INSURANCE Daily

N. 2858 LUNEDÌ 6 OTTOBRE 2025

PRIMO PIANO

Esa, attenzione alle cripto-attività

Neppure l'entrata in vigore del nuovo regolamento europeo Micar potrà proteggere i consumatori da tutti i rischi connessi all'investimento in cripto-attività. Lo hanno ben chiarito le tre autorità europee di vigilanza sul settore finanziario, ossia Eba, Eiopa ed Esma, in un recente avviso in cui mettono in guardia sui principali rischi legati a questo innovativo genere di asset class. "Non tutte le cripto-attività e i servizi per le cripto-attività sono uguali né sono disciplinati allo stesso modo, anche quando rientrano tra quelli regolamentati", si legge nel report firmato dall'Esa. La maggior parte di queste attività, prosegue l'avviso, "rimane di genere volatile e altamente rischiosa". E, proprio per questo motivo, "potrebbero non essere adatte a tutti i consumatori come strumenti di investimento, pagamento o scambio". Il rapporto evidenzia soprattutto che, a seconda del tipo di asset o del fornitore di servizi, il consumatore potrebbe anche non poter disporre di alcun tipo di protezione. "Ciò vale in particolare se investi in cripto-attività o utilizzi servizi di cripto-attività offerti da operatori con sede al di fuori dell'Unione Europea e da fornitori non regolamentati dal Micar".

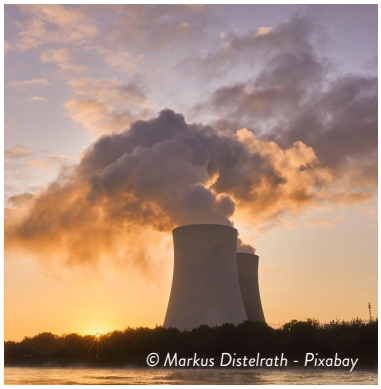
Fra i rischi principali connessi alle cripto-attività, il rapporto cita in particolare la complessità dei prodotti, la volatilità dell'andamento dei prezzi, la carenza di liquidità, la diffusione di informazioni fuorvianti e, in definitiva, la possibilità di incappare in frodi, truffe e attacchi informatici.

Giacomo Corvi

RICERCHE

Quando l'assicurazione non basta: come coprire i rischi Cbrn

Un report di Geneva Association e Iftrip affronta il tema degli incidenti negli ambiti chemical, biological, radiological, nuclear: minacce ad alta severità e bassa frequenza che non possono essere eliminate, ma la cui gestione può essere migliorata attraverso un approccio sistemico, nuovi strumenti di risk transfer e una maggiore cooperazione internazionale


© Markus Distelrath - Pixabay

Il rischio legato a incidenti chimici, biologici, radiologici e nucleari (riuniti sotto l'acronimo Cbrn) è da tempo al centro dell'attenzione di governi, assicuratori e analisti di sicurezza. Nonostante si tratti di eventi piuttosto rari, il loro potenziale catastrofico li rende una delle minacce più complesse da gestire per l'industria assicurativa e riassicurativa. A ribadirlo è il nuovo report congiunto pubblicato a settembre 2025 dalla **Geneva Association** e dall'International Forum of Terrorism Risk (Re)Insurance Pools (**Iftrip**), che mette in evidenza criticità, scenari di perdita e possibili strategie di risposta.

RISCHI ESTREMI E LIMITI DI CAPACITÀ

Il documento chiarisce come la natura dei rischi Cbrn, caratterizzati da bassa frequenza ma altissima intensità, superi ampiamente la capacità assuntiva del mercato privato. La maggior parte delle polizze property & casualty esclude espressamente tali eventi o li copre con sottolimiti, salvo in pochi mercati (come Francia e Spagna) dove l'assicurazione obbligatoria garantisce un livello minimo di protezione. Questa asimmetria genera un significativo protection gap: in caso di evento su larga scala, i costi ricadrebbero in gran parte sui bilanci pubblici, con effetti potenzialmente destabilizzanti anche a livello macroeconomico.

