INSURANCE Daily

GIOVEDÌ 19 DICEMBRE 2019 N. 1667

PRIMO PIANO

2020-2021: su i premi e gli utili

Il prossimo anno e quello successivo saranno positivi per il settore assicurativo globale, secondo le previsioni del rapporto Sigma di Swiss Re. Il dato è notevole soprattutto perché in controtendenza con il quadro economico generale, per cui si prevede un ulteriore indebolimento della crescita nel prossimo biennio.

Secondo il report, la raccolta premi nel settore danni nel biennio 2020-21 dovrebbe crescere al ritmo del 2,7% annuo, in lieve rallentamento rispetto alla stima 2019 del +2,9% e alla media del quinquennio precedente (2014-2018, +3,1%). Il Roe medio del comparto sarà pari al 7,4%, con un'accelerazione rispetto all'anno in corso e al periodo 2014-2018, quando il dato si fermava al 7,2%. Bene anche la raccolta vita, con una crescita media del 3,1% nel prossimo biennio, in progressione sia rispetto alle stime per il 2019 (+2,3%) sia rispetto alla media 2014-2018 (+2,7%). Il Roe andrà oltre il 10% per quest'anno (9,4% medio nel quinquennio precedente), mentre per il prossimo biennio Swiss Re non ha elaborato la proiezione. A trainare la crescita saranno soprattutto India e Cina, anche se in leggera flessione rispetto al passato.

Per leggere tutta la notizia, clicca qui.

Fabrizio Aurilia

RICERCHE

Imprese italiane più attente al rischio

Una survey condotta da Deloitte mostra come, nelle aziende dotate di un sistema di gestione del rischio, la cultura in questo ambito sia molto cresciuta e includa in maniera concreta anche il board. Le minacce in ambito operativo e normativo sono le più temute

Sono i rischi operativi e quelli legati al rispetto delle normative che nell'immediato preoccupano maggiormente le imprese italiane ed europee, mentre guardando ai prossimi tre anni cresce l'attenzione per le minacce in relazione alle nuove tecnologie, che possono riservare incognite nell'applicazione, e ai rischi collegati alla sostenibilità. Sono questi alcuni dei temi emersi da *Emerging risks across industries*, ricerca di **Deloitte** presentata recentemente a Milano, che ha raccolto il punto di vista in tema di rischi emergenti di un campione di chief risk officer italiani ed europei appartenenti a imprese di tutti i settori economici. La survey di Deloitte, svolta presso imprese che hanno già una funzione o un dipartimento di risk management, offre una visione molto pragmatica delle minacce più temute dai risk manager, rischi concreti e derivati dall'attività quotidiana della propria impresa più che dagli scenari globali, che pure appaiono sempre in stretta relazione con gli obiettivi dell'azienda.

Nell'insieme si evidenzia il divario tra il livello di adozione di una politica del rischio nelle società finanziarie rispetto a quelle di altri settori, determinato dalla necessità, emersa con la crisi iniziata nel 2008, di adeguarsi ai requisiti normativi e di dotarsi di strutture di gestione del rischio: in particolare, banche e assicurazioni hanno sviluppato i modelli più consolidati soprattutto per quanto riguarda i rischi finanziari, mentre appaiono più in ritardo in ambito di rischi non finanziari.

IL RUOLO CHIAVE DEL BOARD

Per quanto riguarda la diffusione della cultura del rischio nella propria organizzazione, metà del campione intervistato (ma il 71% delle compagnie assicurative) ritiene che sia adeguatamente condivisa, e solo il 12% pensa sia ancora poco sviluppata. Importante nella formazione e nella pervasività della cultura del rischio è il coinvolgimento attivo del top management: per il 65% delle società intervistate (ma il 100% degli istituti bancari) le competenze dei board aziendali in tema di rischio sono soddisfacenti, solo il 7% le definisce limitate. *(continua a pag. 2)*

INSURANCE Daily

● GIOVEDÌ 19 DICEMBRE 2019 N. 1667

(continua da pag. 1)

In genere, oltre al risk manager, anche altre funzioni o dipartimenti sono coinvolti nel processo di gestione del rischio, tra cui svolgono un ruolo significativo il consiglio di amministrazione e il comitato dei rischi (93%), le direzioni (79%), il settore finanza (71%), l'internal audit (71%) e la compliance (64%), ma anche l'It (50%), l'operation (43%) e l'ufficio legale (29%). Dai dati emersi nella survey, il successo dei piani di *enterprise risk management* è facilitato dal coinvolgimento dei responsabili della gestione del rischio negli organi consiliari di carattere strategico, inoltre nella maggior parte delle imprese il chief risk officer riporta direttamente al ceo.

