Creare lo scenario per investimenti nella business continuity e resiliency

Gli aspetti economici del rischio IT e di reputazione e la loro importanza per i professionisti della business continuity e resiliency

Approfondimento dello studio "IBM Global Study on the Economic Impact of IT Risk"

Indice

2 Introduzione
3 Benchmark per i business case
6 Lo stato attuale della business continuity
9 Un piano di azione per i professionisti della business continuity
10 In che modo IBM può essere di aiuto
11 Informazioni sullo studio

Introduzione

E' finito il tempo in cui i professionisti della business continuity erano focalizzati esclusivamente sulla ripartenza dei computer in seguito ad un importante evento disastroso. La continua disponibilità adesso è un requisito delle procedure di business continuity e resiliency. Particolare attenzione viene riservata alla prevenzione e non solo alla reazione, e il disaster recovery (DR) è soltanto una aspetto dell'argomento e di conseguenza, gli attuali professionisti della business continuity e resiliency hanno responsabilità particolarmente estese: garantire la fattibilità e la conformità del sistema, eseguire una corretta valutazione di fornitori, backup di dati e storage, gestire il budget e fissare le priorità.

Indipendentemente dalla responsabilità a cui vi state dedicando, non si può prescindere dalla valutazione dei costi. Coloro che sono stati intervistati sulla continuity e resiliency nel Global Study on the Economic Impact of information technology (IT) Risk, ritengono che le interruzioni al business e all'IT dovuti a guasti all'IT, nei prossimi 24 mesi, costeranno ad un'organizzazione £13M.

Creare il business case per le attività di continuity e resiliency è stato difficile dato che fino ad oggi, non sono stati disponibili dati dettagliati su tempi e costi del benchmark. L'IBM Global Study on the Economic Impact of IT Risk, tra i più ampi nel suo genere, raccoglie le interviste di 2316 professionisti nell'IT, 1069 dei quali specialisti della business continuity.

Ogni specialista di business continuity ha risposto a domande dettagliate sulle tipologie di guasti verificatisi nella propria organizzazione e le cause. Le loro risposte, presentate in questa loro analisi, possono fornire i dati di benchmark necessari per approfondire ulteriormente la propria strategia di gestione dei rischi per l'IT, dimostrare l'importanza della business continuity e resiliency e, in ultima analisi, creare il business case che giustifichi il budget e le risorse occorrenti per avere successo.

Le minacce e i loro costi

Per aiutare gli intervistati ad individuare i tipi di minacce che causano interruzioni al business e all'IT e i tipi di costi dovuti a queste minacce, l'IBM Global Study on the Economic Impact of IT Risk ha fornito un elenco delle minacce più comuni e delle categorie di costo per i professionisti di IT da prendere in considerazione. Agli intervistati è stato chiesto di valutare:

Sei minacce comuni

1. Errore umano (HE)
2. Guasto del sistema IT
3. Furto/Violazione della sicurezza informatica
4. Guasto di terze parti alla continuità o sicurezza dell'IT
5. Perdita di dati per esito negativo di operazioni di backup o ripristino
6. Eventi catastrofici naturali o da imputare all'uomo.

Sei categorie comuni di costi

1. Danno per la reputazione e il brand
2. Perdita di produttività dovuta al tempo di inattività o alle performance di sistema
3. Mancati guadagni dovuti a problemi di disponibilità del sistema
4. Analisi legali per stabilire le cause
5. Supporto tecnico per il ripristino dei sistemi
6. Costi per il mancato rispetto della conformità e delle normative.

Benchmark per i business case

Il business case per una migliore attività di continuity e resiliency si basa su un dato di fatto: le attività di continuity e resiliency hanno un valore per il business che non riguarda solo il back office ma l'intera azienda, dalla produttività del dipendente all'immagine e al marchio. Ha molto senso, quindi, dal punto di vista finanziario, investire prima nella progettazione di sistemi efficaci di protezione della continuity e resiliency dei sistemi IT, piuttosto che pagare per correggere gli errori dopo che si sono verificati.

Ecco, secondo quanto emerge dallo studio IBM, cosa hanno da dire i vostri colleghi della continuity e resiliency sui costi, le cause e i fattori di rischio. Queste rilevazioni, insieme alla potenziale spesa necessaria per ridurre e correggere gli errori, sono in grado di fornire i dati che mancavano nei precedenti business case.

