IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

Indagine sulle polizze a copertura del *cyber risk*

ottobre 2023

Indagine sulle polizze a copertura del *cyber risk*

Ottobre 2023

A cura di: Annamaria Damiani, Annalisa Bellizzi, Maria Cristina Giustiniani e Rita Greco.

Grafica e stampa a cura della Divisione Editoria e stampa della Banca d'Italia

Indice

1 Introduzione ed *executive summary*

L'IVASS ha svolto un'indagine per approfondire le polizze assicurative contro il rischio *cyber,* c.d. *"polizze cyber",* offerte dalle compagnie di assicurazione a protezione dei singoli individui/famiglie (clienti *retail*) e delle Piccole e Medie Imprese (PMI).

L'indagine trae spunto dalla crescente esposizione al rischio *cyber* riconducibile a più fattori, tra cui: diffusione di nuove tecnologie e crescente interconnessione digitale tra cose, persone, processi e dati; utilizzo della rete *Internet* a scopi relazionali o per acquisti e vendite *online* o per usufruire di servizi *Home banking;* aumento di attacchi informatici anche a seguito di tensioni geopolitiche legate al conflitto in Ucraina. Fattori che rendono gli utenti – famiglie, imprese, enti pubblici – sempre più vulnerabili sotto il profilo della sicurezza informatica.

L'indagine si è basata sull'analisi dei contratti e non entra nella valutazione sulla bontà o convenienza delle polizze e prescinde dal successo commerciale delle medesime e dal livello della raccolta premi a esse associato. Il riferimento alle polizze o iniziative commerciali menzionate nel presente *Report* non implica un'approvazione da parte dell'Istituto.

Il c*yber risk* è la combinazione della probabilità che si verifichino incidenti *cyber* e del loro impatto, intendendo per incidente *cyber* una violazione della sicurezza informatica di un sistema informativo o delle informazioni che il sistema elabora, memorizza o trasmette indipendentemente dal fatto che sia frutto di un'attività dolosa o meno[1].

In particolare, il c*yber risk* può derivare da incidenti che comportano la violazione, la perdita o la diffusione di dati sensibili, di natura personale ma anche finanziaria, truffe ed estorsioni, *cyberbullismo/cyberstalking*, furto di identità, lesioni alla reputazione o all'immagine, frodi su acquisti/vendite *e-commerce*, clonazione di carte di credito/debito, ecc.

Per le imprese, inoltre, il *cyber risk* può a sua volta generare rischi operativi e legali per interruzione dell'attività, violazioni della normativa, richieste estorsive (*ransomware)*, ecc.

Le principali evidenze dell'indagine suggeriscono la crescente diffusione di polizze cyber, destinate in particolare alle PMI e, in misura al momento minore, ad individui e famiglie.

---

1 Definizioni tratte dal **Cyber** *Lexicon FSB*: https://www.fsb.org/wp-content/uploads/P130423-3.pdf

Le coperture per le PMI sono piuttosto articolate, con garanzie che mirano a coprire le aziende sia dai danni dovuti ad attacchi informatici, sia dai danni causati a terzi per effetto degli attacchi, sia le spese legali. Diverse polizze offrono servizi accessori prima del verificarsi di un attacco informatico (identificazione di vulnerabilità, implementazione di presidi di protezione) e nella gestione *post*-evento (ristabilimento dell'operatività informatica, gestione danno reputazionale, ecc.).

Le coperture sono al momento per lo più standardizzate: a tendere potrebbero beneficiare di una maggiore flessibilità, in modo da calibrare e personalizzare maggiormente le garanzie in funzione della specifica operatività ed esigenza di copertura delle aziende.

Nell'ambito delle polizze destinate a individui e famiglie sono coperti i danni conseguenti a furto o clonazione di carte di credito/debito e carte prepagate, furto di identità digitale, acquisti fraudolenti *online*. Spesso viene fornita all'individuo e al suo nucleo familiare assistenza telefonica e digitale, attraverso un servizio di monitoraggio *online* che, in caso di sospetto attacco informatico sui *device* dell'assicurato, consente alla compagnia di contattare un tecnico specializzato per attivare tutte le procedure di analisi e ripristino. Sono presenti coperture anche nella forma della consulenza psicologica a seguito di eventi traumatici legati all'attacco *cyber* quali *cyberbullismo* e *cyberstalking* e dell'assistenza prestata in occasione di frodi nella prenotazione *online* di un viaggio all'estero.

Per entrambe le tipologie si tratta di un mercato destinato a crescere rapidamente, in parallelo al rafforzamento della cultura della sicurezza informatica presso aziende ed individui. L'assistenza di intermediari assicurativi professionisti, adeguatamente aggiornati sui rischi *cyber* e sugli aspetti molto tecnici di queste polizze, è cruciale per lo sviluppo ulteriore dell'offerta.

