INSURANCE Daily

N. 2884 MARTEDÌ 11 NOVEMBRE 2025

PRIMO PIANO

Munich Re, bene nel Q3 2025

Munich Re ha chiuso il terzo trimestre 2025 registrando un utile netto di poco inferiore ai 2 miliardi di euro (1.997 milioni), in crescita rispetto ai 907 milioni ottenuti nello stesso periodo dell'anno scorso. Nei nove mesi l'utile si porta a 5,1 miliardi (anche in questo caso in crescita dai 4,6 miliardi a fine settembre 2024). Tuttavia sono calati nel terzo trimestre i ricavi di assicurazione derivanti dai contratti assicurativi emessi, scesi a 14,5 miliardi di euro principalmente a causa degli effetti negativi della conversione valutaria, mentre sui nove mesi si mantengono in linea con l'analogo periodo 2024 (45,2 miliardi vs 45,5 miliardi). Nel terzo trimestre il risultato tecnico totale è aumentato a 2,8 miliardi (1,7 miliardi nel 2024). Il risultato valutario è stato pari a -189 milioni di euro, principalmente a causa delle perdite sui cambi rispetto al dollaro statunitense. Il risultato operativo è aumentato significativamente a 3 miliardi circa (era 1,1 nel 2024), con un'aliquota fiscale effettiva al 32,9%.

Il business della riassicurazione nel terzo trimestre ha contribuito al risultato netto per 1,7 miliardi di euro (766 milioni nel 2024), e per 4,3 miliardi (2024: 3,9 miliardi) nei nove mesi. I ricavi assicurativi del terzo trimestre derivanti da contratti assicurativi emessi, restando nel business della riassicurazione, sono scesi a 9,2 miliardi (era a 10,2 nel 2024). Molto buona la performance di Ergo, che nel trimestre ha ottenuto un risultato di 304 milioni (141 milioni nel 2024) e di 796 milioni (2024: 629 milioni) nei nove mesi.

Beniamino Musto

NORMATIVA

Varata l'attesa riforma delle professioni ordinistiche

Il disegno di legge introduce principi comuni per le diverse categorie professionali: agrotecnici, architetti, assistenti sociali, attuari, agronomi e forestali, geologi, geometri, giornalisti, ingegneri, periti industriali, spedizionieri doganali e consulenti del lavoro. Restano per il momento esclusi commercialisti e notai, in attesa di un regolamento specifico

SECONDA PARTE


© LEANDRO AGUILAR - Pixabay

Come anticipato, si tratta di una novità di grande rilevanza, che limita la punibilità per omicidio colposo e lesioni personali colpose, commessi nell'esercizio della professione, ai soli casi di colpa grave. Questi ultimi dovranno essere accertati dal giudice, tenendo conto, oltre che della complessità della patologia del paziente, anche della scarsità delle risorse umane e materiali disponibili e delle carenze organizzative delle strutture nelle quali si opera.

Questa norma completa il disposto all'articolo 6 della legge 24/2017 (legge Gelli), che aveva riformato l'articolo 590 del Codice penale e prevedeva quanto segue: "Il professionista sanitario che prova di aver aderito alle buone pratiche cliniche non è più responsabile penalmente".

Ricorderemo che, in caso di lesioni gravi o morte, la magistratura è tenuta a intervenire, ai sensi del disposto degli articoli 589 e 590 del Codice penale. A questo punto, il pubblico ministero svolgerà le indagini preliminari, per raccogliere le prove del caso e decidere se chiedere l'archiviazione o esercitare l'azione penale, portando il caso davanti a un giudice.

Partiranno quindi due procedimenti: quello penale e quello civile (conseguente alle richieste di risarcimento eventualmente avanzate dagli aventi diritto). Avendo il primo processo precedenza temporale sul secondo, il possibile reo si troverà sospeso, anche per lungo tempo, tra le due decisioni, con tutte le conseguenze che ciò può implicare.

Dal momento che la pratica medica, per sua caratteristica, può comportare che il paziente subisca lesioni gravi o addirittura perisca, la necessità per i magistrati di osservare il disposto del Codice penale ha sempre determinato conseguenze assai gravi per i medici, dal punto di vista psicologico da un lato e per quanto attiene alla salvaguardia del prestigio personale, dall'altro. È giusto non dimenticare che questi professionisti svolgono un servizio di grandissima rilevanza e delicatezza, giacché contribuiscono a salvaguardare il dritto alla salute garantito ai cittadini dalla Costituzione del nostro paese. Si è quindi cercato di proteggere questa categoria professionale dall'incorrere così spesso in tali difficili circostanze.