Costo delle interruzioni in base al tempo

Il buonsenso suggerisce che maggiore è l'interruzione del business o dell'IT, maggiori saranno i costi. Tuttavia, c'è molto da imparare sulla durata di un'interruzione.

Gli intervistati sulla business continuity e resiliency hanno opinioni diverse su cosa costituisca un'interruzione di entità marginale, moderata e considerevole e questo può essere influenzato dal tipo di strategia di gestione del rischio adottata dall'organizzazione, sui livelli di tolleranza del settore oltre che dall'esperienza personale. (Vedere Figura 1.)

Oltre ad assegnare una specifica quantità di tempo per le interruzioni al business e all'IT di entità marginale, moderata e considerevole, gli intervistati hanno attribuito un importo per i prossimi 24 mesi. I professionisti della business continuity e resiliency hanno affermato di aver preventivato una spesa di £681.000 su interruzioni di entità marginale, £2.890.000 su interruzioni di entità moderata e £9.420.000 su interruzioni di entità considerevole. Anche se il costo per le interruzioni di entità considerevole sono una prova di buonsenso, è importante ricordare ai professionisti della continuity e resiliency che il 28 percento dei costi deriva da interruzioni di entità marginale e moderata, che tali interruzioni si verificano con maggiore frequenza e che oggi possono essere più facilmente evitate.

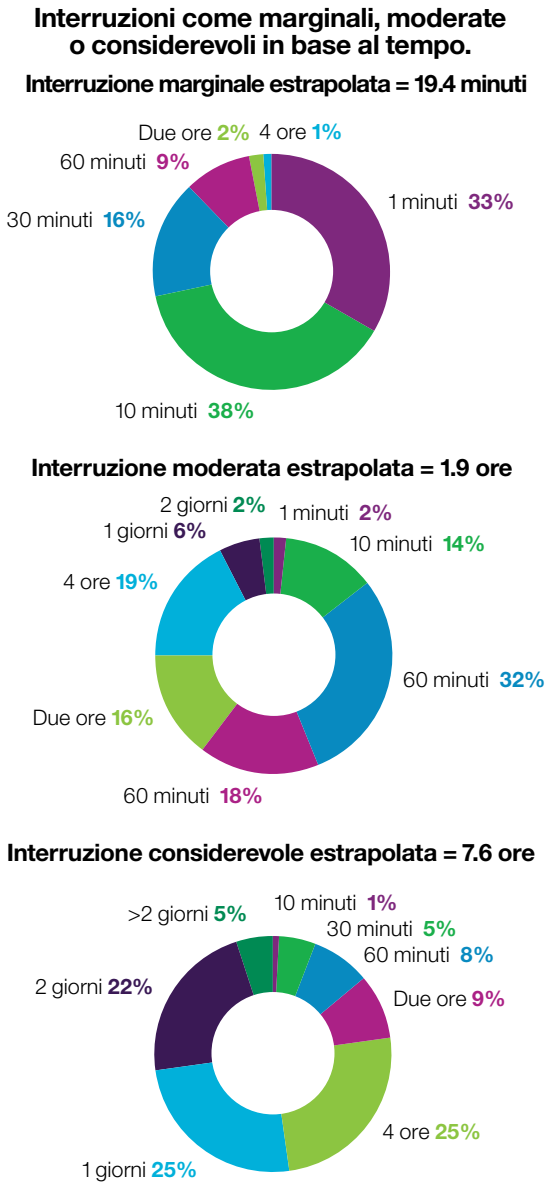


Figura 1. La variazione esistente tra la definizione da parte degli intervistati sul tema della business continuity e resiliency, di interruzioni di entità marginale, moderata e considerevole, può riflettere la tolleranza del rischio nel settore di appartenenza e l'esperienza personale.

