Malcolm Hartwell

Supply chain: ESG, risk management and cyber security

11 - 14 June 2023

45th Annual SAPICS Conference
Century City Conference Centre, Cape Town, South Africa
A supply chain is only as strong as its weakest link

**Agenda**

- Introduction to supply chain risk management
- Discussion on the ‘Eternal Triangle’
- Risk matrix
- Delays: ship
- Incoterms summary
- Delays: demurrage and detention
Sources of Risk

- health and safety
- regulation
- outsourcing
- environmental
- business ethics and anti-corruption
- financial crime
- food and drug
- antitrust and competition
- diversity and inclusion
- real estate
- political risk
- intellectual property
- cyber security
- tax
- brexit
- indigenous rights
- data protection and privacy
- whistleblowing
- directors and officers responsibilities
- representative and class actions
- global standards
- export controls and sanctions
- corporate governance
- supply chain
- investigations
- cross border dealings
- business and human rights
The Eternal Triangle

Contract of Sale

Contract of Carriage

Contract of Insurance
Risk Matrix

- Seller
- Buyer
- Logistics service provider
- Bank/finance
- Underwriter

Contract of sale
- Risk
- Ownership
- Obligations
- Liabilities
- Restrictions
- Off-shore
- Off-set

Logistics contract
- Form
- Obligations
- Who bears the risks?
- New technology

Banking/financing
- Payment?
- Link to logistics?
- Letters to credit

Insurance
- Credit guarantees
- GIT insurance
- Liability insurance
- Identity of carrier

Who is instructing you?
Nature of cargo
- Contingent
- Break-bulk
- Bulk
- Project
- Perishable
- Customs
- Abnormal cargo
- Hazardous cargo
- Newbuild

Types of carriage
- Road/air
- Rail
- Sea
- Multimodal
- Damage

Geography
- Obstacles
- Conflict
- Cross-border

International convention and local laws
- Application of international conventions
- Compulsory insurance
- Regulations

Costs
- Service providers
- Customs and compliance
  - Stops
  - Penalties
  - Duty

Other regulations
- Cybercrime

Dispute resolution
- Recovery, self practice
- Choice of law
- Arbitration
- Jurisdiction
Risk assessment

In each case you have to look at the various risks and consider the risk from:

- The point of view from the seller
- The point of view from the buyer
- The point of view from the banker/financer
- The point of view from one or more of the logistics service providers
- The point of view from the underwriter

Each angle will help you develop the risk matrix
Risk in the legal context

Legal instruments

Contract of sale

Logistics contract

Banking/Finance

Insurance
Risk assessment

What informs those points:

• Who is instructing you?
• Nature of cargo
• Types of carriage/storage/distribution
• Geography
• Commercial context
• International conventions and local laws
• Costs
• Dispute resolution
Reasons for delay

- COVID 19: mandatory port closures
- Labour shortages
- Russia/Ukraine conflict
- Port congestions

“US retail imports rise after three-year slump” FTW

“Norton Rose Fulbright has one of the largest legal footprints in Africa of any international law firm and has been advising on deals in Africa for over 30 years.”
Global shipping trends

Fig. 1: Global Schedule Reliability

Fig. 2: Global Average Delays for Late Vessel Arrivals

Source: Sea-Intelligence, GLP report issue 135
Average monthly schedule reliability of main container carriers from November 2020 to January 2023, by carrier.
Delay: ship

- Hague Visby Rules **do not** make any reference to delay
- Carrier has an implied undertaking under the contract of carriage to proceed with the voyage with due dispatch
- Exercise reasonable due diligence to deliver cargo

... the Institute Cargo Cla

- Do not cover damages or loss cause by delay
- Delay is not an insured peril
mv *MSC Spain* ; *Mediterranean Shipping Co (Pty) Ltd* v *Tebe Trading (Pty) Ltd*

**Main issues : Delay**

- Rerouting of vessel causing delay resulting in damage to perishable cargo
- Bill of lading permitting deviation from route
- Consignee claiming damages from agent of carrier and shipping line

*“Tebe’s claim is for the loss it suffered as a result of the delay brought about by the deviation from the initially proposed route. The appellant was not in any way responsible for that deviation. It was furthermore at all times merely acting as agent, either for the carrier or MSC Geneva. By reason of the clauses in the bills of lading previously mentioned, Tebe would have had no claim in contract or delict against the party responsible for the deviation, whether that party was the carrier or MSC Geneva. Unable to recover from the principal, Tebe seeks in effect to circumvent the consequences of the contract by holding the principal’s agent personally liable in delict for failing to afford Tebe the opportunity of removing its containers from the vessel on a ground not amounting to a breach of contract on the part of the principal. But agents are contractually bound to protect the interests of their principals.”*
The legal duty that Tebe contends was owed to it by the appellant would therefore be in conflict with the contractual obligation which the latter had to its principal. Even if it were to be accepted that the appellant was negligent, there can be no good reason in my view, given the contractual setting, for the existence of a legal duty on the appellant to take such steps as may have been reasonable to prevent the harm. It follows that in my judgment the failure on the part of the appellant to advise Tebe of the deviation so as to afford it the opportunity of removing its containers from the vessel was not wrongful and the claim in delict must fail.
Delays: demurrage and detention

What informs those points:

• Demurrage
• Detention
**Incoterms**

<table>
<thead>
<tr>
<th>‘Wet’ Incoterms</th>
<th>‘Multi-modal’ Incoterms</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the mode of transport is not multi-modal and only involves transport by sea if non-containerised cargo, contracting parties should incorporate the “wet” Incoterms into their agreements.</td>
<td>The Incoterms that deal with the transportation of goods across different modes of transport (rail, air and/or sea) are</td>
</tr>
<tr>
<td>The “wet” incoterms are</td>
<td>• EXW (Ex works)</td>
</tr>
<tr>
<td>• FAS (Free alongside ship)</td>
<td>• FCA (Free carrier alongside)</td>
</tr>
<tr>
<td>• FOB (Free on board)</td>
<td>• CPT (Carriage paid to)</td>
</tr>
<tr>
<td>• CFR (Cost and freight)</td>
<td>• CIP (Carriage and insurance paid)</td>
</tr>
<tr>
<td>• CIF (Cost, insurance and freight)</td>
<td>• DAP (Delivered at place)</td>
</tr>
<tr>
<td>In all instances, either the point of delivery or the point at where the risk in the goods passes is by reference to a sea-going ship. The Incoterms should never be used where cargo has been containerised.</td>
<td>• DPU (Delivered at Place Unloaded) (DAT (Delivered at Terminal))</td>
</tr>
<tr>
<td></td>
<td>• DDP: Delivered duty paid</td>
</tr>
<tr>
<td></td>
<td>These terms are suitable for containerised cargo.</td>
</tr>
</tbody>
</table>
Incoterms do deal with

- When the risk in the goods passes
- Who is responsible for arranging the contract of carriage
- Who is responsible for arranging the insurance of the goods

Incoterms rules specifically address two aspects of the transaction:

- Which of the parties – buyer or seller - is responsible for arranging and paying for the transport of the goods to be delivered to the buyer (includes all activities ancillary to this e.g. loading and unloading of goods, import & export procedures, insuring goods etc.

- At which point of the journey does the risk in the goods shift from the seller to the buyer? This is important to know in the case of the goods becoming lost or damaged in transit – for the purposes of Incoterms this point of the journey is referred to as ‘delivery.’
• **E-Terms:** Buyer is responsible for organising all carriage of goods and the delivery point is at the seller’s premises (e.g. warehouse or factory).

• **F-Terms:** Buyer responsible for arranging main carriage of goods & the delivery point is usually where the goods are handed to the buyer’s first carrier or forwarder.

• **C-Terms:** Seller arranges main carriage of goods to the destination port/place in the buyer’s country at buyer’s risk. Risk transfers (delivery point is) before the main carriage of goods i.e. at the place/port in the seller’s country.

• **D-Terms:** Seller arranges main carriage of goods and risk transfers to the buyer only after the main carriage of goods at an agreed point in the buyer’s country.

• **NB:** As one moves from E – F – C – D terms, the delivery point moves further away from the seller towards the buyer.

• Each change of letter being a shift in the delivery point closer to the buyer.
Physical Stages Involved in the International Dispatch of Goods Sold

The international dispatch of goods from the exporter to the importer into a contract of sale of goods involves a number of distinct physical stages and it is important for the parties to agree on which of them is responsible for arranging each of these stages and who bears the risks and costs associated with this dispatch of goods – agreeing on an appropriate Incoterm brings certainty and clarity to these matters.

• The physical stages of the international dispatch of goods typically involve:
  – Delivery of the goods from the seller's premises (e.g. seller’s warehouse or factory) to a first carrier or port facility.
  – Terminal or port handling at the place/port of export.
  – Clearing goods for export through customs.
  – Main carriage of goods to destination country.
  – Clearing goods for import into the buyer’s country.
  – Terminal or port handling at place/port of import.
  – Final delivery to buyer’s premises.
Cyber Risk - Ransomware

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently encrypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.
Cyber Security – already a problem in our industry

Port of Antwerp 2011 (suspected two year enterprise)
• accessed the Port’s computers to identify containers which had illegal goods
• sent Trojans to Port staff infecting IT system and used key logging to capture passwords
• removed the goods before the containers were checked by authorities.

Other examples
• Interception and redirection (through email infiltration and impersonation) of funds.
• request for payments of bunker invoices redirected by e-mail to a false account
• multiple fake requests to appoint surveyors and other suppliers
• ECDIS outage due to inadvertent contamination by virus
• CMM said publically that "ransomware" attacks, where hackers scramble a ship's computer system and seek a ransom to unscramble it, were one of the main challenges facing it.
Cyber Security – many ways to be vulnerable

• Common security vulnerabilities:
  1. Malware/spyware/ransomware to steal or damage data or hold it hostage
  2. Phishing – request for data from an apparently legitimate third party to steal information – then can redirect funds
  3. Password attacks – to access accounts
  4. DoS attacks (denial of service) – server is overloaded shutting it down

• Being too boring to attract attention of hackers is NOT a defence.
• Hoping it goes away is not a solution

• Accountability to regulators for failure to protect individual’s private information.
• Need to show due diligence.
• Risk of class action suits, breach of contract, and penalties.
Cyber Risk should be addressed proactively in order to be properly risk ready.
Protective Measures

- **Identify**: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

- **Protect**: Implement risk control processes and measures, and contingency planning to protect against a cyber event and ensure continuity of shipping operations.

- **Detect**: Develop and implement activities necessary to detect a cyber event in a timely manner.

- **Respond**: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber event.

- **Recover**: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyberevent.