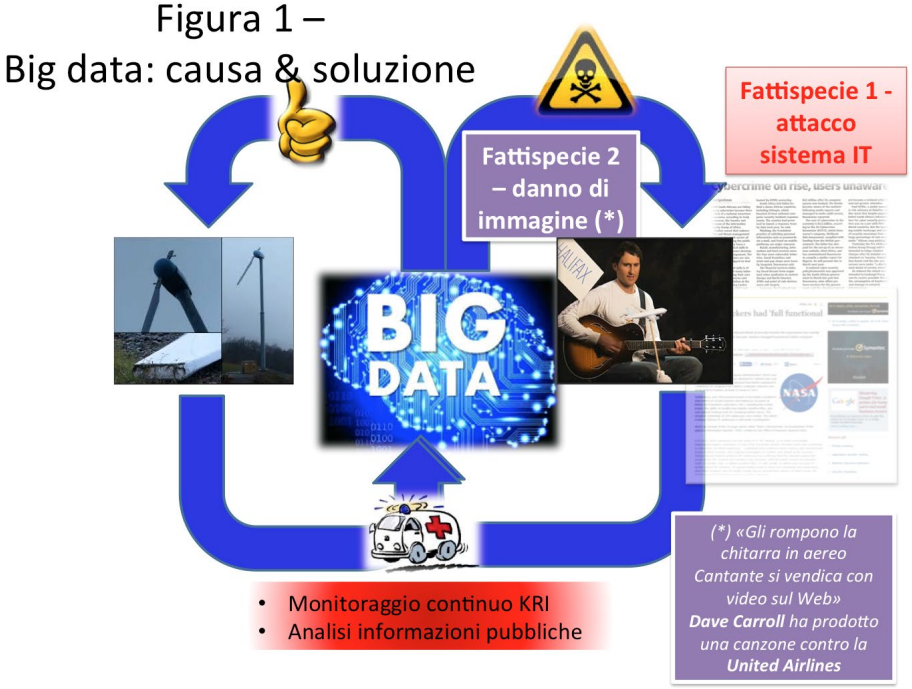
Big Data & Cyber Risks

Il secondo workshop tenuto al convegno ANRA ha visto al centro l'analisi e la trattazione del rischio informatico, con la presentazione dei casi concreti e di proposte per il controllo di questa particolare tipologia di rischio. Paola Luraschi, coordinatrice del workshop, propone la sintesi del proprio intervento

di **Paola Luraschi**
Principal Milliman
paola.luraschi@milliman.com

Secondo una recente pubblicazione del *'Center for strategic and economic studies'* il costo globale annuo dei cybercrime è in costante crescita ed in base ad una delle ultime stime (i.e. 400 miliardi di dollari) ha già superato il PIL di molti paesi. Da solo questo dato può spiegare perché il cyber risk sia diventato in poco tempo uno dei rischi più temuti ma anche meno conosciuti dalle aziende di tutto il mondo. Per tale ragione è opportuno fare un passo indietro chiedendosi che cosa sia il cyber risk. L'osservazione dei suoi effetti suggerisce che, alla stregua di altre tipologie di rischio (e.g. rischio operativo), il cyber risk è caratterizzato da eterogeneità di manifestazioni classificabili in due macro categorie: la prima identifica la fattispecie più comunemente associata al cyber risk e cioè tutti quegli eventi che attengono alla vulnerabilità dei sistemi IT aziendali, mentre la seconda - anche più rilevante in termini di impatto della prima - attiene al possibile danno di immagine derivante dall'utilizzo improprio di canali di comunicazione di massa. Il comune denominatore di entrambe le fattispecie di cyber risk è il ruolo ambivalente dei cosiddetti big data che sono da un certo punto di vista origine del problema ma anche elemento utile e, probabilmente, imprescindibile della sua soluzione come indicato in Figura 1.

Figura 1 –
Big data: causa & soluzione



Vale la pena citare un altro aspetto che accomuna il rischio operativo ed il cyber risk ed è la difficoltà di attingere a dati di perdita che siano robusti da un punto di vista statistico. Inoltre se anche esistesse la possibilità di attingere a dati storici di perdita robusti, un'analisi basata unicamente su di essi (quindi presupponendo la staticità di contesto che consente di dedurre quanto accadrà in futuro dall'osservazione del passato) non potrebbe comunque essere sufficiente per un fenomeno dinamico e in continua evoluzione quale è il cyber risk. Per le ragioni sopra citate una gestione efficace del cyber risk è subordinata al completamento / contestualizzazione dei dati storici con la conoscenza / capacità interpretativa del contesto di riferimento. Come nel caso del rischio operativo è possibile raggiungere tale scopo utilizzando un approccio olistico (i.e. un approccio che si proponga di conoscere, misurare e gestire il cyber risk in quanto elemento di un sistema dinamico con interazioni e condizionamenti esogeni al rischio stesso) con ricorso a KRI automatizzati e a modelli Bayesiani (i.e. modelli di quantificazione che riescono a sintetizzare e completare i dati oggettivi osservati nel passato con la expert opinion di contesto). Si veda Figura 2.