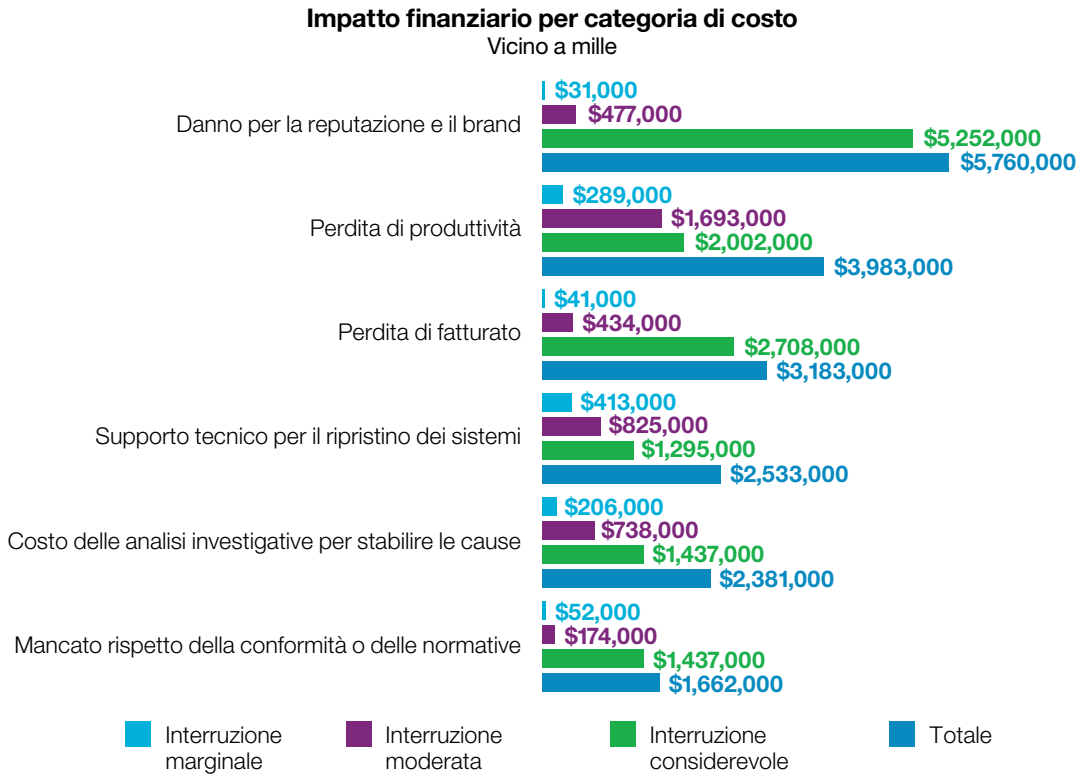


Figura 2. Ai professionisti della business continuity e resiliency viene chiesto di assegnare un costo relativo al malfunzionamento all'IT per sei categorie comuni. Il danno alla reputazione e al brand è la categoria più costosa per eventi di durata considerevole.

Costi per categoria

Nello studio condotto da IBM è stato chiesto ai professionisti della business continuity e resiliency di assegnare un prezzo a ciascuna delle sei categorie comuni di costo, per poi metterle a confronto con la durata del guasto.

Come è possibile vedere nella Figura 2, complessivamente la categoria più costosa è quella del danno alla reputazione e al brand, seguita dalla perdita di produttività e dalla perdita di fatturato. La categoria più costosa per gli eventi di minore durata è risultata essere quella del supporto tecnico. La perdita di produttività è risultata essere la categoria più costosa per gli eventi di media durata mentre il danno alla reputazione e al brand per gli eventi di maggiore durata.

E' interessante notare che la perdita di fatturato, la terza categoria generalmente più costosa, non è risultata essere tra le categorie più costose per durata di evento. Questo non significa che i costi attribuiti alla perdita di fatturato non siano importanti; infatti, i costi reali associati alla perdita di fatturato possono essere notevoli durante qualsiasi durata di un guasto all'IT. Quando la perdita di fatturato viene combinata con altri costi di business (danno alla reputazione al brand, perdita di produttività e mancata conformità e rispetto delle norme), questi costi di business rappresentano il 75 percento pari a £9.5M dei costi totali sostenuti, con un ulteriore rafforzamento del business case.

Attualmente la business continuity è tutta incentrata sulla disponibilità continua e su tecniche proattive per proteggere tale disponibilità.

– Paige A Poore, Director, Worldwide IBM Business Continuity

Perché si verificano le interruzioni: fattori di rischio per l'IT

Nessuna verifica dei costi legati ai guasti all'IT sarebbe completa senza rispondere alla domanda: "Cosa sta causando tali guasti?" La Figura 3 mostra i risultati dei professionisti della continuity e resiliency che valutano i sei più comuni fattori di rischio per l'IT in base all'impatto economico, l'impatto sulla reputazione e le probabilità che accadano.

