Imprese di spedizione e cyber security: aspetti legali, assicurativi e tecnologici

Il focus assicurativo

Alessandro Morelli
Direttore Tecnico SIAT / Responsabile Trasporti e Aviazione UnipolSai

Siat ASSICURAZIONI

Fedespedi, Milano 15 Maggio 2018

Agenda

- ❑ Il rischio cyber: definizione e contesto
- ❑ Potenziali esposizioni per il mondo dello Shipping
  - ✓ Il mondo armatoriale
  - ✓ Gli operatori del Trasporto
- ❑ Le contromisure predisposte dagli operatori dello shipping
- ❑ Le soluzioni assicurative

Il rischio Cyber: definizione e contesto (1)

Rischio di

- perdite economiche e costi (inclusi danni a cose e a persone)
- interruzione di business,
- danno reputazionale

cui un'organizzazione è esposta a causa di

- un errore,
- un disastro,
- un guasto,
- un attacco al sistema di gestione dei dati e delle informazioni

➔ Evento accidentale => **cyber safety**

➔ Attacco malevolo dall'esterno => **cyber security**

4 macroaree fonte di possibile minaccia:

✓ Esterne: attacco malevolo (hacker, malware, phishing)

✓ Interne: dipendenti infedeli o disattenti

✓ Evoluzione tecnologica: IOT, SCADA: IT e OT sempre più pervasive

✓ Regolamentazione: General Data Protection Regulation **(maggio 2018)**

Il rischio Cyber: definizione e contesto (2)

Effetti dannosi del rischio Cyber:

- ❑ Impatto finanziario derivante dalla perdita di dati:
  - perdite di fatturato
  - costi addizionali
  - responsabilità nei confronti di terzi (violazione di privacy, ma non solo…)
- ❑ Danni materiali a cose (non esclusivamente hardware informatici)

- ❖ Specifiche problematiche per il mondo dello Shipping:
  - Armatori (vulnerabilità dei sistemi di bordo delle navi e a terra)
  - Porti e Terminal Containers
  - Spedizionieri e in genere Operatori del Trasporto

- Problematiche accentuate dalla sempre maggiore pervasività dell'informatica, delle reti di dati e dell'automazione

Il rischio Cyber e lo Shipping

Vulnerabilità delle navi:

- sistemi di governo della nave
  - rischio di eventi marittimi causati da mancanza di governo (collisioni e incagli)
- apparati propulsivi,
- sistemi di movimentazione del carico,
- sistemi di controllo accessi e di gestione dei passeggeri,
- gestione dei dati personali dei passeggeri imbarcati
- sistemi di comunicazione tramite network
- Cartografie elettroniche (ECDIS)

Il rischio Cyber e lo Shipping

Vulnerabilità dei porti, dei terminal container, degli operatori di trasporto:

- Container terminals hanno ruolo cruciale nella «supply chain» ➔ interruzione delle loro attività rappresenta rischio per il sistema globale
- Container terminals si basano su Information e Communication Technology (ICT)
- Automazione nelle movimentazioni (gru e mezzi): Mechanical Handling Equipment
- Terminal Operating Systems (TOS): identificazione dei container per stoccaggio nei terminal, movimentazioni e trasbordo: conseguenze di perdite o modifiche di informazioni
- Polizze di carico elettroniche / Manifesti di carico
- Rischio di perdite di merci: impossibilità di localizzazione ovvero localizzazione tardiva rispetto alla natura della merce (es.: merci deperibili)

Il rischio Cyber e lo Shipping

- Incremento degli attacchi cyber nel settore dello shipping (+15% nel 2017):
- AP Moeller Maersk colpita nel giugno 2017 dal malware Petya ➔ serie difficoltà di localizzazione dei carichi in diversi porti
- Collisione di unità US Navy USS McCain con nave mercantile (attacco cyber?)
- Attacco a BW Group luglio 2017

Il rischio Cyber e lo Shipping: contromisure?

- Rafforzamento delle difese preventive per **ridurre la frequenza** del rischio:
  - NIST Cybersecurity Framework (Version 1.1 – 10/1/2017)
  - IMO MSC-FAL.1: Guidelines on Maritime Cyber Risk Management (2017)
  - BIMCO (e altre Organizzazioni, fra cui IUMI): Guidelines on Cyber Security onboard Ships – Version 2.0 (2017)
- Elementi comuni:
  - ✓ Raccomandazioni concernenti cyber security e cyber safety
  - ✓ Importanza della consapevolezza («awareness») e dell'addestramento
    - ✓ Consapevolezza dell'elemento umano ➔ formazione delle persone
    - ✓ Incrementare consapevolezza del rischio ➔ senior management
  - ✓ 5 elementi funzionali: Identify, Protect, Detect, Respond, Recover.

Il rischio Cyber e lo Shipping: contromisure?

- Rafforzamento delle difese preventive per **ridurre la frequenza** del rischio:

- Trasferimento del rischio ai mercati assicurativi per **mitigare la severità** dell'eventuale impatto del rischio

- Analisi sui Mercati assicurativi internazionali
- Coinvolgimento di IUMI
  - Contributo alle Guidelines dell'industria (BIMCO)
  - Current Issues ed. 17/4/20187: punto 4 della sezione «Actions»: Cyber Risk

Le coperture assicurative per il mondo «Marine»

- Cyber Attack Exclusion cl. 380: rischio di eventuali danni alle navi/merci causati da attacco cyber escluso dalle polizze marine
- *…., 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*
- ➔ Cyber Gap Cover
- Operatori dello shipping non esposti solo ai danni materiali ma anche ai danni derivanti dalla perdita di dati o dal blocco dei sistemi informatici
- Esigenza di fornire una protezione assicurativa a 360°, non solo alcuni elementi

Le difficoltà di un prodotto assicurativo «Marine»

➢ **Criticità:**

❖ Limitata esperienza statistica 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 e la conseguente mitigazione del rischio cyber

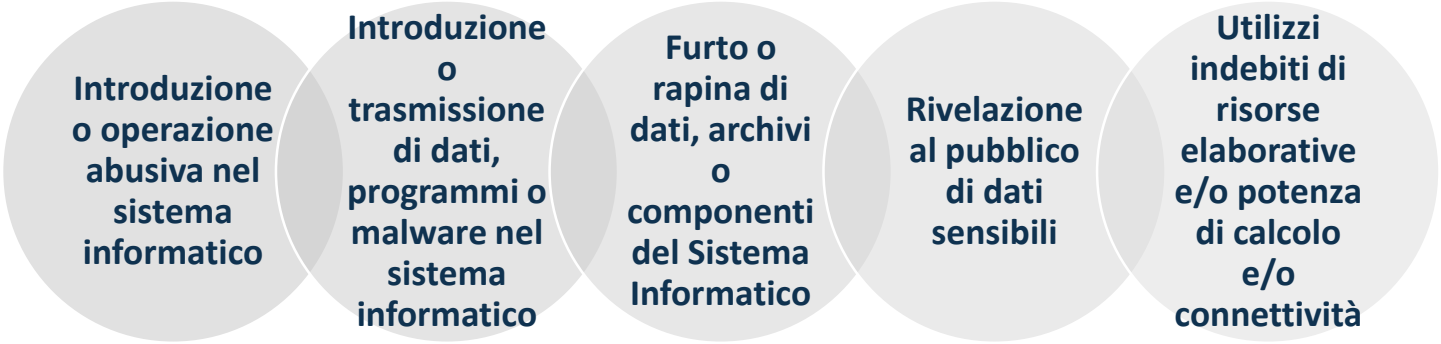
➔ La scelta di Siat di appoggiarsi sul Gruppo UnipolSai

➔ Prodotto Cyber UnipolSai implementato di Sezione RC per danni alle merci

Il Prodotto Cyber del Gruppo UnipolSai

Oggetto dell'assicurazione

- L'Assicurazione è prestata a copertura dei danni indennizzabili causati da **chiunque, tramite una serie di condotte elencate:**



- Danni indennizzabili a seguito di Cyber terrorismo e Cyber Warfare

- Danni causati da Errore Umano da parte di dipendente

La struttura della polizza per gli operatori del trasporto

Danno all'Organizzazione: First Party Damage

- Costi propri
- Informatica
- Dati ed archivi
- Danni da interruzione attività

Danno cagionato a terzi: Third Party Damage

- Responsabilità civile verso terzi

- Responsabilità per danni alle merci

La Cyber Risk Coverage

CAPO I - FIRST PARTY DAMAGE

Costi propri

Costi sostenuti per la gestione della crisi

Informatica

Danni materiali e diretti alle cose assicurate (inclusi IOT e SCADA)

Dati ed archivi

Costo di ricostruzione dati elettronici e software

Danni da interruzione attività

Perdite patrimoniali da interruzione o sospensione totale o parziale di esercizio dell'attività, dovute al blocco, totale o parziale, dei Sistemi Informatici dell'assicurato

Sezione Costi Propri

Sono indennizzati i **compensi**, i **costi** e le **spese** ragionevolmente sostenuti e documentati per :

