

**Dott. Roberto Panzeri**

Manager Casualty and Special Risks Department R.I.B.,  
Reinsurance International Brokers S.p.A., Milano

Il Dott. Riccardo Sabbatini ha parlato dei rischi finanziari, inquadrandoli negli emerging risks che abbiamo visto essere quei nuovi rischi contraddistinti da una difficile comprensione e da una difficile quantificazione, a causa, principalmente, della mancanza di statistiche ed esperienza, da una continua evoluzione e da un elevatissimo danno potenziale, rispetto ad una bassa frequenza. Il World Economic Forum classifica gli emerging risks in cinque macro categorie legate alle dinamiche economiche, climatiche, demografiche, geopolitiche e tecnologiche. Diversi interventi che abbiamo apprezzato nel corso di questo Convegno hanno fatto riferimento proprio alle dinamiche tecnologiche ed è in questo ambito che si inquadra il rischio informatico (o cyber risk).

Il cyber risk è il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia di informazione e comunicazione; stiamo parlando della distruzione, della sospensione e della compromissione di infrastrutture telematiche e banche dati di un individuo o di una Società, che possono essere causate da errore umano, da eventi naturali, problemi tecnici di sistema o da attacchi informatici (cyber crime). Il provider di hardware storage EMC2 ha condotto un'interessante indagine dalla quale si evince che, relativamente alle cause che hanno originato danni informatici nel 2014, gli "errori della macchina" o del programma (hardware failure, loss of power, o software failure) hanno rappresentato ancora la causa principale; notiamo anche come nel 23% dei casi, si registra la presenza di un security breach (violazione di dati), che analizzeremo in seguito.

Le conseguenze per un'azienda che dovesse fronteggiare un evento informatico dannoso possono essere estremamente pericolose e possono tradursi in danni di tipo materiale, come la distruzione della macchina o tecnologie compromesse, e patrimoniale, come ad esempio gli elevatissimi costi di ripristino e i danni da interruzione di attività (mancato profitto, mancata produttività dei dipendenti, ritardo nello sviluppare dei prodotti o dei servizi e opportunità di lavoro mancate); vi sono poi danni di tipo reputazionale e di responsabilità verso terzi (si pensi alla violazione della privacy a seguito di furto di dati).

È sempre EMC2 a dirci che i costi generati dai danni informatici, quali collassi e rotture telematiche, perdita e distruzione-



**Il Rischio Informatico in breve**

Distruzione, Sospensione, Compromissione di:

- Infrastrutture Telematiche
- Banche Dati

A causa di:

- Errore Umano
- Eventi Naturali
- Problemi Tecnici di Sistema
- Cyber Crime

**Le Cause**

WHAT IS CAUSING THESE DISRUPTIONS?

ne dei dati e costi di ripristino, ammontano su scala globale a oltre un trilione e mezzo di dollari, 750 miliardi dei quali sono dovuti alla perdita di dati e 950 miliardi dovuti al periodo di inattività delle macchine.

Secondo il CLUSIT (Associazione Italiana per la Sicurezza Informatica) un risk manager, o più in generale un buon imprenditore, dovrebbe oggi interrogarsi non più sul fatto che la sua azienda possa subire un attacco informatico, ma piuttosto sul quando questo accadrà; e questa preoccupazione non deve riguardare solo le società che vendono servizi online, le internet companies o le software houses, ma anche il singolo professionista che può vedere criptati i propri dati, una piccola impresa che viene derubata del proprio know-how, una Pubblica Amministrazione che non si trova più nella posizione di offrire i servizi ai cittadini o una grande azienda che subisce il furto di un ingente numero di dati personali dei propri clienti.

Quindi, comprendiamo bene come un buon imprenditore debba necessariamente tenere in considerazione il rischio informatico ed essere in grado di quantificare non solo i potenziali danni materiali diretti che la sua azienda può subire, ma anche e soprattutto i danni patrimoniali dovuti all'interruzione della propria attività e le potenziali richieste di risarcimento da parte di terzi, qualora venissero violati i loro dati personali o sensibili, a seguito di un attacco informatico (cyber crime).

Proprio il CLUSIT ha condotto uno studio analizzando 3.700 casi di attacchi informatici avvenuti nel 2014; come per gli anni precedenti, il settore governativo è stato ancora una volta il principale bersaglio, mentre è particolarmente interessante notare il fatto che la categoria others rappresenti il secondo settore maggiormente colpito dal cyber crime. Questo dato conferma quanto dicevamo prima e cioè il fatto che la minaccia informatica, oggi, interessa qualsiasi settore merceologico. Dopo gli online services, l'entertainment, il research e la bank finance che in linea di massima mantengono le medesime posizioni rispetto agli anni precedenti, il settore medico/sanitario (health) è quello che ha fatto segnare il maggiore incremento. Le banche dati di ospedali ed aziende sanitarie sono frutto

Reinsurance International Brokers S.p.A.

