

# Una materia per fronteggiare possibili scenari di rischio

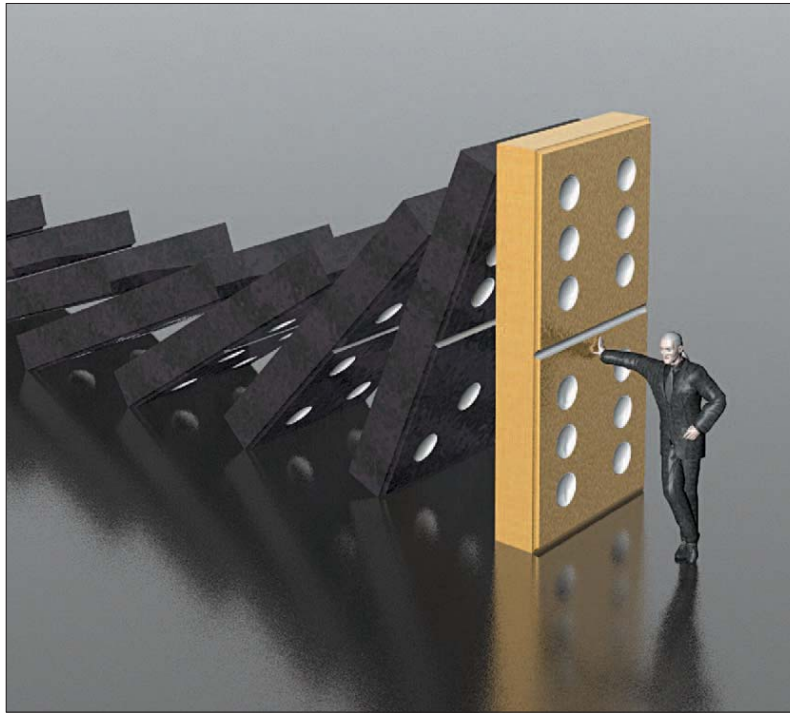
L'importanza di acquisire una capacità strategica per poter rispondere ad incidenti e continuare l'attività ad un livello accettabile.

**ANTHONY CECIL WRIGHT**  
SOCIO CLUSIT, PRESIDENTE ANSSAIF

Che cos'è la Business Continuity? Lo Standard BS25999-1 dà la seguente definizione "strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level". In pratica è una disciplina che mette in grado un'Azienda di adottare formalmente l'approccio reputato più idoneo a fronteggiare possibili scenari di rischio (ad esempio: un terremoto; un black-out; un incendio; un sabotaggio; ecc.), derivanti dal verificarsi di eventi casuali che, sfruttando le vulnerabilità di uno o più asset (sistemi informatici, infrastrutture; persone; ecc.), impediscono di ottemperare ad obblighi istituzionali o provocano danni in grado di influire sulla capacità dell'azienda di continuare la propria attività di business. In passato l'attenzione delle Organizzazioni era principalmente diretta alla salvaguardia del patrimonio informativo, mediante la progettazione e la realizzazione di soluzioni di Disaster Recovery, la cui caratteristica principale era la ridondanza dei supporti magnetici e la disponibilità, all'occorrenza, delle necessarie attrezzature informatiche e di comunicazione posizionate in un altro sito, la cui distanza dal sito primario era funzione dei possibili scenari di rischio. Oggigiorno generalmente le aziende si sono dotate di un piano di Disaster Recovery (DRP).

Gli investimenti sono stati assai elevati, così come lo sono i costi di gestione; infatti, i costi sono cresciuti in modo quasi esponenziale al diminuire del tempo massimo accettabile per la ripresa dell'operatività, interrotta da un evento imprevisto.

Il progetto per il DRP è stato generalmente portato avanti dalla funzione interna informatica. Come vedremo più avanti, la Business Continuity (BC), invece, coinvolge tutta l'Azienda: dalla fase di analisi dei rischi, alla valutazione dell'impatto economico di un'in-



terruzione coinvolgendo i "process owner", sino alla valutazione del Top Management sui rischi da accettare e quelli da mitigare. Non ultimo, in quasi tutte le realtà che hanno realizzato il piano di BC, lo sponsor aziendale è stato il Consiglio di Amministrazione (nel caso delle banche e degli intermediari finanziari, la normativa ne prevede già un forte coinvolgimento) e ciò ha assicurato un forte "commitment" di tutta l'Azienda ed un giusto equilibrio costi / rischi. Le soluzioni adottate si traducono, infine, in piani di continuità, nei quali sono descritti i ruoli, le responsabilità, le procedure da seguire, gli strumenti da utilizzare, e quanto altro serve per poter riprendere l'attività interrotta.

Trattasi perciò di un processo di ricerca di soluzioni condivise di limitazione dei danni, soprattutto preventive, ma anche di emergenza, consentendo l'operatività di quei processi di business che comporterebbero elevati danni econo-

mici già nelle prime ore di interruzione.

