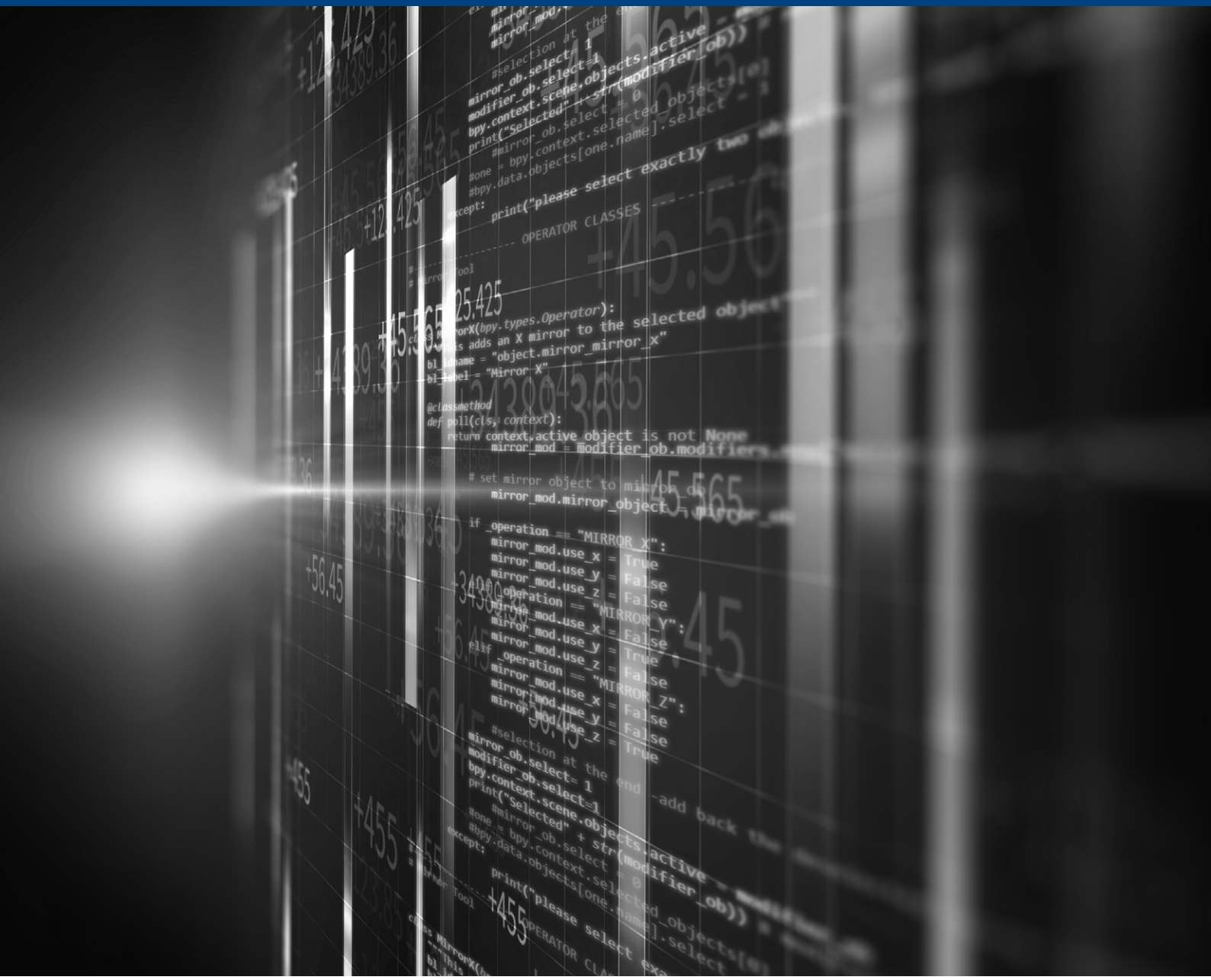

IL RISCHIO DI ATTACCHI CYBER NEL SETTORE MARITTIMO E LE NUOVE LINEE GUIDA BIMCO SULLA SICUREZZA INFORMATICA

Il CEO della IBM ha definito la criminalità informatica come, *"la più grande minaccia per tutte le società del mondo"* e Forbes prevede che i costi dovuti alla criminalità informatica raggiungeranno i US$2 milliardi entro il 2019. Nel 2015, un'indagine svolta dal CEO di Fortune 500 ha messo in luce come la sicurezza informatica fosse una delle sfide più grandi che devono essere affrontate dalle società.