Costi propri

- **Costi di rilevazione e investigazione**
- **Costi di notifica**
- **Monitoraggio del credito**
- **Onorari di consulenti ed esperti**
- **Perdita di immagine limitata alla tutela del proprio diritto all'oblio ed ai costi di consulenza**
- **Minaccia al sistema informatico (escluso il prezzo del riscatto)**

Sezione Informatica

Informatica

- **Danni materiali e diretti** causati ad **apparecchiature elettroniche**, comprese quelle mobili, **strumenti IoT e sistemi SCADA**, causati da un qualunque **evento Cyber Crime**.
- **I sistemi fisici a cui si applicano gli strumenti IoT e sistemi SCADA**, si intendono **compresi in garanzia**, qualora il loro valore assicurabile sia dichiarato all'atto della sottoscrizione della Polizza.
- **Valore Intero**
- **Esclusioni: Danni al fabbricato e relativo contenuto**

Sezione Perdita di Dati e Archivi

Dati ed archivi

- Costi diretti per la ricostruzione ed il ripristino degli archivi perduti causati da:

  - **Evento Cyber crime**
  - **Furto o rapina**

- Si intendono indennizzabili anche i costi documentati sostenuti per la ricostituzione degli **Archivi perduti o alterati non di proprietà dell'Assicurato**, sui quali egli operi o che abbia in consegna o custodia.

Sezione Danni da Interruzione attività

Danni da interruzione attività

- Perdite dovute alla **riduzione del fatturato e l'aumento dei co**sti derivante da interruzione dell'attività causate da un evento Cyber Crime che abbia provocato un **blocco del sistema**

- **Maggiori costi per la prosecuzione dell'attività assicurata**

- **Interdipendenza interna**

- **Interdipendenza fornitori**

CAPO II - THIRD PARTY DAMAGE

La società si obbliga a tenere indenne l'assicurato di quanto questi sia tenuto a pagare a terzi quale civilmente responsabile

Responsabilità civile verso terzi

- a titolo di risarcimento di **danni patrimoniali, danni materiali e danni alla persona in relazione allo svolgimento delle attività dichiarate in polizza**

Responsabilità per danni alle merci

- in qualità di spedizioniere/spedizioniere-vettore/operatore multimodale e/o logistico, per danni alle merci

Sezione R.C.T

Responsabilità civile verso terzi

- Danni materiali, danni alla persona e perdite patrimoniali cagionati a Terzi in ragione della detenzione di dati e informazioni personali o commerciali.
- Danni materiali, danni alla persona e perdite patrimoniali cagionati a Terzi, per i quali l'assicurato sia civilmente responsabile in ragione di un evento Cyber
- Danni materiali e perdite patrimoniali conseguenti alla trasmissione di malware
- Perdite patrimoniali e danni alla persona subiti da un terzo in ragione della pubblicazione e diffusione di contenuti digitali
- Perdite patrimoniali cagionate a terzi per la detenzione di informazioni/dati relativi a carte di pagamento
- Danni da interruzione o sospensione dell'attività

Sezione R.C. Danni alle merci

Responsabilità per danni alle merci

➘ Danni materiali subiti dalle Merci consegnategli per la spedizione o il trasporto

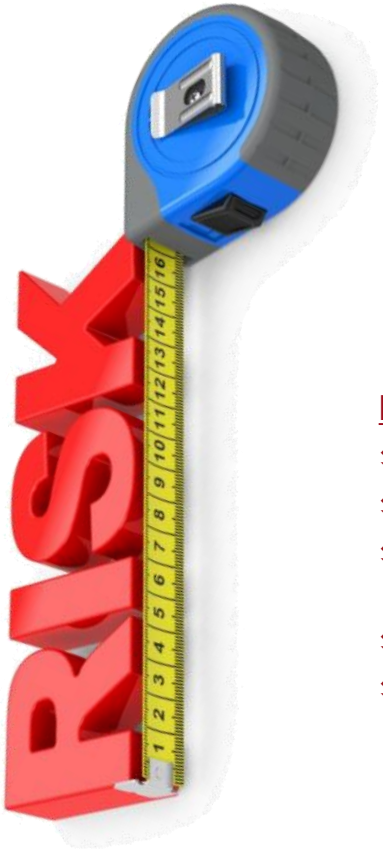
➘ Danni patrimoniali subiti dall'avente diritto sulle Merci a seguito di:

- inadempimenti contrattuali dai quali derivi una erronea o ritardata esecuzione delle spedizioni;
- consegna delle Merci non conforme alle istruzioni ricevute ovvero mancato ritiro dei documenti rappresentativi delle
- mancata o erronea compilazione e/o inoltro di documenti che siano in connessione con l'esecuzione di ordini di spedizione o trasporto;
- omissioni od errori nel far valere i diritti di regresso dell'avente diritto;
- errori od omissioni nelle disposizioni impartite al vettore per l'esecuzione del trasporto;
- mancato od erroneo prelievo di campioni ed errata constatazione di pesi e misure.