Dall'analisi è emerso inoltre che:

- alcune compagnie richiedono specifiche condizioni di operatività della persona o dell'azienda da assicurare, come prerequisiti o condizioni per rendere il rischio assicurabile e, di conseguenza, la copertura efficacemente operativa (cfr. par. 3.1.2 e par. 3.2.6);
- sono presenti a volte esclusioni e franchigie che ne riducono ampiezza e applicabilità, anche con margini di ambiguità. Ad esempio, la clausola di esclusione in caso di "guerra", presente nella maggior parte dei contratti esaminati, non esplicita se il termine "guerra" include anche la "guerra informatica", di particolare attualità, posto che gli attuali conflitti bellici si svolgono anche attraverso attacchi informatici (cfr., in particolare, par. 3.1.4 e par. 3.1.5);
- i glossari presentano margini di miglioramento per quanto concerne esaustività e ed univocità dei termini utilizzati (cfr. cap. 4).

2. Perimetro dell'analisi

L'analisi ha riguardato **50 polizze assicurative** per la protezione dal rischio *cyber* rivolte a individui, famiglie e PMI in commercio al 30 luglio 2023 di tipo:

- **stand alone**, ossia polizze espressamente disegnate per la copertura del rischio *cyber;*
- **modulari**, vale a dire polizze che offrono un'ampia gamma di garanzie per il cliente, a copertura della persona o dei beni, organizzate in moduli variamente combinabili e che hanno coperture *cyber* opzionabili, da acquistare in abbinamento ad altre garanzie.

Per effettuare l'analisi sono stati esaminati i set informativi dei contratti con copertura *cyber* presenti sui siti *web* delle compagnie.

Il campione analizzato è costituito in particolare da:

a) 26 polizze rivolte alle PMI:

- **14** *stand alone;*
- **12** modulari;

b) 24 polizze rivolte a individui e famiglie:

- **6** polizze *stand alone;*
- **18** polizze modulari.

3. Tipologie di *polizze cyber*

3.1 Polizze *cyber stand alone* rivolte alle PMI

Le polizze *cyber stand alone* rivolte alle PMI intendono tutelare il patrimonio dell'assicurato (imprenditore, persona giuridica, professionista o commerciante) dalle spese e dai danni direttamente subiti o provocati a terzi a seguito di un attacco al sistema informatico aziendale.

Tali polizze garantiscono la copertura delle spese e gli interventi necessari a ripristinare i dati e il sistema informatico, oltre ai risarcimenti richiesti all'assicurato da terzi a cui ha cagionato danni e alla tutela legale per controversie che scaturiscono dall'attacco informatico.

Le **14** polizze esaminate sono standardizzate, garantiscono coperture base a cui, spesso, è possibile aggiungere coperture facoltative, acquistabili separatamente e che offrono tutele crescenti a seconda del numero di coperture aggiunte alle garanzie di base.

La maggior parte delle polizze *stand alone* si rivolge a piccole e medie imprese che svolgono attività produttive (anche artigianali) nel settore manifatturiero o dei servizi (compresi i servizi IT), esercizi commerciali, studi professionali, strutture ricettive. Il premio di polizza spesso è rapportato al fatturato.

Sono solo 5 le polizze dedicate a imprese di grandi dimensioni.

3.1.1 Coperture (con esclusioni e limitazioni specifiche della garanzia)

Tutte le prestazioni hanno come presupposto il verificarsi di un attacco informatico al sistema informatico dell'impresa assicurata. Di seguito vengono illustrate più in dettaglio le principali garanzie, con evidenza anche delle relative esclusioni e limitazioni specifiche della singola garanzia.

3.1.1.1 Perdite pecuniarie

Le garanzie per le **perdite pecuniarie** risarciscono i danni diretti subiti dall'assicurato per il ripristino dei dati e dei sistemi informatici a seguito di un attacco informatico e i costi sostenuti per l'interruzione dell'attività conseguente ai medesimi eventi.

Tali garanzie di base spesso **sono integrate da coperture relative** a: costi di istruttoria per accertare le cause e le modalità dell'attacco; costi di notifica ai terzi interessati delle conseguenze di un attacco informatico, ad esempio la

compromissione dei sistemi seguita dalla diffusione di dati sensibili di terzi in custodia presso l'assicurato (data *breach*); costi sostenuti per ottenere nuovamente il rilascio di carte di credito/debito o prepagate (certificazioni PCI-DSS – *Payment Card Industry Data Security Standard*[2]); riconoscimento di una diaria giornaliera per ciascun giorno di inattività forzata; costi per la consulenza di esperti nella gestione degli attacchi informatici subiti.

Due compagnie assicurano anche i danni alle apparecchiature informatiche utilizzate dall'assicurato, otto compagnie assicurano i danni derivanti da estorsioni o tentativi di estorsione *cyber* prevedendo un indennizzo per le spese sostenute (ripristino dati, rimozione del *malware*), mentre risulta generalmente escluso il rimborso di spese sostenute per il pagamento di riscatti a seguito di estorsioni *cyber*.

➢ *Esclusioni e Limitazioni specifiche della garanzia:*

- assenza di *antivirus* o di aggiornamenti da oltre 6 mesi o esclusiva presenza di *antivirus freeware*;
- condotte dolose di prestatori di lavoro dell'assicurato;
- utilizzo di credenziali di *default* non modificate dall'assicurato;
- guasto di *network* esterni o interruzioni di alimentazione di utenze pubbliche;
- atti di guerra e terrorismo;
- danni da esplosione o emanazione di calore o di radiazioni;
- danni in occasione di attacchi con armi chimiche, biologiche, biochimiche o elettromagnetiche;
- danni dovuti a scarico/dispersione/infiltrazione/rilascio/fuga di sostanze pericolose, contaminanti o inquinanti;
- danni da furto, violazione, divulgazione di proprietà intellettuale;
- estorsioni di qualsiasi tipo (a eccezione di polizze che coprono anche tale evento);
- danni dovuti a *ransomware*, richieste di riscatto (a eccezione di polizze che coprono anche tale evento);
- i costi per ripristinare/recuperare/reinstallare o ricostituire i dati elettronici o *software* o riparare/noleggiare o sostituire un sistema informatico o uno dei suoi componenti.

---

2 La certificazione **PCI-DSS** (*Payment Card Industry Data Security Standard*) serve a garantire la tutela dei dati dei titolari di carta di credito e indica precisi requisiti per procedure, architettura di rete e software cui devono rispondere le aziende che gestiscono i numeri di carte di credito. Aderire allo standard PCI DSS è un requisito per tutti gli operatori che archiviano, elaborano o trasmettono dati di carte di credito.

3.1.1.2 Responsabilità Civile

Per quanto riguarda le coperture relative alla **responsabilità civile**, le garanzie offerte dalla generalità delle compagnie riguardano il risarcimento dei danni causati a terzi da un attacco informatico che ne provoca una violazione della *privacy* su dati riservati e della sicurezza informatica in generale.

Alcune compagnie **assicurano altre fattispecie**, quali la responsabilità civile da danni reputazionali del terzo interessato, violazioni della proprietà intellettuale, costi sostenuti per l'intervento di esperti finalizzato al contenimento del danno o alla sua eliminazione, costi sostenuti dai terzi per l'interruzione dell'attività, sanzioni/ammende per inadempimento di obblighi amministrativi e danni patrimoniali e di immagine per la mancata notifica a altri soggetti interessati dell'attacco informatico subito dall'assicurato, perdite patrimoniali cagionate a terzi da inadeguate soluzioni tecniche adottate dall'assicurato per l'utilizzo della Firma Elettronica Avanzata (FEA) nelle relazioni istituzionali, societarie o commerciali.

- *Esclusioni e Limitazioni specifiche della garanzia:*
  - danni derivanti da responsabilità contrattuali;
  - danni derivanti da pubblicazioni su siti *web* non controllati dall'assicurato;
  - responsabilità non derivanti dalla legge;
  - danni derivanti da mancata rimozione, a seguito di denuncia o richiesta di risarcimento da parte di terzi, di contenuto, da siti *web* che siano sotto il controllo dell'assicurato.

3.1.1.3 Tutela Legale

Con riferimento alle coperture in materia di **tutela legale**, la compagnia di assicurazione riconosce le spese legali in relazione a vertenze che coinvolgono l'assicurato per la difesa dei suoi interessi.

Le coperture offerte riguardano principalmente la tutela legale per i danni extracontrattuali subìti per fatti illeciti di terzi e i danni causati a terzi per delitti dolosi, colposi o per contravvenzioni connessi all'utilizzo del *web* e dei *social media* nel corso dell'attività d'impresa o professionale.

In molti casi, alla tutela legale nelle sedi pertinenti, si accompagna anche la consulenza legale telefonica da parte di esperti in materia legale.

In alcuni casi, sono incluse anche le garanzie relative a: controversie legali con fornitori di servizi informatici, quali ad esempio quelli di posta elettronica, *software*, connessione *Internet*, gestione di siti *web*, ecc.; l'uso fraudolento da parte di terzi

di carte di credito e simili di proprietà dell'assicurato; il ricorso all'Arbitro Bancario e Finanziario, ecc.

Dall'indagine è emerso che le coperture relative alla tutela legale sono meno ampie e residuali rispetto a quelle riguardanti le perdite pecuniarie e la responsabilità civile e spesso sono fornite all'assicurato soltanto alcune garanzie di base, che soltanto in alcuni casi offrono al cliente a possibilità di integrare le stesse con garanzie accessorie. Inoltre, in alcuni casi, tali tipologie di coperture sono offerte soltanto a condizione che siano acquistate le garanzie per le perdite pecuniarie e/o la responsabilità civile.

È stato altresì rilevato che spesso i sinistri sono gestiti in *outsourcing* da Centrali Operative di società assicuratrici specializzate nel ramo tutela legale.

- *Esclusioni e Limitazioni specifiche della garanzia*:
  - spese di esecuzione forzata;
  - spese dell'Organismo di mediazione, se la mediazione non è obbligatoria;
  - spese legali non concordate con la compagnia;
  - danni da utilizzo fraudolento dell'identità digitale dell'assicurato;
  - inadempimenti contrattuali dell'assicurato;
  - risarcimenti di carattere punitivo;
  - multe, sanzioni e oneri fiscali.

3.1.1.4 Copertura assicurativa per richieste di riscatto

Nel panorama delle minacce *cyber* si assiste a una crescente diffusione del *ransomware*[3].