UN DETERIORAMENTO NEGLI STANDARD DI SICUREZZA

Il report sottolinea come il contesto geopolitico e tecnologico stia aumentando l'esposizione al rischio. Secondo il database dell'Università del Maryland, tra il 1990 e il 2023 sono stati registrati 273 attacchi Cbrn da parte di attori non statali violenti, con quasi il 90% dei casi legati ad agenti chimici. Seppur in calo negli ultimi anni, la minaccia non è scomparsa: il governo britannico ha stimato come "probabile" un attacco terroristico Cbrn entro il 2030. A preoccupare è anche la proliferazione di tecnologie dual use. Droni commerciali, strumenti di bioingegneria come Crispr e intelligenza artificiale applicata al settore biologico abbassano le barriere di accesso per gruppi estremisti o criminali. La Nuclear Threat Initiative ha inoltre segnalato un deterioramento degli standard di sicurezza nucleare in diversi paesi, con un aumento delle opportunità di furto o sabotaggio.

DANNI DIRETTI, MA ANCHE CONSEGUENZE SISTEMICHE

Gli impatti di un evento Cbrn, si legge nel rapporto, non si limiterebbero alle vittime dirette: le analisi mostrano come la componente economica e sociale possa

risultare di gran lunga più pesante. Interruzioni delle catene di fornitura, chiusura di aree produttive, crollo del turismo e ritardi negli investimenti esteri sono solo alcuni degli effetti di lungo periodo.

Gli esempi storici riportati nel report sono eloquenti: dal disastro di Bhopal (1984) al meltdown di Chernobyl (1986), fino a Fukushima (2011), i costi stimati hanno raggiunto centinaia di miliardi di dollari, includendo decontaminazione, danni ambientali, perdita di fiducia nei mercati e contrazione della crescita economica. Anche eventi di scala minore, come le contaminazioni da antrace negli Stati Uniti (2001) o gli avvelenamenti da Novichok nel Regno Unito (2018), hanno prodotto spese ingenti per bonifiche, indagini e impatto reputazionale.

IL QUADRO NORMATIVO E LE SFIDE REGOLATORIE

Uno degli elementi che aggravano la complessità del rischio Cbrn è la frammentazione normativa. A livello internazionale esistono convenzioni consolidate solo per il settore nucleare (come la Convenzione di Vienna sulla responsabilità civile per danni nucleari o la Convenzione di Parigi nel campo dell'energia nucleare) che definiscono criteri di responsabilità e massimali. Tuttavia, non tutti i paesi hanno ratificato tali strumenti, e spesso coesistono legislazioni nazionali differenti.

Al di fuori del comparto nucleare, i vuoti regolatori sono ancora più ampi. Non esistono convenzioni internazionali robuste che disciplinino la responsabilità per danni derivanti da incidenti chimici o biologici di matrice dolosa, lasciando di fatto le vittime a percorsi di contenzioso civile incerti e lunghi. Questo quadro, secondo il report, contribuisce a scoraggiare l'offerta assicurativa, in assenza di regole chiare sulla ripartizione delle responsabilità e sull'indennizzo transfrontaliero.

LA GOVERNANCE DEL RISCHIO PER LE IMPRESE

Per le aziende esposte, dall'energia all'industria chimica, dai trasporti alla sanità, il tema Cbrn rappresenta una sfida di governance. Sempre più investitori e board chiedono strategie di resilienza che includano scenari estremi, anche se a bassa probabilità. Il report sottolinea come sia cruciale integrare la gestione del rischio Cbrn nei piani di continuità operativa.

Secondo lo studio, la crescente attenzione di autorità di vigilanza come Eiopa in Europa o Naic negli Stati Uniti lascia intendere che, in futuro, le imprese dovranno rendicontare con maggiore trasparenza il livello di esposizione a rischi sistemici come quelli Cbrn. In questo senso, le compagnie di assicurazione potrebbero non limitarsi al ruolo di indennizzatori ma diventare partner attivi nella costruzione di piani di prevenzione, resilienza e risposta alle crisi.