A questo proposito, l'85% degli intervistati considera completata l'implementazione di processi e procedure dedicate al risk management, il 71% afferma di aver realizzato una risk strategy che collega gli obiettivi di business e di redditività al profilo di rischio dell'azienda, e il 79% afferma di aver definito il proprio risk appetite, determinando la propensione e i relativi limiti di rischio. In tema di metodologie di misurazione dei rischi, prevalgono i modelli di misurazione delle perdite inattese in ottica probabilistica (Value at Risk, VaR), affiancati da tecniche di stima dei costi totali a rischio, includendo i costi delle coperture assicurative, i costi riferiti agli eventi da perdita operativa e i costi di ripristino dell'operatività aziendale.

© Gina Sanders - Fotolia

© Choreograph - iStock

I RISCHI PIÙ TEMUTI SONO QUELLI QUOTIDIANI

La maggiore attenzione dei chief risk officer si concentra sui rischi operativi e regolamentari, percepiti come i più concreti e diffusi: si tratta di minacce eterogenee che spaziano in ambiti che vanno dalle frodi interne ed esterne ai rischi legali, fino all'efficienza del sistema dei controlli interni e alle risorse umane. I rischi finanziari, tra cui in particolare il peggioramento del merito creditizio e il rischio di default sovrano (entrambi al 79%), sono molto sentiti dalle aziende, anche se non ci si attende un loro peggioramento per i prossimi pochi anni. A proposito di futuro, una quota consistente di intervistati (79%) percepisce già oggi come una minaccia da monitorare l'evoluzione dei processi di trasformazione digitale in atto: la grande maggioranza delle aziende intervistate pensa sarà necessario focalizzarsi sui rischi legati al cyber (79%), in particolare quelli legati alla non corretta implementazione delle tecnologie di intelligenza artificiale e blockchain nei sistemi aziendali, e quelli reputazionali correlati ai flussi informativi (soprattutto i social media, 44%). Altro tema sensibile è la sostenibilità in ambito ambientale, sociale ed economico, dove si evidenziano timori di maggiori rischi di eventi naturali estremi e preoccupazione per la mancanza di competenze.

PRIMO RISCHIO STRATEGICO SONO I PIANI AZIENDALI

Guardando ai rischi strategici, il rischio più temuto è l'errata o la mancata attuazione dei piani aziendali (82% degli intervistati) mentre nei prossimi tre anni avranno maggiore attenzione i rischi connessi all'innovazione di prodotto (41%) e alla capacità delle imprese di reagire ai cambiamenti di mercato (35%). Sempre riguardo ai rischi strategici, **Alessandro Di Lorenzo**, partner di Deloitte, pone il focus sui cambiamenti normativi a livello nazionale e internazionale, che "rimangono un fattore d'attenzione costante nel tempo. Per il 93% degli intervistati l'introduzione di leggi a tutela dei consumatori rimane un punto di attenzione per via degli impatti organizzativi, tecnologici e finanziari la cui implementazione comporta per le aziende"; nel medio termine invece il 50% degli intervistati si aspetta un maggiore impatto legato alle politiche protezionistiche, soprattutto in questa fase storica caratterizzata da tendenze di carattere isolazionista quali la Brexit.

Maria Moro

INSURANCE Daily

● GIOVEDÌ 19 DICEMBRE 2019 N. 1667

NORMATIVA

Gli ultimi provvedimenti normativi in materia di cyber security

Con lo specifico decreto emanato a settembre, il governo integra le disposizioni nazionali con le indicazioni contenute nel Regolamento Ue approvato in primavera. Punti cardine gli investimenti stranieri e la supervisione strategica sulle reti

La sicurezza informatica è sempre più di attualità, anche a seguito dell'escalation di attacchi messi a segno dai criminali informatici che si sono mostrati in grado di paralizzare città intere, senza tralasciare naturalmente le infrastrutture critiche, come possono essere quelle relative alle telecomunicazioni e ai servizi sanitari. L'attenzione verso il tema, ha reso di recente la cyber security oggetto dell'attenzione del nostro legislatore. Il Governo italiano, infatti, nel mese di settembre 2019 ha approvato il cosiddetto *Decreto Cyber Security* (dl n. 105/2019 - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica, convertito con modificazioni dalla legge n. 133/2019), che si colloca nel più ampio contesto della lotta ai crimini cibernetici giocata a livello sovranazionale, posto che il fenomeno, come è ben chiaro tra l'altro al legislatore comunitario, può essere arginato e mitigato solo mettendo a fattor comune gli sforzi collettivi.

