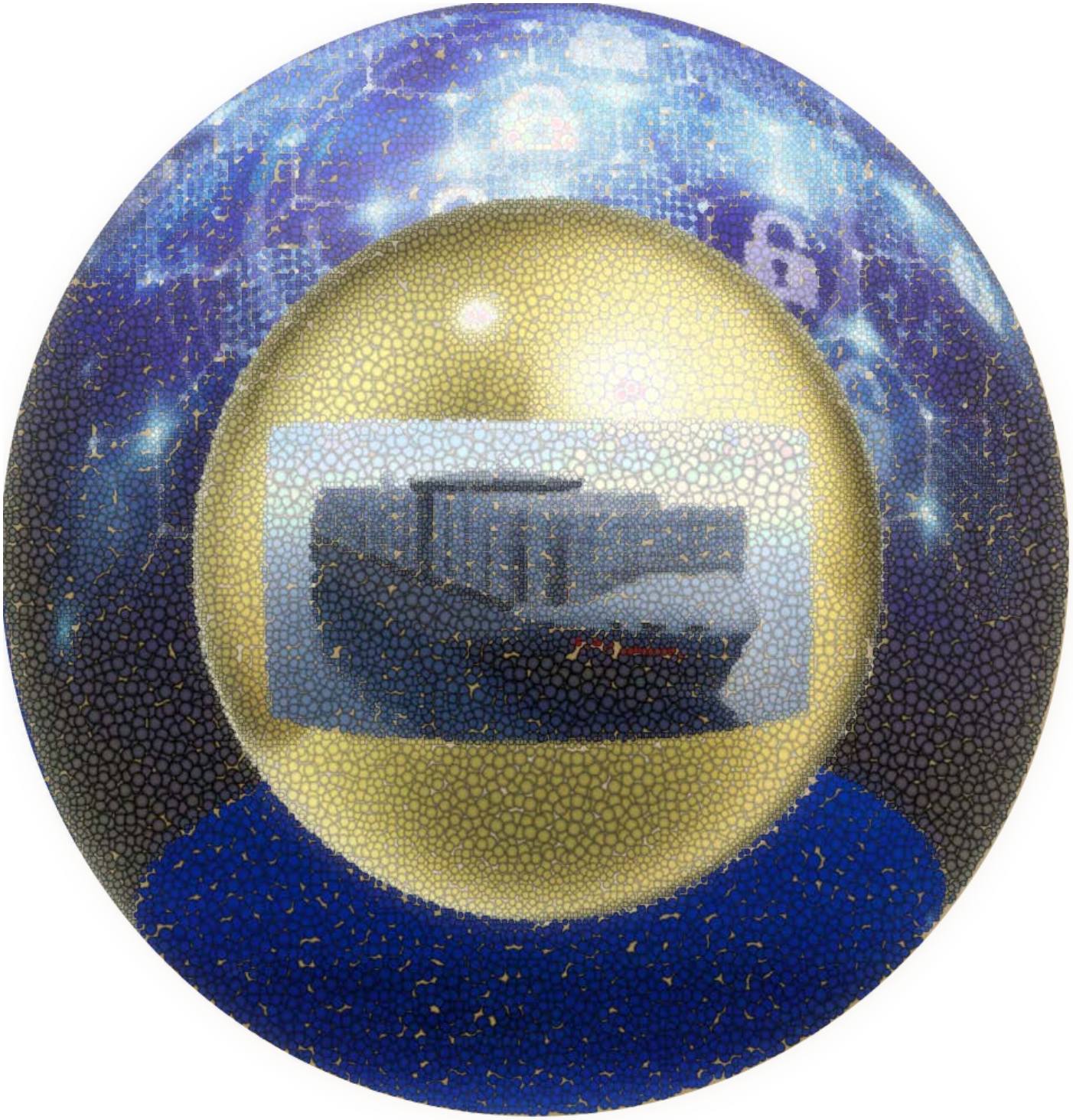
Ania

Associazione Nazionale
fra le Imprese Assicuratrici

IL RISCHIO CYBER NELLO SHIPPING

INDICE

Executive Summary	1
Petya o NotPetya?	3
La vulnerabilità del sistema ed i suoi potenziali effetti	5
Cyber security: le linee guida internazionali	11
La strategia europea	21
Profili assicurativi	25
Appendice - Le clausole internazionali	34
Bibliografia	43



EXECUTIVE SUMMARY

Le minacce alla sicurezza informatica diventano sempre più complesse: si propagano grazie alla capacità di operare a livello transfrontaliero e all'interconnettività, sono alimentate dalla labilità dei confini tra mondo fisico e digitale e sfruttano le disparità sociali ed economiche.

Negli ultimi dieci anni la natura della minaccia cyber è cambiata. Gli attacchi che nel recente passato venivano per lo più perpetrati per acquisire illecitamente dati sensibili di natura personale o finanziaria si stanno trasformando in intrusioni altamente sofisticate che mirano ad infliggere danni a beni e processi operativi con il fine ultimo di ottenere il dominio dei sistemi di controllo industriale.
La continua espansione delle tecnologie quali strumenti di lavoro e nella realtà di tutti i giorni - attraverso la diffusione dei social network, dei dispositivi mobili e dei servizi cloud - se da un lato offre enormi opportunità, dall'altro ha portato ad una maggiore vulnerabilità dell'intero spazio cibernetico. Questa tendenza dovrebbe aumentare ulteriormente, parallelamente agli sviluppi tecnologici, come la proliferazione di dispositivi legati all'Internet of Things (IoT). Per contro, cresce il livello di consapevolezza di imprese e società nel considerare la *cyber security* come un rischio d'impresa e nella conseguente esigenza di ricercare metodi via via più affidabili e completi per assicurare la continuità del proprio business in caso di attacchi informatici.

Anche le infrastrutture marittime dipendono molto più che in passato dalla tecnologia informatica. I sistemi di navigazione e propulsione delle navi, la movimentazione del carico, il tracciamento dei container, sia nei porti che a bordo delle navi, gli inventari dei cantieri navali e i processi automatizzati sono tutti controllati da software che sono fondamentali per un funzionamento regolare delle attività.

Ci sono più di 50.000 navi mercantili che operano a livello internazionale, trasportando ogni tipo di merce.

L'industria marittima rappresenta il 90% degli scambi commerciali effettuati a livello mondiale e da essa dipendono le catene di approvvigionamento dei principali ambiti produttivi.

Un incidente cibernetico nel settore marittimo oltre a pesanti riflessi commerciali e logistici può portare ad un grave disastro ambientale o perfino causare la perdita di vite umane. Questo documento si concentra sui rischi del cyberspazio legati all'industria dello Shipping per la quale la gestione dei rischi informatici sta diventando sempre più una priorità, sia sotto il profilo commerciale, sia sotto il profilo di conformità normativa.

PETYA O NOTPETYA?

€

Maersk ha stimato un danno di circa 300 milioni di $ subendo la chiusura di alcuni terminal portuali gestiti dalla sua controllata APM

La criminalità informatica è una minaccia globale in rapida crescita in tutti i settori e la catena di approvvigionamento marittima è vulnerabile come hanno dimostrato i problemi riscontrati da Maersk nel 2017. La compagnia danese di navigazione AP Moller-Maersk, il più importante vettore nel trasporto di container e di general cargo, che controlla circa il 18% dei traffici mondiali, ha subito il 27 giugno 2017 l'attacco del malware NotPetya, che ne ha limitato temporaneamente l'operatività commerciale e logistica (per effetto dei danni al sistema di prenotazione della società e di rallentamento dei processi di container tracking) ma anche causato congestione e pesanti interruzioni di servizio in almeno 17 terminals in tutto il mondo gestiti dalla sua controllata APM (incluso quello di Rotterdam, un hub strategico per la distribuzione di frutta e verdura a livello europeo).

In quell'incidente i problemi a terra hanno avuto un effetto a catena sulle navi, evidenziando il fatto che man mano che le operazioni di trasporto marittimo diventano più connesse, maggiori sono le possibili ripercussioni sui sistemi sia a terra che a bordo.

Fino a quel momento l'industria marittima, nota per le sue radici tradizionali e la sua resilienza a modifiche non convenzionali, aveva avuto una consapevolezza molto limitata del fenomeno e, conseguentemente, adottato solo sporadicamente politiche aziendali in grado, sotto il profilo sia gestionale sia normativo, di far fronte ai maggiori e diversi rischi connessi ai più recenti progressi tecnologici.

Il malware NotPetya non solo ha detto molto circa il livello di vulnerabilità del settore marittimo ai cyber risk - dato il successo di un attacco contro un colosso mondiale della navigazione e della logistica come Maersk nonostante le avanzate difese informatiche adottate dalla società - ma ha anche sottolineato agli operatori del settore la carenza di linee guida o standard specifici per prevenire un attacco informatico di rilievo specificamente mirato all'industria della logistica marittima o, quanto meno, limitarne le conseguenze.

A fine 2011 l'ENISA (European Network Information Security Agency) nel suo report "*Analysis of Cyber Security Aspects in the Maritime Sector*" laconicamente rilevava che "*awarness is currently low to non-existant*".

