FEDESPEDI

ALSEA

SEMINARIO

IMPRESE E CYBER SECURITY: ASPETTI LEGALI, ASSICURATIVI E TECNOLOGICI

Milano, 15 maggio 2018

Avv. Prof. Enrico Righetti

STUDIO LEGALE RIGHETTI

Genova – Milano – La Spezia - Trieste

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

2017

anno nero per l'intensità e gravità di cyber attacks

nel corso degli ultimi decenni l'incremento dell'uso della tecnologia ha certamente determinato significativi vantaggi in termini di efficienza in tutti i settori, ivi incluso quello dei trasporti e della logistica, incrementando tuttavia i rischi legati alla potenziale vulnerabilità dei processi informatici dedicati al funzionamento dei vari sistemi

WannaCry

nel maggio 2017, un *ransomware* ha messo in ginocchio 200.000 computer in tutto il mondo, colpendo 74 paesi e centinaia di aziende

in particolare si è introdotto nel sistema produttivo dell'azienda giapponese Honda che ha dichiarato che in una sua fabbrica la produzione di circa mille automobili è saltata a casa del *malware*

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

2017

anno nero per l'intensità e gravità di cyber attacks

WannaCry

cuore di questo attacco informatico sarebbe lo sfruttamento di una falla presente nell'SMB Server del sistema operativo Windows

→ il *ransomware* – che costituisce in pratica una sorta di rapimento a fini di riscatto - blocca il sistema sul quale è stato installato, rendendone impossibile l'utilizzo e impedendo l'accesso ai dati salvati sino a quando non viene attivata una procedura di sblocco basata sul pagamento di una somma (riscatto)

→ l'importo richiesto è stato inizialmente di US$ 300, da pagare in *Bitcoin*, ma alcune informative hanno riferito che la cifra è in seguito aumentata sino a US$ 600

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

2017

anno nero per l'intensità e gravità di cyber attacks

NotPetya

nel giugno 2017 si è verificato un altro attacco denominato NotPetya (altro *malware* simile a un *ransomware*) che ha colpito diverse decine di aziende in tutto il mondo → fra queste la francese Saint-Gobain (società che si occupa di materiali edili), l'inglese WPP (che si occupa di pubblicità), le russe Evraz e Rosneft (appartenenti ai settori siderurgici e petroliferi)

→ nel settore dei trasporti marittimi, la compagnia danese Maersk, i cui terminal portuali gestiti dalla controllata APM in molti paesi del mondo sono rimasti bloccati per giorni con perdite stimate nell'ordine dei 300 milioni di dollari

FEDESPEDI

ALSEA

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

2017

anno nero per l'intensità e gravità di cyber attacks

un altro nome rilevante, fra le tante vittime, è quello della TNT, nota azienda di trasporti e logistica → il *malware*, insinuatosi nei computer aziendali sembrerebbe grazie ad alcune vulnerabilità della rete LAN, ha fatto saltare il sistema di tracciamento delle spedizioni

«Messaggio importante: come molte aziende e istituzioni di tutto il mondo, stiamo affrontando anche noi problemi con alcuni dei nostri sistemi all'interno della rete TNT. Stiamo procedendo il più velocemente possibile all'implementazione di azioni correttive per fornire supporto ai clienti che hanno subito alcune interruzioni nelle operazioni di ritiro e consegna e di accesso ai sistemi di tracking. Ci scusiamo con i nostri clienti per qualsiasi inconveniente»

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

un attacco *cyber* può pregiudicare non solo i sistemi informatici delle compagnie di navigazione ed i dati sensibili ivi contenuti, ma può colpire anche le stesse navi che, essendo sempre più computerizzate, sono quindi anch'esse esposte alla pirateria informatica

→ in quest'ottica, la prospettiva del previsto futuro impiego di navi c.d. "*unmanned*", se da un lato può aumentare l'efficienza (operativa ed economica) del trasporto marittimo, evitando gli errori umani, dall'altro lato potrebbe, tuttavia, incrementare il rischio potenziale di attacchi *cyber* che rischiano di causare dirottamenti, sequestri a fini di pirateria anche a distanza o altri danni di estrema pericolosità → i sistemi di navigazione di bordo sono spesso senza alcuna protezione e possono essere violati con disarmante facilità, anche con l'inconsapevole contributo degli equipaggi

