L'IMPATTO PER IL SETTORE ASSICURATIVO

di CINZIA ALTOMARE

SOTTO LA SPINTA DEL NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY, IL MERCATO DELLE COPERTURE CONNESSE AL RISCHIO INFORMATICO POTREBBE ATTESTARSI A OLTRE 700 MILIONI DI EURO IN EUROPA. MA LA COMPLESSITÀ DEL FENOMENO CONTINUA A FRENARE COMPAGNIE E RIASSICURATORI

Dal punto di vista assicurativo, il rischio cyber costituisce una sfida non indifferente.
Esso rappresenta certamente una grande opportunità, data l'ampiezza dello spettro di attività coinvolte e l'enorme impatto di questo fenomeno su ogni soggetto giuridico operante nella civiltà digitale in cui viviamo.
La nuova normativa introdotta dal Regolamento europeo 679 del 2016, infatti, impone a tutte le aziende e agli individui che gestiscano, conservino o trattino a qualunque titolo dati personali, di adottare un'articolata politica di risk management, per garantire il possesso dei requisiti di sicurezza previsti per la salvaguardia dei dati personali amministrati. Ciò presuppone una crescente sensibilità degli individui per la sorte dei propri dati e implica uno sviluppo dei prodotti assicurativi inerenti la gestione del rischio cyber, che lo pongono sotto una luce assai accattivante per tutti gli operatori del settore, specialmente nell'ottica di un mercato ormai asfittico che negli ultimi anni ha assistito a una costante flessione dei premi incassati su quasi tutte le linee di business.
In questo settore, invece, parliamo di un potenziale globale di premi che è stato stimato in circa 2 miliardi di dollari. Di questo ammontare, solo 150 milioni atterrebbero alla parte europea, ma si prevede che il nuovo regolamento fornisca una grande spinta allo sviluppo di questo mercato che, secondo uno studio di **Guy Carpenter**, potrebbe rapidamente attestarsi oltre i 700 milioni di euro.
D'altro canto, però, la complessità del fenomeno, l'entità potenzialmente devastante delle sue conseguenze e la penuria di dati storici scientificamente attendibili, costituiscono un grosso ostacolo per gli attuari ed i sottoscrittori che cercassero di elaborare modelli e parametri per valutarlo e quotarlo adeguatamente. Da qui la riluttanza di molti riassicuratori, e conseguentemente delle loro cedenti, ad offrire copertura per questo tipo di rischi.

I COSTI DEGLI ATTACCHI INFORMATICI

Violazioni e compromissioni dei dati possono causare accumulazioni di rischio da interdipendenza, attraverso la catena distributiva globale, danneggiando l'intero sistema produttivo di un'azienda e influendo direttamente sulla sua capacità di condurre l'attività svolta, con serie conseguenze per la sua reputazione e costi ingenti per recuperare i dati perduti e per resistere alle eventuali azioni di risarcimento intraprese da terzi.
I soli costi causati dagli attacchi informatici, che rappresentano più o meno il 40% delle compromissioni totali,

sono attualmente valutati in circa 500 miliardi all'anno. In Italia, si ritiene che si attestino appena al di sotto del miliardo di euro, ma i danni alla reputazione e da perdita di profitto sono valutati da **McAfee** nell'ordine di 8,5 miliardi di euro, pari a circa lo 0,6% del Pil, mentre le perdite causate da interruzioni operative dei sistemi supererebbero addirittura i 14 miliardi di euro.
È facile dunque intuire come la portata catastrofale di questo tipo di eventi dannosi possa scoraggiare molti assicuratori, mantenendo ancora bassa l'offerta di prodotti specifici.
D'altra parte, la mancanza di un mercato ampio e disponibile, unitamente alla difficoltà a valutare una tipologia di rischio tanto esteso e multiforme e di orientarsi sulla scelta più adatta, anche da parte dei risk manager, non può che comportare il mantenimento di costi relativamente alti per questo tipo di coperture.