LE SFIDE PER IL SETTORE ASSICURATIVO

Dal punto di vista assicurativo, il problema principale resta la difficoltà di modellizzare scenari ad alta incertezza. Le compagnie, sostiene lo studio, faticano a stimare in modo affidabile probabilità e severità di questi eventi, limitando così la capacità di sottoscrizione. Attualmente esistono soluzioni parziali: captive aziendali, schemi mutualistici nel nucleare, pool nazionali per il terrorismo. Tuttavia, la diffusione di tale copertura è frammentaria e non uniforme, con forti differenze tra mercati e linee di business. Il report mette in guardia sul fatto che la resilienza finanziaria in caso di evento Cbrn dipenderà sempre più dalla cooperazione pubblico-privata e dalla condivisione internazionale del rischio. L'attuale mosaico di clausole, esclusioni e sottolimiti non è sufficiente a fronteggiare uno scenario di perdita su larga scala. Ecco perché Geneva Association e Iftrip propongono tre linee di azione principali. La prima riguarda la condivisione di best practice tra i pool nazionali, inclusa la promozione di modelli alternativi di finanziamento e programmi di formazione specifica sulla modellizzazione dei rischi Cbrn. La seconda linea di azione è relativa all'esplorazione di schemi di reciprocità internazionale, analoghi a quelli già esistenti nel settore nucleare, per superare la frammentazione dei mercati nazionali. Infine, il rapporto raccomanda l'avvio di un "dialogo rafforzato tra compagnie, governi e policy maker globali, per sviluppare soluzioni innovative di gestione del rischio e prevenire gap di copertura che ricadrebbero su stati e cittadini".

UNO SFORZO DI SISTEMA

È dunque evidente che in contesto così complesso nessun attore, da solo, può fronteggiare la portata di un evento Cbrn. Per questo, secondo gli autori dello studio, è necessario costruire "un'architettura multilivello che includa compagnie, governi, istituzioni internazionali e imprese stesse". In assenza di un tale coordinamento, ogni incidente rischia di trasformarsi in una crisi finanziaria e sociale amplificata. La sfida, dunque, non riguarda soltanto la capacità di pagare i sinistri, ma il ruolo dell'assicurazione come infrastruttura critica di stabilità economica. Costruire strumenti di copertura condivisi e robusti, in grado di ridurre il protection gap oggi evidente, rappresenta la vera frontiera per il settore assicurativo globale.

Beniamino Musto

Per approfondire su www.insurancetrade.it:

- *Danni all'ambiente, solo lo 0,45% delle imprese italiane è assicurato*

INSURANCE Daily

N. 2858 LUNEDÌ 6 OTTOBRE 2025

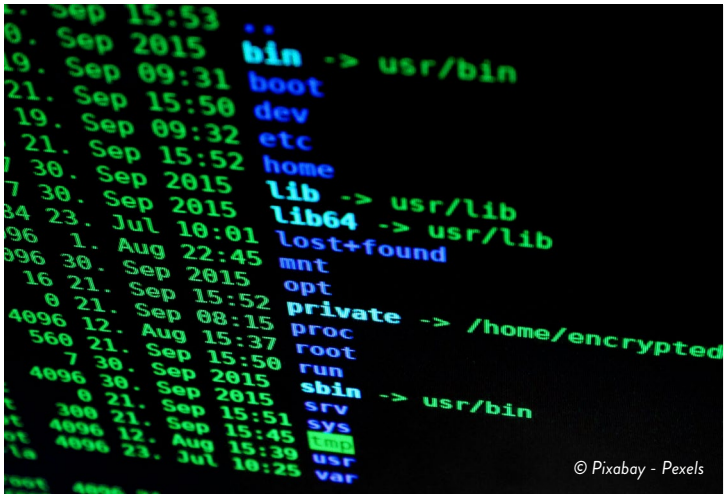
RICERCHE

Cybercrime, aziende sempre più resilienti

Nonostante un panorama di minacce in continua evoluzione, quest'anno le imprese assicurate hanno mostrato una maggiore preparazione agli attacchi informatici. Secondo gli analisti di Allianz Commercial, ora gli ambiti di rischio si stanno spostando sempre più verso supply chain e gestione dei dati, in particolare per le Pmi

Nel 2025 il novero delle minacce digitali ha continuato a espandersi ma le aziende sembrano in grado di rispondere meglio, soprattutto quelle coperte da assicurazioni informatiche. Secondo il recente *Cyber Security Resilience Outlook* di **Allianz Commercial**, nel primo semestre dell'anno la frequenza dei sinistri cyber è rimasta stabile (rispetto allo stesso periodo del 2024), mentre la gravità delle perdite è calata di oltre il 50%: un dato che riflette l'efficacia delle strategie di protezione, preparazione e risposta agli attacchi.