### Le Conseguenze

- Danno Materiale;
- Danno Patrimoniale (costi di ripristino e danni da interruzione attività);
- Danno Reputazionale;
- Violazione della Privacy (furto di dati).

Reinsurance International Brokers S.p.A.

### Le Conseguenze

Perdita di dati e periodo di inattività

Danni patrimoniali e da interruzione attività

Reinsurance International Brokers S.p.A.

### Così come il Rischio Informatico di "Data Breach"?

Non solamente le Internet Companies, le Software Houses, ma anche:

- Il Singolo Professionista che può vedere i propri dati criptati;
- La PMI che scopre, magari con ritardo, di esser stata derubata del proprio know-how;
- La Pubblica Amministrazione che non può più offrire servizi essenziali ai cittadini;
- La grande impresa che subisce il furto di milioni di dati personali dei propri clienti.

Reinsurance International Brokers S.p.A.

### Vittime di Cyber Crime 2014

Tipologia e distribuzione delle vittime nel 2014

Settore	Percentuale
Gov - MI - U - meriggio	12%
Others	12%
Online Services / Cloud	10%
Insurance / News	8%
Research / Education	8%
Banking / Finance	8%
Organization - HR	8%
Gov / Not Profit	8%
Health	8%
ESG / Retail	8%
Telco	8%
Digital Infrastructure	8%
Gov. Contractors / Consulting	8%
Religion	8%
Chemical / Medical	8%

© Clusit - Rapporto 2015 Info Sicurezza ICT e Fido

di lucro ingente per chi se ne impossessasse; il prezzo di una cartella clinica, sul mercato underground, può raggiungere i 60 dollari, in relazione alle informazioni in essa contenute. Il settore della Grande Distribuzione Organizzata, pur rappresentando solo il 2% del numero degli attacchi, è il settore che genera i maggiori danni, in termini di perdite economiche; ad esempio, negli Stati Uniti, il malware BlackPOS, facilmente reperibile sul mercato underground per circa 1.800 dollari, ha generato danni certi alla catena di negozi fai da te Home Depot per 62 milioni di dollari e di addirittura 148 milioni alla catena di grande distribuzione alimentare Target.

Sono proprio gli Stati Uniti il Paese che ha fatto registrare il maggior numero di attacchi informatici; va detto che l'obbligo di notifica all'autorità garante, e spesso anche direttamente ai consumatori, introdotto a partire dai primi anni 2000 in diversi Stati americani, ha influito di molto su questo dato, poiché sono innumerevoli i casi di attacchi informatici non notificati e quindi non censiti, verificatisi nelle varie nazioni ove questo obbligo non sia, o non sia ancora, in essere.

Un altro dato interessante che emerge dallo studio del CLUSIT riguarda le tecniche adottate dagli hacker. Le tecniche sconosciute, tra il 2011 e il 2014, hanno rappresentato la seconda causa più frequente e nel 2014 addirittura la prima; è un'ulteriore dimostrazione di come gli emerging risks, e nello specifico il rischio informatico, siano a tutti gli effetti una minaccia in continua evoluzione.

Gli attacchi hacker hanno come principale finalità il cyber crime (furto, manomissione, modifica e distruzione di dati) ma sono frequenti anche i casi di hacktivism, che rappresentano una sorta di manifestazione virtuale (pensiamo al defacement dei siti internet a scopi dimostrativi). Le attività di spionaggio e guerra cibernetica, con una bassa incidenza percentuale, rappresentano le altre finalità catalogate degli attaccanti informatici.

Tra i più celebri attacchi di cyber crime, avvenuti e pubblicamente notificati negli ultimi 2 anni, oltre ai già citati casi di Home Depot e Target (furto di dati relativi a milioni di carte di credito dei loro clienti), si registrano,



ad esempio, quelli di Ebay, che ha subito il furto di 145 milioni di record contenenti sia dati personali che password criptate dei suoi clienti, e Sony, a cui furono rubati 28 milioni di file, inclusi 10 anni di e-mail e stipendi del personale, film ancora non usciti, documenti riservati contenenti dati sensibili, dati relativi ad altre aziende ed in alcuni casi estremamente imbarazzanti (danno ancora non quantificato, ma si parla di cifre elevatissime). A Benetton vennero sottratti i bozzetti della collezione 0-12 ed in seguito a questo furto vennero addirittura trovati dei capi di abbigliamento in vendita in alcuni negozi siriani. La compagnia di assicurazione Anthem ha subito il furto di 80 milioni di record, contenenti dati personali relativi alla salute dei loro clienti e dipendenti; al sito di incontri extra coniugali Ashely Madison sono stati sottratti e divulgati i dati di 37 milioni di utenti i quali tutto avrebbero desiderato, fuorché di essere smascherati.

