Sinergie tra *cyber security, business continuity* e *disaster recovery*

di Fabrizio Cirilli e Gianluca Riglietti

Cybersecurity, Business Continuity e Disaster Recovery: cosa sono e come sono collegate tra loro?
Termini spesso abusati, senza troppa convinzione e con scarsi punti di riferimento - proviamo a mettere le basi per chiarire cosa sono e come sono collegati. La stampa e talvolta la letteratura specializzata confondono la terminologia, probabilmente per carenza di informazioni più dettagliate o per insufficienza di riferimenti certi. Purtroppo, questa confusione terminologica genera processi e attività incongrue a livello produttivo, determinando a volte situazioni di stallo disastrose con costi esorbitanti.
Negli ultimi anni sono emerse sempre più le sinergie tra *cyber security*, *business continuity* e *disaster recovery*. Ciò è dovuto a una crescente vulnerabilità degli *asset* digitali che nel tempo sono divenuti sempre più importanti. Nonostante si possa pensare che queste tre funzioni siano separate e distinte, in realtà è necessario che operino in allineamento, se non addirittura in simbiosi.
Come riportato dal BCI *Cyber Resilience Report* 2018, su un campione di oltre 500 organizzazioni da tutto il mondo, l'85% riporta l'implementazione di sistemi di *business continuity* per contrastare degli attacchi *cyber*. Questo non è sorprendente, dal momento che spesso le conseguenze di tali attacchi vanno a impattare su reputazione, comunicazione, finanze o sistemi ICT, tutti processi che possono beneficiare da un programma di *business continuity*. Un simile studio sulla continuità e la resilienza evidenzia inoltre come tra varie funzioni la *business continuity* figuri tra le tre più utilizzate, insieme a quella di *information security* e *business operations*.
Si sente sempre più spesso parlare del bisogno di sistemi olistici per garantire la sicurezza digitale delle organizzazioni e, di conseguenza, non è possibile pensare di adottare solo misure prettamente tecniche per contrastare delle minacce che, pur presentandosi tramite il mondo digitale, hanno ripercussioni molto reali sulle aziende. Basti pensare ai numerosi casi in cui ospedali, banche o centrali elettriche sono risultate vittima di attacchi, causando un'interruzione della vita quotidiana. In questo senso, il *business continuity management* adotta l'approccio olistico che per molto è mancato alla *cyber security*, curandosi del lato umano, comunicativo e organizzativo della risposta, ponendosi potenzialmente come coordinatore al centro di una crisi.
Una volta stabilita la connessione tra *cyber security* e *business continuity,* è importante individuare il ruolo del *disaster recovery*, che potrebbe essere considerato come una serie di soluzioni tecniche al servizio *della business continuity*, per garantire il ripristino delle soluzioni informatiche. Ad ogni modo, al fine di collocare meglio tali funzioni, la seguente sezione fornisce delle definizioni a riguardo.
Vediamo di chiarire innanzitutto le definizioni, da fonti certe:

- *Disaster Recovery* - L'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare, indisponibilità prolungate (fonte agid.gov.it);
- *Cyber Security* - La definizione di *Cyber Security* individua un ambito di applicabilità ben definito, riferito alla tecnologia informatica e delle telecomunicazioni; in ragione dell'evoluzione in atto, che tende alla progressiva digitalizzazione di ogni tipo di informazione, tale definizione punta a estendersi al mondo dell'automazione e dell'intelligenza artificiale, assumendo sempre di più attributi che riguardano il più ampio contesto dell'*Information Security* (fonte sicurezzait.gov.it).

Entrambe le definizioni fanno esplicito e diretto riferimento alle tecnologie ICT, diverso è per la *business continuity*:

- *Business Continuity* - un processo gestionale olistico che identifica potenziali minacce a un'organizzazione e gli impatti sulle attività che quelle minacce potrebbero causare, e che fornisce un quadro per costruire una resilienza organizzativa con la capacità di un'efficace risposta a un evento critico, che salvaguardi gli interessi degli *stakeholder* chiave, della reputazione, del *brand* e delle attività che creano valore (fonte ISO 22301:2019).

BCM e disaster recovery

BCM	Disaster recovery
E' un sistema di gestione con diverse fasi che punta a rendere un'organizzazione resiliente	E' una misura di risposta verso interruzioni legate al settore tecnologico
E' responsabile per la progettazione di soluzioni di continuità operativa	E' una soluzione che deriva dal sistema di gestione della continuità operativa
Non è una funzione strettamente legata alla tecnologia ma più ai processi	E' una funzione strettamente legata alla tecnologia

Appare chiaro che la BC si riferisce al *business*, all'organizzazione e non alla sola componente tecnologica dell'ICT. Ovviamente questa fa parte, in alcune aziende in modo determinante, del tema della BC ma non è la tecnologia a guidare il *business*, semmai ne è lo strumento.
Qualsiasi organizzazione ha l'esigenza di assicurare la propria continuità a fronte di vari scenari di crisi, derivanti da disastri naturali, pandemie o danni generati dall'uomo, volontari e non.
Il fattore determinante è probabilmente il rischio. Il rischio inteso come possibilità che un impatto indesiderato si verifichi portando a un'interruzione del *business* e provocando una serie di danni economici, finanziari, legali, reputazionali ecc.
È proprio la gestione del rischio al centro della BC e della *cybersecurity*. Il DR è invece una risposta tecnologica da attuare quando e se la BC non riesce a sostenere l'organizzazione come necessario.
Paradossalmente la BC può esistere senza un DR, mentre diventa più difficile immaginare il contrario. Anche riattivando un *data center* secondario quale uso posso farne se il *business* a cui era destinato viene meno?
La *cybersecurity* (un mix di sicurezza delle informazioni e sicurezza informatica) integra concetti di BC e DR in un quadro più ampio e strutturato, aggiungendo anche gli aspetti di protezione dei dati e *privacy*.
Ecco quindi l'apparente soluzione: la BC guida l'organizzazione nella gestione dei disastri, supportata dalla *cybersecurity* e dal DR. In quest'ottica la limitazione all'ICT si riduce e permette di beneficiare

dei vantaggi delle tre tematiche, senza farle confluire in un groviglio confuso di termini e attività.

Discussione

In tale contesto, si inseriscono delle pratiche chiave del *business continuity management* che possono contribuire in maniera pratica ad alzare i livelli di resilienza agli attacchi:

1. l'analisi d'impatto aziendale (*business impact analysis*), che consente di evidenziare i processi e i fornitori critici di un'organizzazione e comprendere le vulnerabilità interne;
2. le analisi di *horizon scanning* e dei rischi, che consentono di individuare le maggiori minacce alla propria organizzazione nel breve, medio e lungo periodo;
3. l'incorporazione di una mentalità resiliente partendo dal *top management*, per propagare una cultura di continuità su tutti i livelli;
4. la progettazione di soluzioni di continuità, come ad esempio il *back-up* di dati, basata sui risultati dell'analisi di impatto aziendale;
5. le esercitazioni e i test dei piani, per consolidare e migliorare il lavoro svolto.

Quando queste tematiche non funzionano? Ecco alcuni degli elementi che possono determinare l'insuccesso per la *cybersecurity*, per la BC e il DR:

- assenza del *Top management* e/o della proprietà come *sponsor*;
- *debole commitment*, progetto operativo anziché strategico;
- approccio *bottom up*, dal tecnicismo alla *governance;*
- assenza degli aspetti di monetizzazione del disastro (RPO, RTO, MTPD, MBCO ecc.);
- piani e procedure di continuità poco attuabili e/o scarsamente condivisi con tutte le parti interessate (inclusi clienti e fornitori principali);
- programmi di formazione e sensibilizzazione deboli, sporadici o del tutto assenti;
- verifiche operative occasionali e non mirate;
- assenza di rivalutazione periodica degli scenari di impatto e dei rischi correlati.

Fabrizio Cirilli
CEO & Founder PDCA Srl
Gianluca Riglietti
Head of Research and Intelligence Panta Ray Srl

SYNERGIES BETWEEN CYBER SECURITY, BUSINESS CONTINUITY AND DISASTER RECOVERY

Cybersecurity, Business Continuity and Disaster Recovery: What are they and how are they linked together?
Often abused terms, without too much conviction and with little reference points - let's try to lay the groundwork to clarify what they are and how they are connected.
The press and sometimes specialized literature confuse the terminology, probably due to a lack of more detailed information or a lack of certain references.
Unfortunately, this terminological confusion generates processes and activities that are incongruous at the production level, sometimes leading to disastrous stalemates with exorbitant costs.
In recent years, synergies between cyber security, business continuity and disaster recovery have increasingly emerged. This is due to a growing vulnerability of digital assets which over time have become increasingly important. More details in this article.