RP Legal & Tax

Avv. Claudio Perrella

INNOVAZIONE TECNOLOGICA NELLE ASSICURAZIONI MARINE

Institute Cyber Attack Exclusion Clause – Cl . 380 10/11/2003

1.1 …….. in no case shall this insurance cover loss damage liability or expense ***directly or indirectly*** *caused by or contributed to by or arising from the use or operation,* ***as a means for inflicting harm,*** *of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.*

Se la clausola viene adottata in una polizza rischi guerra/terrorismo la copertura opera se l'*electronic system* è impiegato "*in the launch and/or guidance system and/or firing mechanism of any weapon or missile*".

Ritenuta troppo restrittiva e drastica nelle esclusioni

Esclude eventi e sinistri altrimenti coperti (es. *grounding* determinato da un attacco *hacker*)

L'esclusione opera tutte le volte che viene impiegato un *electronic system*.

Polizza di carico falsificata con un *electronic device* per ottenere la consegna del carico. E' una fattispecie coperta? In caso di impiego di fotocopiatrice?

Il Joint Cargo Committee dopo una serie di consultazioni ha introdotto la JC2019-004 nel luglio 2019, con l'obiettivo di sostituire la Cl. 380

JC2019-004 : Cyber Coverage Clause

1.1 It shall be a condition of cover under this insurance that the Insured can demonstrate that they have implemented ***reasonable measures*** *to ensure compliance with the US or UK National Cyber Security Centre recommendations, or equivalent national recommendations, current at inception of this insurance. If the Insured cannot provide evidence that these measures, or such other measures that may be required by Insurers were undertaken, then there shall be no cover under this insurance for losses arising from the use of Software.*

JC2019-004 : Cyber Coverage Clause

1.2 this insurance shall indemnify the Insured for any physical loss or damage, liability or expense, which would otherwise be covered under this insurance, which affects **solely the Insured or the Insured's property**, **and arises from the use of Software.**

Software shall mean the programs, source codes, scripts, applications and other operating information used to instruct computers to perform one or more task(s).

1.3 **Other than whilst the subject matter insured is on board any means of conveyance**, this insurance excludes physical loss or damage, liability or expense arising from the use of Software, which leads to a Systemic Loss.

A **Systemic Loss** shall mean physical loss or damage, liability or expense ..... **which affects more than this Insured or this Insured's property**.

Opera in caso di malicious e non malicious cyber

- Attacco *cyber* che disattiva il sistema antifurto di un magazzino di proprietà dell'assicurato seguito da furto della merce ivi depositata?

- Attacco ad un magazzino di terzi contenente merce (anche) di proprietà dell'assicurato?

Grounding della nave e danno al carico a seguito di un *cyber attack*?

La mancata adozione di un efficace sistema di prevenzione e di gestione di un *cyber attack* potrebbe integrare un caso di *unseaworthiness* e di mancato esercizio della dovuta diligenza nel rendere la nave idonea alla navigazione, e una violazione degli articoli III. 1. e IV.1. delle Hague Visby Rules.

Article III

1. The carrier shall be bound before and at the beginning of the voyage to exercise due diligence to:
(a) Make the ship seaworthy;
(b) Properly man, equip and supply the ship;

Article IV

1. Neither the carrier nor the ship shall be liable for loss or damage arising or resulting from unseaworthiness unless caused by want of due diligence on the part of the carrier to make the ship seaworthy, and to secure that the ship is properly manned, equipped and supplied

Impatto della mancata adozione di misure preventive/protettive sulla copertura assicurativa di armatori, vettori ed operatori del mondo *shipping*?

Rilievo della condotta dell'assicurato (colpa grave, *willful misconduct*) e dei suoi preposti?

Riconducibilità delle omissioni al Comandante, all'equipaggio, al management e/o al Cyber Risk Officer?

