INSURANCE Daily

● GIOVEDÌ 30 APRILE 2020 N. 1742

PRIMO PIANO

Ania/OoSs, linee guida aggiornate

L'Ania e le organizzazioni sindacali First Cisl, Fisac Cgil, Fna, Snfia e Uilca hanno condiviso, "con specifico riferimento all'accesso alle prestazioni ordinarie del fondo di solidarietà nei casi di riduzione/sospensione dell'attività lavorativa", la necessità di integrare il protocollo siglato lo scorso 24 marzo con le linee guida di riferimento per le imprese e le rappresentanze sindacali aziendali in caso di avvio dell'iter necessario all'accesso all'assegno ordinario. Lo annuncia un comunicato delle parti.

Queste linee guida prevedono in sostanza che, nel caso in cui l'azienda intenda ricorrere al sostegno al reddito, l'assegno ordinario corrisposto dall'Inps venga integrato dall'azienda fino al 100% della retribuzione individuata dall'istituto, che il lavoratore avrebbe percepito in assenza della riduzione/sospensione dell'attività lavorativa, fermo restando che, a livello aziendale, si potrà tenere conto delle specifiche peculiarità dell'organizzazione del lavoro dell'impresa.

Inoltre, conclude il comunicato, "l'eventuale riduzione/sospensione dell'attività lavorativa non avrà effetti sugli altri istituti riguardanti il rapporto di lavoro", quali, ad esempio, la previdenza complementare e l'assistenza sanitaria.

Beniamino Musto

RISK MANAGEMENT

Business interruption e cyber risk, due minacce interconnesse

Crimine informatico e sospensione dell'attività sono due rischi che agiscono in osmosi: anche gli incidenti informatici, infatti, possono paralizzare le operazioni di un'impresa. Secondo le stime, il costo medio di un attacco informatico è aumentato del 62% negli ultimi cinque anni e una tipica violazione dei dati può costare a un'azienda anche più di quattro milioni di euro

Le catastrofi naturali occupano solo il terzo posto tra i rischi considerati globalmente più preoccupanti, secondo l'edizione 2019 dello studio che **Allianz Global Corporate and Specialty** (Agcs) effettua ogni anno: l'ormai noto *Allianz Risk Barometer*. Il primo posto è infatti occupato, ex equo, dai rischi derivanti dalle interruzioni di esercizio (*business interruption*) e dal *cyber risk*.

La medesima graduatoria si rispecchierebbe anche sulla ricerca effettuata per il solo mercato italiano, nel quale il cyber risk, invece che dividere la prima posizione come accade a livello globale, si piazza al secondo posto dopo i problemi legati alla business interruption.

DUE RISCHI IN OSMOSI

L'impatto dell'interruzione d'esercizio, con particolare riguardo all'interruzione delle catene di distribuzione e fornitura, ha rappresentato il rischio più temuto dalle aziende anche nel 2019, per il settimo anno consecutivo, e con il 37% delle risposte fornite dai risk manager.

Al secondo posto, come abbiamo detto, si posiziona il cyber crime, o crimine informatico, ma c'è da notare che questi due rischi subiscono una certa osmosi, poiché anche gli incidenti informatici possono paralizzare le operazioni di un'azienda o compromettere gravemente la sua capacità di erogare i propri servizi.

Tuttavia, indipendentemente dal fatto che derivi da cyber crime o da esposizioni tradizionali, come un incendio in un impianto di produzione o una catastrofe naturale, un'interruzione della catena di approvvigionamento può avere un effetto enorme sui ricavi di un'azienda, anche se l'evento si verificasse a miglia di distanza da essa. Inoltre, l'impatto che ne deriva costituisce uno dei rischi più difficili da valutare, a causa della sempre maggiore interconnessione e globalizzazione rilevabile nei rapporti commerciali. *(continua a pag. 2)*

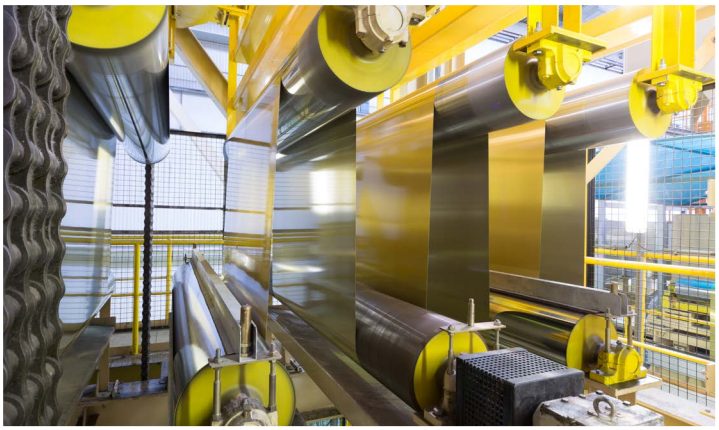
INSURANCE Daily

GIOVEDÌ 30 APRILE 2020 N. 1742

(continua da pag. 1)

UN NUMERO CRESCENTE DI SCENARI

La grande rilevanza di questo genere di rischio è dimostrata dal fatto che oramai quasi tutti i risarcimenti e gli indennizzi assicurativi nell'ambito dei rami *property* comportano elementi di *business interruption* in quantità sempre più importante, tanto da costituire la maggior parte del danno, laddove in precedenza la proporzione era assai più vicina al 50%.



