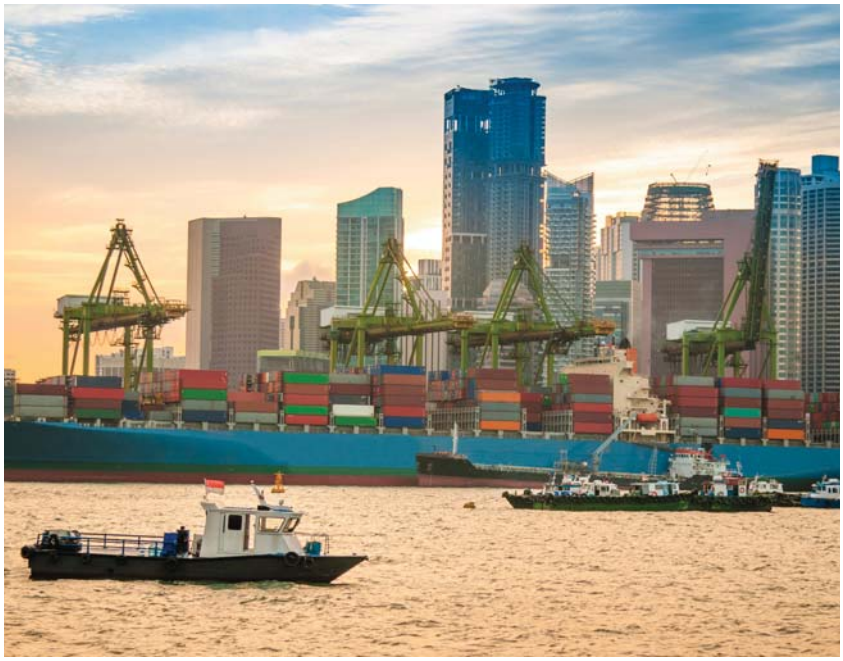
THE ROLE OF INSURANCE IN A BLACK SWAN EVENT

Although employers' liability, public liability, property damage, and business interruption policies will be drawn upon in the event of a "normal loss," insurance should never be considered as a comprehensive risk treatment. Furthermore, insurance protection against black swan risks is far from straightforward. In its traditional form, insurance is limited in scale of coverage, is specific to individual risks, and provides a low speed of payment. Post event, there may be a very short time period of weeks or even days to persuade financiers, creditors, regulators, and the government that the business has the cash to see it through the crisis in an orderly manner.

There is therefore a need for enhanced insurance solutions to deal with potential black swans for ports and terminals.

This includes broader policy wording and rapid settlement of claims through the use of parametric triggers where claims payments are made within set time frames based on pre-agreed terms. Such solutions compliment a well-structured risk management and risk-financing strategy, including a contingency plan for cash flow after a black swan event.

Prior to creating financial solutions, there is a need for thorough analytical stress testing of business impacts, combined with insurance and finance responsiveness. This analysis should then be overlaid with risk appetite and risk tolerance to create bespoke insurance and finance solutions.



There is a need for enhanced insurance solutions to deal with potential black swans for ports and terminals.

CONCLUSION

Black swan events present a unique challenge for ports and terminals, both in terms of the difficulty in predicting and mitigating such events and the potentially devastating consequences they can bring about. The risks these events pose for these often critical infrastructures cannot be underestimated. In order to best guarantee the future success of ports and terminals, there should be a thorough appraisal of this key area of risk, combining horizon scanning, resilience, insurance, and financial stress testing. This detailed analysis will enable the creation of more robust controls, including financial and non-financial, to ensure the sustainable returns of a port or terminal following a catastrophic event.

About Marsh

Marsh is a global leader in insurance broking and risk management. Marsh helps clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 30,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. With annual revenue of US$13 billion and approximately 60,000 colleagues worldwide, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a leader in providing risk and reinsurance intermediary services; Mercer, a leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a leader in management consulting. Follow Marsh on Twitter, @MarshGlobal; LinkedIn; Facebook; and YouTube.

About this report

This report has been produced by Marsh's Global Marine Practice, which is at the forefront of advising the maritime industry on risk and insurance issues, and has a reputation for delivering insight and solutions for the challenges that our clients face. The practice comprises more than 600 marine specialists dedicated to serving the industry and manages premium volume in excess of US$3 billion. With operations in more than 100 countries, led from 12 strategic hubs, we are a global leader in marine broking and risk management.

MARSH

For more information, please contact:

NICK MAY

Vice President
Global Marine Practice
+ 44 (0)20 7357 2180
nick.may@marsh.com

EDWIN CHARNAUD

Chairman
Global Infrastructure Practice
+ 44 (0)20 7357 3157
edwin.charnaud@marsh.com

MARCUS BAKER

Chairman
Global Marine Practice
+ 44 (0)20 7357 1780
marcus.baker@marsh.com