Il miglioramento della resilienza non significa però fine dei problemi. Le minacce stanno cambiando volto, spostandosi da attacchi diretti verso modalità più indirette e sofisticate come l'ingegneria sociale, il furto di credenziali o l'interruzione delle catene di fornitura digitali. E parallelamente sta crescendo il peso della normativa sulla privacy e il correlato rischio di contenziosi.



© Pixabay - Pexels

Ransomware ancora al primo posto

Il ransomware continua a essere il principale responsabile dei sinistri assicurativi, causando circa il 60% del valore delle perdite informatiche gravi (cioè quelle superiori a un milione di euro) nei primi sei mesi del 2025. Nulla di strano, se si considera che solo nella prima metà dell'anno scorso i gruppi ransomware sono aumentati del 50%. La novità è che gli attacchi si stanno spostando verso le imprese più piccole e meno protette, soprattutto in Asia e America Latina. Secondo gli ultimi dati, il ransomware è coinvolto nell'88% delle violazioni alle Pmi, contro il 39% registrato nelle grandi aziende.

Gli analisti di Allianz Commercial hanno rilevato anche un aumento degli attacchi basati sull'esfiltrazione dei dati, cioè il furto di informazioni da usare come leva per l'estorsione. Questo tipo di violazione ha interessato il 40% del valore dei grandi sinistri nei primi sei mesi del 2025, in crescita rispetto al 25% dell'anno precedente. La sottrazione di dati è resa ancora più redditizia dalla presenza di normative severe sulla protezione delle informazioni personali: il costo medio globale di una violazione ha sfiorato il record di cinque milioni di dollari nel 2024, e le probabilità di pagamento del riscatto aumentano significativamente in caso di fuga di dati sensibili.

Le nuove armi del crimine informatico

Il report prosegue segnalando un crollo nell'utilizzo di malware: oggi l'80% degli attacchi non prevede un software

dannoso ma si basa su credenziali rubate, phishing o social engineering (dal 40% nel 2019). Circa sei violazioni su dieci nel 2024 hanno coinvolto un fattore umano, mentre gli attacchi tramite fornitori terzi sono raddoppiati, arrivando al 30%.

Questo spostamento strategico dei cybercriminali riflette un'altra criticità, ovvero la vulnerabilità delle catene di fornitura, spesso meno sorvegliate rispetto ai sistemi interni aziendali. Gli eventi di interruzione operativa legati alla supply chain IT hanno rappresentato il 15% del valore dei grandi sinistri nella prima metà del 2025, quasi il triplo rispetto all'anno precedente. Il motivo è semplice: sempre più aziende dipendono da software, cloud e fornitori digitali esterni per il proprio funzionamento quotidiano.

Le sole intrusioni nei servizi cloud, a titolo di esempio, sono aumentate del 136% nei primi sei mesi del 2025. Nonostante i progressi delle aziende nei controlli interni, il rischio legato ai partner esterni resta difficile da gestire e spesso del tutto fuori dal perimetro di controllo aziendale.

Vulnerabilità e violazione dei dati personali

L'industria manifatturiera continua a essere il settore più colpito in termini di valore dei sinistri (33%), seguita dai servizi professionali (18%) e dal commercio al dettaglio (9%). I rivenditori, in particolare, sono bersagli privilegiati per la mole di dati trattati e la complessità dei loro sistemi, spesso meno protetti rispetto a settori come quello bancario. Anche il numero elevato di fornitori e dipendenti espone queste aziende a maggiori rischi di attacco, rendendole vulnerabili anche dal punto di vista umano.

Gli analisti precisano infatti che non tutti gli incidenti informatici sono causati da attacchi: nel 2024, il 28% del valore dei grandi sinistri è stato generato da guasti tecnici, blackout e violazioni della privacy, senza coinvolgimento diretto di malware o hacker.