L'errore umano è la causa più frequente di interruzione al business e all'IT e con l'impatto economico più significativo. Questo è vero sia nell'IT che tra gli utenti generici. L'errore umano è anche la causa dell'82 percento in più dei danni alla reputazione di quanti i professionisti di continuity e resiliency hanno pronosticato.

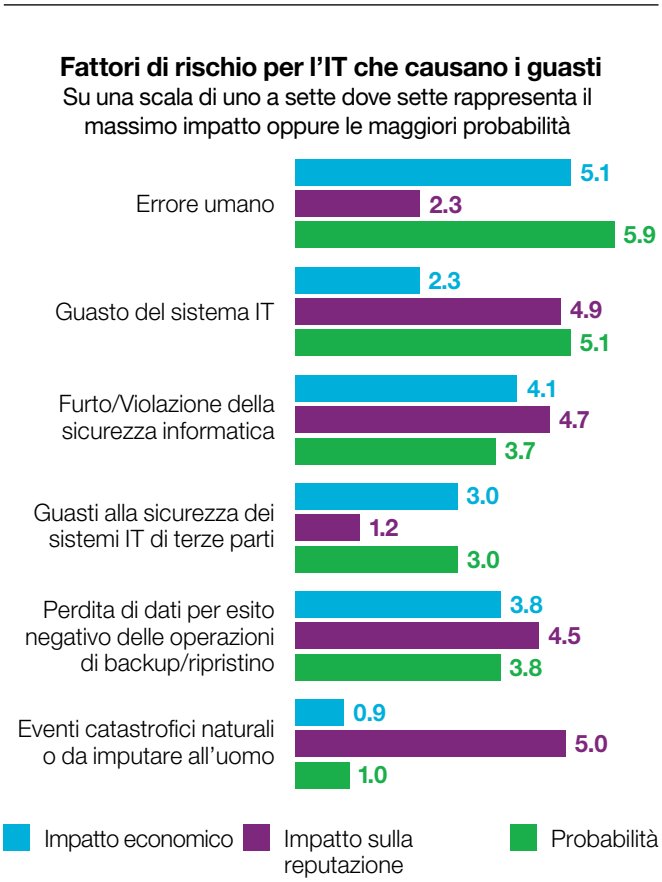


Figura 3. L'errore umano è il fattore di rischio per l'IT con il maggiore impatto economico e con la più elevata probabilità che si verifichi, secondo gli intervistati sul tema della business continuity e resiliency nell'"IBM Global Study of the Economic Impact of IT Risk".

Il modo migliore per evitare l'errore umano è implementare l'automazione nell'azienda. Può avere la forma della virtualization, del backup gestito e fornitura in cloud delle risorse di sistema, software e dati. Il backup automatico per singoli utenti e la fornitura attraverso il cloud di software e dati possono aiutare anche a ridurre le interruzioni al business e all'IT dovute alla perdita o alla erronea codifica dei dati, per non parlare della possibile riduzione dei costi richiesti dal supporto tecnico.

Il guasto al sistema IT si trova al secondo posto per i professionisti della continuity e resiliency intervistati nell'IBM Global Study of the Economic Impact of IT Risk, sia per probabilità che per conseguenze sulla reputazione di un'organizzazione. Il primo posto per l'impatto sulla reputazione viene assegnato agli eventi disastrosi naturali o imputabili all'uomo, mentre gli stessi eventi disastrosi si trovano all'ultimo posto per impatto economico e probabilità di accadimento.

La dicotomia esistente per gli eventi disastrosi tra i punteggi relativi all'impatto sulla reputazione, all'impatto economico e alle probabilità, rappresenta un buon esempio per cui è importante includere tutti e tre gli aspetti nell'analisi del proprio business case. Le notizie riportano rapidamente i problemi legati all' IT di un'organizzazione dovuti ad esempio una grande tempesta o un importante guasto al sistema, cosa che fa percepire gli eventi disastrosi come particolarmente influenti sulla reputazione. Ma dato che gli eventi disastrosi non si verificano con grande frequenza nelle singole organizzazioni, si potrebbe richiedere lo stanziamento di un budget ridotto rispetto a quello assegnato in passato.

Lo stato attuale della business continuity

Negli ultimi anni, c'è stato un importante cambiamento nelle attività di business continuity e resiliency. E' diminuita la focalizzazione sul DR e sulla risposta ai problemi. Il DR ora è soltanto una parte della business continuity e resiliency, mentre la focalizzazione è passata dalla reattività alla prevenzione.