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

- **per mettere in luce le pesanti lacune che ancora caratterizzano i sistemi informatici nel settore marittimo, durante un Convegno '*Le rotte digitali del trasporto – IoT e big data: opportunità e rischi della digital transformation*' organizzato a Genova lo scorso anno dal quotidiano Il Secolo XIX, l'A.D. di una società specializzata nella prevenzione del *cyber risk,* ha violato in diretta, a scopo dimostrativo e senza però procurare alcun danno alla stessa, i sistemi informatici di una nave in soli 10 minuti, con un semplice computer portatile e la connessione internet**

- **nello stesso Convegno ci si è posti il problema di cosa succederebbe se un attacco *cyber* fosse rivolto a E-port - il Port Community System del porto di Genova oggi il più avanzato in Italia – che copre quasi tutte le attività svolte nello scalo processando 12 milioni di informazioni all'anno e che è anche il primo PCS italiano ad essere entrato nella Piattaforma Logistica Nazionale**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Altri esempi presi da Internet di eventi *cyber* nei settori dello '*shipping*' e, più in generale, dei trasporti e della logistica

- **un porto europeo ha subito per più di due anni la violazione dei suoi sistemi informatici → durante questo periodo dei pirati informatici ne avevano utilizzato i sistemi per contrabbandare merci illegali, estraendo i codici di apertura ed i documenti per la consegna di container dai terminal portuali**
- **in diverse occasioni pirati informatici sono stati in grado di accedere ai sistemi di un vettore o di un operatore logistico per sapere quali merci vengono trasportate da una determinata nave o camion oppure si trovano depositate in un determinato magazzino per poi rapinarli**
- **si sono verificati anche episodi di dirottamento del pagamenti di noli o di altri corrispettivi**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Definizione di rischio *cyber*

- **il rischio *cyber* per i sistemi informatici era stato definito dall'Institute of Risk Management – IRM 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, nel concetto di «avaria» rientrano non solo i guasti dei sistemi informatici, che possono essere causati anche da incidenti, quali gli effetti di fulmini, i cali o gli eccessi di tensione elettrica o le interruzioni per *black-out*, ma debbono essere inclusi fra i rischi *cyber* anche :**
  - **gli errori accidentali dei dipendenti all'interno di una società**
  - **l'infiltrazione intenzionale o il danneggiamento da parte di terzi (*hacking*, *malware*)**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

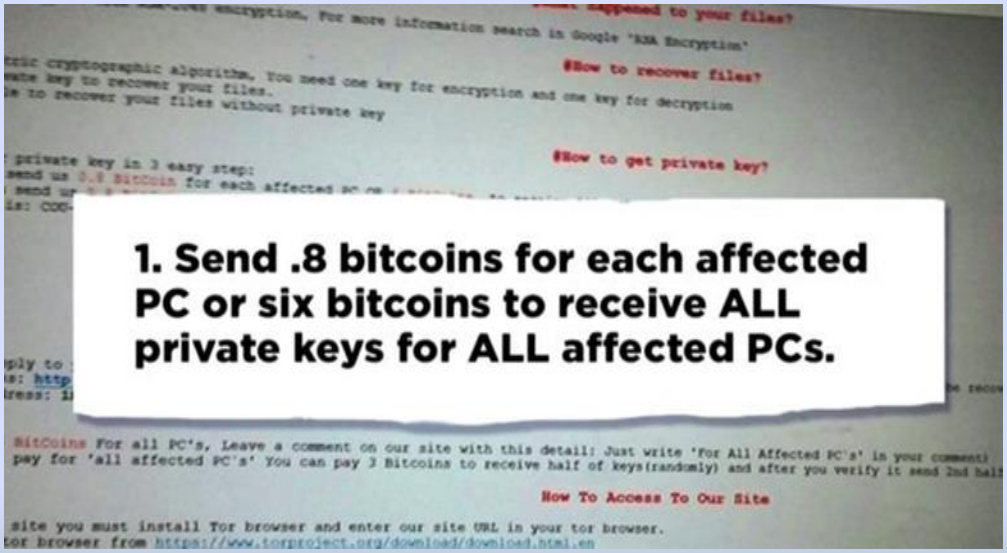
Le possibili conseguenze pregiudizievoli di un attacco *cyber*

- **interruzione dell'attività commerciale ed operativa**
- **danneggiamento delle strutture network aziendali**
- **perdita di dati riservati propri o di terzi (clienti)**
- **danno di immagine e alla reputazione**
- **perdite economiche:**
  - **l'intercettazione e il re-indirizzamento di pagamenti attraverso infiltrazioni e impersonificazioni via email**
  - **il pagamento di un "riscatto"**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Le possibili conseguenze pregiudizievoli di un attacco *cyber*

→ **in caso di un attacco *ransomware* la stragrande maggioranza delle aziende che subiscono un attacco informatico tendono a pagare il riscatto e, quando possibile, a non divulgare nessuna notizia all'esterno**



IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Principali danni patrimoniali che possono essere subiti dalle imprese

- **perdita di fatturato per interruzione dell'attività**
- **costi di ripristino delle infrastrutture informatiche**
- **perdita di fatturato e di clientela per la divulgazione di informazioni riservate**
- **perdita di fornitori o partner commerciali**
- **azione di risarcimento dei titolari dei dati personali divulgati**
- **costi legali per gestire le conseguenze del danno**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Iniziative IMO e BIMCO

- **recentemente sia l'IMO che il BIMCO hanno emanato delle Linee Guida al fine di aiutare gli armatori a proteggersi dagli attacchi di pirateria informatica**

- **nel giugno 2017 il Comitato IMO ha adottato le raccomandazioni incluse nella Risoluzione MSC.428(98) - *Maritime Cyber Risk Management in Safety Management Systems*, nelle quali si evidenzia che il sistema di gestione della sicurezza (SMS) dovrebbe tener conto della gestione del rischio informatico in conformità agli obiettivi e ai requisiti funzionali del Codice ISM (art. 1) → secondo l'IMO è quindi necessario garantire che i rischi informatici siano adeguatamente affrontati nell'ambito del SMS entro la prima verifica annuale del documento di conformità della società seguente al 1 gennaio 2021 (art. 2)**

- **il successivo 5 luglio 2017, l'IMO ha elaborato un secondo documento, il MSC-FAL.1/Circ.3, *Guidelines on maritime cyber risk management* recante una serie di raccomandazioni rivolte a tutte le organizzazioni del settore marittimo per incoraggiare pratiche di gestione della sicurezza nel cyber spazio per salvaguardare le spedizioni dalle minacce e dalle vulnerabilità informatiche (art. 2.2.1)**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Iniziative IMO e BIMCO

- **in tali Linee Guida l'IMO identifica alcuni dei sistemi più vulnerabili alle aggressioni cyber, tra i quali, per esempio, i sistemi informatici mediante i quali sono gestiti i carichi trasportati, i dispositivi elettronici per la navigazione e per la comunicazione, nonché i sistemi informatici correlati ai servizi forniti ai passeggeri (art. 2.1.1)**

- **individuati i sistemi più vulnerabili, nella gestione del rischio informatico, ogni società dovrebbe considerare la distinzione esistente tra i sistemi della *information technology* (nei quali i dati sono usati come informazioni) e quelli della *operational technology* (in cui i dati sono usati per scopi diversi, ovvero per controllare o monitorare processi fisici)**

- **la *cyber-security* dovrebbe essere implementata in entrambi i sistemi oltre che nello scambio di dati tra gli stessi (art. 2.1.2) al fine di limitare i rischi derivanti da vari fattori, quali, ad esempio, operazioni inadeguate, protezioni vetuste e minacce informatiche intenzionali (come *hacking* o introduzione di *malware*) e non intenzionali (come manutenzione del *software*) (artt. 2.1.3-4)**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Iniziative IMO e BIMCO

- **di conseguenza, l'IMO suggerisce di affrontare la questione dei *cyber risks* nel contesto più generale del sistema di gestione della sicurezza aziendale (SMS), adottando un approccio che sia in grado di resistere ai pericoli informatici noti e che sia, al contempo, in grado di progredire tenuto conto dell'evoluzione delle minacce informatiche**

- **tutto ciò, mediante l'istituzione di diversi meccanismi di controllo dei rischi informatici da un punto di vista operativo, procedurale e tecnico (art. 3)**

- **anche il Baltic and International Maritime Council - BIMCO, nel luglio 2017, ha offerto il suo contributo e con la partecipazione di altre organizzazioni (CLIA, ICS, INTERCARGO, INTERTANKO, IUMI e OCIMF), ha pubblicato una nuova edizione del documento *The Guidelines on Cyber Security Onboard Ships* recante Linee Guida dirette a fornire assistenza agli armatori e agli operatori a bordo delle navi**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Iniziative IMO e BIMCO

The Guidelines on Cyber Security Onboard Ships

- **tale documento si focalizza sui sei aspetti considerati critici nella gestione della *cyber-security*, ossia :**
- **(i) l'identificazione delle minacce**
- **(ii) l'individuazione delle vulnerabilità nel sistema di sicurezza informatica della nave**
- **(iii) la valutazione della probabilità di essere esposti a minacce esterne**
- **(iv) lo sviluppo di misure di protezione e di rilevamento per ridurre al massimo l'impatto**
- **(v) l'istituzione di piani di emergenza per ridurre l'incidenza di minacce**
- **(vi) l'individuazione della risposta agli incidenti relativi alla *cyber-security*, con la previsione di una copertura assicurativa *ad hoc* quale parte integrante della strategia di gestione dei rischi informatici**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Iniziative IMO e BIMCO