Polizze parametriche

Crescente applicazione per la copertura di

a) Rischi cyber

b) Business Interruption/Contingent Business Interruption

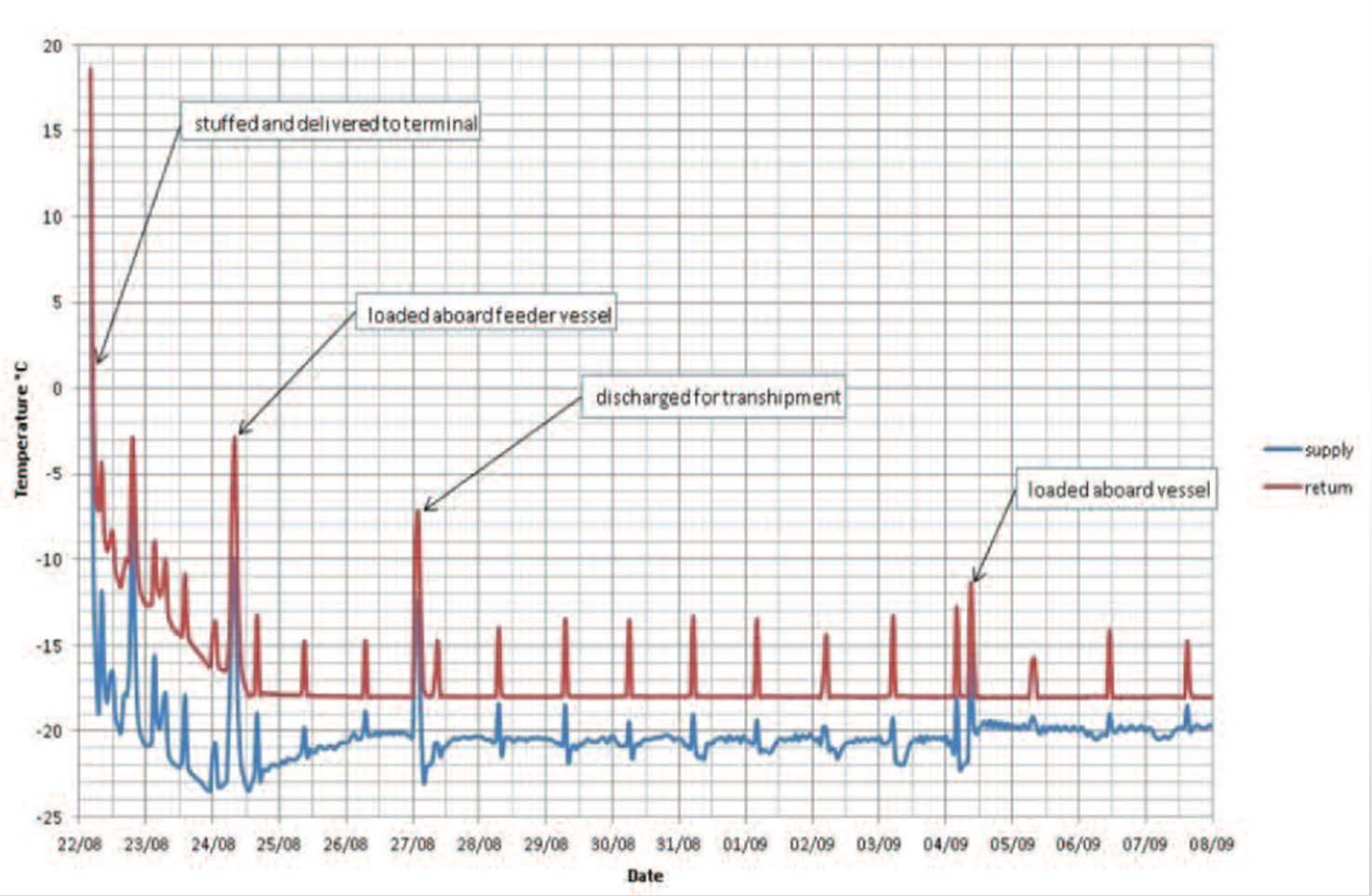
c) Non Damage Business Interruption

d) Danni causati da eventi meteo

Ampio ricorso a sistemi di *blockchain* e *smart contracts*

Meccanismi di indennizzo basati su uno o più *trigger*

Indennizzo automatico in caso di alterazione nel corso del trasporto o del deposito delle temperature prescritte per la corretta conservazione del carico


stuffed and delivered to terminal
loaded aboard feeder vessel
discharged for transhipment
loaded aboard vessel
supply
return
Temperature °C
Date
20
15
10
5
0
-5
-10
-15
-20
-25
22/08
23/08
24/08
25/08
26/08
27/08
28/08
29/08
30/08
31/08
01/09
02/09
03/09
04/09
05/09
06/09
07/09
08/09

Possibili profili di criticità per le polizze parametriche

Violazione del principio indennitario, in virtù del quale l'assicurato può essere risarcito esclusivamente per il danno subito, l'assicurazione non può essere fonte di lucro.

Generalmente ritenuto di ordine pubblico

MA Esistono eccezioni, es. la polizza stimata

Valore Stimato

Valore che, mediante apposito patto speciale, le parti (Contraente/Assicurato e Società) convengono di attribuire all'oggetto Assicurato, rinunciando all'applicazione dell'art. 1907 c.c. Qualunque dichiarazione o perizia estimativa non espressamente approvata per iscritto dalla Società deve intendersi nulla e priva di effetto ai fini contrattuali.

Che accade se invece un evento che non raggiunge la soglia *trigger* si rivela comunque molto dannoso?

E' possible equiparare il sistema del *trigger* a franchigie, sotto-limiti, SIR?

Quale valutazione di congruità ed idoneità della copertura?

Necessità di individuare *trigger* oggettivi, misurabili, certi


Grazie