“Il non riuscire a proteggere la nave da un evento cyber potrebbe essere considerato un mancato esercizio della dovuta diligenza nel rendere la nave idonea alla navigazione, e anche una violazione degli Articoli 3(1) e 4(1) delle Regole dell’Aja/Aja-Visby.”

In un caso di pirateria informatica, un gruppo di malfattori ha usato delle email trappola per sottrarre i login di accesso ai sistemi di controllo di un’acciaieria tedesca per cui una parte degli impianti è venuta meno, con il risultato che un altoforno non poteva essere spento come normalmente avviene, causando un danno enorme.

Il settore marittimo non è rimasto immune dalle conseguenze derivanti dal cyber attacco effettuato dal ransomware NotPetya lo scorso giugno ai danni di imprese ed istituzioni.

Molte imprese marittime ne sono rimaste colpite, tra queste anche il colosso Maersk che ha stimato un danno di circa $ 300 milioni, subendo la chiusura di alcuni terminal portuali gestiti dalla sua controllata APM.

Invero, per lungo tempo si era creduto che il settore shipping necessitasse di una maggiore protezione nei confronti di hackers, ma tale necessità era stata forse fino ad oggi in parte sottovalutata.

Oggi più che mai, le imprese del settore sono divenute consapevoli che le operazioni di trasporto marittimo sono esposte a questo tipo di rischi.

Infatti, il pericolo di un attacco riguarda non solo i sistemi informatici delle compagnie di navigazione ed i dati sensibili ivi contenuti, ma coinvolge anche le stesse navi, le quali sono sempre più computerizzate e quindi anch’esse esposte alla pirateria informatica.

I Malware, tra cui NotPetya e molti altri virus, infatti, sono progettati per diffondersi da computer a computer su di un network, il che vuol dire che dispositivi collegati a bordo di navi sono anch’essi potenzialmente esposti.

Ovviamente, il settore marittimo, come molti altri, ha ancora tanto su cui lavorare per queste questioni, ma la consapevolezza di ciò sta man mano crescendo ed il recente attacco ransomware ha dimostrato che le questioni relative alla cyber-security vanno prese seriamente.

In questa edizione speciale del Bollettino Marittimo, riportiamo i recenti sviluppi in materia, anche per quanto attiene alle nuove linee guida recentemente lanciate dal BIMCO e dall’IMO, con l’intento di aiutare gli armatori a proteggersi dagli attacchi di pirateria informatica. Inoltre, analizziamo alcune questioni contrattuali che riguardono i rischi di attacchi cyber.

Definizione di rischio cyber

Il rischio posto da un attacco cyber ai sistemi informatici è definito dall’Institute of Risk Management come *“qualsiasi rischio legato a perdite finanziarie, turbative o danni all’immagine di un’organizzazione derivante da un’avaria nei suoi sistemi informatici”*. In realtà, si tratta di molto di più di un semplice guasto dei sistemi informatici, includendo anche l’infiltrazione intenzionale o il danneggiamento da parte di terzi (malfattori) di quei sistemi tecnologici e la vulnerabilità dei dipendenti e delle loro mansioni all’interno di una società.

Quali possono essere le conseguenze di un attacco cyber?

In particolare, si potrebbero verificare i seguenti rischi :

- La perdita della proprietà intellettuale propria e di terzi;
- Perdita economica: come ad esempio la deviazione, l’intercettazione ed il reindirizzamento di pagamenti attraverso infiltrazioni e impersonificazioni via email;
- Interruzione del business: a seguito di un evento cyber avvenuto nell’ottobre 2015, una società di telecomunicazioni ha perso

101,000 clienti e subito dei costi per 60 milioni di sterline;

- Danno alla reputazione: potrebbe essere molto imbarazzante dire ai clienti di aver perso i loro dati;
- Costi: legali, normativi e informatici per gestire e riparare il danno.

Alcuni esempi di eventi cyber nei settori 'commodities' e 'shipping'

Un porto europeo ha subito la violazione dei suoi sistemi informatici per più di due anni prima che venisse scoperta. Durante questo periodo di tempo, dei pirati informatici avevano utilizzato i loro sistemi per contrabbandare merci illegali, estraendo i codici di apertura ed i documenti per la consegna di container dai terminal di trasporto.

Sono stati dirottati i pagamenti di noli, noleggi e contratti di vendita.

Un hacker ha causato il parziale ribaltamento di una piattaforma petrolifera situata al largo della costa d'Africa, costringendola a chiudere temporaneamente.

Gli effetti degli attacchi cyber sui contratti di noleggio

La clausola off-hire

La maggior parte dei contratti di noleggio a tempo includono una clausola che prevede che la nave sia da considerarsi off-hire laddove risulti impossibilitata a performare il servizio richiesto. La clausola off-hire nel formulario NYPE 1946 prevede che "... in caso di perdita di tempo derivante da un guasto o danni al corpo, macchina o all'equipaggiamento... o da ogni altra causa che impedisca il pieno funzionamento della nave, il pagamento del nolo verrá sospeso per il tempo perduto *("breakdown or damages to hull, machinery or equipment... or by any other cause preventing the full working of the vessel, the payment of hire shall cease for the time thereby lost").* In questo contesto, *"Any other cause"* effettivamente significa ogni altra causa come quelle di cui alla lista summenzionata – pertanto, se un evento cyber possa essere considerato un evento off-hire o meno dipende dal modo nel quale esso si manifesta, ed il modo nel quale impedisce il pieno funzionamento della nave.

Tuttavia, per chiarezza in materia, o per il noleggiatore che vorrebbe fare affidamento sulla clausola fuori nolo, si potrebbe includere uno specifico riferimento ad eventi cyber, usando, per esempio, un wording simile al seguente:

"In the event of the loss of time from deficiency of men or stores, fire, breakdown or damages to hull, machinery or equipment, grounding, detention by average accidents to ship or cargo, drydocking for the purpose of examination or painting bottom, Cyber Event, or by any other cause preventing the full working of the vessel, the payment of hire shall cease for the time thereby lost".

Per "Cyber Event" si intende (e potrebbe essere esposto nel contratto) ogni azione di terzi contro i computer di bordo di una nave, i sistemi o i software dei computer attraverso o mediante l'uso di codici, virus informatici, procedure o qualsiasi altro strumento elettronico senza il consenso degli armatori.

Altresì, come recentemente sottolineato dalla decisione della Suprema Corte nel caso 'GLOBAL SANTOSH', è chiaro che nulla può sostituire una dicitura adeguata nei contratti di noleggio atta a ripartire appropriatamente il rischio tra le parti.

Il pagamento del nolo

Molti contratti charteparty prevedono che il nolo debba essere pagato attraverso un trasferimento elettronico di fondi; il nolo viene ritenuto pagato quando è stato ricevuto sul conto bancario dell'armatore. Se il noleggiatore effettua un pagamento che non raggiunge il conto corrente bancario dell'armatore entro la data del pagamento (o laddove il pagamento non avvenga), allora il noleggiatore risulterà inadempiente.

Consideriamo un esempio ricorrente: il noleggiatore riceve una fattura ed effettua il pagamento sul conto corrente ivi indicato, per poi scoprire più tardi che la fattura non era stata trasmessa dall'armatore

"La criminalità informatica è *"la più grande minaccia per tutte le società del mondo"* (CEO della IBM)."

