

## Il Trasferimento dei “rischi residui” derivanti dalle attività informatiche. (tramite polizze Assicurative)

### Premessa

Storicamente, due pilastri dell'economia moderna, il mondo del credito e quello delle assicurazioni, sono stati fondamentali per garantire sviluppo ed investimenti necessari all'affermarsi di un sistema di relazioni economiche basate su stabilità e prospettive di sviluppo.

Le crisi ricorrenti dell'economia mondiale (ricordo il 1929 in parallelo con quella odierna) potrebbero essere considerate tutto sommato alla stregua delle “malattie della crescita” di una delle parti essenziali del sistema di relazioni umane, quella che ormai caratterizza costantemente la civiltà del 19mo e 20mo secolo nel suo sviluppo verso il futuro.

Solo nell'ultimo periodo del passato millennio una tecnica rivoluzionaria unita alla scienza del trattamento delle informazioni ha determinato il diffondersi in tutte le attività umane dell'utilizzo massiccio ed a tappeto dell'informatica.

Il carattere esponenziale di tale diffusione e delle caratteristiche intrinseche delle continue innovazioni (pensiamo solo alla rivoluzione delle trasmissioni via etere) pone sia gli “addetti ai lavori” che gli “utilizzatori” finali di fronte ad una serie di scelte e valutazioni sempre più complesse e difficili.

Il mondo del credito supporta economicamente le varie attività nelle loro scelte di investimento e garantisce una sicurezza di pianificazione dei progetti e dei ritorni economici nel tempo, quello assicurativo viene coinvolto al fine di proteggere sia le attività che gli investimenti, dagli accidenti e dalle minacce presenti nell'alea degli eventi possibili.

Sappiamo tutti, come Soci del CLUSIT, che il raggiungimento degli obiettivi economici comporta un equilibrio tra spese e ricavi e che la “sicurezza informatica” non si sottrae a questo fatto. In effetti abbiamo la certezza che non sarà mai conveniente, nè possibile per svariate motivazioni, cercare di ottenere il 100% della sicurezza e protezione di una attività economica.

E' quindi indispensabile considerare che un accidente od una minaccia possano colpire i nostri sistemi e quindi la nostra attività economica che li utilizza, al di là delle prevenzioni e protezioni che sono state messe in atto.

La stima dei rischi residui in questo campo è estremamente difficile per il fatto che le variabili da considerare sono in numero estremamente elevato e che oltretutto sono soggette ad una variazione nel tempo estremamente rapida, sia come casistica, sia come magnitudo.

Tipicamente il punto di vista di un'analisi tecnica di risk management specifica (da una prospettiva ingegneristica) diverge da quella elaborata dal comparto assicurativo poiché partono da esperienze e postulati differenti.

Inoltre un improvvido atteggiamento degli “addetti ai lavori”, inclusi i fornitori di sicurezza, tende a minimizzare le % e la magnitudo degli accadimenti residuali (e a limitarla assolutamente a quelli conosciuti), rendendo così le stime sui rischi residui, e gli atteggiamenti conseguenti, più favorevoli a che uno spirito imprenditoriale aggressivo si senta tranquillo di acquisire il rischio residuo “in proprio” senza difficoltà.

In genere gli assicuratori tengono riservati i loro calcoli e le stime dei rischi residuali nei confronti dei clienti per evitare di passare per i “giona” della situazione. I clienti non amano essere informati su proiezioni di disastri che possono colpire le proprie attività, e umanamente preferiscono considerarsi privi di accidenti per il futuro (non è successo nel passato quindi...).

Così mentre per il resto dei comparti assicurativi il trasferimento dei rischi residuali è ormai una pratica consolidata (in Italia un po' meno, ci sono ancora decine di migliaia di aziende non ancora assicurate contro le perdite di profitto, per esempio) nel settore assicurazioni dell'attività informatica i ritardi del comparto assicurativo sono nel nostro paese siderali, e si contano sulla punta di alcune dita di una sola mano gli assicuratori che accettano di fornire polizze specifiche sulle perdite di profitto determinate da eventi informatici dannosi.

## **Trasferire il rischio informatico: un'operazione sia tecnica che economica**

Attualmente è difficile per un imprenditore se pur attore di un segmento del business dell'informatica, comprendere pienamente i propri rischi, prefigurare una casistica e valutare l'imponderabile, anche perché la sua propensione è quella proprio di evitare tramite il proprio lavoro i cosiddetti "incidenti di percorso".

Tuttavia per chi i rischi li assicura, cioè per chi si accolla l'imponderabile difficilmente valutabile, il pagamento degli eventi dannosi che avvengono in giro per il mondo è una pesante borsa da tenere in equilibrio tra perdite e ricavi.

Esistono differenti punti di vista, nondimeno spesso la collaborazione tra clienti e assicuratori si rivela fondamentale per la comprensione dei reciproci punti di vista, e se da una parte i "survey" degli assicurati comportano la dolorosa constatazione di alcune *défaillances* nei propri sistemi, dall'altra spesso ciò è solo possibile in virtù dell'esperienza degli assicuratori che utilizzano criteri di varia natura, incluso quelli empirici, ma che lo sono solo perché basati sull'esperienza (dei sinistri pagati), a prescindere dalla costruzione di teorie scientifiche o ingegneristiche specifiche.

Consideriamo quindi la collaborazione con gli assicuratori la base di ogni approccio alla valutazione del trasferimento dei rischi residui.