LE CONSEGUENZE SUL PIANO ASSICURATIVO

Ricorderemo che l'ultima riforma delle professioni, il dpr 137/2012, ha istituito l'obbligo di stipulare una polizza di responsabilità civile per tutte le categorie di professionisti. Da tale vincolo furono temporaneamente esclusi gli avvocati e i professionisti sanitari, dal momento che per tali categorie sarebbero intervenute rispettivamente la nuova disciplina dell'ordinamento della professione forense (legge 31 dicembre 2012, n. 247) e la Legge Gelli (24/2017), che recavano entrambe il medesimo obbligo. Dato il tempo trascorso, quindi, una riforma che riguardasse le più importanti categorie professionali operanti in Italia era quanto mai attesa, soprattutto alla luce della rivoluzione determinata dall'uso delle nuove tecnologie e dall'avvento dell'AI.

Quando parliamo di professionisti, ci riferiamo a quasi due milioni di soggetti, che producono un reddito complessivo stimato in oltre 40 miliardi di euro e contribuiscono grandemente all'economia del paese.

Si tratta di un numero cospicuo di persone che ricoprono ruoli assai importanti, anche sul piano sociale. Basti pensare, ad esempio, ai professionisti sanitari, che si occupano di un settore nevralgico come quello della salute pubblica.

L'assicurazione obbligatoria per la responsabilità professionale è nata, da un lato, con lo scopo di proteggere i redditi dei professionisti, minacciati dall'eventualità di dover pagare richieste di risarcimento anche molto consistenti, avanzate dai clienti. Dall'altro, con l'obiettivo di proteggere il diritto di ciascun cliente a essere risarcito per eventuali perdite subite in conseguenza di un errore involontariamente commesso dagli stessi professionisti, nel prestare il loro servizio.

Questa funzione di protezione dei diritti del cittadino-cliente e del professionista si è manifestata di volta in volta in tutte le norme che sono state varate sulle varie categorie professionali e, a questo riguardo, le ultime leggi delega non costituiscono un'eccezione.

EFFETTI POSITIVI

La novità è invece rappresentata dalla necessità di allineare gli ordinamenti professionali italiani agli standard europei, armonizzando le regole e semplificando il sistema, in risposta alle trasformazioni tecnologiche, alla digitalizzazione e alla rivoluzione rappresentata dall'uso dell'AI.

E tutto questo non potrà che avere effetti positivi sulla qualità e sulla gestione di questa categoria di rischi, che si caratterizza per un'estrema complessità, sia sul piano giuridico sia su quello squisitamente assicurativo.

Un report pubblicato da **Finaccord** nell'ormai lontano 2015 rivelava come in Europa l'Italia fosse quasi al livello di Germania e Francia (paesi che avevano un numero di abitanti alquanto superiore al nostro) per numero di professionisti e imprese professionali. Conseguentemente, l'importo dei premi di assicurazione relativi alla responsabilità contrattuale (e professionale in genere) veniva stimato in oltre 750 milioni di sterline, il che faceva del nostro paese un mercato di riferimento in Europa, allocando l'Italia al quarto posto nel ranking complessivo, dopo Regno Unito, Germania e Francia.

UN MIGLIORAMENTO NELLA GESTIONE DEL RISCHIO

Come sappiamo, l'assicurazione della responsabilità che fa capo a questi soggetti è quanto mai complessa, perché alla molteplicità delle professioni corrisponde una grande diversità di profili giuridici: ogni attività comporta obblighi diversi e un diverso profilo assicurativo; ogni attività determina un particolare tipo di esposizione, che necessita di condizioni di polizza che la rispecchino e si riflettono in premi di polizza anche molto differenti.

La presenza di regole sempre più chiare e puntuali e di ordini professionali in grado di vigilare e gestire più attentamente l'operato dei loro iscritti, come previsto dalla nuova legislazione, dovrebbe quindi comportare un miglioramento nella gestione del rischio che fa capo a ciascuna specialità. Per quanto attiene alle professioni mediche, poi, il completamento di quanto disposto dalla legge Gelli, sotto il profilo penale, dovrebbe dare un po' più di respiro a una categoria che continua a essere tartassata, per lo più immeritatamente, dalle richieste di pazienti adirati o insoddisfatti.