In effetti, debolezze significative nella sicurezza informatica sono state identificate a livello generale nella tecnologia utilizzata per la navigazione in mare come si vedrà a breve. E più digitalizzato diventerà il settore marittimo, più esposto sarà alle minacce informatiche.

È chiaramente questo lo scenario del prossimo futuro per un ambiente altamente competitivo in cui riduzione dei costi (tagli degli equipaggi) e potenziamento dei servizi (navi gigantesche gestite efficacemente da sistemi informatici) costituiscono fattori chiave per la sopravvivenza.

LA VULNERABILITA' DEL SISTEMA ED I SUOI POTENZIALI EFFETTI

I porti in generale e i loro terminal container dipendono sempre di più da sistemi di comunicazione e gestione elettronica che permettono di semplificare e velocizzare le operazioni di imbarco/sbarco, lo stoccaggio e l'inoltro delle merci. È evidente che qualsiasi errore o disfunzione dei sistemi di gestione IT può causare gravi disservizi in catene di approvvigionamento sempre più complesse. Il processo incalzante di digitalizzazione nello Shipping se non correttamente controllato è inevitabilmente destinato a creare rischi di accessi non autorizzati ai sistemi elettronici di gestione delle navi e dei porti o di attacchi dolosi ai sistemi o alle reti.

Ogni nave di nuova costruzione usa un software quasi sempre aggiornato da remoto per il funzionamento dei motori; i sistemi di carico complessi sono gestiti in digitale; anche le gru funzionano sulla base di sistemi GPS satellitari. La tecnologia dell'informazione è ampiamente utilizzata anche nei sistemi di navigazione marittima. Dal 1° luglio 2012 l'ECDIS (*Electronic Chart Displays and Information System*) è diventato obbligatorio a bordo di tutte le navi secondo quanto stabilito dalla Convenzione SOLAS(*Convenzione internazionale per la salvaguardia della vita umana in mare*). Lo scopo primario dell'ECDIS - un sistema di navigazione elettronico in tempo reale, cioè in simultanea, che permette di visualizzare e gestire informazioni cartografiche (quali le coordinate geografiche o i livelli di profondità) su uno schermo - è quello di contribuire a rendere la navigazione più sicura alleggerendo il carico di lavoro dell'Ufficiale di guardia.

Inoltre, tutte le navi passeggeri e le navi da carico di stazza lorda superiore a 500 GT (tonnellate di stazza lorda) e le navi di oltre 300 GT (se impegnate nel commercio internazionale) sono tenute dalla Organizzazione Marittima Internazionale (IMO) a dotarsi di un sistema automatico di tracciamento (AIS - *Automatic Identification System*) di ausilio ai sistemi radar, allo scopo di evitare collisioni fra le unità in navigazione. Il sistema AIS deve essere in grado di scambiare automaticamente informazioni, riguardanti l'identità, il tipo, la posizione, la rotta, la velocità, lo stato di navigazione e altri dati relativi alla sicurezza, con altre navi, impianti a terra e aeromobili. Tuttavia, poiché l'AIS non dispone di un meccanismo integrato per crittografare o autenticare i segnali, è considerato un bersaglio facile per gli attacchi informatici.
Infine, le strutture portuali, che muovono più di 1.000 miliardi di dollari di merci ogni anno, si affidano sempre più all'automazione per semplificare le operazioni.
Armatori e operatori portuali si stanno orientando verso sistemi di controllo industriale marittimo (ICS) sempre più integrati.

La tecnologia ha permesso al settore marittimo di migliorare la produzione, i costi e di ridurre i tempi di consegna. Tuttavia, questi cambiamenti tecnologici hanno aperto la porta a minacce e vulnerabilità emergenti in quanto strutture e strumentazioni sono diventate accessibili a soggetti esterni.

Passiamo in rassegna i punti più critici.

Gestione del carico

- Sistemi digitali per la gestione e il controllo dei carichi, compresi quelli pericolosi, che possono interfacciarsi con molti sistemi informatici di terra (inclusi porti e terminali marittimi)

Ponte di comando

- Sistemi digitali di navigazione interfacciati con i network di terra che provvedono ad aggiornare continuativamente i dati necessari. Un'azione dolosa potrebbe estendersi fino a rendere il controllo della nave difficile o impossibile, andando a interferire con i sistemi ECDIS, GPS/GNSS, AIS, VDR e radar/ARPA

Sistemi di propulsione

- Sistemi di propulsione, generatori e impianti digitali per ottimizzare la navigazione, limitare i consumi e ridurre gli equipaggi. La vulnerabilità sarà tanto più elevata quanto maggiore sarà l'integrazione tra questi sistemi e quelli del ponte di comando

Controllo degli accessi

- Sistemi di prevenzione utilizzati per supportare il controllo degli accessi e garantire la sicurezza materiale di passeggeri ed equipaggi nelle diverse parti della nave, soprattutto se da crociera

Gestione e servizi per i passeggeri

- Dispositivi che permettono di gestire imbarchi/sbarchi di passeggeri, il loro controllo a bordo utilizzandone anche i relativi dati sensibili. L'utilizzo da parte del personale di bordo di tablet, scanner o palmari per questa gestione può aumentare i rischi di infiltrazione di *malware*

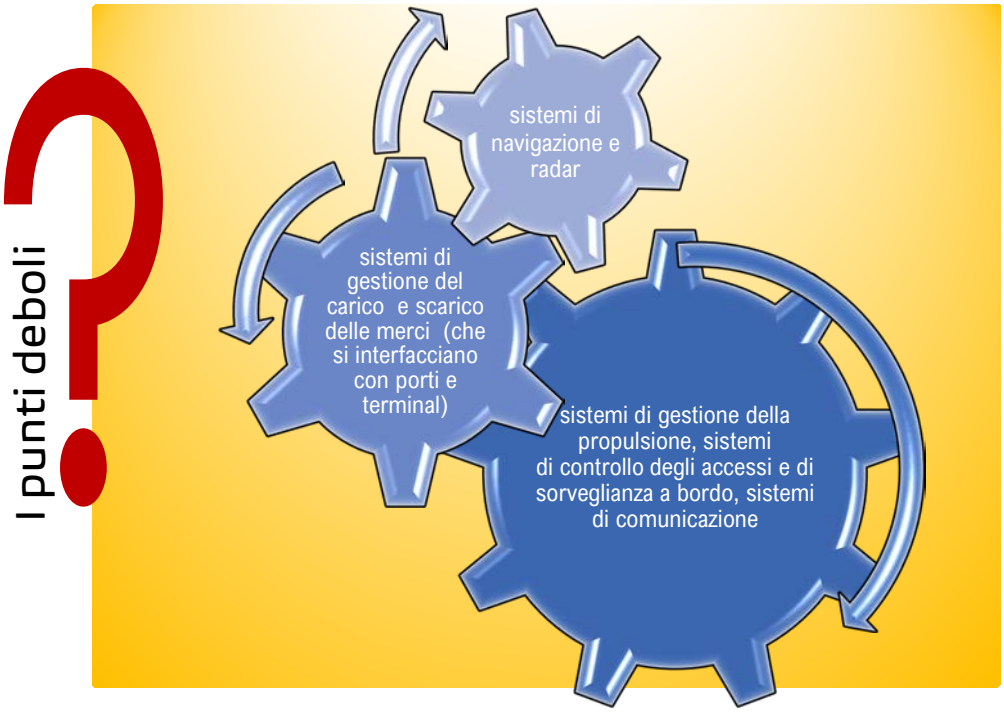
Network pubblici a disposizione dei passeggeri

- Reti fisse o wireless collegate a internet istallate a bordo a beneficio dei passeggeri sono di difficile controllo e non dovranno pertanto avere connessioni dirette o indirette con qualsiasi altro sistema critico di bordo per la navigazione

Sistemi amministrativi e di welfare dell'equipaggio

- Network per il governo in genere della nave e del personale di bordo. I sistemi di bordo utilizzati per il governo della nave divengono anch'essi particolarmente sensibili quando sono collegati via internet

La vulnerabilità appare ancora più evidente se si pensa ai progressi della tecnologia che stanno aprendo la strada ad un futuro assai prossimo in cui le navi opereranno senza equipaggio ("navi-drone").



Un attacco cyber può causare il furto di dati o del carico, estorsioni, danni materiali, senza escludere catastrofi, anche ambientali (si pensi ad es. all'incaglio di una nave portacontainer di gas liquido). A livello più strettamente gestionale possono venir paralizzati i sistemi di navigazione o di controllo a bordo, o sabotato il sistema GPS per dirigere la nave in acque non sicure e vulnerabili agli attacchi fisici da parte dei pirati. La minaccia di gran lunga maggiore è rappresentata da gruppi terroristici, che possono *hackerare* il sistema di navigazione di una nave per causare perdite di vite umane o danni materiali significativi, non ultima la perdita della nave stessa.

È chiaro quindi come l'adozione di misure atte a garantire la sicurezza degli operatori e delle informazioni da essi gestite per mezzo dei sistemi di bordo sia un tema preminente anche nel settore marittimo.

In questo contesto si collocano le linee guida dell'International Maritime Organisation (IMO) sulla *cyber security* che nascono proprio dalla consapevolezza dei pericoli per il comparto marittimo, derivati da campagne come WannaCry e Petya.