I *ransomware* si diffondono attraverso l'installazione da parte di un utente di un file "*.exe*". Nella maggior parte dei casi, l'installazione di questi file avviene inavvertitamente, attraverso il *clickjacking*[4] o come conseguenza di un attacco

3 *Ransomware: malware* utilizzato per eseguire estorsioni danneggiando o alterando il sistema e/o le informazioni contenute in esso (es. crittografia dei dati) consentendo così all'attaccante di chiedere un riscatto per ripristinare il normale funzionamento.

4 *Clickjacking* ("rapimento del clic) è una tecnica informatica fraudolenta. Durante una normale navigazione *web*, l'utente clicca con un puntatore del *mouse* su di un oggetto (ad esempio un *link*), ma in realtà il suo clic viene reindirizzato, a sua insaputa, su di un altro oggetto, che può portare alle più svariate conseguenze: dal semplice invio di *spam*, al *download* di un file, fino all'ordinare prodotti da siti di *e-commerce*.

phishing[5]: una volta installata, questa particolare tipologia di *malware*[6] impedisce agli utenti di accedere ai dati che risiedono nel computer "infettato" cifrandone il contenuto. Una volta entrato nella rete il *ransomware* può avere anche la capacità di diffondersi su altri sistemi vulnerabili in maniera silente ed autonoma. A seguito di un attacco *ransomware* i criminali informatici chiedono alla vittima il pagamento di un riscatto, entro una determinata data, solitamente mediante criptovalute (come ad esempio *Bitcoin*), per decriptare i dati o evitare l'eliminazione degli stessi.

I *ransomware* possono essere utilizzati anche per diffondere pubblicamente in rete dati riservati, come informazioni personali relative a individui o la divulgazione di segreti industriali.

Due compagnie estere che operano in Italia coprono le perdite pecuniarie derivanti all'impresa dalla richiesta di riscatto a seguito di un attacco *ransomware*. Un'impresa offre una polizza *cyber* con una garanzia per attacchi informatici a scopo estorsivo, con copertura delle perdite risultanti da una minaccia che include le somme pagate dall'assicurato a titolo di riscatto per fare cessare l'estorsione, oltre l'indennizzo delle spese sostenute per il ricorso a consulenti specializzati in estorsioni informatiche. La copertura è prestata dalla compagnia a condizione che la sottoscrizione della polizza sia mantenuta riservata e che sia data pronta informativa alle Autorità della minaccia di estorsione.

3.1.2 Condizioni di assicurabilità

Per poter assicurare il rischio *cyber*, le compagnie di assicurazione richiedono alle aziende requisiti minimi di assicurabilità e, in particolare, di avere operato in termini di sicurezza preventiva. La compagnia è così in grado di valutare per varie tipologie di attacchi informatici la possibile reazione dell'azienda assicurata sulla base dell'analisi del rischio, della tecnologia adottata, dei presidi di sicurezza e della formazione digitale dei responsabili della sicurezza e dei dipendenti.

Di seguito si riportano le principali condizioni di assicurabilità rinvenute nelle polizze:

- presenza di idonei presidi informatici per prevenire/fronteggiare gli attacchi informatici;
- installazione e aggiornamento frequente di adeguati sistemi *antivirus* e *firewall*;
- svolgimento di periodici e frequenti *backup* dei sistemi informatici;

---

5 *Phishing*: una forma digitale di ingegneria sociale eseguita attraverso una comunicazione elettronica (solitamente *e-mail*) ed impersonando un'entità fidata allo scopo di acquisire informazioni personali o confidenziali della vittima.

6 *Malware*: qualsiasi *software* o codice dannoso progettato per ottenere l'accesso illecito e/o interrompere il funzionamento del sistema informatico.

- adeguata connessione *Internet* per consentire le riparazioni tecniche da remoto;
- adeguati presidi organizzativi per la corretta e la consapevole gestione dei rischi informatici, quali procedure, esistenza di strutture dedicate interne o esterne per il presidio delle funzioni IT, formazione digitale continua del personale, ecc.;
- la sottoscrizione e il mantenimento per tutto il periodo di vigenza della polizza di un contratto di assistenza tecnica e di manutenzione sia per l'*hardware* che per il *software*.

3.1.3 Formula "*claims made*" e retroattività

L'indagine ha evidenziato che in molte polizze *cyber* le garanzie operano secondo la formula "*claims made*", ossia la garanzia assicurativa opera per i sinistri denunciati per la prima volta nel corso del periodo di validità della polizza, anche se avvenuti in precedenza, o nel periodo di denuncia postuma[7], se previsto dal contratto.

È emerso inoltre che in altri casi, accanto ad una copertura "base" per sinistri avvenuti durante la validità della polizza, è offerta al cliente la possibilità di beneficiare, come garanzia accessoria *(Top/Premium/Full)*, di un periodo di "retroattività" dell'efficacia della polizza, che copre anche i sinistri verificatisi prima della sottoscrizione. In questi casi la copertura è attiva anche per le richieste di risarcimento presentate per la prima volta all'assicurato durante il periodo di validità della polizza a condizione che il comportamento colposo dell'assicurato si sia verificato durante il periodo di assicurazione o non prima del periodo di retroattività indicato nella polizza. La data indicata nella polizza come "*data di retroattività*" rappresenta la data, prima della quale, un evento assicurato non viene coperto dall'assicurazione.