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

ma da qualche malfattore. Questi pirati informatici possono essere abbastanza credibili, dal momento che utilizzano indirizzi email quasi identici a quelli dell’armatore.

Una *“anti-technicality clause”*, a seconda della sua portata, potrebbe almeno permettere ad un noleggiatore di avere più tempo per pagare, ma è necessario che paghino (di nuovo) o l’armatore sarà autorizzato a ritirare la nave.

Benché un noleggiatore non possa essere in grado di evitare l’obbligo di pagare, potrebbero essere utili delle clausole contrattuali che almeno gli consentano di avere più tempo per pagare, includendo un metodo alternativo di pagamento. Un wording in inglese simile al seguente potrebbe essere valutato, per esempio:

“Qualora un Cyber Event dovesse impedire i pagamenti del nolo da parte dei noleggiatori ai sensi di questo contratto di noleggio, i noleggiatori avranno l’opzione di effettuare il pagamento entro [ ] giorni lavorativi dalla data di scadenza del termine concesso per effettuare il pagamento, con il consenso dell’armatore (tale consenso non può essere irragionevolmente negato). Tali pagamenti saranno ritenuti tempestivi.

“Cyber Event” significa ogni azione di terzi che colpisca i computer, i sistemi o i software del noleggiatore o dell’armatore (o delle loro rispettive banche e/o agenti) attraverso o mediante l’uso di codici, virus informatici, procedure o altri mezzi elettronici di alcun tipo, senza il consenso della parte colpita.”

Interruzioni di stallie e controstallie

Le interruzioni delle stallie e delle controstallie decorrono continuativamente e senza interruzioni, salvo che si applichi una clausola di esclusione o vi sia un ritardo causato dall’armatore. Le più comuni clausole di esclusione di stallie sono circoscritte nella loro formulazione e relative solo alla nave in sé. Una tale clausola di esclusione potrebbe ben rispondere ad un evento cyber che riguarda la nave direttamente, ma probabilmente non includerà una situazione in cui è il porto o il terminale ad aver subito un evento cyber. D’altronde, sarà difficile che un armatore accetti la responsabilitá per ritardi dovuti a problemi informatici di un porto o di un terminale, che considererà entro la sfera di responsabilità del noleggiatore.

L’idoneità alla navigazione

L’obbligo di common law in capo all’armatore di fornire una nave idonea alla navigazione si compone di due requisiti: in primo luogo, la nave, l’equipaggio e l’attrezzatura di bordo devono essere di qualità sana ed in grado di far fronte ai pericoli del mare che ordinariamente si incontrano nel corso del viaggio previsto. In secondo luogo, la nave deve essere adatta a trasportare il carico previsto dal contratto. L’obbligazione si estende oltre al mero stato della nave ed include adeguati sistemi, armamenti ed i documenti di bordo. Una nave moderna non può operare in sicurezza (ed a volte non può proprio operare) senza i dispositivi elettronici per la navigazione e la comunicazione. Il non riuscire a proteggere la nave da un evento cyber potrebbe essere considerato un mancato esercizio della dovuta diligenza nel rendere la nave idonea alla navigazione, e anche una violazione degli Articoli 3(1) e 4(1) delle Regole dell’Aja/Aja-Visby, tale da poter condurre ad un reclamo ai sensi di una polizza di carico o di un contratto di noleggio.

Riguardo deve essere inoltre prestato al Codice ISM, che stabilisce gli standard previsti per la gestione in sicurezza della nave. Né il Codice ISM né il Codice ISPS affrontano specificamente eventi cyber. Una posizione analoga riguarda SIRE e Rightship. BIMCO ha proposto che i Codici ISM e ISPS usino le loro procedure di rapida diffusione per far fronte ai rischi connessi ad eventi cyber. Nel gennaio 2016, il BIMCO ha pubblicato le linee guida per migliorare la sicurezza informatica a bordo delle navi. Le parti dovrebbero familiarizzare con esse e fare attenzione agli sviluppi futuri in tema di sicurezza informatica.