Ma andiamo con ordine: senza pretese di completezza e tralasciando gli aspetti più squisitamente tecnici, che sono appannaggio degli esperti informatici, cerchiamo di ripercorrere la genesi del decreto, iniziando con il chiarire, prendendo spunto dal comunicato stampa del Governo del 19 settembre, quali sono le sue finalità. Esso "mira ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure idonee a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi consentendo, al contempo, la più estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione", prevedendo il coinvolgimento del Comitato interministeriale per la sicurezza della Repubblica (**Cisr**) nella fase attuativa.

© jamesteohart - iStock

Controllo di investimenti e poteri sul 5G

Nel contesto sopra descritto, alla luce della rilevanza che alcuni settori, come quello delle telecomunicazioni, hanno per il corretto e ordinato funzionamento delle transazioni economiche, tra le quali anche quelle legate al mondo assicurativo (sempre più tecnologico e iper connesso), di particolare interesse sono gli aspetti connessi all'integrazione e all'adeguamento della normativa interna in tema di poteri speciali del Governo sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni (il cosiddetto *Golden power*).

Il decreto, infatti, coordina e integra il quadro normativo interno (dl n. 21 del 2012) con il Regolamento (UE) 2019/452 del marzo 2019, che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione, con importanti conseguenze, tra l'altro, per l'esercizio di poteri speciali in relazione alle reti, ai sistemi informativi e ai servizi strategici di comunicazione a banda larga basati sulla tecnologia 5G.

Da ultimo, tra le novità contenute nel dl n. 105 del 2019 ci sono anche quelle che prevedono, sempre come sottolineato dal Governo nel comunicato stampa del 19 settembre, modalità di acquisto più sicure per i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica che intendano procedere all'affidamento di forniture di beni e servizi Ict destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti.

Concludendo, nel sottolineare che l'impianto normativo sopra sinteticamente descritto necessita di ulteriori passaggi normativi per trovare piena attuazione, cogliamo l'occasione per inviare ai lettori di *Insurance Daily* i nostri migliori auguri in vista delle imminenti festività natalizie.

Andrea Maura
www.legalgrounds.eu a member of Aliant, an International law firm

INSURANCE Daily

● GIOVEDÌ 19 DICEMBRE 2019 N. 1667

RICERCHE

Crif, crescono le frodi creditizie

Nel primo semestre del 2019 si sono contati circa 16.700 episodi, in rialzo del 36,7% su base annua il danno complessivo è stimato in 77 milioni di euro

Cresce il fenomeno delle frodi creditizie mediante il furto di identità. Nei primi sei mesi del 2019, secondo l'ultimo osservatorio di **Crif**, si sono contati circa 16.700 casi di sottrazione illecita di dati che poi sarebbero stati utilizzati per accedere a un credito e acquisire beni e servizi senza poi rimborsare il prestito. Il dato risulta in crescita del 36,7% rispetto ai primi sei mesi del 2018. E risulta ancora più preoccupante se si considera che i picchi massimi di frodi si registrano storicamente ad agosto e nel periodo natalizio, esclusi dal contesto d'indagine. Il danno economico complessivo è stimato in circa 77 milioni di euro, per una media di 4.662 euro sottratti illecitamente in ogni singolo episodio.

"In Italia il furto di identità è un fenomeno sempre più diffuso, che coinvolge persone e aziende", ha commentato **Beatrice Rubini**, direttrice della linea *Mister Credit* di Crif. "La vulnerabilità alle frodi creditizie perpetrate attraverso un furto di identità – ha aggiunto – è accresciuta anche dal fatto che sul web spesso vengono pubblicati dati anagrafici e identificativi, come il codice fiscale, o i recapiti personali, come l'email o il numero di cellulare".

La maggior parte delle vittime risulta essere uomini (64,9%) e, a differenza di quello che si potrebbe pensare, piuttosto giovani: la fascia di età nella quale si rileva il maggior incremento dei casi è quella dei 18-30enni (+23,2%) e dei 31-40enni (+6,4%), mentre diminuiscono i 51-60enni (-11%) e gli over 60 (-15,7%). A livello geografico, invece, le regioni che registrano una maggior incidenza sono Lombardia, Campania, Lazio e Sicilia. La crescita più rilevante si è registrata in Molise (+66,7%), che tuttavia viaggia su livelli ancora modesti, seguita da Liguria (+13,9%), Lombardia (+11,2%) e Sicilia (+9,8%).

L'accesso fraudolento a finanziamenti per l'acquisto di elettrodomestici risulta la modalità più diffusa (30,5%), di fronte ad auto e moto (13,7%) e articoli di arredamento (7,9%). In deciso aumento, invece, i casi relativi a abbigliamento e prodotti di lusso, che crescono del 55,3% e arrivano a ricoprire una quota del 6,9%, a prodotti di elettronica, informatica e telefonia (+29,6%) e trattamenti estetici e medici (+8,8%).

Giacomo Corvi

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