Ma prima di passare all'illustrazione delle guidelines merita rammentare che il Centre for Risk Studies dell'Università di Cambridge nel 2019 ha elaborato, in collaborazione con i LLoyd's, un ipotetico scenario catastrofale legato ad un attacco cibernetico nel settore marittimo: Shen attack, dal nome di un mostro marino mutante della mitologia cinese.

Il rapporto analizza un ipotetico attacco informatico contro i principali porti asiatici del Pacifico, stimando che si verifichino perdite fino a 110 miliardi di dollari in uno scenario estremo in cui un virus informatico costringe alla chiusura 15 porti.

"Shen attack" descrive uno scenario plausibile in cui viene lanciato un attacco tramite un virus informatico a bordo delle navi, che altera i record dei database di gestione del carico nei porti principali e porta a gravi interruzioni di operatività. Il rapporto mostra come un attacco di questa portata causerebbe un danno economico sostanziale a un'ampia gamma di settori di attività a livello globale a causa della interconnettività della catena di approvvigionamento marittimo.

Lo scenario stima che i settori dei trasporti, dell'aviazione e dell'aerospazio sarebbero i più colpiti (28,2 miliardi di dollari di perdite economiche in totale), seguiti dal settore manifatturiero (23,6 miliardi di dollari) e delle vendite al dettaglio (18,5 miliardi di dollari).

Le perdite di produttività colpirebbero ogni paese che intrattiene scambi bilaterali con i porti attaccati.

L'Asia sarebbe la regione più colpita, destinata a perdere fino a 27 miliardi di dollari in perdite economiche indirette, seguita dall'Europa con perdite per 623 milioni di dollari e dal Nord America con 266 milioni di dollari.

Il rapporto indica che l'economia globale è poco preparata per un simile attacco con il 92% dei costi economici totali non assicurati, lasciando un gap assicurativo di 101 miliardi di dollari.

La catena di approvvigionamento marittima è un sistema complesso di economie interconnesse.

Non c'è dubbio che la tecnologia abbia migliorato il settore delle spedizioni consentendo un migliore monitoraggio, una gestione ottimizzata e consegne just-in-time; tuttavia, l'invecchiamento delle navi costituisce un problema.

Molte navi in navigazione hanno più di 30 anni e non sono state progettate pensando al rischio cyber. Rispondere a queste sfide è quindi fondamentale per il benessere dell'industria marittima e di coloro che la assicurano.

CYBER SECURITY: LE LINEE GUIDA INTERNAZIONALI

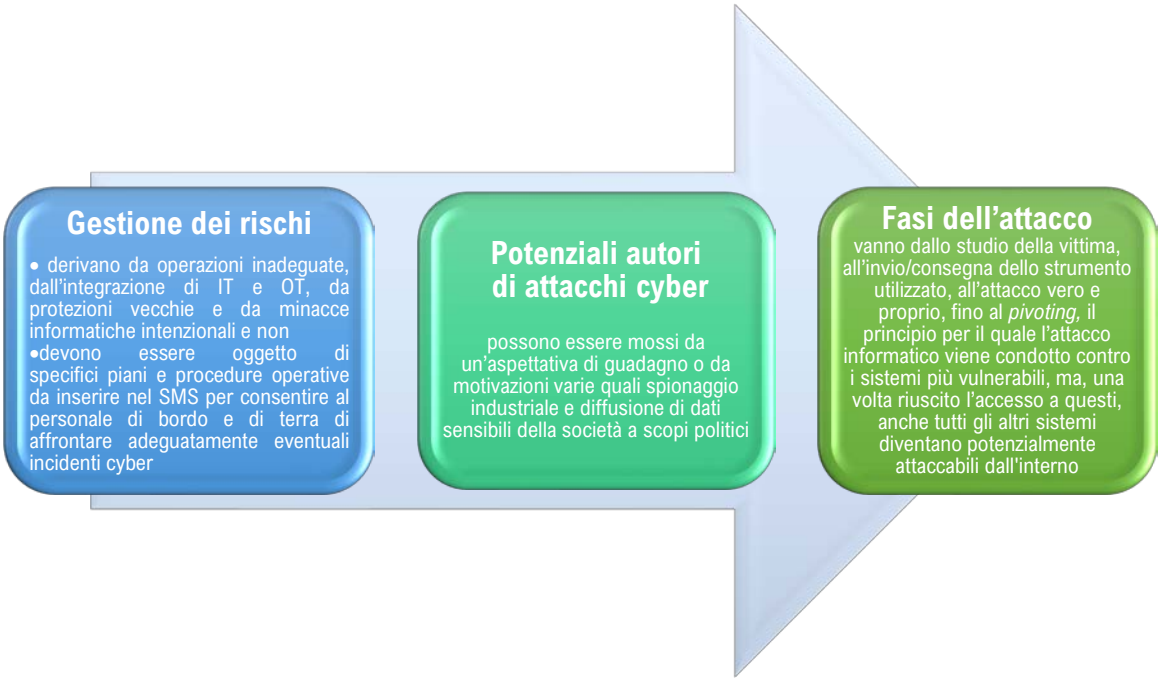
A garantire la tutela e la sicurezza dello Shipping a livello globale è intervenuta in primis l'International Maritime Organization (IMO) che nell'ambito del Maritime Safety Committee ha adottato, nel giugno del 2017, la Resolution MSC.428 (98) **"Maritime Cyber Risk Management in Safety Management Systems"** in cui si afferma che i rischi informatici dovrebbero essere considerati e gestiti nel sistema SMS in conformità con gli obiettivi ed i requisiti funzionali previsti dall'ISM Code[1]. Gli Armatori dovranno adeguare i sistemi di controllo alle prescrizioni entro il 2021, ma le compagnie marittime si sono già attivate in modo da rendersi adempienti con anticipo (attraverso, tra l'altro, l'individuazione di un Cyber Risk Officer). L'IMO - nel fornire orientamenti provvisori sulla gestione del rischio informatico marittimo - intende sottolineare l'esigenza per il settore dello Shipping di adottare un approccio di risk management resiliente ai pericoli e controllabile, tenendo conto dei costi e dei benefici delle azioni intraprese dalle parti interessate.

Rischi informatici e ISM Code

Il 2021 è vicino e ci sarà molto da fare per identificare rischi e vulnerabilità e prendere provvedimenti per prepararsi e rispondere alle minacce informatiche che possono interessare quasi ogni settore di una compagnia di navigazione.

[1] Entrato in vigore il 1° luglio 1988, l'ISM Code fornisce uno standard internazionale per la sicurezza nella gestione e nell'esercizio delle navi e per la prevenzione dell'inquinamento. I suoi obiettivi sono quelli di garantire la sicurezza in mare, prevenire danni alle persone o perdite di vite umane ed evitare danni all'ambiente, in particolare a quello marino. È applicabile a tutte le navi d'altura superiori a 500 GT e al loro Armatore o alla società di gestione responsabile dell'esercizio della nave. Il codice ISM prevede che gli armatori e gli operatori di navi mettano in atto un Sistema di Gestione della Sicurezza (SMS) che ne incorpori gli obiettivi e coinvolga la totalità delle operazioni della società e delle navi gestite.

Le Guidelines IMO – il cui obiettivo primario è quello di sostenere una navigazione sicura - pongono l'attenzione sulle seguenti aree:



ed evidenziano che un approccio completo al problema cyber deve coinvolgere tutti gli aspetti di gestione del rischio, da quello operativo al procedurale, fino al tecnico.

Anche la più grande delle associazioni marittime internazionali che rappresentano gli armatori, il Baltic and International Maritime Council (BIMCO), nel luglio del 2019, ha offerto il proprio contributo al riguardo, pubblicando **"The Guidelines on Cyber Security on Board Ships"**, che riprendono i temi affrontati dall'IMO e forniscono un utile sistema di valutazione e gestione degli attacchi, che include la classificazione del rischio (impatto potenziale basso/medio/alto) e incoraggiano inoltre la formazione sia del personale di bordo (inclusi comandanti e ufficiali) che di quello a terra, al fine di promuoverne la conoscenza di tutti i sistemi computerizzati e la consapevolezza di come la sicurezza possa essere compromessa da un incidente informatico. Secondo le Guidelines citate, un approccio manageriale alla gestione del rischio cibernetico richiede, in primo luogo, uguale attenzione alla *cyber security* e alla

cyber safety, entrambe importanti per il loro potenziale effetto sul personale, la nave, l'ambiente, la società e il carico. La *cyber security* riguarda la protezione di IT, OT, informazioni e dati da accessi non autorizzati, tentativi di manipolazione e interruzione di attività; la *cyber safety* riguarda i rischi derivanti dalla perdita di disponibilità o integrità dei dati critici per la sicurezza e l'OT.

Information Technology e Operation Technology

In estrema sintesi, i sistemi OT controllano il mondo fisico e, quindi, i dispositivi materiali e i processi; i sistemi IT riguardano lo spettro delle tecnologie per l'elaborazione delle informazioni, inclusi software, hardware e tecniche di comunicazione. Con Internet questi sistemi storicamente indipendenti si stanno avvicinando ed integrando.

La corretta gestione del rischio cyber (Cyber Risk management approach) - come declinata nelle Guidelines - prevede una serie di azioni su ciascuna delle quali ci soffermeremo brevemente.