Nel giugno di quest'anno, durante l'incontro del Comitato IMO per la sicurezza marittima, il Comitato ha adottato le raccomandazioni incluse nella Risoluzione MSC.428(98) sull'attuazione della gestione del rischio cibernetico. Ciò significa che gli armatori e gli operatori dovranno adesso tenere in considerazione la gestione del rischio cibernetico nei loro sistemi di gestione del rischio (SMS).

La sicurezza dei porti

La definizione classica di 'safety' si incentra su pericoli fisici come secche, scogli od oggetti sporgenti. La definizione si è ampliata per coprire rischi politici (come requisizioni, ribellioni e guerre), rischi giuridici (come il sequestro della nave) e rischi per la salute (come quarantene ed epidemie). Non è chiaro se un evento cyber possa rendere un porto non sicuro. Senza dubbio, un porto potrebbe non esserlo se subisse ripetuti eventi cyber dovuti a scarsa sicurezza informatica. Gli sviluppi futuri dovranno essere monitorati con attenzione.

Analisi della copertura assicurativa per rischi cyber

La copertura assicurativa dovrebbe essere parte della strategia di gestione dei rischi cyber, e non sostituirsi ad essa. Con così tanto commercio internazionale condotto ancora attraverso trasporti marittimi di vario tipo, la sicurezza di navi, equipaggi, passeggeri, lavoratori, porti, terminal, carichi e catene di fornitura interconnesse è fondamentale per l'efficace esecuzione delle attività quotidiane.

Gli assicuratori stanno cercando di sviluppare prodotti che indirizzano non solo i rischi tradizionali ma anche le attività attuali ed i relativi rischi associati ai nuovi modi di fare business.

Vi sono adesso più di 60 società nel Regno Unito che propongono al mercato polizze assicurative specifiche contro rischi cyber e più di 70 negli Stati Uniti d'America.

Tuttavia, mentre potrebbe esserci una certa comunanza nel nome delle polizze e in alcuni dei rischi coperti, è importante da tenere in mente, come sempre, che sono i dettagli che contano. Non tutti gli assicuratori offrono lo stesso prodotto e molti wording risultano inadeguati. I titolari delle polizze ed i loro consulenti dovrebbero inoltre studiare se alcuni o tutti i rischi cyber (ed i costi ad essi associati) sono coperti ai sensi delle loro tradizionali polizze "all risks", o ai sensi delle polizze per la responsabilità civile. È improbabile, salvo che non sia espressamente e chiaramente previsto, ma va verificato.

Al momento, in linea generale, è improbabile che polizze assicurative cyber indipendenti assicurino danni alla proprietà. Di contro, la maggior parte dei formulari per la copertura assicurativa relativa a proprietà e terrorismo difficilmente assicurano (e possono anche espressamente escludere dalla copertura) perdite dovute ad eventi cyber ad opera di malfattori. Una esclusione molto comune nel settore marittimo ed in altri mercati specializzati è l'appendice CL380 (o un equivalente) conosciuta come la clausola "Institute Cyber Attack Exclusion Clause', seppure si compiano tentativi per modificarla nelle varie polizze a causa delle pressioni derivanti dal mercato. Molti operatori nel mercato assicurativo cyber si concentrano nel fornire ai titolari di polizze assistenza e sostegno dalla conseguenze di un evento cyber. Ciò è molto utile alle piccole e medie imprese e nelle operazioni di più piccola entità che potrebbero non avere abbastanza risorse per coordinare in maniera efficiente la risposta ad una violazione.

Tali prodotti dovrebbero coprire perdite dovute a:

- il costo per le comunicazioni della violazione di dati personali;
- il costo per le indagini forensi per investigare e sigillare la violazione e salvaguardare le prove;
- i costi per il recupero dei dati;
- la consulenza per le pubbliche relazioni;
- le spese di monitoraggio del credito;
- il furto d'identità.