Le aziende affrontano infatti un numero crescente di scenari, man mano che la natura del rischio si evolve in una società oramai totalmente interconnessa. Molti di questi scenari possono anche non presentare danni materiali, ma comportano tuttavia elevate perdite sul piano finanziario.

Si tratta di eventi molto diversificati, che vanno dal guasto dei sistemi informatici al richiamo dei prodotti in seguito a problemi sulla loro sicurezza e qualità, eventi di terrorismo o a matrice politica, incidenti ambientali o episodi di inquinamento e persino semplici modifiche alla normativa del Paese ospitante, che possono causare un arresto temporaneo o prolungato dell'attività e avere un effetto devastante sul fatturato.

Il ritiro dei prodotti, ad esempio, rappresenta una crescente minaccia nell'ambito della business interruption, anche perché un prodotto inadeguato, che si trovasse all'inizio della catena di approvvigionamento, potrebbe influire sull'intero processo e sul prodotto finale. Pensiamo al settore automobilistico, caratterizzato da un'estrema dislocazione territoriale delle località produttive, che è quanto mai esposto a risarcimenti ingenti, qualora le autovetture vendute provocassero danni ai loro occupanti e questi derivassero da una carenza nella sicurezza di un loro componente.

IL RISCHIO POLITICO E I SUOI ANNESSI

Gli eventi collegati al cosiddetto rischio politico, inoltre, non sono certo poco probabili, com'è stato dimostrato dalle rivolte e proteste verificatesi in Francia negli ultimi mesi del 2018: in quel caso la **Federazione francese delle attività di vendita al dettaglio** ha dichiarato una perdita di circa un miliardo di euro da parte dei negozianti che furono costretti a chiudere i battenti durante quei fatti.

L'interruzione d'esercizio può anche essere causata da problemi ambientali, come l'inquinamento in un sito produttivo. È questo un tipo di esposizione alla business spesso trascurato, ma le spese conseguenti all'interruzione della catena di approvvigionamento possono crescere assai rapidamente nel corso degli interventi di riparazione, durante i quali le imprese potrebbero non essere in grado di operare o fornire prodotti o servizi.

Infine, un panorama politico e commerciale incerto come quello provocato dalla *Brexit* può comportare rischi significativi nell'ambito della business interruption. L'interruzione della catena di approvvigionamento può infatti essere causata dalla chiusura dei confini di un Paese e, se un'azienda manifatturiera avesse bisogno di un componente prodotto nel Regno Unito, i tempi necessari per riceverlo potrebbero risultare assai maggiori del previsto. Sono già stati segnalati casi in cui in Regno Unito si starebbero esaurendo gli spazi di stoccaggio dei prodotti alimentari, in seguito al timore che le catene di approvvigionamento vengano interrotte dopo il periodo di transizione e la definitva uscita del Regno Unito dall'Unione Europea.

Secondo lo studio di Allianz, l'indennizzo medio da business interruption ammonta oggi ad oltre tre milioni di euro ed è aumentato di circa un terzo dalla media registrata solo cinque anni fa. Molti assicuratori stanno cercando di supportare le imprese, fornendo nuove soluzioni sempre più esclusive e specifiche.

INIZIATIVE PER IL CONTENIMENTO DEI COSTI

Dal punto di vista delle iniziative volte al contenimento dei costi complessivi a livello globale, è probabile che i riassicuratori suggeriscano l'applicazione di limiti di risarcimento atti a evitare che un evento solo possa causare perdite di dimensioni ingestibili, proprio a causa delle dimensioni globali che ogni minaccia assume ormai in ambito business interruption, tali cioè da provocare il fallimento di uno o più operatori. Non sarebbe la prima volta che questo pericolo verrebbe corso dal comparto assicurativo: per fare un esempio, il danno al prodotto interno lordo dell'economia newyorkese, in seguito all'attacco alle *Torri Gemelle*, fu stimato in 27,3 miliardi di dollari solo nel periodo compreso tra gli ultimi tre mesi del 2001 e tutto il 2002.

LE IMPLICAZIONI DERIVANTI DAL CRIMINE CIBERNETICO

Per la prima volta, gli incidenti informatici si collocano nella parte più alta del barometro del rischio elaborato da Allianz, in particolare per le loro implicazioni in ambito di business interruption, a causa della crescente dipendenza del mondo produttivo dalla tecnologia e dell'aumento indiscriminato degli attacchi provocati dai criminali informatici e financo da certi governi nazionali.