3.1.4 Esclusioni comuni a tutte le garanzie

Dall'analisi emerge che in larga parte sono applicate le esclusioni tipiche dei contratti assicurativi, oltre a **esclusioni specifiche per il rischio cyber**, alcune delle quali hanno l'effetto di limitare le garanzie, con riferimento in particolare alla:

- clausola generale relativa a guerre, sommosse, insurrezioni, ecc., tenuto conto che sempre di più gli attacchi informatici possono scaturire da eventi bellici o terroristici. In alcuni casi le compagnie escludono espressamente l'applicabilità delle coperture in caso di "guerra informatica", in altri casi la previsione fa riferimento genericamente alla "guerra". Il glossario in appendice del contratto non sempre contiene una definizione esplicita di cosa si intenda per "guerra" o "guerra informatica";

7 In alcune polizze difatti è anche previsto un periodo di denuncia postuma del sinistro, cioè un periodo di ultrattività, talvolta indicato anche come garanzia postuma, che prolunga il termine temporale entro il quale è possibile denunciare un sinistro.

- clausola volta a escludere le interruzioni di attività di infrastrutture elettriche, informatiche, ecc. prevista nella quasi totalità delle polizze esaminate relativamente ai danni – non risarcibili – derivanti da guasti, interruzioni, indisponibilità di sistemi di comunicazione, *Internet service*, fornitura di elettricità e di altra infrastruttura esterna che non sia sotto il controllo dell'assicurato.

È emerso altresì che le condizioni che per alcune compagnie configurano l'impossibilità di assicurare il rischio *cyber* (cfr. 3.1.2 sulle condizioni di assicurabilità), per altre rappresentano cause di esclusione o limitazione delle garanzie. Ne sono esempi:

- il mancato possesso di idonei presidi informatici per prevenire/fronteggiare eventuali attacchi *cyber;*
- la mancata installazione di adeguati sistemi *antivirus* o il mancato aggiornamento periodico degli stessi;
- la mancata installazione di idonei sistemi *firewall*;
- il mancato svolgimento di periodici e frequenti *backup* dei sistemi informatici;
- l'utilizzo di credenziali di *default* per l'accesso, non personalizzate dagli utenti;
- la non risarcibilità di eventuali riscatti pagati dall'assicurato vittima di un tentativo di estorsione *cyber*, anche quando risulta assicurato l'evento principale (*ransomware*);
- in alcuni casi, sono espressamente escluse le spese per il danneggiamento dell'*hardware* utilizzato, essendo tuttavia indennizzabili i danni al/ai *software* aziendale/i utilizzati.

3.1.5 Limiti territoriali, franchigie, massimali e periodi di carenza

Sono stati rilevati alcuni limiti di territorialità a seconda delle garanzie prestate. E in particolare:

- la garanzia "Perdite pecuniarie per danni al sistema informatico aziendale": vale per i danni che colpiscono il sistema informatico ubicato in Italia, Repubblica di San Marino, Città del Vaticano. I servizi di assistenza sono garantiti da remoto, mediante tele-collegamento sull'intero territorio dell'UE; l'eventuale intervento fisico di un operatore è garantito solo in Italia;
- la garanzia "Responsabilità civile": in alcune polizze vale per i danni che si verificano nel mondo, mentre altre polizze prevedono la copertura delle richieste di risarcimento originate da violazioni della *privacy* e/o violazioni della sicurezza commesse dall'assicurato nei territori della UE e/o avanzate innanzi all'autorità giudiziaria italiana e/o aventi a oggetto decisioni rese da autorità giudiziarie straniere e riconosciute in Italia;
- la garanzia "Tutela legale": vale in tutti gli Stati europei, per le controversie processuali per danni extracontrattuali e procedimenti penali; in UE, Svizzera,

Liechtenstein, Principato di Monaco, Norvegia, Andorra, Città del Vaticano, Repubblica di San Marino, per le vertenze di natura contrattuale; in Italia, Città del Vaticano, Repubblica di San Marino, per cause amministrative e per la consulenza legale telefonica.

Le polizze *cyber* dedicate alle PMI prevedono franchigie fisse, che si deducono dall'indennizzo, e franchigie temporali, che corrispondono al numero di giorni d'interruzione di attività aziendale stabilito nel contratto, trascorso il quale matura il diritto d'indennizzo.

I massimali vengono fissati per singolo sinistro o per importo massimo risarcibile nell'anno di riferimento.

Alcune garanzie delle polizze *cyber*, come la Tutela legale o l'Interruzione di attività, prevedono periodi di carenza contrattuale[8] anche di 90 giorni.

3.2 Polizze *cyber stand alone* rivolte a individui e famiglie

Le polizze *stand alone* dedicate alla clientela *retail*, individui e famiglie sono risultate meno numerose delle corrispondenti polizze per le PMI.