COPERTURE CYBER

Si sono però sviluppati prodotti dedicati, a partire dal mercato americano, in grado di coprire i danni causati da perdita o danneggiamento di dati e direttamente riconducibili a cyber crime, computer virus, guasti alle apparecchiature, errori umani ecc.
Queste polizze coprono i costi necessari per il recupero dei dati sottratti o perduti e per il ripristino e la decontaminazione dei sistemi danneggiati ma anche i danni consequenziali e la perdita di profitto o l'aumento dei costi di esercizio causati dall'interruzione dell'attività esercitata e il *contingency risk*, ovvero il rischio di interdipendenza nell'ambito della catena produttiva e distributiva.
Sono comprese le spese sostenute per le ricerche forensi, necessarie a determinare le cause della violazione e identificarne le vittime per informarle dell'accaduto, nonché le spese legali, i costi per il monitoraggio del credito (nei casi di furto di identità) e le spese per le pubbliche relazioni, il rilancio del brand, ecc.
Infine, viene assicurata la responsabilità civile verso terzi, derivante dalla violazione delle vigenti norme sulla privacy e, se possibile, anche le multe e le ammende eventualmente inflitte dai Garanti.
Queste *cyber policies* rappresentano un preciso e sofisticato prodotto, offerto da alcune grandi compagnie di assicurazione di vocazione globale, frutto di una lunga ricerca e di una specifica pattuizione con le compagnie di riassicurazione che sostengono i loro trattati.
Tuttavia, frammenti più o meno ampi delle coperture ora riconosciute come cyber si possono annidare nelle polizze tradizionali ed è possibile che, in assenza di specifiche esclusioni o limitazioni, siano *inconsciamente* assicurati rischi difficilmente controllabili, senza averne potuto incassare il corrispettivo premio e, cosa più grave, in mancanza della necessaria copertura riassicurativa.

LIMITAZIONI E CONTENIMENTO DI POSSIBILI DANNI

Occorre dunque controllare attentamente la portata dei trattati di riassicurazione, per capire fino a che punto e

LE INSIDIE NELLE CONDIZIONI DI POLIZZA

La civiltà digitale ha mutato radicalmente il mondo in cui viviamo e sono numerosissimi gli ambiti nei quali questi cambiamenti possono generare oggi effetti che solo qualche anno fa erano semplicemente impensabili.
Quale esperto di coperture per il *Ritiro di prodotti difettosi* poteva immaginare che un hacker si sarebbe inserito nel sistema di guida di una moderna autovettura e ne avrebbe messo a repentaglio la sicurezza, penetrando nel computer di bordo?
E chi avrebbe potuto prevedere le massicce estorsioni perpetrate oggi ai danni di società commerciali, banche ed enti pubblici, attraverso il furto di migliaia di dati personali dei loro clienti o le interruzioni di attività produttive e di servizi causate dagli spettacolari attacchi informatici assurti recentemente agli onori delle cronache in tutto il mondo?
Chi si aspettava che ogni professionista sarebbe stato oggi responsabile del trattamento delle informazioni personali dei suoi clienti, fino a essere tenuto a intraprendere una complessa attività di risk management per assicurarne su base permanente la riservatezza e l'integrità, garantendo l'inattaccabilità dei sistemi di gestione adottati?
I requisiti di sicurezza necessari per attività, prodotti e servizi di qualunque tipo vanno oggi al di là di quanto si potesse prevedere al tempo, ancorchè recente, in cui le condizioni di tante polizze sono state studiate e pubblicate ed è ora imperativo procedere con il loro aggiornamento, per accertarsi che questi wording siano in grado di affrontare le temibili sfide imposte dal contesto sempre più virtuale in cui operiamo.

in quali termini il rischio cyber sia escluso e controllare accuratamente i *wording* di polizza, per decidere quale e quanta parte di questo rischio sia possibile sostenere, intervenendo opportunamente sulle clausole di restrizione e sugli eventuali limiti ivi previsti.
Le polizze *Tutti i rischi dell'elettronica*, ad esempio, sono state pensate in un tempo in cui le problematiche derivanti dall'avvento della civiltà digitale non erano ancora ipotizzabili. La portata di certe estensioni, quindi, potrebbe andare oggi ben al di là del dovuto, ovvero oltre i limiti previsti dai più recenti trattati riassicurativi che governano i rami tecnologici.
Allo stesso modo, i testi delle polizze che assicurano la responsabilità civile dei dirigenti e amministratori di società (*D&O*) e i relativi premi sono stati pensati senza tener conto degli obblighi cui oggi devono attenersi questi soggetti, alla luce di normative sempre più stringenti in tema di trattamento dei dati, nè degli adempimenti cui essi devono far fronte, sotto pena di incappare in sanzioni pecuniarie assai cospicue.
Per chi non volesse fronteggiare sinistri di portata catastrofale in quest'ambito, quindi, sarebbe consigliabile intervenire con opportune limitazioni, per contenere l'ammontare del danno.