Ania

Associazione Nazionale
fra le Imprese Assicuratrici

CYBER RISKS NELL'ASSICURAZIONE CARGO E MARINE LIABILITIES

GMC

Paolo Lovatti

Global Marine Consultant

Milano, 17 maggio 2018

1959 – I wanna …….

2017 – Wanna Cry

- L’attacco il 12 maggio 2017 a Telefonica Spagna e al NHS britannico
- La richiesta di pagamento per sbloccare i sistemi
- La rapida propagazione del virus anche a sistemi meno importanti
- La richiesta di pagamento in bitcoin

Un passo indietro: il Millennium bug o Y2K

- Il timore di un potenziale difetto informatico (bug) al cambio di data della mezzanotte tra il venerdì 31 dicembre 1999 e il sabato 1º gennaio 2000.
- La reazione del mercato assicurativo Marine
- La Clause 380 predisposta al riguardo

10/11/2003

INSTITUTE CYBER ATTACK EXCLUSION CLAUSE

1. SUBJECT ONLY TO CLAUSE 1.2 BELOW, IN NO CASE SHALL THIS INSURANCE COVER LOSS DAMAGE LIABILITY OR EXPENSE DIRECTLY OR INDIRECTLY CAUSE 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.

2. WHERE THIS CLAUSE IS ENDORSED ON POLICIES COVERING RISKS OF WAR, CIVIL WAR, REVOLUTION, REBELLION, INSURRECTION, OR CIVIL STRIFE ARISING THEREFROM, OR ANY HOSTILE ACT BY OR AGAINST A BELLIGERENT POWER, OR TERRORISM OR ANY PERSON ACTING FROM A POLITICAL MOTIVE, CLAUSE 1.1 SHALL NOT OPERATE TO EXCLUDE LOSSES (WHICH WOULD OTHERWISE BE COVERED) ARISING FROM THE USE OF ANY COMPUTER, COMPUTER SYSTEM OR COMPUTER SOFTWARE PROGRAMME OR ANY OTHER ELECTRONIC SYSTEM IN THE LAUNCH AND/OR GUIDANCE SYSTEM AND/OR FIRING MECHANISM OF ANY WEAPON OR MISSILE.

Cambia il nome: Golden Eye o Petya o NotPetya ma gli effetti sono identici

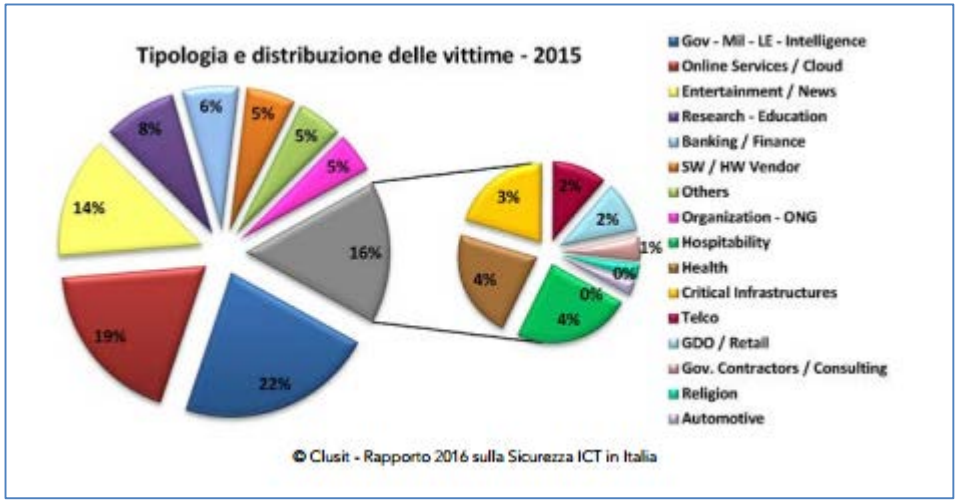
- L'attacco alla Moller-Maersk S/A (APM) il 28 giugno 2017
- La rapida propagazione del virus nei suoi terminal dislocati in 76 Paesi nel mondo
- Le caratteristiche di questo worm distruttivo auto-propagatorio in grado di diffondersi rapidamente attraverso reti di computer scarsamente protette
- Il terminal di Rotterdam Maasvlakte II in grado di operare solo al 15% del suo potenziale a seguito dell'attacco
- La flessione della capacità di carico da 210.000 a 160.000 container
- Una riduzione delle entrate per Maersk per il 3° trimester 2017 prevista fra $200m e $300m.

Una lezione assimilata?
Un nuovo attacco di WannaCry

- Anche la Boeing nel mirino degli hacker
- L'infezione che ha colpito i bracci robotici di assemblaggio degli aerei
- La possibilità che il malware si possa estendere ad altre funzioni di produzione e di test degli aerei, se non agli stessi software
- La minimizzazione del problema da parte di Boeing

Il rapporto Clusit 2018

- CLUSIT: l'Associazione Italiana per la Sicurezza Informatica
- Anno 2017: 1127 attacchi gravi a livello mondiale
- Una crescita degli attacchi del 240% rispetto al 2011
- Il costo mondiale degli attacchi cyber che ha raggiunto i 500 miliardi di dollari
- Le perdite in Italia nel 2016 stimate in 10 miliardi
- Gli incidenti tenuti nascosti e la miriade di casi non dichiarati con conseguenze di lieve entità
- «Perché deve succedere proprio a me?!»