"Potrebbero essere utili delle clausole contrattuali che almeno ... consentano di avere più tempo per pagare, includendo un metodo alternativo di pagamento..."

Alcuni assicuratori stanno offrendo copertura assicurativa contro i danni alla reputazione. Tuttavia, alle parti deve essere chiaro fin dall'inizio come tale danno debba essere quantificato. La copertura per i danni subiti da terzi è mirata a proteggere l'assicurato principalmente contro la responsabilità nei confronti di terzi rispetto a perdite risultanti da accessi non autorizzati o a divulgazione di informazioni private e confidenziali o commerciali riservate. Sono inoltre frequenti i costi per la difesa di azioni e rimostranze in relazione a inchieste normative. Assicuratori specializzati continuamente cercano di distinguersi dai concorrenti, inserendo clausole di copertura aggiuntive, ma è essenziale un'attenta negoziazione e un esame del wording della polizza applicabile, oltre ad una consulenza professionale specifica.

Iniziative IMO e BIMCO

Da quando esposto sopra, lo scorso giugno il Comitato IMO ha adottato le raccomandazioni incluse nella Risoluzione MSC.428(98) sull'attuazione della gestione del rischio cibernetico, con l'effetto che adesso gli armatori e gli operatori dovranno tenere in considerazione la gestione del rischio cibernetico nei loro sistemi di gestione del rischio (SMS).

Il Comitato IMO ha inoltre fornito un calendario per l'attuazione di queste modifiche dichiarando che una società di SMS avrà bisogno di assicurare che i rischi cibernetici siano appropriatamente indirizzati non più tardi della prima verifica annuale del Documento di Conformità dopo il 1º gennaio 2021.

Nel corso degli ultimi anni, BIMCO ha giocato un ruolo chiave nel ricercare i potenziali rischi posti dall'aumento della tecnologia a bordo delle navi. Ciò è culminato nella prima edizione delle loro linee guida sulla sicurezza informatica a bordo delle navi (di seguito, "le Linee Guida") che sono state pubblicate nel gennaio 2016. Ora, BIMCO ha pubblicato la versione 2.0 delle linee guida che, come per la prima edizione, sono supportate dall'International Chamber of Shipping, da Intertanko, da Intercargo e dalla Cruise Lines International Association.

BIMCO rappresenta il 60% della flotta mercantile mondiale. Al fine di potenziare le prime Linee guida, hanno lavorato con la Guardia Costiera degli Stati Uniti ed il registro della bandiera liberiana anche dando ai ricercatori del settore marittimo accesso ad alcune navi dei membri BIMCO per indagare su potenziali attacchi. Come per molti altri studi, i risultati hanno dimostrato un notevole potenziale per cyber disruption. Le Linee Guida mirano a fornire assistenza agli armatori e agli operatori su come valutare le loro operazioni, identificare le vulnerabilità nei loro sistemi e adottare le misure per proteggersi. Più che essere un documento a sé stante, sono complementari a regolamenti esistenti ai sensi dell'International Safety Management Code (ISM Code) e dell'International Ship and Port Facilities Security Code (ISPS Code).

BIMCO evidenzia giustamente che l'approccio al tema della sicurezza deve essere specifico per la società e la nave, ma dovrà anche essere guidato da standard appropriati. Le Linee Guida si focalizzavano su sei aspetti critici di sensibilizzazione alla cyber-security, ossia:

- Identificare le minacce e comprendere le minacce alla sicurezza informatica della nave;
- Identificare le vulnerabilità nel sistema di sicurezza informatica della nave;
- Valutare l'esposizione ai rischi e la probabilità di essere esposti a minacce esterne;
- Lo sviluppo di misure di protezione e di rilevamento al fine di ridurre al massimo l'impatto;

“Un hacker ha causato il parziale ribaltamento di una piattaforma petrolifera situata al largo della costa d’Africa, costringendola a chiudere temporaneamente.”