Le violazioni dei dati personali, in particolare, pesano sempre più sui sinistri cyber e nel 2024 hanno rappresentato il 18% del valore dei grandi risarcimenti, triplicando in tre anni. Nello stesso periodo negli Stati Uniti sono state avviate circa 1.500 cause per violazione della normativa sui dati. Per le aziende, restare al passo con regole sempre più complesse è una sfida resa ancor più difficile dall'uso crescente dell'AI.

L'importanza dell'AI e delle difese automatizzate

Una delle evidenze più forti del rapporto riguarda il ruolo decisivo della preparazione e della risposta agli incidenti. In oltre l'80% dei grandi sinistri, le decisioni prese dagli assicurati hanno inciso sull'entità della perdita. Strumenti come backup, segmentazione della rete e autenticazione multi-fattore possono ridurre il danno anche di mille volte.

In questo nuovo equilibrio tra attaccanti e difensori, l'intelligenza artificiale gioca un ruolo sempre più centrale. Da un lato, permette ai criminali informatici di automatizzare attacchi, creare campagne di phishing convincenti e scoprire vulnerabilità in modo sistematico. Dall'altro, sta rivoluzionando la sicurezza informatica, grazie a sistemi intelligenti di monitoraggio e risposta automatizzata.

Secondo gli ultimi dati, le aziende che hanno adottato AI e automazione hanno risparmiato in media 2,2 milioni di dollari rispetto a quelle che non l'hanno fatto. Una cifra che conferma il valore strategico di questi strumenti, anche alla luce dell'arrivo delle nuove normative europee, che impongono requisiti più severi in materia di resilienza digitale.

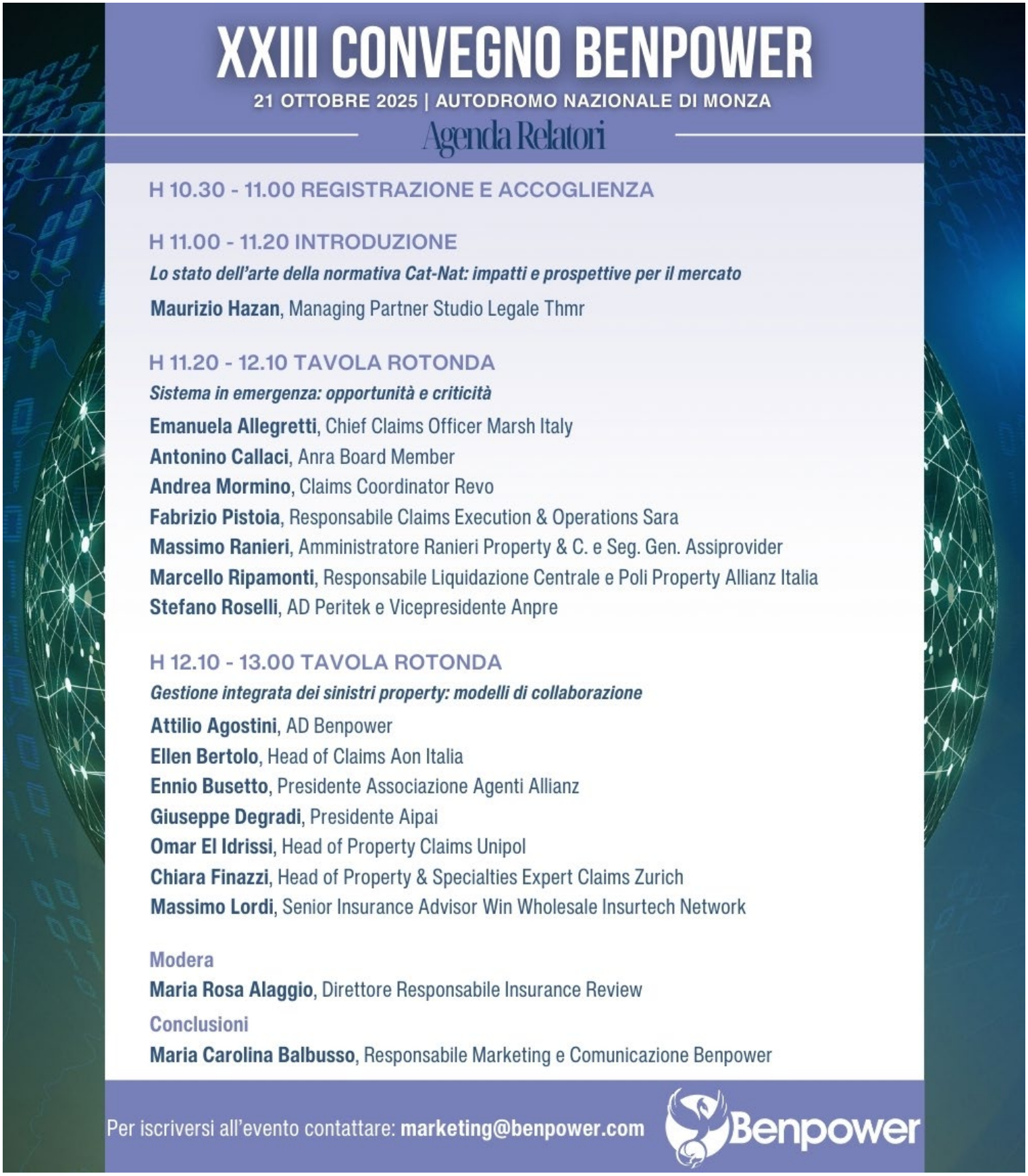
Il documenti, infine, evidenzia una crescita del divario tra aziende assicurate e non assicurate: le prime mostrano impatti economici più contenuti e una maggiore prontezza nella risposta. Non a caso, si prevede che il mercato globale delle assicurazioni cyber raddoppierà entro il 2030, toccando i 30 miliardi di dollari.