IN ATTESA DEI DECRETI ATTUATIVI

Sul piano civilistico, e quindi dal punto di vista assicurativo, le conseguenze dovrebbero quindi essere positive, perché la magistratura civile ha sempre dovuto attendere lo sviluppo del processo penale a carico del professionista, per poi tenerne conto. Inoltre, non dovendosi attendere la fine della causa penale per giungere allo svolgimento di quella civile, l'intero meccanismo dovrebbe risultare più rapido ed efficiente. Tutto ciò ha fatto sì che questa riforma fosse salutata con entusiasmo da parte delle varie associazioni di categoria. Da segnalare, infine, la possibilità di ricoprire cariche di amministratore o presidente di società da parte degli appartenenti alla categoria degli avvocati, il che dovrebbe avere conseguenze positive nel miglioramento della gestione del rischio delle polizze D&O contratte dalle società medesime.

Potremo comunque misurare appieno i vantaggi della riforma non appena verranno pubblicati i relativi decreti attuativi, purché i tempi della loro promulgazione rispettino la tabella prevista.

Non dimentichiamo che per la Legge Gelli si è dovuto attendere molti anni.

Cinzia Altomare

La prima parte dell'articolo è stata pubblicata su Insurance Daily di lunedì 10 novembre.

INSURANCE Daily

N. 2884 MARTEDÌ 11 NOVEMBRE 2025

RISK MANAGEMENT

Cloud e AI, opportunità e rischi di una trasformazione inevitabile

Secondo il nuovo Cyber Resilience Report di Qbe, l'adozione dell'intelligenza artificiale e le potenzialità delle piattaforme cloud stanno trasformando la gestione dei rischi, ma la velocità e la portata di questo cambiamento offrono terreno fertile per ransomware, frodi e interruzioni causate da terze parti

Il passaggio a piattaforme cloud pubbliche, private e ibride sta trasformando i modelli operativi delle aziende, migliorando l'automazione e favorendo l'integrazione dell'intelligenza artificiale. Ma a un'accresciuta efficienza corrisponde anche una crescita esponenziale dei rischi informatici. Il *Cyber Resilience Report 2025* di **Qbe Insurance Group**, realizzato in collaborazione con **Control Risks**, evidenzia come l'aumento globale della dipendenza dalle infrastrutture cloud stia aprendo nuove vulnerabilità, quali controlli deboli sull'identità digitale, errori di configurazione e dati sensibili non protetti adeguatamente.

Stando al documento, l'ampia diffusione dei servizi cloud rende urgente un approccio sistemico alla sicurezza. Entro il 2034, il mercato globale del cloud supererà i 5.000 miliardi di dollari, rispetto ai 912 miliardi previsti per il 2025. Con lo spostamento online di infrastrutture e dati, anche gli alert ad alta gravità sono cresciuti del 235% nel solo 2024, segnalando una pressione crescente da parte di hacker sempre più organizzati.

Le nuove varianti dei ransomware

Secondo il report, quasi la metà dei dati aziendali archiviati nel cloud è classificata come sensibile, un patrimonio appetibile per chi diffonde ransomware. Le nuove varianti di questi malware sono progettate per infiltrarsi negli strumenti di collaborazione e muoversi lateralmente tra sistemi on-premises e cloud, esfiltrando o cifrando dati lungo il percorso.

Il phishing resta il principale vettore d'attacco: un terzo delle intrusioni avvenute tra 2023 e 2024 è partito da email ingannevoli, spesso veicolate attraverso piattaforme note e

legittime. Tecniche come gli attacchi *adversary-in-the-middle* consentono di rubare credenziali autentiche, rendendo più difficile l'individuazione.

La crescente interconnessione tra fornitori e clienti, inoltre, amplifica l'impatto delle violazioni: la compromissione di un singolo provider può esporre centinaia di aziende. E con metà dei dati mondiali destinata a risiedere nel cloud entro il 2025, i fornitori di servizi digitali diventano bersagli di primaria importanza.

GenAI: alleato o minaccia?

L'intelligenza artificiale generativa sta ridefinendo tanto la difesa quanto l'attacco nel cyberspazio. Il suo impiego, sempre più diffuso nelle imprese di tutto il mondo, promette efficienza e produttività ma apre scenari inediti di rischio. Tra

il 2024 e il 2025 l'adozione di strumenti come ChatGpt è cresciuta del 33%, e attualmente il 78% delle aziende impiega l'AI in almeno una funzione aziendale.

Parallelamente, la stessa tecnologia è divenuta un'arma nelle mani dei criminali. I deepfake, per esempio, sono spesso utilizzati per impersonare dirigenti o figure pubbliche e indurre trasferimenti di denaro fraudolenti: nel 2024 sono stati impiegati in circa il 10% degli attacchi riusciti, con perdite finanziarie tra 250mila e oltre 20 milioni di dollari.