Figure 1: Cyber risk management approach as set out in the guidelines

1 Identificare le minacce

Secondo le linee guida le minacce possono pervenire da quattro gruppi diversi, ciascuno con motivazioni e obiettivi differenti. In aggiunta è anche possibile che il personale di bordo o di terra arrivi a compromettere la sicurezza del sistema, in generale per errore o in modo non intenzionale, ma senza poter totalmente escludere l'eventualità di un intervento doloso.

Group	Motivation	Objective
Activists (including disgruntled employees)	▪ reputational damage ▪ disruption of operations	▪ destruction of data ▪ publication of sensitive data ▪ media attention ▪ denial of access to the service or system ▪ targeted
Criminals	▪ financial gain ▪ commercial espionage ▪ industrial espionage	▪ selling stolen data ▪ ransoming stolen data ▪ ransoming system operability ▪ arranging fraudulent transportation of cargo ▪ gathering intelligence for more sophisticated crime, exact cargo location, ship transportation and handling plans etc
Opportunists	▪ the challenge	▪ getting through cyber security defences ▪ financial gain
States/State sponsored Organisations/Terrorists	▪ political gain ▪ espionage	▪ gaining knowledge ▪ disruption to economies and critical national infrastructure

Table 2: Motivation and objectives THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS v3

In generale esistono due categorie di cyber attack che possono impattare su compagnie di navigazione e navi. Gli attacchi non mirati dove la nave, i dati, il sistema colpito rappresentano uno dei tanti potenziali bersagli; gli attacchi mirati dove la nave, i dati, il sistema colpito costituiscono proprio gli obiettivi perseguiti. Aldilà delle varie forme di attacchi informatici (phishing, spear phishing, botnet e water holing) che sono spiegate nel documento, l'aspetto essenziale in caso di attacco è rappresentato dalla consapevolezza del personale riguardo ai potenziali rischi per la sicurezza informatica e dal livello di preparazione ed addestramento a identificarne la natura e a mitigare il rischio.

2 Individuare i punti deboli

È importante che, nel valutare i rischi informatici, l'azienda consideri anche i rischi per il business che possono derivare dalle misure di sicurezza informatica e come tali misure influenzeranno le pratiche e le relazioni commerciali sia interne che con i clienti.

Le Guidelines BIMCO suggeriscono che la **Cyber Security Framework** elaborata dal **National Institute of Standards and Technology (NIST)** - organo ufficiale del governo USA per la sicurezza informatica - può aiutare a sviluppare un approccio corretto alla sicurezza.

Le fasi descritte dal NIST sono Identificare, Proteggere, Rilevare, Rispondere, Ripristinare.

Una prima valutazione del rischio richiede la verifica di una serie di aspetti e variabili. Si tratta di una sorta di check list: quali sistemi informatici e quali tecnologie operative sono vulnerabili? Quali sono i principali aspetti di debolezza? Vi è incluso il fattore umano?

Il risultato finale della valutazione dovrebbe essere una relazione che identifichi tutte le vulnerabilità e valuti il rischio in termini di impatto e probabilità. Dovrebbero inoltre essere raccomandate azioni correttive per ridurre il rischio.

3 Valutare l'esposizione al rischio

La valutazione del rischio informatico dovrebbe iniziare a livello di alta dirigenza di una società, anziché essere immediatamente delegata al responsabile della sicurezza della nave o al capo del dipartimento IT.

Il modello CIA[2] fornisce un quadro per la valutazione dell'impatto che possono avere

- un accesso non autorizzato e la divulgazione di informazioni o dati relativi alla nave, all'equipaggio, al carico e ai passeggeri,
- la perdita di integrità, che potrebbe modificare o distruggere informazioni e dati relativi ad una sicura ed efficiente gestione e amministrazione della nave,
- la perdita di disponibilità a causa della distruzione delle informazioni e dei dati e/o dell'interruzione di servizi e del funzionamento dei sistemi navali.

Il processo di stima del rischio inizia con la valutazione dei sistemi di bordo da parte della stessa compagnia di navigazione, al fine di mapparne la robustezza per gestire l'effettivo livello di minacce informatiche. La valutazione dovrebbe coinvolgere i sistemi IT e OT a bordo.

Le autovalutazioni possono essere un buon inizio, ma andrebbero integrate con le verifiche effettuate da terze parti, in grado di approfondire e individuare i rischi e le lacune che non sono stati riscontrati durante l'autovalutazione.

[2] Il modello CIA descrive i tre obiettivi primari della sicurezza informatica. La C sta per riservatezza (CONFIDENTIALITY). La sicurezza informatica richiede privacy nei dati e nelle informazioni che non dovrebbero essere visibili indiscriminatamente. La I sta per integrità (INTEGRITY). La sicurezza informatica impone di essere sicuri che i dati trasmessi, elaborati e memorizzati non siano stati modificati rispetto alla loro forma originale, né accidentalmente né intenzionalmente. Infine, la lettera A sta per disponibilità (AVAILABILITY). Gli utenti autorizzati dovrebbero essere in grado di accedere alle risorse di cui hanno bisogno per svolgere il loro lavoro con facilità.

Mitigazione dei rischi

4

Le misure da adottare per ridurre o mitigare il rischio saranno uniche per ogni azienda. In generale ci saranno due tipi di risposta: le risposte tecniche, quelle che riguardano direttamente le attrezzature, e quelle procedurali che si concentreranno maggiormente sul modo in cui i sistemi sono utilizzati e come gli esseri umani interagiscono con i sistemi. Le risposte tecniche saranno quelle che possono fornire vittorie rapide. Per ottenere un controllo procedurale è necessario modificare le pratiche e gli atteggiamenti esistenti e sarà necessario aumentare la consapevolezza e la formazione; cosa che richiederà tempo.

Avere un piano B

5

In contemporanea all'attivazione dei sistemi di protezione occorre che vengano sviluppati e posti in essere piani di emergenza per tenere conto di vari scenari imprevisti. Le linee guida hanno individuato un elenco di alcuni degli elementi critici relativi alle navi:

- sapere cosa fare in caso di disabilitazione o manipolazione di tutti i tipi di apparecchiature elettroniche di navigazione;
- sapere cosa fare in caso di disabilitazione o manipolazione dei sistemi di controllo per la propulsione, dei sistemi ausiliari e di altri sistemi critici;
- saper verificare l'integrità dei dati nei casi di sospetta violazione;
- conoscere le procedure per la gestione di eventi ransomware;
- saper affrontare le contingenze operative in caso di perdita di dati locali.

6 Risposta, ripristino, indagine

Un incidente informatico richiede una reazione ossia un processo che porti in primo luogo alla identificazione dell'incidente stesso, ad indagarne, quindi, le cause e, infine, al recupero dei dati/sistemi interessati.

Il recupero delle funzioni essenziali della nave o del sistema relative al funzionamento e alla navigazione in condizioni di sicurezza può essere necessario con l'assistenza a terra. Come e dove ottenere assistenza, ad esempio procedendo verso un porto, deve far parte del *recovery plan* stabilito di concerto tra le parti interessate (comandante della nave, armatore, operatore di terra). Le indagini dovrebbero consentire una migliore comprensione delle minacce cui sono esposte le compagnie di navigazione e le navi che esse operano, compresi gli insegnamenti tratti e gli eventuali aggiornamenti necessari per i controlli tecnici e procedurali.

Un altro aspetto legato alla prevenzione degli incidenti di sicurezza considerato da BIMCO riguarda i fornitori esterni. I servizi erogati dalle aziende sono infatti sempre più integrati all'interno di processi produttivi e lo scambio di informazioni con soggetti terzi (noleggiatori, appaltatori e fornitori di servizi, operatori logistici, autorità di controllo) diventa imprescindibile per il raggiungimento dei risultati attesi e impone, allo stesso tempo, un'armonizzazione delle procedure di *cyber security* fra i vari attori della filiera.

Tra l'altro la mancata adozione di un efficace sistema di prevenzione e di gestione di un cyber attack potrebbe integrare un caso di *unseaworthiness* (innavigabilità della nave) e di mancato esercizio della dovuta diligenza nel rendere la nave idonea alla navigazione e, pertanto, una violazione degli articoli III.1 e IV.1 delle Hague Visby Rules.
Art. 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 …
Art. 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 ….. Whenever loss or damage has resulted from unseaworthiness the burden of proving the exercise of due diligence shall be on the carrier or other person claiming exemption under this article.

In sintesi, un piano efficace di *cyber security* nel settore marittimo implica il coinvolgimento di tutti gli assi portanti del sistema: tecnologie, processi, elemento umano. Inoltre, richiede un costante *risk assessment* in quanto tecnologie e strumentazioni connesse portano in dote nuovi rischi.

Per quanto si possa essere preparati, il rischio che una minaccia informatica si concretizzi è elevato. Ogni organizzazione dovrebbe pertanto puntare sulla preparazione a reagire e a riprendersi, sviluppando in tal modo la propria resilienza.

Gli orientamenti e le decisioni prese dai vertici a livello operativo e di gestione dei media sono essenziali per la continuità aziendale.