Michele Starace

Per approfondire su www.insurancetrade.it:

- *Il rischio cyber è la prima preoccupazione delle aziende*
- *Il futuro del cyber risk tra ransomware e conflitti geopolitici*

INSURANCE DAILY
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e redazione: Insurance Connect Srl – Via Montepulciano, 21 – 20124 Milano
T: 02.36768000 email: redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare: info@insuranceconnect.it
Supplemento al 6 ottobre di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577


XXIII CONVEGNO BENPOWER
21 OTTOBRE 2025 | AUTODROMO NAZIONALE DI MONZA
Agenda Relatori
H 10.30 - 11.00 REGISTRAZIONE E ACCOGLIENZA
H 11.00 - 11.20 INTRODUZIONE
Lo stato dell'arte della normativa Cat-Nat: impatti e prospettive per il mercato
Maurizio Hazan, Managing Partner Studio Legale Thmr
H 11.20 - 12.10 TAVOLA ROTONDA
Sistema in emergenza: opportunità e criticità
Emanuela Allegretti, Chief Claims Officer Marsh Italy
Antonino Callaci, Anra Board Member
Andrea Mormino, Claims Coordinator Revo
Fabrizio Pistoia, Responsabile Claims Execution & Operations Sara
Massimo Ranieri, Amministratore Ranieri Property & C. e Seg. Gen. Assiprovider
Marcello Ripamonti, Responsabile Liquidazione Centrale e Poli Property Allianz Italia
Stefano Roselli, AD Peritek e Vicepresidente Anpre
H 12.10 - 13.00 TAVOLA ROTONDA
Gestione integrata dei sinistri property: modelli di collaborazione
Attilio Agostini, AD Benpower
Ellen Bertolo, Head of Claims Aon Italia
Ennio Busetto, Presidente Associazione Agenti Allianz
Giuseppe Degradi, Presidente Aipai
Omar El Idrissi, Head of Property Claims Unipol
Chiara Finazzi, Head of Property & Specialties Expert Claims Zurich
Massimo Lordi, Senior Insurance Advisor Win Wholesale Insurtech Network
Modera
Maria Rosa Alaggio, Direttore Responsabile Insurance Review
Conclusioni
Maria Carolina Balbusso, Responsabile Marketing e Comunicazione Benpower
Per iscriversi all'evento contattare: marketing@benpower.com
Benpower