- Istituire piani di emergenza per ridurre l’incidenza di minacce;
- Rispondere agli incidenti relativi alla cyber-security.

La versione 2.0 si basa sulle Linee Guida esistenti cercando di allinearle con le linee guida IMO, piuttosto che cercare di scrivere nuovamente la versione originale. Gli articoli aggiornati includono una guida su:

- La cyber-safety (ossia la perdita della disponibilità o integrità di dati sensibili relativi alla sicurezza e alla tecnologia operativa), che è una questione significativa quanto quella della cyber-security;
- La necessità di controllare e monitorare le connessioni internet nel percorso dalla nave a terra e porre una maggiore attenzione all’interfaccia da nave a terra;
- Separare le reti a bordo ed evitare le comunicazioni tra reti controllate e non;
- Acquisire un approccio di “difesa in profondità” usando molteplici livelli di misure di protezione per proteggere sistemi e dati sensibili;
- Tenere in conto il rischio posto dai visitatori delle navi, incluse autorità, tecnici, agenti e ufficiali di porto;
- Garantire una “Risposta efficace” anche avendo un team di impiegati e/o esperti esterni per adottare le azioni opportune;
- Le perdite derivanti da un incidente informatico e la necessità di garantire che vi siano adeguate coperture assicurative.

La versione 2.0 delle Linee Guida BIMCO può essere adesso considerata la guida più completa per il settore shipping sulla base della conoscenza e dell’esperienza acquisita dal BIMCO nel corso degli ultimi diciotto mesi.

Da quanto discusso sopra si evince che, laddove uno dei sistemi informatici degli armatori venga violato, e questi non possano provare di aver agito con adeguata diligenza nel gestire i rischi informatici e proteggere le loro navi, allora vi è il rischio che una nave possa essere considerata *“unseaworthy”* in violazione del contratto di trasporto. Ciò potrebbe anche avere implicazioni sulle coperture assicurative in essere. A tal riguardo, riportiamo una saggia dichiarazione da parte del Segretario Generale del BIMCO, Angus Frew, il quale ha recentemente dichiarato che *“l’ignoranza non è più un’opzione poiché noi tutti stiamo rapidamente rendendocene conto”*.

HWF è uno studio legale di primo piano nel settore con una competenza specifica nell’ambito dei rischi marittimi e del crisis management ed è in grado di fornire assistenza per necessità inerenti alla cyber-security. Possiamo prestare assistenza nella valutazione dei rischi, la formazione professionale, la pianificazione per la crisi e la risposta ad essa nel caso di violazioni in modo tale da evitare violazioni o comunque minimizzarne gli effetti qualora si dovessero verificare.

Per qualsiasi ulteriore informazione in merito, non esitate a contattare:

RICHARD MABANE
Partner, London
T +44 (0)20 7264 8505
M +44 (0)7881 827952
E richard.mabane@hfw.com

HFW conta più di 500 avvocati che prestano assistenza negli uffici in Australia, Asia, Medio Oriente, Europa e le Americhe. Per maggiori informazioni circa la nostra competenza in materia di shipping, si prega di visitare il sito hfw.com/shipping

hfw.com

© 2017 Holman Fenwick Willan LLP. Tutti i diritti riservati.
Pur essendo stata esercitata la massima diligenza nel verificare l'accuratezza delle informazioni contenute in questo bollettino al momento della distribuzione, tali informazioni sono da considerarsi meramente indicative. Non sono da considerarsi un parere legale. Holman Fenwick Willan LLP è titolare del trattamento dei dati personali relativi ai destinatari. Per correggere i Vostri dettagli personali o cambiare le Vostre preferenze di posta elettronica, Vi preghiamo di contattare Souhir Jemai al +44 (0)20 7264 8415 o all'indirizzo email souhir.jemai@hfw.com.

Beirut Bruxelles Dubai Ginevra Hong Kong Houston Kuwait Londra Melbourne Parigi Perth Pireo Riyad San Paulo Shanghai Singapore Sydney