Il business Marine e i cyber risk
Anno 2003: un'abdicazione?

.. **in nessun caso** questa assicurazione copre perdite, danni, responsabilità o spese direttamente o indirettamente causate, derivanti o favorite dall'uso o dall'impiego, al fine di arrecare un danno, di qualsiasi computer, sistema informatico, programma informatico, codice software malevolo, virus o processo informatico o di qualsiasi altro sistema elettronico.

- Il timore di cumuli di rischio imprevedibili
- Una parificazione astratta ai cumuli di rischio imprevedibili, tipici dei rischi Guerra e Nucleari
- Un mercato *Marine* mondiale compatto nella volontà a non voler garantire i rischi *Cyber* in tutti i suoi settori
- Il peso dei Trattati di riassicurazione
- L'evoluzione del rischio *Cyber* negli anni: dal *bug* al *Cyber Crime*
- L'interesse all'assicurazione dei rischi Cyber da parte di altri Rami
- Lo sviluppo di questo business negli ultimi anni.

Scenari di rischio reali e presunti

- Il superstorm Sandy è costato agli assicuratori fra US$ 50 e 70 miliardi
- Il disastro di Tianjin è stato valutato tra US$ 1.5 e 3.3 miliardi
- L'Emerging Risks Report 2017 - Technology - del Cyence dei Lloyds' che stima il risultato di due ipotetici attacchi cibernetici catastrofali:
  - a un fornitore di servizi *Cloud* con perdite stimate di US$ 53 miliardi
  - a sistemi operativi di computer utilizzati da un elevato numero di aziende in tutto il mondo con perdite stimate complessivamente in US$ 28,7 miliardi
- Quali riflessi sul settore *marine* ?

Ipotesi di sinistri *Trasporti* a seguito di un attacco informatico

- Il furto di beni durante il trasporto: il pericolo di intromissione dolosa nei documenti e-freight
- Le responsabilità degli spedizionieri/vettori ad esempio per ritardi e penali
- I possibili danni a merci deperibili in giacenza conseguenti a un blocco dei sistemi di refrigerazione

Presente e …..

- L'attuale posizione del mercato Italiano
  - Cargo: una situazione compatta da parte degli assicuratori nell'utilizzo della Clause 380
  - RCV e liabilities: una posizione degli assicuratori eterogenea

- Il mercato inglese:
  - Il sollecito da parte dell'Autorità di controllo per l'effettiva comprensione dei rischi cibernetici da parte degli assicuratori Marine
  - L'avvio da parte del JCC di uno studio per la valutazione di potenziali esposizioni massive collegate ai rischi cibernetici
  - L'identificazione da parte del gruppo di lavoro di possibili potenziali di vulnerabilità cyber relativa a cumuli statici in magazzini a temperatura controllata nei più importanti porti

…… e futuro prossimo

- La disponibilità presente di alcuni underwriter inglesi a garantire il rischio di furto conseguente a un attacco cibernetico a parziale deroga della Cl. 380
- L'attuale offerta di copertura proposta da altre linee di rischio per l'assicurazione *cyber* che potrebbe comunque non soddisfare completamente le esigenze specifiche dei clienti *marine*
- I *cyber risk*: una nuova sfida per gli assicuratori *marine?*
- La necessità di abbattere un muro: nuove opportunità di premio per gli assicuratori

…… aspetti pratici e considerazioni

- L'attuale posizione del mercato riassicurativo
- E' effettivamente necessario un supporto da parte dei riassicuratori?
- L'analisi della tipologia degli attuali attacchi informatici: esiste effettivamente una possibilità di danno catastrofale nei settori *cargo* e *marine liabilities*?
- L'esperienza di altre linee di rischio maturata in questi ultimi anni: un possibile punto di partenza per la definizione di copertura mirate specifiche per i rischi *marine*
    - l'assicurazione delle merci
    - la copertura delle responsabilità a carico dello spedizioniere
- Nuove opportunità per gli assicuratori *marine*: il ritorno sulla scena assicurativa da attori principali, nel rispetto dello spirito originario del *marine underwriting*

Una clausola possibile

INSTITUTE CYBER ATTACK EXCLUSION CLAUSE

1.1 Subject only to clause 1.2 below, 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, **where claim is above € 500.000,00**.

2.1 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or
any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

Prua al vento o in balia delle onde ?

Una domanda:

a seguito di un attacco informatico alla nave e conseguente dichiarazione di Avaria Comune, quali potrebbero essere le conseguenze assicurative per il carico?

Ania

Associazione Nazionale
fra le Imprese Assicuratrici

Grazie per l'attenzione

CYBER RISKS NELL'ASSICURAZIONE CARGO E MARINE LIABILITIES

Paolo Lovatti - Global Marine Consultant

Milano, 17 maggio 2018

GMC