I dipendenti a tutti i livelli (basso-medio-alto) dovrebbero essere consapevoli delle possibili minacce informatiche e dei piani di risposta per mitigare i danni

Essere proattivi è un must; pertanto, un investimento nella protezione dell'organizzazione e la consapevolezza dei dipendenti si dimostrano essere più economici rispetto alla conseguente perdita finanziaria dovuta ad attacchi informatici

Piani di risposta e di ripristino dovrebbero essere testati e aggiornati frequentemente al fine di includere nuove azioni di mitigazione delle possibili minacce informatiche

LA STRATEGIA EUROPEA

In un mondo sempre più connesso, dove entro il 2024 dovrebbero essere utilizzati 22,3 miliardi di dispositivi IoT, le crescenti sfide nel panorama della sicurezza informatica hanno portato l'UE a riflettere su come migliorare la protezione dei suoi cittadini e delle sue aziende contro le minacce e gli attacchi informatici.

All'interno dell'Unione europea, i primi documenti ufficiali attinenti alla sicurezza delle reti e delle informazioni risalgono agli inizi del 2000, a testimonianza del fatto che questa tematica è relativamente nuova ed in continua evoluzione. L'approccio europeo alla *cyber security* ha proceduto, in questi anni, a passi relativamente lenti, soprattutto se paragonati a quelli di alcuni paesi come Stati Uniti o Regno Unito. Nel febbraio 2013 l'Unione europea ha adottato la propria strategia di cyber sicurezza, invitando tutti gli Stati membri a fare altrettanto, allo scopo principale di garantire uno spazio cibernetico "aperto e sicuro", accessibile a tutti e, allo stesso tempo, dotato degli strumenti adeguati ad assicurare la riservatezza dei dati e delle informazioni in esso contenuti.
Il documento delinea cinque priorità fondamentali.

1. Sviluppare la Cyber resilienza

Sviluppare, cioè, la capacità di una rete o di un sistema di preservare le proprie capacità ed i propri servizi, in caso di attacco. Altrettanto importante per la *cyber security* e complementare a ciò è la capacità di *recovery,* vale a dire il ripristino delle funzioni allo stadio iniziale.

2. Ridurre il Cybercrime

Attuare una lotta drastica al *cybercrime*, che rappresenta oggi la causa principale di perdite di tipo economico, soprattutto a danno del settore privato.

Frodi telematiche, violazione dei dati personali, furto della proprietà intellettuale e dell'identità digitale, spionaggio industriale: questi fenomeni sono all'ordine del giorno e causano danni economici estremamente rilevanti e probabilmente sottostimati.

3. Cyber difesa e PSDC

Sviluppare una politica e capacità di cyber difesa connesse alla Politica di Sicurezza e di Difesa Comune. La *cyber defence*, quindi, si presenta rilevante al fine di tutelare la difesa e gli interessi di sicurezza nazionale degli Stati membri. Per garantire un'adeguata *cyber defence*, è necessario coinvolgere tutti gli aspetti del processo di sviluppo delle capacità: la dottrina, la leadership, l'organizzazione, il personale, la formazione, la tecnologia, l'infrastruttura, la logistica e l'interoperabilità.

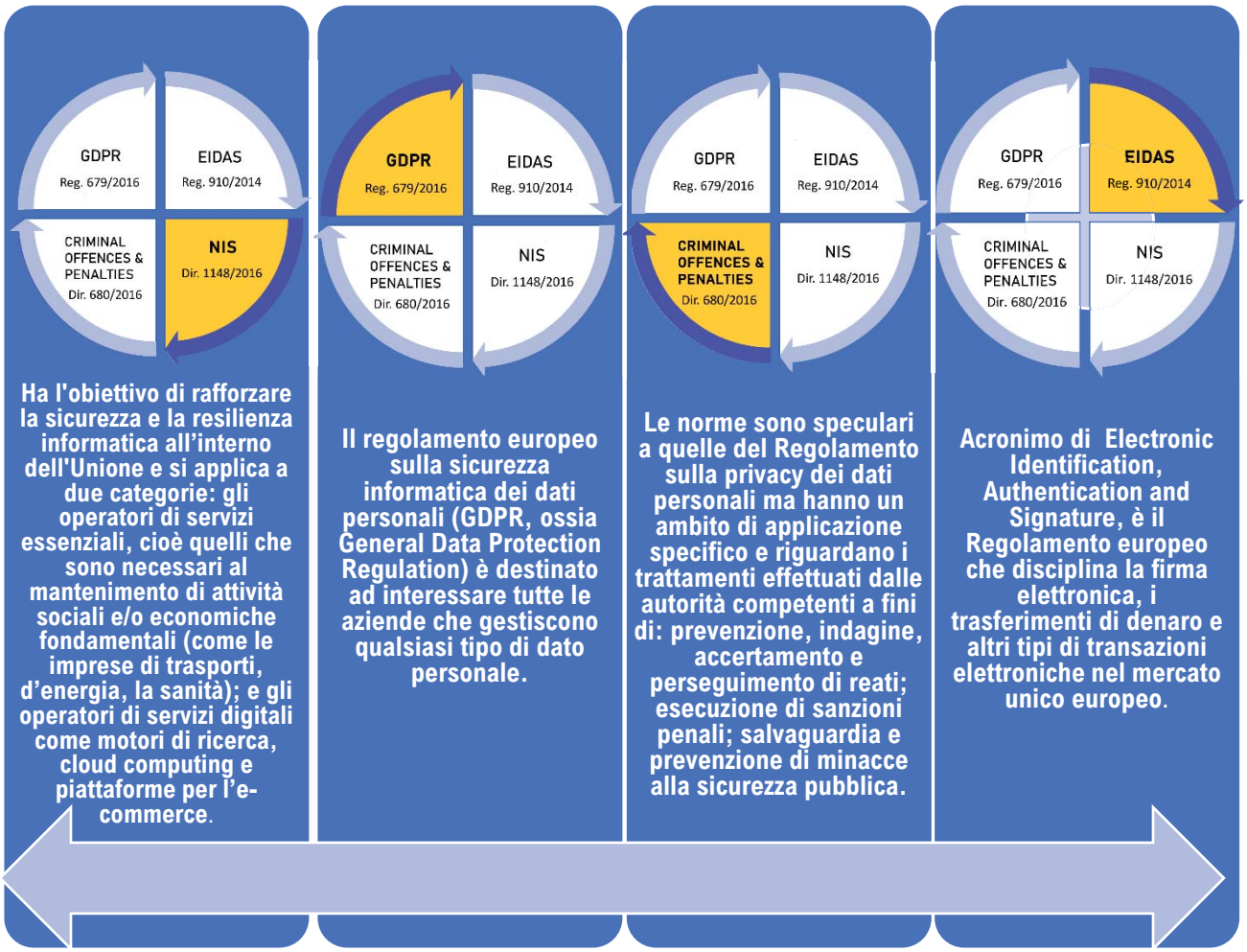
4. Sviluppare le risorse per la Cyber sicurezza

Sottolineare l'importanza di progredire dal lato tecnologico, per essere in grado di gestire le situazioni di crisi.

5. Cyber sicurezza e politica internazionale

Creare una politica internazionale coerente dell'Unione europea sul cyber spazio e promuovere i valori costitutivi dell'UE. La quinta priorità proietta la questione della *cyber security* sul piano internazionale, a testimonianza del fatto che solo una proficua collaborazione a livello globale può portare a risultati importanti, nella sfida contro le minacce asimmetriche provenienti dal cyber spazio.

Il 2018 è stato l'anno della sicurezza informatica. L'Europa ha varato una cornice di riferimento sulla *cyber security* costituita da due regolamenti e due direttive, entro cui si collocano tutte le leggi e le applicazioni nazionali.



La direttiva NIS è stata resa esecutiva in Italia con il decreto legislativo 18 maggio 2018, n. 65. Il decreto – nonostante la facoltà concessa dall'UE agli Stati membri di estendere l'ambito di applicazione delle disposizioni - ha mantenuto l'impostazione della direttiva focalizzata su alcuni settori (ossia energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali; nonché motori di ricerca, servizi cloud e piattaforme di commercio elettronico).

Nel giugno 2019 entra in vigore il *Cyber Security Act*, il regolamento volto a creare un quadro europeo per la certificazione della sicurezza informatica di prodotti ICT (Information and Communication Technologies) e servizi digitali, e a rafforzare il ruolo dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA). La sicurezza informatica rimane un'area prioritaria per ulteriori azioni negli anni a venire nell'ambito della nuova strategia digitale dell'UE per il 2019-2024. E ulteriori sforzi andranno fatti per superare le notevoli disparità esistenti nelle norme di implementazione adottate dai singoli Stati membri con riguardo, in particolare, alla gestione degli incidenti informatici.

Dall'inizio della pandemia di Covid-19, negli Stati membri si è registrato un aggravamento dell'attività cibernetica dannosa - anche in connessione ad un indebolimento delle misure di sicurezza informatica esistenti attraverso cambiamenti nei modelli di lavoro e di infrastruttura causati dalla crisi sanitaria - nonché dei rischi legati all'aumento dell'e-commerce e dei pagamenti online.