L'“Operazione Newcaster” ha rappresentato una grandissima operazione di cyber spionaggio; in due anni, gli hacker hanno messo insieme una falsa agenzia giornalistica (la Newsnair) ed hanno creato vari falsi profili su diversi social network; tramite questa operazione sono riusciti ad ottenere parecchie informazioni su personale militare e diplomatico, oltre che su giornalisti e contractor della difesa delle Nazioni Unite. Pensiamo al paradosso dell'Hacking Team, azienda di hacker che lavora per conto dei governi di diverse nazioni, che è stata a sua volta “hackerata” e pensiamo che persino i siti web della Nato e del Centro di Difesa Cibernetica dell'Organizzazione di Bruxelles hanno subito un defacement da parte di attivisti ucraini filorusi. Possiamo solo ribadire, nuovamente, che proprio nessuno si può considerare al sicuro.

Secondo la PricewaterhouseCoopers il 96% delle grandi ed il 71% delle piccole e medie imprese dichiarano di avere riscontrato almeno un problema di sicurezza informatica nel corso del 2014 e per l'Allianz Risk Barometer il rischio informatico è risalito, nella scala dei rischi percepiti, dall'ottavo al quinto posto; l'Insurance Information Institute di New York ha riscontrato che, secondo il giudizio dell'80% dei manager intervistati, il settore assicurativo cyber sarà quello maggiormente in crescita.

Comprendiamo quindi che le aziende, oggi,

**Attacchi Cyber: Impatto e Percezione del Rischio Informatico**

- Il 96% delle Grandi Imprese ed il 71% delle Piccole Imprese dichiara di aver riscontrato almeno un problema di sicurezza informatica nel 2014 (PwC)
- La Settore Assicurativo Cyber sarà quello maggiormente in crescita secondo l'80% dei manager intervistati (Insurance Information Institute di New York)
- Il Rischio percepito su base mondiale è salito dall'ottavo al quinto posto (Allianz Risk Barometer)

**Attacchi Cyber: Impatto e Percezione del Rischio Informatico**

- 117.000 attacchi informatici al giorno (PwC 2014), con previsione di aumento del 38% per il 2015.
- 600.000.000 di dati violati (Allianz Global Corporate Solutions)
- 445.000.000.000 USD di danni (Centre for Strategic and International Studies) su scala globale dei quali:
  - 100.000.000.000 USD di danni negli Stati Uniti (Report World Economic Forum 2015)
  - 9.000.000.000 EUR di danni derivanti da attacchi informatici in Italia (Rapporto Clusit 2015)

**USA ed Europa: parallelismo normativo ed assicurativo**

- Stima raccolta premi 2015 per le coperture Cyber:
  - Worldwide: USD 2.500.000.000 (PwC)
  - USA: USD 2.000.000.000
  - Europa: EUR 150.000.000
- 2012 – Stati Uniti: Security Breach Notification Laws (e successive implementazioni). Obbligo di notifica a Garante e Consumatori.
- 2012 – Europa: General Data Protection Regulation (GDPR) in via di implementazione con attuazione prevista per il 2017. Obbligo di notifica a Garante e Consumatori nel caso di effettivo impatto.

hanno iniziato a capire e ad analizzare questi nuovi rischi, dovuti alla tecnologia, e sono pronte a tenere in considerazione il cyber risk e a studiare delle misure di tutela via via crescenti; anche perché stiamo parlando di 117mila attacchi informatici al giorno (PwC), naturalmente di varie entità, numero che è destinato a crescere del 38% per il 2015, e di 900 milioni di dati violati (Allianz Global Corporate Solutions).

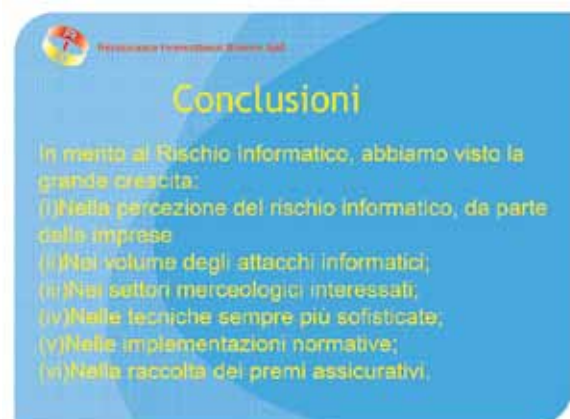
Per il Centre for Strategic and Studies, il volume dei danni stimati, causati dal cyber crime, è pari a 445 miliardi di dollari, dei quali 100 miliardi solamente negli Stati Uniti (World Economic Forum 2015); la stima del volume dei danni, relativamente alle aziende italiane, ce la fornisce il CLUSIT che parla di oltre 9 miliardi di danni, a seguito di attacchi informatici. Il parallelismo numerico trova riscontro anche nel mercato assicurativo, il quale è a sua volta figlio anche del quadro normativo di riferimento.