Il primo risultato che l'Azienda si porta a casa è una valutazione "tecnico-assicurativa" del proprio rischio ,una "campana" proveniente da un settore che di eventi imponderabili se ne intende, al contrario di altri.

Un effetto "collaterale" positivo di questa collaborazione è quello che in rapporto a questo risultato la propria impresa è stata sollecitata nei suoi vari dipartimenti a comporre la cosiddetta "valutazione della perdita economica" negli scenari che saranno reputati più critici e dannosi, e di qui si arriva alla quantificazione finale del (dei) massimo (i) danno (i) probabile (i) .

In effetti, è da questi risultati che si arriva poi a una decisione della proprietà aziendale su quale scelta è opportuno fare per una buona gestione dell'attività.

L'esperienza ci dice che il massimo danno informatico probabile, riduce drasticamente gli utili netti dell'anno in corso e di quello successivo, e in questi periodi di difficoltà economica e di grande concorrenza proveniente dall'estero (extra UE), ciò comporta una seria ipoteca alla sopravvivenza dell'attività economica aziendale.

Alcune aziende preferiscono accantonare annualmente un capitale di rischio nel proprio bilancio, ma a parte le considerazioni inerenti la nuova normativa sulla struttura del bilancio europeo, la stima dell'accantonamento - ove sia possibile - ricade nelle incertezze di valutazione anzidette, per cui nella media sicuramente l'ammontare accantonato sarà sufficiente per rischi che ricadono nell'area della ripetitività, ma non sarà mai sufficientemente importante da coprire la "punta di rischio", ciò che costituisce l'oggetto di una polizza di assicurazione informatica.

La scelta dell'accantonamento è comunque rara tra le aziende e la maggior parte di quelle che non si assicurano preferisce semplicemente non prendere in considerazione i rischi informatici.

Avviene così che il processo di trasferimento del rischio residuo da una azienda a un assicuratore si sostanzia sia tecnicamente sia economicamente attraverso parametri reciprocamente verificati e accettati di modo che entrambi arrivano ad un risultato conveniente e produttivo.

Recenti articoli economici in Italia e all'estero esprimono il fermento che si sviluppa attorno a questo argomento. La sicurezza dei fidi bancari è meglio garantita in dipendenza dell'ampiezza delle coperture assicurative a garanzia dell'attività economica dell'impresa e della certezza dei suoi profitti. Basilea 2 e successive hanno inserito tra i pilastri del sistema di valutazione (migliore valutazione = minori accantonamenti a garanzia) i "rischi operativi", di cui il rischio informatico è il principale attore.

In altri paesi europei, più avanzati nell'adeguamento alle nuove normative di Basilea 2 (B2), già il trasferimento dei rischi "informatici bancari" a copertura delle conseguenze finanziarie ed economiche è una realtà concretizzata in contratti assicurativi importanti, tali possibilità sono realizzabili anche in Italia nel prosieguo dell'adeguamento a tali normative da parte di tutte le Banche Italiane, le quali evidentemente non

si sono fatte ancora i conti in casa di quanto risparmierebbero con il miglioramento della valutazione B2 sugli accantonamenti propri.

In conclusione l'operazione di trasferimento dei rischi residuali rappresenterebbe una soluzione aziendalemente riconosciuta sia tecnicamente che economicamente valida e consistente.

## **I RISCHI TIPICAMENTE TRASFERITI AL MERCATO ASSICURATIVO**

Vengono tipicamente trasferiti i rischi immateriali definiti come :

### 1 – Danni Diretti, cioè le perdite sofferte dall'Azienda direttamente sorgenti dagli effetti di :

- **Programmi dannosi** (come virus, troyan, worm, spyware, black hole, etc..)
- **Errori degli operatori** (come scelta del programma, di settaggio firewall, trasferimento librerie, back-up, inizializzazione patch nei sistemi, etc...)
- **Errori delle società di servizio** (in genere una copertura accessoria)
- **Dolo dipendenti** (spyware, Bomba Logica, privacy, furto informazioni, etc..)
- **Dolo di terzi** (Hacker, cracker, cybercriminal, spionaggio industriale, malavita organizzata, D.O.S. etc...)

che abbiano cancellato, alterato o modificato i Data (programmi e dati sia propri che di terzi) e/o ridotto o arrestato l'attività di elaborazione e/o le attività connesse e conseguenti.

### 2- Danni Indiretti, quelli conseguenti ad uno degli eventi diretti sofferti e cioè i costi/ le perdite di :

- **profitto,**
- **marginie di contribuzione,**
- **marginie di intermediazione,**
- **spese fisse insopprimibili,**
- **spese extra,**
- **spese straordinarie**
- **difesa del Brand**
- **spese da interruzione telecomunicazioni**
- **privacy**
- **penalties**

Più raramente vengono trasferite anche le perdite patrimoniali e i danni diretti/indiretti sofferti a causa dei seguenti rischi (che sono già presenti in altre polizze di specifici segmenti di mercato):

- **- Frode**
- **- Infedeltà dipendenti**
- **- Risarcimenti da responsabilità professionali**
- **- Guasti macchine (macchinari industriali)**
- **- Perdite di merci in lavorazione (industria)**
- **- interruzioni di processi produttivi (Industria, energia)**

Riccardo Scalici  
Socio Fondatore del Clusit  
Senior Underwriter Dir. Technical Lines  
ACE European Group Ltd  
[riccardo.scalici@acegroup.com](mailto:riccardo.scalici@acegroup.com)