→ **gli interventi sopra riferiti sono indicatori di un'accresciuta sensibilità degli operatori del settore marittimo in tema di *cyber risks* conseguente anche ad una presa di coscienza delle numerose implicazioni legali ed economiche ipotizzabili in conseguenza di un attacco informatico nei confronti di una compagnia marittima**

→ **in particolare, qualora l'armatore non sia in grado di provare di aver agito con la dovuta diligenza nel proteggere una nave da attacchi informatici, non si può escludere che tale nave sia considerata "*innavigabile*" e che ciò costituisca un inadempimento (*breach*) del contratto di noleggio o di trasporto**

→ **infatti, tale mancanza potrebbe essere considerata come un inadempimento del dovere di diligenza dell'armatore nel rendere la nave idonea alla navigazione e/o come una violazione dell'art. 3, par. 1, lett. a) delle Regole dell'Aja-Visby, per il quale "*the carrier shall be bound before and at the beginning of the voyage to exercise due diligence to: (a) make the ship seaworthy*"**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

BIMCO

Risks on board ships

5

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Direttiva (UE) 2016/1148 del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione - "Direttiva NIS"

- **il primo aspetto di questa direttiva è di ritenere che la cyber security necessiti di un approccio globale che contempli la creazione di disposizioni minime in materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali**
- **il secondo aspetto, e forse più importante, è che le norme devono individuare i soggetti e le responsabilità poste a loro carico a seguito di inadempimenti o di violazioni alle prescrizioni**
- **proprio per questo la Direttiva 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Direttiva NIS) appare un traguardo molto importante: la direttiva, valida in tutta l'Unione Europea, riguarda sia gli Stati membri sia le aziende private che si occupano di gestire servizi essenziali come trasporti, fornitura di acqua, energia ecc.**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Direttiva (UE) 2016/1148 del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione - "Direttiva NIS"

- **entro novembre 2018 ogni nazione dovrà identificare per ciascun settore e sotto-settore gli operatori di servizi essenziali sul territorio, la cui lista dovrà essere aggiornata ogni due anni**
- **le varie aziende dovranno fornire tutte le informazioni ritenute necessarie alla relativa autorità politica, che potrà di conseguenza valutare la sicurezza delle imprese e ordinare cambiamenti e modifiche ai sistemi di cyber security; inoltre sarà obbligatorio notificare qualsiasi tipo di incidente all'autorità nazionale, che valuterà il danno e nominerà nuove commissioni responsabili del trattamento e della sicurezza dei dati → la direttiva NIS pone infatti grande enfasi sulla protezione dei dati dei clienti e dei dipendenti delle aziende, introducendo il diritto all'oblio e il diritto alla portabilità (la possibilità di trasferire i propri dati liberamente su diverse piattaforme)**
- **l'altra grande innovazione introdotta con la direttiva è l'attenzione alla cooperazione a livello internazionale, per trasformare la strategia dell'Unione Europea da una corsa al risolvere le minacce più in fretta possibile, ad un più complesso, efficace e razionale metodo di prevenzione**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Profili di responsabilità dello spedizioniere

1. Ipotesi in cui il *cyber attack* colpisce direttamente i sistemi informatici dello spedizioniere

- **art. 1218 c.c. : «il debitore che non esegue esattamente la prestazione dovuta è tenuto al risarcimento del danno, se non prova che l'inadempimento o il ritardo è stato determinato da impossibilità della prestazione derivante da causa a lui non imputabile»**

→ il quadro della responsabilità dello spedizioniere si presenta assai complesso a prescindere dal fatto che la violazione sia frutto di un guasto, di un errore, di un atto di infedeltà o dell'azione delittuosa di un *hacker*

→ qualora il cliente agisca in giudizio nei confronti dello spedizioniere per chiedere il risarcimento dei danni, questi, ove la violazione fosse opera di un *hacker*, potrebbe invocare elementi esimenti della sua responsabilità soltanto se riuscisse a dimostrare di aver fatto tutto quanto in suo potere per evitare la violazione

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Profili di responsabilità dello spedizioniere

1. Ipotesi in cui il *cyber attack* colpisce direttamente i sistemi informatici dello spedizioniere

→ il gestore dei dati di terzi risponde in via diretta, ai sensi della legge sulla privacy, del danno o della divulgazione che possono essere provocati da danni materiali all'hardware o da atto di infedeltà di un dipendenti