La pericolosità e pervasività del rischio cyber ha messo in luce l'importanza della prevenzione e della cooperazione tra Stati membri, attraverso la condivisione di informazioni e di *best practice*. Il 20 ottobre 2020, ENISA ha pubblicato un rapporto che consta di 22 diversi report che analizzano le prime 15 minacce informatiche nel corso del periodo gennaio 2019-aprile 2020 e fornisce linee guida per mitigarne gli effetti. Il rapporto identifica il malware come la minaccia informatica numero uno nell'UE, con un aumento del phishing, del furto di identità e del ransomware. La monetizzazione continua ad essere la motivazione primaria degli attacchi. L'emergenza COVID-19 ha inoltre portato ad un aumento di cyber-attacchi "personalizzati", utilizzando metodi e tecniche sempre più sofisticate.

Il 20 ottobre, ENISA ha pubblicato il rapporto Threat Landscape 2020 *"Cyber-attacks becoming more sophisticated, targeted, widespread and undetected*

PROFILI ASSICURATIVI

Il pericolo reale e attuale rappresentato dal rischio informatico per le imprese e la società deve essere affrontato su più livelli. L'assicurazione è una componente importante nella gestione di queste minacce in rapida crescita quale fattore di mitigazione e trasferimento del rischio. È indubbio che il settore assicurativo stia migliorando la comprensione della natura unica, mutevole e complessa del rischio informatico per fornire una solida copertura assicurativa ai propri clienti. D'altro canto, la mancanza di dati affidabili, il continuo e rapido mutamento delle minacce informatiche, la natura globale del rischio informatico con il suo potenziale di cumulo, sono tutti fattori che hanno condizionato lo sviluppo del mercato dell'assicurazione contro i rischi cyber.

Il ricorso a coperture contro i rischi informatici nel settore *Marine* è fenomeno relativamente recente anche se l'industria marittima sta cambiando rapidamente. Fino a poco tempo fa le navi erano isolate e il processo logistico non era tecnologicamente avanzato. Ma le sopravvenute esigenze di comunicazioni e connettività digitali stanno creando nuovi scenari, di efficienza ma anche di rischio.
Va rilevato che il mercato potenzialmente interessato è molto più grande di quello delle navi portacontainer che vengono in mente quali primario fattore di rischio.
Il settore *Marine* è molto ampio; ricomprende navi portarinfuse (bulk carrier), navi cisterna (tanker), navi passeggeri e navi da crociera. Ognuna ha profili di rischio molto diversi Il *Marine* comprende anche le operazioni portuali, le attività dei cantieri per container, dei cantieri navali tradizionali e la gestione dei terminali per rinfuse.
Ad oggi, la maggior parte degli attacchi registrati sono stati malware non mirati e di conseguenza per lo più i CdA all'interno del settore non hanno considerato la sicurezza informatica quale rischio prioritario.

Nonostante questo, ci sono molti potenziali vettori di attacco all'interno dell'industria marittima che potrebbero essere utilizzati per ottenere un punto d'appoggio in una rete e i casi Maersk e Cosco ne sono significativi esempi.
Inoltre, i rischi possono manifestarsi tanto sui sistemi di bordo, quanto al di fuori di essi. I sistemi di comunicazione satellitare e, quando vicino alla costa, le reti 4G e 5G consentono infatti di accedere alle reti e ai dati di bordo.
Da quanto detto finora emerge quanto risultino necessari skills trasversali per la gestione della *cyber security* nel settore marittimo.
Sussistono oggettive difficoltà riscontrabili – in parte comuni anche ad altre linee di business - legate a:

- mutevolezza degli scenari,
- insufficienza dei dati statistici sui sinistri che consenta la valutazione di un premio proporzionato al rischio,
- difficoltà di gestire le possibili accumulazioni di rischio derivanti da un attacco che colpisca più soggetti,
- difficoltà di valutare le misure preventive adottate dalle singole organizzazioni,
- criticità circa l'ammissibilità delle coperture dei riscatti per il rilascio dei dati,
- mancata denuncia degli attacchi per timore di perdere clienti, di spaventare gli azionisti o di subire danni reputazionali e d'immagine.

Si spiega quindi la riluttanza ad offrire una copertura per questi rischi anche se – sia pur lentamente - il mercato assicurativo sta fornendo risposte.

La maggior parte delle polizze assicurative che coprono navi, cantieri navali, strutture per la movimentazione del carico, merci includono la clausole di esclusione del mercato inglese (come noto il mercato di riferimento a livello mondiale per l'assicurazione e la riassicurazione *Marine* e *Aviation*) CL380 Institute Cyber Attack Exclusion Clause del 10/11/2003 che esclude dalla garanzia assicurativa qualsiasi perdita, danno o responsabilità causati, direttamente o indirettamente, dall'uso al fine di arrecare danno di un computer e dei relativi sistemi associati e software.

"..... 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".

CL 380
Cyber attack exclusion clause
10.11.2003

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*".
La stessa clausola è usata anche nei trattati di riassicurazione.
La formulazione della clausola 380 (praticamente impiegata a livello mondiale) è stata di recente ritenuta troppo restrittiva e drastica nelle esclusioni e quindi *not fit for purpose*. In effetti la copertura è esclusa anche quando il cyber è semplicemente un fattore scatenante di una perdita che sarebbe altrimenti coperta (ad es. un attacco al sistema di navigazione di una nave che comporta un grounding o il danneggiamento del carico). L'esclusione opera tutte le volte che viene impiegato un *electronic system*.

Ma che dire di una polizza di carico falsificata per ottenere la consegna del carico anziché con un *electronic device* tramite l'impiego di una fotocopiatrice?
La copertura è inoltre esclusa solo in caso di attacco informatico; ma cosa succede nel caso di una perdita (accidentale) di dati dovuta ad esempio ad un errore di digitazione o ad un aggiornamento tecnico di manutenzione che non va a buon fine?

Affirmative Cyber risk

insurance policies that explicitly include coverage for cyber risk

Non-affirmative cyber risk

policies that do not explicitly include or exclude coverage for cyber risk

For completeness, the 'non-affirmative' cyber risk is often referred to as 'silent' cyber risk

Inoltre, restano zone di ambiguità in quanto una polizza può offrire una copertura cyber "silente" se la Cl.380 non è utilizzata ma può offrire una copertura cyber silente per i *non malicious acts*, anche se la Cl.380 è impiegata.

Nel Regno Unito, la Prudential Regulation Authority (PRA) e gli stessi Lloyd's hanno evidenziato la necessità di dare certezza in caso di "*non-affirmative*" o "*silent*" *cyber cover*. In altre parole, gli assicuratori devono escludere il rischio espressamente oppure fornire una copertura a seguito di un processo di identificazione, quantificazione e gestione dell'esposizione al rischio cyber. Il Regolatore UK aveva evidenziato preoccupazioni in merito alla fornitura di copertura potenzialmente non intenzionale o poco chiara per rischi informatici all'interno di varie classi di attività assicurative. In particolare, ha declinato le aspettative delle società per quanto riguarda la fornitura di coperture *non-affirmative*, precedentemente note come "silenziose", contro i rischi informatici considerando i seguenti possibili approcci:

- adeguare il premio in modo da riflettere il rischio supplementare e offrire una copertura esplicita,

- introdurre forti esclusioni nella formulazione;
- e/o fissare limiti specifici di copertura.

In risposta al PRA, il Joint Cargo Committee – un Comitato unificato della Lloyd's Market Association (LMA) e dell'International Underwriting Association of London (IUA) – ha deciso di elaborare una nuova clausola da utilizzare nel mercato del trasporto merci e, dopo una serie di consultazioni, ha introdotto, nel luglio 2019, la JC2019-004, con l'obiettivo di sostituire la Cl. 380.

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
18.07.2019

1.2 Subject to paragraph 1.1 above, 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. (...)
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 otherwise recoverable under paragraph 1.2 but which affects more than this Insured or this Insured's property.
1.4 Any cover granted by virtue of this clause shall be limited to: -USD {response} *each and every loss, or series of losses arising out of one event and*
-USD {response} *in the annual aggregate.*

La clausola offre una copertura cibernetica "affermativa" ma con limitazioni che riflettono la propensione al rischio degli assicuratori del trasporto merci. Opera in caso di *malicious* e *non malicious cyber risks,* pone come condizione che gli assicuratori dimostrino una ragionevole conformità alle raccomandazioni e agli orientamenti internazionali in materia di cibernetica; fornisce la definizione dei termini "Software" e "Systemic loss" e prevede infine la possibilità di offrire un limite specificato e aggregato.

Le principali preoccupazioni degli assicuratori sono rappresentate dal rischio sistemico e dai potenziali fenomeni di aggregazione dei rischi.

La percezione è che mentre il carico è in transito (a bordo di un mezzo di trasporto) il rischio di aggregazione sia scarso. Le vere criticità sono invece costituite dalla giacenza del carico nei porti o nei depositi dei terminal.

I limiti previsti per evento ed in aggregato annuo dovrebbero consentire agli assicuratori di proteggersi contro esposizioni di tipo catastrofale.

Sempre in risposta alle indicazioni formulate dal PRA, in merito alla fornitura di coperture potenzialmente non intenzionali o non chiare sotto il profilo dei rischi informatici in vari rami del settore assicurativo, si collocano altre clausole inglesi sviluppate appositamente per il settore *Marine*.