Se ritorniamo per un attimo al tema dei costi relativi al Disaster Recovery, come si può comprendere da quanto anzidetto, il tempo massimo accettabile di interruzione dell'operatività, ottenuto nel corso del ciclo di Business Continuity Management, è fondamentale per decidere quale soluzione di DRP adottare e, pertanto, è importante per un corretto equilibrio costi / rischi. Ciò spiega perché la Business Continuity include il DR.

L'attenzione alla BC e lo sviluppo della metodologia sono praticamente nati dopo l'11 Settembre 2001, e si sono perfezionati nel corso di questi ultimi anni.

Il tragico evento ha messo in luce, come sappiamo, alcuni fatti innovativi: l'accadere di un evento prima di allora giudicato assolutamente improbabile (uso di aerei da attentatori suicidi; due enormi grattacieli colpiti...); ma, soprattutto, la perdita di tante persone, oltre ad

uffici, sistemi e documenti cartacei.

Vi è stato anche un secondo evento, rappresentato dall'epidemia di SARS in Asia nel 2003.

Il numero di vittime è stato limitato, ma invece alto è stato il numero di Aziende che hanno dovuto interrompere improvvisamente le loro attività a causa dell'assenza di personale, in quanto ricoverato in ospedale o messo al domicilio coatto, in quarantena. Molte di queste sono fallite nei successivi due anni.

In Italia un grande impulso è derivato dall'esperienza che le Banche hanno fatto, a seguito dell'applicazione dell'accordo di Basilea sul capitale di rischio e alla normativa della Banca d'Italia, la cui preoccupazione - in linea con le altre Banche Centrali - deriva dai possibili impatti sul sistema finanziario italiano che si possono avere a seguito di eventi catastrofici.

Le banche, che hanno terminato nei tempi stabiliti i rispettivi progetti<sup>2</sup>, hanno messo a disposizione

un forte know-how basato sull'esperienza diretta. In particolare, si è potuto vedere che la maggioranza delle soluzioni di continuità adottate dalle Banche hanno sfruttato le persone e le infrastrutture esistenti, evitando così investimenti per duplicazioni.

In alcuni casi, sono stati formalizzati degli accordi con Società di Servizi in grado di prendere in carico parte dell'attività dell'Azienda. Molti di questi contratti non hanno richiesto l'esborso di somme anticipate.

Alcune significative esperienze consentono di affermare che implementare la BC non significa dover affrontare elevati investimenti.

Intensa deve invece essere, da parte dell'Azienda, l'attività di sensibilizzazione del personale sul tema della continuità operativa e la formazione atta a consentire di mantenere correttamente l'impianto di BC.

Infatti, siccome l'Azienda non è immobile, non è statica, gli impatti mutano, così come le vulnerabilità, il livello di esposizione al rischio, il livello di accettazione dei rischi ("risk appetite"), ogni anno, o ad ogni variazione organizzativa significativa, l'Azienda deve ripercorrere il ciclo di BC (analisi del rischio, valutazione degli impatti, ecc.).

Importante, oltre alla formazione, è anche la simulazione, in quanto consente di ottenere vari vantaggi: provare l'efficacia dei piani redatti, familiarizzare e sensibilizzare il personale, abituare a prevedere, e a prepararsi ad ogni evenienza. L'esperienza ha dimostrato che dei potenziali disastri sono rimasti a livello di incidente, contenendo i danni, grazie proprio a questo approccio e allo spirito di squadra che si era creato fra il personale operante sui processi critici e quello tecnico di intervento. ♦

<sup>1</sup> "capacità strategica e tattica di una organizzazione di pianificare e rispondere ad incidenti e gravi interruzioni del business al fine di poter continuare l'attività di business ad un livello accettabile predefinito" [Trad. dell'Autore].

<sup>2</sup> La normativa, emanata nel luglio 2004, ha previsto l'adeguamento della continuità operativa ai nuovi scenari entro il dicembre 2006.

## Il Premio Clusit per incoraggiare la ricerca universitaria

Al via la terza edizione del premio "Innovare la sicurezza delle Informazioni", riservato alle migliori tesi di laurea sulla materia. Il premio ha anche lo scopo di promuovere una collaborazione tra aziende, Università e studenti ed è già diventato un punto di scambio tra mondo produttivo e mondo scientifico, tra studenti e mondo del lavoro. Saranno premiate le 5 migliori tesi (2.000 Euro per il primo classificato). Per un approfondimento: <https://tesi.clusit.it/>

## Promozione, formazione e professionalità

Far crescere la cultura della sicurezza informatica in tutti gli ambiti è la missione primaria del Clusit. La tutela di una risorsa così critica come la rete dipende, infatti, dall'azione congiunta, consapevole e quotidiana di ciascuno, unita ad un alto livello di professionalità. Clusit organizza i seminari Clusit Education (<https://edu.clusit.it/>) e collabora alla realizzazione di oltre 50 convegni all'anno. Clusit è il partner scientifico della più importante manifestazione fieristica del settore: Infosecurity Italia ([www.infosecurity.it/](http://www.infosecurity.it/)), la cui prossima edizione è prevista a febbraio 2008.