Nelle polizze rivolte a individui, le cui coperture spesso possono essere estese all'intero nucleo familiare, le garanzie più diffuse riguardano, come per le imprese, le **perdite pecuniarie** (danni diretti all'assicurato), la **responsabilità civile** per danni a terzi, la **tutela legale** per vertenze derivanti dall'evento assicurato, a cui si aggiunge l'**assistenza** alla persona.

3.2.1 *Perdite pecuniarie*

Nell'ambito delle coperture relative alle perdite pecuniarie di individui e famiglie, risultano essere coperti i danni diretti all'assicurato ed eventualmente al suo nucleo familiare, in conseguenza di furto o clonazione di carte di credito/debito e carte prepagate, furto di identità digitale, acquisti fraudolenti *online*.

3.2.2 *Responsabilità civile*

Per quanto riguarda le coperture in materia di responsabilità civile, le garanzie offerte riguardano l'indennizzo delle spese che l'assicurato è tenuto a pagare,

8 Periodo iniziale, che decorre dalla data di validità del contratto, durante il quale l'eventuale sinistro non è in garanzia (detto anche termine di aspettativa).

a titolo di risarcimento, per danni patrimoniali e non, involontariamente cagionati a terzi a seguito di un attacco *cyber*.

In diversi casi, la garanzia di base può essere integrata con altre fattispecie, quali l'indennizzo per i danni derivanti dall'uso improprio di materiale protetto da *copyright* e/o diritto d'autore, dalla pubblicazione impropria di contenuti che causano un danno di immagine a terzi, la violazione della *privacy* o la diffusione di dati personali di terzi, sempreché ciò avvenga mediante l'uso di dispositivi elettronici e reti informatiche.

3.2.3 *Tutela legale*

Per quanto riguarda la tutela legale, le coperture offerte non si discostano da quelle già esaminate per i prodotti destinati alle PMI.

3.2.4 *Assistenza*

In queste polizze spesso viene fornita all'individuo e al suo nucleo familiare **assistenza psicologica, telefonica e digitale**, attraverso un servizio di monitoraggio *online* che, mediante preventiva registrazione dell'assicurato su una piattaforma digitale, invia un *alert* in caso di sospetto attacco informatico sui suoi *device*. In tal modo, la struttura organizzativa della compagnia è subito informata e provvede tempestivamente a contattare un tecnico specializzato per attivare tutte le procedure di analisi e ripristino.

Sono presenti coperture per assistenza alla persona, anche nella forma della **consulenza psicologica a** seguito di eventi traumatici legati all'attacco *cyber*, quali **il furto dell'identità digitale, cyberbullismo e cyberstalking** (per maggiori dettagli, cfr. par. 3.2.5*)*, e dell'assistenza prestata in occasione di frodi nella prenotazione *online* di un viaggio all'estero.

3.2.5 *Cyberbullismo/cyberstalking*

All'interno delle polizze rivolte alla clientela *retail*, spesso le compagnie offrono una copertura specifica volta a tutelare individui e famiglie nel caso in cui subiscano **episodi di cyberbullismo/cyberstalking; spesso la medesima copertura opera anche nelle ipotesi di molestie e revenge porn.**

La garanzia è prevista nella forma dell'assistenza alla persona/nucleo familiare per il rimborso delle spese sostenute per ottenere un supporto psicologico a causa del manifestarsi di situazioni di disagio o stress psicofisico conseguenti a episodi di *cyberbullismo, cyberstalking*, molestie attraverso supporti informatici, ecc.

In alcuni casi, accanto al rimborso delle spese mediche per il supporto psicologico, all'assicurato è offerto anche un supporto informatico, sotto forma di assistenza da parte di esperti informatici, per eliminare/ridurre gli effetti dell'attacco subito, ad esempio eliminando dal *web* contenuti offensivi o lesivi della reputazione personale, effettuando diagnosi approfondite delle modalità e delle conseguenze dell'attacco subito, ecc.

In altri casi, all'assicurato è offerta anche la copertura delle spese legali sostenute per inoltrare **l'istanza di oscuramento di siti web/pagine di social media** ai sensi di legge o per rivolgersi al Garante per la Protezione dei Dati Personali.

Nella maggior parte dei casi le diverse forme di assistenza garantite all'assicurato sono fornite in *outsourcing* da parte di operatori specializzati.

Nel caso della garanzia più diffusa, quella relativa al rimborso delle spese mediche, è sempre richiesto all'assicurato di denunciare il sinistro entro un certo lasso di tempo dal verificarsi dell'attacco e secondo procedure codificate. All'assicurato è sempre richiesto di produrre la documentazione medica attestante la necessità del supporto psicologico. Sono altresì sempre previsti massimali per il rimborso delle spese sostenute, per numero di sinistri e/o per importo rimborsato. In alcuni casi, le compagnie escludono espressamente dal perimetro della copertura i casi di patologie psichiatriche preesistenti, abuso di alcolici, psicofarmaci nonché uso non terapeutico di stupefacenti e allucinogeni.