Gli assicuratori nel Regno Unito sono tenuti ad applicare le nuove impostazioni dal 1° gennaio 2020.

LMA5402
Marine Cyber Exclusion
11.11.2019

La clausola oltre ad escludere tutti i rischi informatici, ha anche natura di clausola "paramount" destinata cioè a prevalere su qualsiasi disposizione di polizza incoerente con essa. Questa clausola è in realtà molto più ampia della CL 380 e "afferma" che i rischi informatici, con l'intento di infliggere danni o meno, sono assolutamente esclusi

LMA5403 Marine Cyber Endorsement
11.11.2019

Una copertura limitata per il cyber può essere fornita tramite questa clausola con la quale si dichiara in modo esplicito che se manca l'intento di infliggere danno le perdite, anche se derivanti da una "causa informatica" saranno tenute coperte alle condizioni di polizza

JCC Clause 437 Cyber Exclusion and Write Back
18.11.2019

Questa clausola rappresenta una parziale reinclusione in copertura dei rischi esclusi nella LMA 5402 su base "named perils", ossia solo se espressamente indicati in polizza. Si tratta in particolare dei rischi nominati di cui alla Institute Cargo Clause C (quella più restrittiva) più il rischio furto, indipendentemente dal fatto che la causa sia un cyber act malicious o accidentale.
È altresì prevista una sezione per stabilire eventuali sotto-limiti di copertura (per ovviare a potenziali esposizioni catastrofali), in linea con la richiesta del PRA di quantificare le esposizioni stesse

Marine Cargo Cyber Exclusion and Affirmation Endorsement – (JC2020-014)
29.06.2020

Clausola elaborata dal Joint Cargo Committee di Londra che riecheggia i contenuti della clausola dei Lloyd's LMA 5403 specifica per il Marine Cargo

Anche il mercato statunitense ha elaborato una clausola di esclusione cyber totale ed una per una parziale reinclusione del rischio cibernetico in polizza.

American Institute Cyber Exclusion Clause
11/06/2015

Adottata l'11 giugno del 2015 la clausola – il cui studio è stato avviato all'inizio del 2014, per una possibile sostituzione della London market Clause 380 la cui formulazione risale al 2003 - è applicabile a tutte le polizze Marine (responsabilità, corpi, merci) ed esclude le perdite o danni causati da atti informatici dannosi

American Institute Cyber Exclusion and Limited Buy-back Clause (12202019)

Approvata da AIMU Management Committee il 02.06.2020

Questa clausola mantiene comunque l'esclusione del rischio cyber dalla copertura ma ammette a certe condizioni la garanzia per danni o perdite alla merce causati da malicious cyber-related acts durante l'ordinario corso del viaggio (in due course of transit)

Con riguardo alle responsabilità armatoriali, le coperture, c.d. *Protection and Indemnity* dei P&I Clubs - associazioni mutualistiche (di armatori) specializzate in coperture assicurative a favore dei propri membri, contro possibili richieste di risarcimento da parte di equipaggio, passeggeri e terzi per collisione, danni materiali, inquinamento da idrocarburi, danni ambientali e rimozione di relitti - attualmente non contemplano specifiche esclusioni dei cyber risk. I membri sono quindi assicurati contro questi rischi anche quando gli eventi dannosi siano causati da un rischio informatico (ferma tuttavia l'esclusione dei rischi di guerra). Sono invece esclusi dalla copertura offerta dai P&I gli *excepted perils,* quali: i pericoli di guerra (a parte limitate eccezioni), danni per le radiazioni ionizzanti, commercio illegale di materiali pericolosi o gli "atti di Dio" (qualsiasi pericolo naturale al di fuori del controllo umano, come un terremoto o uno tsunami).

La protezione offerta dai P&I presuppone l'esistenza di una polizza di assicurazione della nave (polizza Corpi), cui si affianca, a tutela dell'armatore in tutte le ipotesi di danni e responsabilità da essa non coperti

L'International Group of P&I Clubs è costituito dalla quasi totalità degli armatori mondiali che ne sono anche membri; ciascuno di essi versa, un premio detto "call" in misura sufficiente a pagare le richieste in caso di sinistrosità, i costi di riassicurazione e l'amministrazione del Club.

Dalla breve sintesi riportata, si evince che in generale le coperture disponibili all'interno delle linee di assicurazione convenzionali spesso comportano lacune per quanto riguarda i rischi informatici. L'industria assicurativa marittima si sta attrezzando (con il mercato di Londra come sempre a fungere da apripista) ma l'esclusione dei rischi cyber è ancora un elemento prevalente. Tra gli strumenti che si stanno sviluppando per migliorare la garanzia offerta alla clientela figurano polizze stand-alone (ossia copertura assicurative a sé stanti) o estensioni di garanzia o ancora le "drop-down cover" (contratto di assicurazione complementare ad altra garanzia assicurativa, di cui abbia il medesimo oggetto, e operante solo per la parte di danno che supera l'indennizzo dovuto dal primo assicuratore). Queste protezioni aggiuntive per il rischio informatico sono destinate a crescere in linea con la continua espansione del fenomeno. È pur vero che le polizze stand-alone che abbiano come rischio primario il cyber (e quindi di tipo *all risks* per cui se il virus colpisce i sistemi OT ogni perdita, danno responsabilità è coperto nei limiti di polizza) sono pochissime.

Anche se rimangono molte questioni in sospeso, ciò che sembra certo è che le questioni informatiche nell'industria marittima rimarranno in prima piano, per i soggetti che operano nel settore e per gli assicuratori *Marine,* per il prossimo futuro.

There has been a massive 400% increase in attempted hacks since February 2020 coinciding with a period when the maritime industry turned to greater use of technology and working from home due to the Coronavirus pandemic.

Israeli cybersecurity specialist
Naval Dome

LE CLAUSOLE INTERNAZIONALI

(richiamate nell'ordine in cui appaiono nel documento)

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.

1.2 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.

10/11/03
CL380

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.

1.2 Subject to paragraph 1.1 above, 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.

For the purpose of this clause, 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 otherwise recoverable under paragraph 1.2 but which affects more than this Insured or this Insured's property.

1.4 Any cover granted by virtue of this clause shall be limited to:-

USD {*response*} each and every loss, or series of losses arising out of one event and
USD {*response*} in the annual aggregate.

JC2019-004
18/07/2019

Marine Cyber Exclusion

This clause shall be paramount and shall override anything in this insurance inconsistent therewith.

1 In no case shall this insurance cover any loss, damage, liability or expense directly or indirectly caused by, contributed to by or arising from:

1.1 the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system, or

1.2 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.

LMA5402
11 November 2019

Marine Cyber Endorsement

1 Subject only to paragraph 3 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, computer process or any other electronic system.

2 Subject to the conditions, limitations and exclusions of the policy to which this clause attaches, the indemnity otherwise recoverable hereunder shall not be prejudiced by the use or operation of any computer, computer system, computer software programme, computer process or any other electronic system, if such use or operation is not as a means for inflicting harm.

3 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, paragraph 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.

LMA5403
11 November 2019

JCC Cyber Exclusion and Write-Back Clause

This clause shall be paramount and shall override anything in this (re)insurance inconsistent therewith.

1. In no case shall this insurance cover any loss, damage, liability or expense directly or indirectly caused by, contributed to by or arising from:

   1.1 the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system, or

   1.2 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. In consideration of an additional premium and subject to any deductibles contained within the Policy to which this insurance attaches, paragraph 1 will not apply to physical loss or physical damage, general average or salvage charges covered elsewhere in this insurance where directly caused by or arising from one or more of the perils listed below:-

   (a) fire or explosion
   (b) vessel or craft being stranded grounded sunk or capsized
   (c) overturning or derailment of land conveyance
   (d) collision or contact of vessel craft or conveyance with any external object
   (e) general average sacrifice
   (f) jettison
   (g) theft

where such peril results from:-

2.1 the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system, or

2.2 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.

3. Any cover granted by virtue of paragraph 2 of this clause will be subject to a limit of:-

(a) {*response*} each and every loss, or series of losses arising out of one event.

(b) {*response*} in the aggregate for the period of insurance.

These sub-limits shall apply within the full Policy limit and not in addition thereto.

4. Any cover granted by virtue of this clause will be subject to an additional premium of:-

{response}

CL. 437
18/11/2019

Marine Cargo Cyber Exclusion and Affirmation Endorsement

1 Notwithstanding anything within this (re)insurance to the contrary and subject only to paragraph 3 below, in no case shall this (re)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, computer process or any other electronic system.

2 Subject to the conditions, limitations and exclusions of the policy to which this clause attaches, the indemnity otherwise recoverable hereunder shall not be prejudiced by the use or operation of any computer, computer system, computer software programme, computer process or any other electronic system, if such use or operation is not as a means for inflicting harm.

3 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, paragraph 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.

JC2020-014
29 June 2020

American Institute
CYBER EXCLUSION CLAUSE
(11/06/2015)

This clause shall be paramount and shall override anything contained in this insurance (including any endorsement(s)) inconsistent therewith.