I danni causati in questi eventi possono causare perdite molto ingenti. Il crimine informatico rappresenta un fattore in grado di attirare l'attenzione dei media, ma spesso bastano guasti tecnici anche banali, o il semplice errore umano, a causare perdite veramente importanti per le aziende e i loro eventuali assicuratori. *(continua a pag. 3)*

INSURANCE Daily

GIOVEDÌ 30 APRILE 2020 N. 1742

(continua da pag. 2)

Secondo l'analisi di Agcs, sulla scia degli attacchi di malware globali *WannaCry* e *NotPetya*, negli ultimi cinque anni il danno medio causato dagli incidenti informatici ha superato i due milioni di euro e i maggiori eventi hanno raggiunto importi complessivi nell'ordine di centinaia di milioni.

DOVE SI CORRONO MAGGIORI PERICOLI

I sistemi di information technology sono passati da una funzione di supporto a una risorsa fondamentale e critica per le aziende e ci si augura che il rischio cyber diventi sempre più centrale per i risk manager, al punto da decidere di mantenerlo saldamente nei loro radar. In ogni caso, poiché le aziende detengono grandi quantità di dati personali, le violazioni stanno aumentando in termini di dimensioni e costi.

I maggiori rischi si segnalano nei settori: aviazione; intrattenimento e media servizi finanziari; servizi pubblici e amministrativi; servizi professionali; tecnologia; telecomunicazioni

Recenti mega violazioni dei dati hanno infatti coinvolto **Equifax** (143 milioni di persone), **Facebook** (50 milioni) e **Uber** (57 milioni), per non parlare dell'attacco che ha colpito circa 380 milioni di clienti degli hotel **Marriott** alla fine del 2018, che è considerato uno dei più gravi mai registrati.

Questi episodi comporteranno molto probabilmente una riduzione nell'appetito di certi assicuratori per determinate categorie di rischio o l'introduzione di esclusioni o limitazioni consistenti sulle estensioni di copertura che riguardano l'elenco di attività menzionate.

IL COSTO DI UN ATTACCO

Il **Ponemon Institute** e **Accenture** hanno infatti rivelato che il costo medio di un attacco informatico è aumentato del 62% negli ultimi cinque anni e che una tipica violazione dei dati può costare a un'azienda anche più di quattro milioni di euro, contro i due milioni indicati da Agcs. Il costo della violazione subita dal Marriott è stato stimato tra i 200 e i 600 milioni di dollari da **Air Worldwide**. Nell'agosto del 2018, un fornitore chiave per **Apple**, il produttore di semiconduttori **Taiwan Semiconductor Manufacturing Company**, ha perso oltre un giorno di produzione a causa di un macchinario infettato da virus negli stabilimenti di Taiwan: il virus era una variante di WannaCry.

Nel frattempo, i porti di Barcellona e San Diego sono stati vittime di attacchi ransomware, che hanno colpito server e sistemi amministrativi, e anche la compagnia di navigazione **Cosco** ha subito la disabilitazione dei suoi sistemi tecnologici negli Stati Uniti. Tutti questi eventi hanno determinato richieste superiori ai 100 milioni di dollari per gli assicuratori. In realtà, si ritiene che i danni da cyber crime costino oggi quasi 600 miliardi all'anno (**Center for strategic and international studies**), cioè tre volte la perdita economica causata in media dalle catastrofi naturali negli ultimi dieci anni.

I progressi della tecnologia generano sempre nuove minacce e vulnerabilità informatiche. Si pensi ad esempio all'effetto dell'aumento della connettività e agli sviluppi della cosiddetta intelligenza artificiale e dell'IoT: la digitalizzazione delle catene di approvvigionamento non può che creare nuovi fronti di attacco che i criminali informatici possono sfruttare.

Si prevede che i costi finali dell'attacco NotPetya ammonteranno a circa tre miliardi di dollari per gli assicuratori, secondo un calcolo di **Property Claims Services** (Pcs).

Pare che circa il 90% di questo ammontare sia attribuibile alle cosiddette esposizioni silenziose, ovvero a quelle che rientrano nelle coperture di tipo tradizionale, come sono ad esempio le polizze property e relative danni indiretti, ma che non sono prestate intenzionalmente dai sottoscrittori.

Si tratta delle esposizioni più pericolose, perché da una parte non forniscono coperture adeguate agli assicurati (non essendo pensate per gli incidenti che si verificano) e dall'altra nascondono temibili sorprese per le compagnie assicuratrici, che non sono in grado di proteggersi da danni completamente imprevedibili, per i quali hanno insufficienti o nessuna copertura riassicurativa.

Cinzia Altomare

INSURANCE Daily

● GIOVEDÌ 30 APRILE 2020 N. 1742

Insurance Daily
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e Redazione: Insurance Connect Srl – Via Montepulciano 21 – 20124 Milano
T: 02.36768000 **E-mail:** redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare info@insuranceconnect.it
Supplemento al 30 aprile di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577