3.2.6 Condizioni di assicurabilità

Tra le condizioni di assicurabilità nei prodotti per clientela *retail*, è richiesta soprattutto l'attivazione di una connessione Internet (di solito di almeno 2 Mbps *download*, 0,80 Mbps *upload*), poiché la maggior parte delle polizze prevede, in caso d'introduzione di *malware*, interventi tecnici per il ripristino del sistema informatico dell'assicurato o del suo nucleo familiare mediante assistenza da remoto.

Alcune società stabiliscono che l'operatività della garanzia è condizionata anche alla sussistenza dei seguenti presupposti: a) che le apparecchiature utilizzate dall'assicurato siano esclusivamente *computer notebook* o *desktop* e non siano utilizzate esclusivamente per attività professionali/commerciali/artigianali, escludendo, quindi, *tablet/smartphone* e memorie esterne; b) che gli apparecchi digitali "*home*" o "mobili" siano provvisti di *software open source* e di regolare licenza; c) che gli apparecchi e i dispositivi non beneficino ancora della garanzia del fabbricante e che siano certificati CE; d) che l'assicurato effettui *backup* dei dati, controlli periodici per verificare la presenza di programmi non autorizzati e abbia adottato programmi di protezione dalle minacce o da eventi malevoli, nonché che abbia effettuato l'aggiornamento anche del programma del recupero dei dati; c) che il computer operi in ambiente Microsoft Windows, Apple MacOS o GNU/Linux.

3.3 Polizze modulari con copertura *cyber* per PMI, individui e famiglie

Diverse polizze per la copertura del rischio *cyber*, rivolte a una clientela *retail* e alle PMI, sono offerte al pubblico sotto forma di moduli che è possibile aggiungere ad altre polizze a copertura della persona/azienda o dei beni (polizze modulari).

In linea generale, si tratta di polizze in cui la copertura *cyber* è di portata contenuta.

Le polizze modulari sono per lo più rivolte a singoli ma estensibili al nucleo familiare, contengono la copertura *cyber* opzionale acquistando le garanzie Tutela legale, Assistenza e Responsabilità civile. Si tratta di polizze flessibili e personalizzabili in cui sono presenti servizi di assistenza all'assicurato, quali consulenza telefonica e psicologica a seguito di eventi traumatici legati all'attacco informatico o a seguito di episodi di *cyberbullismo* e *cyberstalking*. Di recente tale copertura è stata inserita anche nella garanzia Corpi Veicoli Terrestri.

Per quanto riguarda gli acquisti *e-commerce*, in molte polizze sono espressamente esclusi i sinistri derivanti dall'acquisto di un'ampia gamma di beni, di solito elencati in modo puntuale nelle polizze *cyber*, e che, tra gli altri, comprendono gioielli, beni preziosi, oggetti d'arte acquistati in aste *online*; denaro e strumenti finanziari di vario genere, veicoli a motore/natanti, beni deperibili, quali cibo e bevande, armi, medicinali; animali e vegetali.

Nelle polizze rivolte alle PMI, le coperture più diffuse riguardano la tutela legale per vertenze relative ai danni subìti per fatti illeciti di terzi e a i danni causati a terzi per delitti dolosi, colposi o per contravvenzioni connessi all'utilizzo del *web* e dei *social media* nel corso dell'attività d'impresa, a eventuali vertenze con fornitori di servizi informatici, a vertenze relative all'uso fraudolento da parte di terzi di carte di credito e simili di proprietà dell'assicurato. Sono inoltre previste coperture sotto forma di assistenza per il recupero dei dati informatici e il ripristino dei sistemi informatici danneggiati dall'attacco (laddove nelle polizze *stand alone* corrispondenti viene invece offerto anche l'indennizzo delle perdite pecuniarie associate alla medesima fattispecie).

In alcune polizze sono presenti coperture per il risarcimento del danno derivante dalla responsabilità civile, soprattutto in caso di danni a sistemi informatici di terzi, furto, perdita o divulgazione non autorizzata di dati informatici di terzi e lesioni reputazionali.

L'indagine ha consentito inoltre di rilevare che, anche nell'ambito delle polizze Corpi Veicoli Terrestri (CVT), sono presenti coperture per eventi *cyber* direttamente o indirettamente collegati all'evento principale assicurato: in particolare, è stata individuata una polizza danni auto di tipo modulare che prevede anche la copertura

per attacchi *cyber*, che tuttavia, in virtù delle esclusioni previste[9], copre, di fatto, solo il ritrovamento delle chiavi dell'autovettura.

Alcune compagnie estere attive sul mercato mondiale iniziano a sviluppare polizze *cyber* modulari personalizzate per le PMI. In un caso è offerta anche in Italia una polizza modulare flessibile che copre esclusivamente il rischio *cyber* e permette al contraente (PMI) la possibilità di scegliere tra i vari moduli di polizza le coperture più adatte alle esigenze di protezione della sua impresa.

3.4 Polizze multirischio con copertura *cyber* per PMI, individui e famiglie

Dall'analisi è emerso che sono numerose le polizze multirischio con sezioni opzionabili, dedicate alla clientela *retail* e alle PMI, che rispondono ai bisogni di protezione dei beni e del patrimonio dell'assicurato (proprietario o locatario o PMI), in cui la copertura *cyber* è presente nelle garanzie Tutela legale e Assistenza.