La possibilità di utilizzare i big data per concretizzare e coadiuvare modelli Bayesiani / approccio olistico può ridurre in modo significativo la rilevanza del rischio (i.e. ridurne impatto e probabilità) cogliendo al contempo le cyber opportunity. Si consideri a questo proposito il seguente esempio di gestione proattiva della fattispecie di cyber risk che attiene il danno di immagine e che riesce a trasformar-

Figura 2 –
Comprendere la complessità

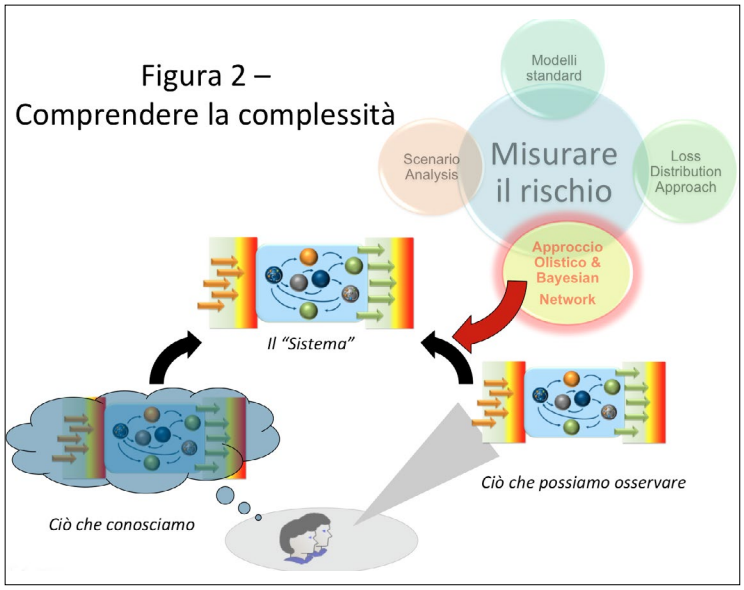
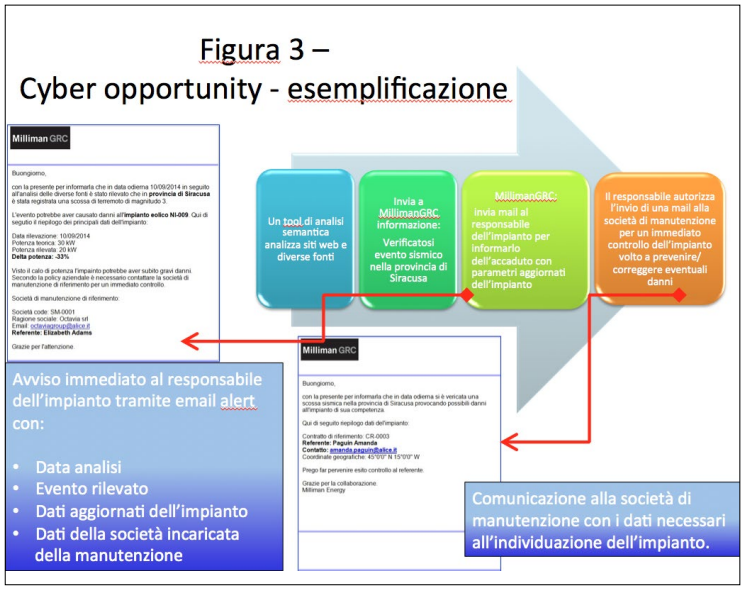


Figura 3 –
Cyber opportunity - esemplificazione



lo in opportunità di efficientamento reale del business. Si consideri a titolo di esempio una società che produce energia eolica. Si supponga di avere attuato con uno strumento ERM di automazione della governance e del risk assessment (quale ad esempio MillimanGRC) una gestione olistica dei rischi di tale società con un sistema di monitoraggio e governo automatizzato. Tale gestione ricomprenderà, in particolare, la gestione del cyber risk e quella del rischio di fermo impianto (i.e. mancata o ridotta produzione di energia eolica presso un impianto a causa di una guasto). Ipotizzando l'interfacciamento di MillimanGRC con un tool di analisi semantica si può pensare alla situazione in cui tale tool rileva tramite analisi delle informazioni disponibili in rete (big data) una scossa sismica di magnitudo ridotta che non ha prodotto danni rilevanti a cose / persone per cui la notizia, di interesse locale, non è stata e non verrà diffusa dai big media.

L'invio a MillimanGRC della informazione implica lo scandagliamento di MillimanGRC di tutte le possibili connessioni tra il fatto di cronaca e la vita aziendale con rilevazione della presenza di un impianto eolico dell'azienda proprio nelle vicinanze dell'epicentro del sisma. In questo caso vi sarebbe una segnalazione in tempo reale, da parte di MillimanGRC, tanto al responsabile interno della manutenzione aziendale quanto alla società esterna di manutenzione, della possibile presenza di anomalie nell'impianto in questione con conseguente immediata reazione preventiva del danno nella produzione. Questo esempio indica come l'analisi di big data pubblici al fine di individuare possibili fonti di danno di immagine, se opportunamente gestita e contestualizzata in un framework olistico di risk management, possa trasformarsi in opportunità di efficientamento del business come illustrato dalla Figura 3 .