→ se, invece, la causa fosse l'azione di *hackers*, la responsabilità del gestore sarebbe limitata all'inosservanza dell'obbligo di notifica e di quello relativo al rispetto delle misure di protezione minime prescritte

→ a tal fine, il GDPR 679/2016, che entrerà in vigore a fine mese, ha definito gli obblighi in capo alle società che gestiscono nei propri sistemi informatici dati e informazioni di terzi, come segue:

- **l'adozione di misure di protezione preventiva contro gli attacchi esterni**
- **la denuncia all'autorità ed ai titolari dei dati affidati in gestione di ogni attacco che dovesse provenire dall'esterno, del quale il gestore fosse a conoscenza, anche se deve ancora avvenire**
- **anche l'adozione di una politica strutturata di *risk management* per la pianificazione degli interventi e per l'aggiornamento delle tecniche di intervento**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Profili di responsabilità dello spedizioniere

1. Ipotesi in cui il *cyber attack* colpisce direttamente i sistemi informatici dello spedizioniere

→ il GDPR 679 fornisce, in definitiva, gli elementi che consentirebbero al gestore di dati di terzi, in caso di violazione derivante da pirateria informatica, di mettersi nelle condizioni di esimersi dalla responsabilità potendosi quest'ultima ascrivere a **causa di forza maggiore**

→ tuttavia, la velocità con la quale progredisce l'abilità degli *hackers* è tale da rendere inadeguate anche le difese che fino a qualche giorno prima potevano essere considerate idonee → si può affermare che, a fronte di un simile scenario, il limite accettabile del livello di idoneità delle protezioni *anti-hacker* è un traguardo in continuo movimento

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Profili di responsabilità dello spedizioniere

2. Ipotesi in cui il *cyber attack* colpisce i sistemi informatici del vettore materiale o di altro ausiliario incaricato dallo spedizioniere

- **SPEDIZIONIERE "PURO"** (art. 1737 codice civile)

  Il contratto di spedizione è un mandato col quale lo spedizioniere assume l'obbligo di concludere, in nome proprio e per conto del mandante, un contratto di trasporto e di compiere le operazioni accessorie

- **SPEDIZIONIERE-VETTORE** (art. 1741 codice civile)

  Lo spedizioniere che con mezzi propri o altrui assume l'esecuzione del trasporto in tutto o in parte, ha gli obblighi e i diritti del vettore

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Profili di responsabilità dello spedizioniere

2. Ipotesi in cui il *cyber attack* colpisce i sistemi informatici del vettore materiale o di altro ausiliario incaricato dallo spedizioniere

→ **lo spedizioniere puro è tenuto unicamente a una obbligazione di mezzi = concludere con il vettore il contratto di trasporto per conto del proprio mandante e compiere le operazioni accessorie**

→ **è quindi in linea generale responsabile soltanto degli errori derivanti dall'inosservanza delle istruzioni ricevute dal proprio mandante e risponde della negligente scelta di un vettore inadeguato (c.d. *mala electio*)**

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Profili di responsabilità dello spedizioniere

2. Ipotesi in cui il *cyber attack* colpisce i sistemi informatici del vettore materiale o di altro ausiliario incaricato dallo spedizioniere

- art. 1710 c.c. : lo **spedizioniere puro** è tenuto a eseguire il mandato con la diligenza del «*buon padre di famiglia*» ed è tenuto a rendere note al mandante le circostanze sopravvenute che possono determinare [la revoca o] la modificazione del mandato

  → lo spedizioniere ha l'obbligo di informare il proprio committente, chiedere istruzioni e, se del caso, provvedere alla custodia delle cose

- artt. 1740, 2° c., e 1720 c.c. : il mandante deve rimborsare allo spedizioniere le spese da questi anticipate in caso di un suo intervento

IMPRESE E CYBER SECURITY: ASPETTI LEGALI

Profili di responsabilità dello spedizioniere

2. Ipotesi in cui il *cyber attack* colpisce i sistemi informatici del vettore materiale o di altro ausiliario incaricato dallo spedizioniere

→ **il vettore - e quindi anche lo spedizioniere-vettore (art. 1741 c.c.) - si obbliga invece a trasferire le merci ed è quindi tenuto ad una obbligazione di risultato**

→ **risponde quindi dei fatti dolosi o colposi imputabili a terzi → vettori, sub-vettori ed altri ausiliari (es. terminal portuali)**

≠ a meno che non fornisca la prova dell'esistenza di una causa di esonero da responsabilità → forza maggiore

GRAZIE PER L'ATTENZIONE