La copertura comprende anche:

- i costi per l'invio all'esatta destinazione di un carico erroneamente inoltrato in luogo diverso;
- i costi di rimozione, disinfezione, fumigazione e distruzione di Merci a seguito di un Sinistro per il quale l'Assicurato risulti responsabile ai sensi del primo paragrafo.

Risk Assessment



Informazioni Aggiuntive

- **Sistemi informatici:**
  - Manutenzione del sistema informatico
- **Risk Management**
  - Breach response plan
  - Disaster recovery plan
  - Business continuity plan
  - Confronto con il Team IT
- **Rapporti con fornitori**
  - Sistemi informativi Outsourcing
  - Controlli standard di sicurezza
  - Contratti tra le parti
- **Sinistri e circostanze**

Processo di quotazione

- **Questionario Web-Based :**
- **Comprensione dei sistemi critici per il business**
- **Comprensione delle procedure e degli standard di sicurezza**
- **Backups e data centers**
- **Comprensione situazione finanziaria**

Questionario Web-based

La prima valutazione del rischio viene effettuato sulla base del **questionario tecnico assuntivo**, predisposto tramite **tool on-line**, dove il cliente potrà accedere direttamente per la compilazione.

Questionario realizzato con la **consulenza di una società esterna specializzata in Cyber Security** e con l'attiva **partecipazione del team IT interno di Unipolsai**

Questa importante innovazione, oltre ad avere **vantaggi commerciali**, sul lato pratico consentirà al prospect di potersi **interfacciare con tutte le proprie aree aziendali** in maniera più rapida e precisa.

Il cliente potrà beneficiare di **tempi di risposta celeri** da parte della compagnia e **migliori termini e condizioni di polizza**

Questionario Web-based

Il questionario prevede **quattro sezioni** separate :

1. **Dati generali cliente ed attività svolta**

- **Anagrafica**
- **Settore di attività**
- **Somme assicurate apparecchiature elettroniche / Scada – IoT**
- **Fatturato / Profitto lordo**
- **Dichiarazione assenza sinistri e circostanze**

2. **Identificazione ambiti di polizza**

- **Descrizione dei processi aziendali, richiedendo la tipologia di applicativi e database utilizzati.**

3. **Processi IT esternalizzati**

- **Nominativi outsourcers ed i relativi servizi prestati**

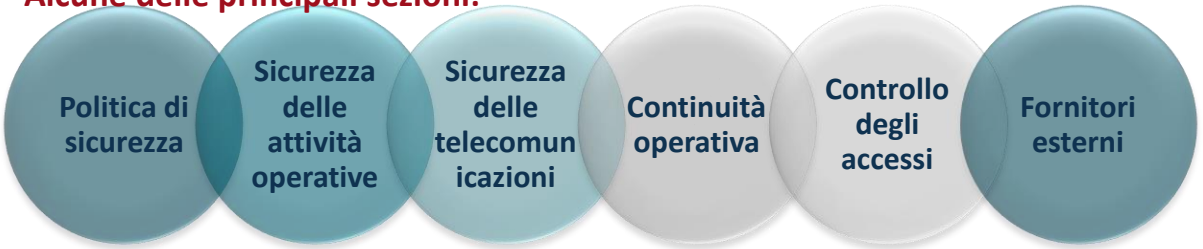
Questionario Web-based

4. Domande tecniche a risposta chiusa

- **In questa sezione sono contenute le domande tecniche utili per definire il profilo di rischio dell'assicurato.**

Le domande ricomprendono tutti i processi aziendali, focalizzandosi sui **sistemi di sicurezza** e sulle **procedure** adottate **in ambito IT**

Alcune delle principali sezioni:



Informazioni aggiuntive

A discrezione della Compagnia, a seconda della tipologia di attività, dimensioni aziendali, risposte fornite tramite il questionario, può essere richiesta **documentazione a supporto** del questionario tecnico assuntivo come:

- **Breach response plan**
- **Disaster recovery plan**
- **Business continuity plan**
- **Documentazione sinistri e circostanze**

Inoltre ci riserviamo la possibilità di un **confronto con il Team IT del prospect** e la possibilità di **effettuare un penetration test** con il supporto della società inthecyber.

http://www.inthecyber.com/

Grazie per l’attenzione