In no case shall this insurance cover loss, damage, liability, or expense directly or indirectly caused by or contributed to or arising from

1. any “malicious act” involving the use of any “computer system”, "electronic data communications system", “computer virus”, or process or any other electronic system; and/or

2. any access to or disclosure of any “personally identifiable information” or any person's or organization's confidential information, including, but not limited to, patents, trade secrets, processing methods, customer lists, financial information, credit card information, or any other type of nonpublic information; and/or

3. any action or omission that violates or is alleged to violate any federal, state or local statute that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating, or distribution of any written or electronic material or information.

Where this policy provides coverage for War Risks, section 1 above shall not operate to exclude losses which would otherwise be covered by such War Risks coverage.

Definitions

"Computer system" means computer hardware of any kind; "electronic computer program"; "electronic data processing media"; operating system; media microchip; microprocessor (computer chip); integrated circuit or similar device; computer network and networking equipment; firmware; server; website; extranet; and all input, output, processing, storage, and off-line media libraries.

"Computer virus" means any corrupting, harmful or otherwise unauthorized instructions or code including, but not limited to, any maliciously introduced unauthorized instructions or code, programmatic or otherwise, that propagate themselves through a “computer system” or network of whatsoever nature.

"Electronic computer program" means computer software, application software, and other recorded instructions for the processing, sequencing, collecting, transmitting, recording, retrieval, or storage of "electronic data".

"Electronic data" means information or knowledge recorded or transmitted in a form usable in a "computer system", microchip, integrated circuit or similar device in non-computer equipment, and which can be stored on "electronic data processing media" for use by an "electronic computer program".

"Electronic data communications system" means any communication system, including a "computer system" and the internet, which provides the Assured with access to another "computer system", microchip, integrated circuit or similar device in non-computer equipment, or which provides any party access to the Assured's "computer system", microchips, integrated circuits or similar devices in non-computer equipment.

"Electronic data processing media" means punch cards, paper tapes, floppy disks, CD-ROM, hard drives, magnetic tapes, magnetic discs or any other tangible personal property on which "Electronic data" or "electronic computer programs" are recorded or transmitted, but not the "electronic data" or "electronic computer programs" themselves. Money or securities are not "electronic data processing media".

"Malicious act" shall mean the intentional and wrongful action or actions of one or more persons, whether or not agents of a sovereign power.

"Personally identifiable information" shall mean information, whether printed or digital, encrypted or unencrypted, in the care custody or control of any Assured which alone or in conjunction with other information can be used to uniquely identify an individual. However, "personally identifiable information" does not include information which is lawfully available to the general public.

American Institute

Cyber Exclusion and Limited Buy Back Clause (Cargo)

(FINAL 12202019)

CYBER EXCLUSION

In no case shall this insurance cover loss, damage, liability, or expense directly or indirectly caused by or contributed to or arising from

A. any "malicious act" involving the use of any "computer system", "electronic data communications system", "computer virus", or process or any other electronic system; and/or

B. any access to or disclosure of any "personally identifiable information" or any person's or organization's confidential information, including, but not limited to, patents, trade secrets, processing methods, customer lists, financial information, credit card information, or any other type of nonpublic information; and/or

C. any action or omission that violates or is alleged to violate any federal, state or local statute that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating, or distribution of any written or electronic material or information.

LIMITED BUY BACK

The limited coverage provided below remains subject to all other terms, conditions, limitations and exclusions contained in the Policy to which this endorsement is attached and all other endorsements thereto.

Notwithstanding the CYBER EXCLUSION section above, this insurance shall cover loss, damage, or expense directly caused by or contributed to or arising from the risks described in A above only, **PROVIDED THAT:**

(1) any such claim recoverable under A above is not otherwise excluded by the Free of Capture & Seizure Warranty, Extended Radioactive Contamination Exclusion Clause (Extended RACE Clause), Delay Warranty, Accumulation Clause or Chemical, Biological, or Bio-Chemical and Electromagnetic Exclusion Clause (CBE) Clause) in the Policy to which this endorsement is attached; and

(2) the property insured must be in the ordinary course of transit; and

(3) the Assured must register an official complaint with the Federal Bureau of Investigation (FBI) and the Internet Crime Complaint Center (IC3) or equivalent reporting agencies of other countries or equivalent agencies of any sovereign power where property is being transported from or to within 60 days of the discovery of the occurrence which gives rise to coverage; and

(4) In any event coverage provided for herein, **shall terminate**:

(i) As per the Warehouse to Warehouse Clause, Marine Extension Clause, 60 Day South American Clause and any other clauses relating to duration of transit contained or endorsed onto the Policy; or

(ii) on delivery to the consignee's or other final warehouse or place of storage at the destination named herein; or

(ii) on delivery to any warehouse or place of storage, whether prior to or at the destination named herein, which the Assured elects to use either for storage other than in the ordinary course of transit or for allocation or distribution; or

(iv) in respect of marine transits, on the expiry of 60 days after completion of discharge overside of the property insured from the vessel at the port of discharge; or

(v) in respect of air transits, on the expiry of 30 days after unloading the property insured from the aircraft at the place of discharge;

whichever shall first occur.

Nothing in this endorsement shall be construed to cover any loss, damage or expense directly or indirectly caused by or contributed to or arising from any of the following:

a. loss of market, inherent vice, and delay;

b. business interruption and consequential loss howsoever;

c. infidelity or any dishonest act done by or at the instigation of the Assured;

c. hostilities, warlike operations, civil war, revolution, rebellion or insurrection, or civil strife arising therefrom;

Where this policy provides coverage for War Risks, the CYBER EXCLUSION above shall not operate to exclude losses which would otherwise be covered by such War Risks coverage.

This coverage shall be subject to a limit of $ _____ per any one occurrence, but in no event to exceed $_____ in any 12 month period in consideration of a premium of $_____.

DEDUCTIBLE: $_____each loss/occurrence

Notwithstanding anything contained elsewhere herein, this clause does not extend to any other limit of insurance provided by the Policy to which this endorsement is attached or any other endorsement thereto.

Definitions

"Computer system" means computer hardware of any kind; "electronic computer program"; "electronic data processing media"; operating system; media microchip; microprocessor (computer chip); integrated circuit or similar device; computer network and networking equipment; firmware; server; website; extranet; and all input, output, processing, storage, and off-line media libraries.

"Computer virus" means any corrupting, harmful or otherwise unauthorized instructions or code including, but not limited to, any maliciously introduced unauthorized instructions or code, programmatic or otherwise, that propagate themselves through a “computer system” or network of whatsoever nature.

"Electronic computer program" means computer software, application software, and other recorded instructions for the processing, sequencing, collecting, transmitting, recording, retrieval, or storage of "electronic data".

"Electronic data" means information or knowledge recorded or transmitted in a form usable in a "computer system", microchip, integrated circuit or similar device in non-computer equipment, and which can be stored on "electronic data processing media" for use by an "electronic computer program".

Electronic data communications system" means any communication system, including a "computer system" and the internet, which provides the Assured with access to another "computer system", microchip, integrated

circuit or similar device in non-computer equipment, or which provides any party access to the Assured's "computer system", microchips, integrated circuits or similar devices in non-computer equipment.

"Electronic data processing media" means punch cards, paper tapes, floppy disks, CD-ROM, hard drives, magnetic tapes, magnetic discs or any other tangible personal property on which "Electronic data" or "electronic computer programs" are recorded or transmitted, but not the "electronic data" or "electronic computer programs" themselves. Money or securities are not "electronic data processing media".

"Malicious act" shall mean the intentional and wrongful action or actions of one or more persons, whether or not agents of a sovereign power.

"Personally identifiable information" shall mean information, whether printed or digital, encrypted or unencrypted, in the care custody or control of any Assured which alone or in conjunction with other information can be used to uniquely identify an individual. However, "personally identifiable information" does not include information which is lawfully available to the general public.

BIBLIOGRAFIA

(principali riferimenti consultati)

- EIOPA Strategy on cyber underwriting, 2020
- ENISA Threat Landscape, 2020
- IOCTA 2020 Europol internet organised crime threat assessment
- OECD (2020) Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation
- Rapporto CLUSIT 2020 sulla sicurezza ICT in Italia
- Willis Towers Watson, Cyber risk in the maritime sector, 2020
- The Cyber Threat Preparedness in the Maritime Logistics Industry, 2020
- CyRiM report 2019, Shen attack-Cyber risk in Asia Pacific ports
- BIMCO, The Guidelines on Cyber Security onboard Ships - Version 3, 2018
- National Institute of Standards and Technology - Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018
- Dadiani, Davit, "Cyber-security and marine insurance" (2018). World Maritime University Dissertations.607
- IMO Resolution MSC.428 (98) Maritime Cyber Risk Management in Safety Management Systems, 2017
- Il rischio di attacchi cyber nel settore marittimo e le nuove linee guida BIMCO sulla sicurezza informatica (HFW), 2017
- Cyber Risks in the Marine Transportation System -The U.S. Coast Guard Approach, 2017
- Bank of England, Prudential Regulatory Authority - Policy Statement | PS15/17 Cyber insurance underwriting risk, July 2017
- Maritime Insurance Cyber Security – Framing the Exposure (Swiss Re), 2015
- The risk of cyber-attack to the Maritime sector (Marsh), 2014

There are only two types of companies: those that have been hacked and those that will be

Robert S Mueller III, Director Federal Bureau of Investigation
RSA Cyber Security Conference