Le caratteristiche di tali polizze, sia per quanto attiene alle coperture offerte, sia per quanto concerne le esclusioni e le limitazioni, le franchigie e i massimali, non si discostano da quanto illustrato per le altre tipologie di polizze.

9 La copertura cyber opera solo per *cyberterrorismo*, se si acquista espressamente il modulo "Eventi sociopolitici".

4. Glossari

Le verifiche effettuate sui Glossari delle polizze *cyber* hanno evidenziato una non univocità nell'indicazione delle definizioni tecniche di termini inerenti al rischio cibernetico.

A titolo di esempio, il termine **"dati"** in alcuni glossari viene dettagliatamente definito quale "qualsiasi informazione digitale, presente nel sistema informatico dell'assicurato e memorizzata all'esterno della memoria ad accesso casuale (RAM), indipendentemente dalla forma o modo in cui viene utilizzata o visualizzata (ad esempio testo, immagini, video, *software*)"; in un altro glossario, per "dati" si intendono invece genericamente "i dati elettronici e il *software*".

Anche nel caso del termine **"attacco informatico"** sono state riscontrate differenze nelle definizioni fornite nei glossari. In un caso, ad esempio, l'"*attacco informatico*" viene individuato sinteticamente quale "*atto doloso, malware, furto contro il sistema informatico dell'assicurato*"; in un altro caso, esso è definito quale "*atto illecito commesso deliberatamente da un soggetto che utilizzando le risorse di sistema e/o di rete dell'assicurato, determini conseguenze in ordine alla riservatezza, la disponibilità o l'integrità dei dati e del sistema informatico. In dettaglio: 1) acquisizione, accesso, divulgazione non autorizzati o la sottrazione di dati e/o dati personali che sono in carico, in custodia o sotto il controllo dell'assicurato o di terzi in base a un contratto con l'assicurato; 2) accesso o uso non autorizzato del sistema informatico dell'assicurato, perdita, alterazione, corruzione o danno ai programmi, alle applicazioni o ai dati e/o dati personali presenti nei sistemi informatici dell'assicurato; 3) infezione e corruzione del sistema informatico dell'assicurato attraverso l'utilizzo di programmi dannosi; 4) trasmissione di programmi dannosi dal sistema informatico dell'assicurato verso terzi; 5) attacco DoS (Denial of Service); 6) estorsione informatica"*.

In altri casi, i glossari non forniscono una esaustiva definizione di alcuni termini (come nel caso della definizione del termine "guerra", che specie in una polizza *cyber* dovrebbe comprendere anche la "guerra informatica", o di "*malware*", "*ransonmware*" o "dati sensibili", "furto dati", o "*phishing*")[10].

10 Cfr. par. 3.1.1.4

5. Conclusioni

La fotografia del mercato assicurativo italiano delle polizze *cyber* che emerge dall'analisi porta con sé alcune considerazioni sulle prospettive di un'evoluzione delle stesse in ottica di *consumer centricity*.

L'affinamento e la granularità del *Target Market*, tematica che riveste in via generale primaria importanza per tutti i prodotti assicurativi, assume un ruolo cruciale anche per le polizze *cyber* che risultano, allo stato, standardizzate.

Le polizze potrebbero essere maggiormente flessibili e calibrate sulle effettive e specifiche esigenze del cliente/consumatore finale ponendo maggiore attenzione altresì alla profilazione ed al grado di esposizione al rischio *cyber:* ad esempio, una piccola impresa che non opera tramite *e-commerce* avrà un profilo di rischio *cyber* diverso rispetto ad una che invece vende i prodotti anche *online*.

La rilevazione dell'operatività del cliente è importante per poter offrire una polizza in linea e confacente con il suo profilo "digitale", con la sua operatività specifica in tale mondo e dunque, con la sua esposizione al rischio *cyber*.

Le polizze in argomento potrebbero anche beneficiare di una revisione delle esclusioni, che dovrebbero inoltre tenere conto anch'esse della granularità e delle esigenze effettive del *Target Market* di riferimento.

Opportuna l'adozione di un glossario unico per le definizioni così da garantire omogeneità e certezza: al riguardo, le compagnie potrebbero fare riferimento al **Cyber Lexicon FSB**[11], che offre una serie di definizioni consolidate ed accettate nella comunità digitale.

È inoltre importante un'adeguata formazione e aggiornamento della rete distributiva sulle polizze *cyber*, in considerazione della complessità tecnica che possono avere queste polizze e delle condizioni di assicurabilità previste.

Dal lato delle aziende è importante che esse valutino i loro rischi specifici e si consultino con un professionista intermediario assicurativo per determinare il livello appropriato di copertura informatica necessaria. Fattori come la natura dell'azienda, il volume dei dati sensibili, la dipendenza dalla tecnologia e le normative del settore dovrebbero essere presi in considerazione quando si valuta la necessità e l'estensione della copertura assicurativa informatica. Importante discutere e verificare anche gli aspetti relativi alle condizioni di assicurabilità e alle esclusioni.

11 https://www.fsb.org/wp-content/uploads/P130423-3.pdf