Anche gli attacchi sponsorizzati da Stati sfruttano la GenAI per generare codici malevoli, condurre attività di ricognizione o manipolare i modelli linguistici aziendali, compromettendo l'integrità dei sistemi. L'intelligenza artificiale, insomma, si conferma un catalizzatore di innovazione ma anche un acceleratore del rischio.

Il costo della compromissione

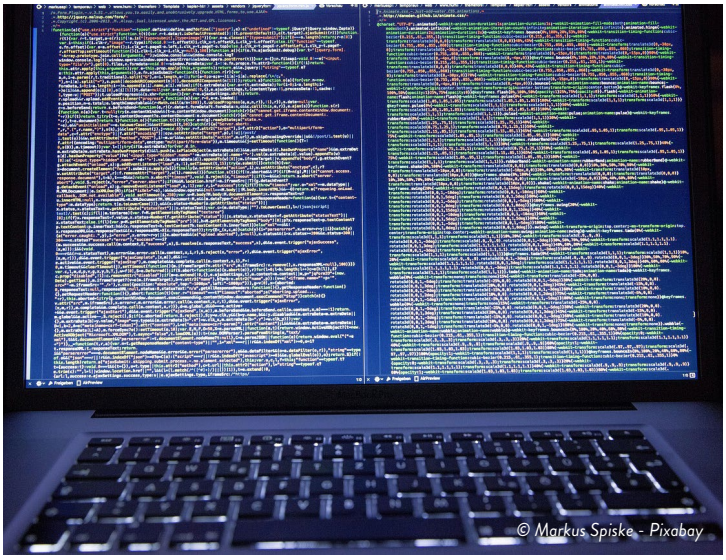
Gli effetti economici degli attacchi ransomware, prosegue il rapporto, si estendono ormai ben oltre la singola vittima: le perdite dirette si accompagnano infatti a danni reputazionali e azioni legali, coinvolgendo fornitori e clienti.

Negli ultimi anni la crescente dipendenza dai servizi cloud e SaaS (software as a service) ha coinciso con un aumento costante degli incidenti. Il caso più emblematico resta l'aggiornamento difettoso del Falcon Sensor di **CrowdStrike**, nel 2024, che ha provocato un blackout globale su 8,5 milioni di dispositivi Windows. Pur non essendo un attacco informatico, l'incidente ha generato un'ondata di phishing che sfruttava la crisi per infettare nuovi sistemi. L'episodio ha mostrato come un singolo malfunzionamento possa avere effetti sistemici, richiamando precedenti come MOVEit o NotPetya, che causarono danni a catena su scala mondiale.

Oggi le organizzazioni devono fronteggiare una superficie d'attacco sempre più ampia, alimentata dall'uso di software di terze parti, hosting cloud e strumenti di AI. Le minacce non risparmiano alcun settore e impongono una riflessione strategica sulla resilienza digitale.

Costruire la cyber resilience

Per Qbe e Control Risks, l'unica risposta efficace è integrare fin dal principio la gestione del rischio informatico nei cicli di vita della tecnologia. Ciò significa adottare solide pratiche di *identity and access management*, audit regolari delle configurazioni e crittografia end-to-end dei dati sensibili. Altrettanto cruciali sono il monitoraggio continuo, la threat intelligence e piani di risposta agli incidenti in grado di contenere gli incidenti prima che degenerino. Anche la valutazione della sicurezza dei fornitori e la definizione di protocolli di gestione del rischio lungo la supply chain rappresentano dei tasselli fondamentali per garantire la continuità operativa. Le organizzazioni più mature sviluppano la propria cyber resilience attraverso step mirati: mappare i profili di rischio, definire il livello di esposizione accettabile, prioritizzare gli interventi, simulare crisi reali e aggiornare costantemente le difese.


© Markus Spiske - Pixabay

In un panorama digitale in continua evoluzione, conclude il report, la resilienza informatica non è più un vantaggio competitivo ma una condizione di sopravvivenza. Solo integrando prevenzione, preparazione e capacità di risposta nel proprio dna operativo, le imprese potranno mantenere la fiducia dei clienti e resistere alle sfide di un ecosistema sempre più interconnesso e vulnerabile.

Michele Starace

Per approfondire su www.insurancetrade.it:

- Cyber risk, il conto in Europa
- Cybersecurity, guai a sottovalutare i piani di risposta agli incidenti

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 11 novembre di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577