Infatti, a partire dal 2002, in California è nata la Security Breach Notification Law che, con le sue successive implementazioni e attuazione anche in altri Stati d'America, imponeva ed impone alle aziende l'obbligo di notifica sia all'autorità garante sia ai consumatori, in caso di data breach.

In Europa, il tema della violazione dei dati, è divenuto sempre più attuale e dibattuto fino a quando, nel 2012, è stato emanato il General Data Protection Regulation (GDPR), la cui attuazione è prevista per il 2017; tale regolamento europeo prevedrà l'obbligo di notifica a garante e consumatori, anche se, a differenza di quanto previsto per gli Stati Uniti, solamente nel caso in cui detta violazione (breach) abbia realmente avuto un impatto sui dati dei consumatori stessi.

La conseguenza di dette normative si è naturalmente riflessa, dicevamo, sul mercato assicurativo; la PwC stima che i premi spesi per le coperture cyber ammontino, su scala globale, a circa 2,5 miliardi di dollari, 2 miliardi dei quali sono stati spesi solamente negli Stati Uniti.

Al momento, in Europa, si stimano premi solamente per circa 150 milioni di euro ed è quindi facile prevedere una crescita in questo settore, a causa dell'aumento esponenziale degli attacchi informatici su larga scala e della via via crescente percezione del rischio da parte degli imprenditori e dei risk manager. A questo, dobbiamo aggiungere anche l'aumentata informatizzazione delle imprese, la diffusione delle app, l'internet of things, le innumerevoli informazioni custodite nelle banche dati delle aziende di tantissimi settori e, perché no, il ricorso delle imprese stesse al web ed alla comunicazione informatica, anche e soprattutto tramite social network.



**Conclusioni**

In merito al Rischio informatico, abbiamo visto la grande crescita:

- (i) Nella percezione del rischio informatico, da parte delle imprese
- (ii) Nel volume degli attacchi informatici;
- (iii) Nei settori merceologici interessati;
- (iv) Nelle tecniche sempre più sofisticate;
- (v) Nelle implementazioni normative;
- (vi) Nella raccolta dei premi assicurativi.

Anche i consumatori hanno modificato la propria sensibilità e percezione del rischio stesso e le direttive ed i regolamenti della Comunità Europea non potranno che influire significativamente, così come già accaduto in America una decina di anni prima, nello sviluppo del settore assicurativo.

I grandi Assicuratori hanno già sviluppato prodotti dedicati che stanno costantemente aggiornando e modificando, soprattutto in base all'esperienza che stanno maturando, nonché adattando alle differenze dei vari Paesi; i noti player internazionali, come ad esempio Allianz, Axa, Zurich, ACE, Aig ed i Lloyd's di Londra, pur partendo con poca esperienza ed alta aleatorietà stanno affermandosi come punti di riferimento per il mercato e la stessa direzione è stata intrapresa anche dalle varie Compagnie dei mercati domestici europei.

È un terreno fertile ed è proprio in questo contesto, di percezione di rischio ed innovazione tecnologica ed assicurativa, che i broker assicurativi e riassicurativi devono operare sia come facilitatori per la comprensione del rischio da parte dell'Assicuratore, sia come "traduttori" delle esigenze specifiche dei vari clienti che, ciascuno per la propria nazione, per la tipologia di industria, il livello di risk management e il volume di dati trattati, presentano esigenze diverse e sempre più particolareggiate.



**Conclusioni**

Nei settore assicurativo i grandi player internazionali hanno cominciato da diversi anni ed in diversi Paesi a distribuire prodotti in continua evoluzione.

La portata della tecnologia in tutti i settori tecnologia (e l' "Internet of Things") ha sensibilizzato le Aziende riguardo ai rischi che ne derivano ed ha creato un immenso spazio per la misurazione, la valutazione e l'assicurazione dei Rischi Informatici



**Conclusioni**

Anche l'approccio culturale si sta modificando e le nuove normative stanno introducendo nuove regole e nuovi obblighi per le Aziende.

Grandi prospettive in termini di premi ed auspicio di collaborazione tra pubblico e privato.

Assottigliamento tra domanda ed offerta assicurativa e prodotti assicurativi innovativi