Tuttavia, i programmi di business continuity e resiliency di molte organizzazioni hanno ancora molto lavoro da fare. Soltanto il 20 percento dei professionisti della business continuity e resiliency dice che il programma di gestione o le attività di business continuity sono pienamente mature, mentre il 13 percento non è riuscito a determinarne la maturità. Il danno alla reputazione e al brand è la categoria dal costo più elevato, ma soltanto il 35 percento dei professionisti della continuity e resiliency afferma che i leader della loro organizzazione riconoscono che i rischi per l'IT influiscono sull'immagine del brand.

La strategia è essenziale

Ogni programma maturo di continuity e resiliency ha bisogno di una strategia forte e coerente. Eppure, soltanto il 17 percento degli intervistati ha una strategia formale applicata nell'azienda mentre il 29 percento non ha alcuna strategia. Anche se creare o rafforzare la propria strategia di continuity e resiliency può essere molto impegnativo, esistono degli strumenti in grado di aiutare.

Uno degli strumenti è l' IBM Business Continuity Index. L'Index mostra una serie di domande online sulle attività di continuity e resiliency, fornisce un'analisi delle aree più mature della propria strategia di business continuity e mette in luce gli elementi su cui sarebbe necessario porre maggiore attenzione.

Confrontare la percezione della minaccia per l'IT con la realtà

E' fondamentale garantire che la strategia di continuity e resiliency della propria organizzazione e il business case siano basati sulla realtà dei fatti piuttosto sulla loro percezione.

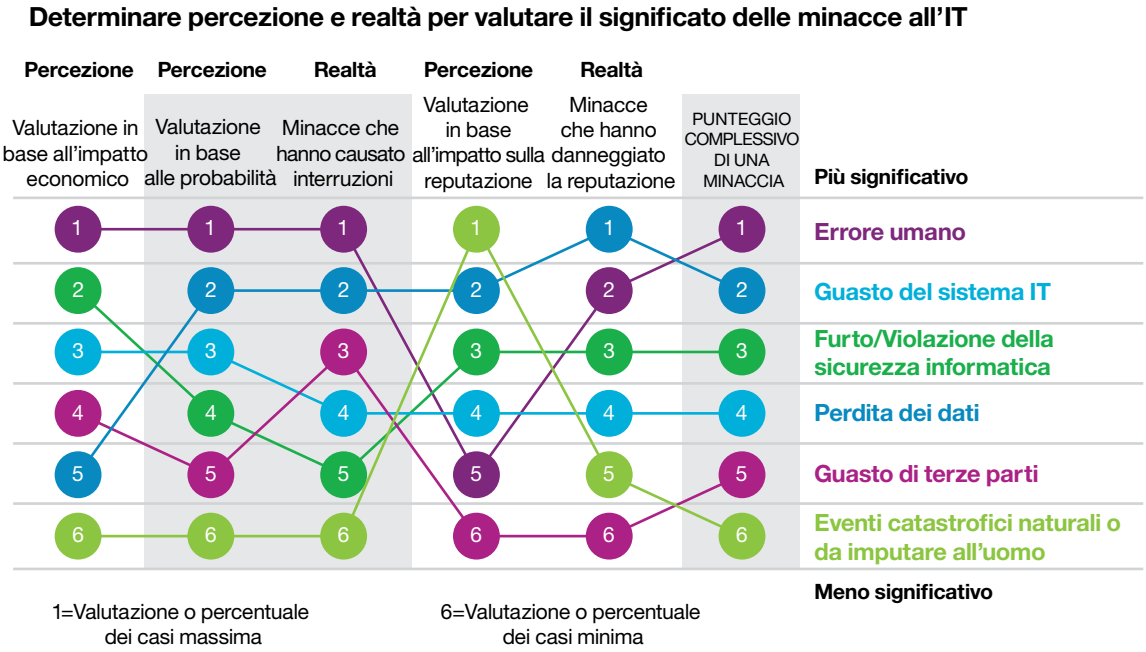


Figura 4. Confrontando le valutazioni espresse dagli intervistati sul tema della business continuity e resiliency sulle possibili minacce all'IT con l'effettivo verificarsi di tali casi, emerge un quadro più realistico dell'importanza della minaccia.

Come è possibile vedere nella Figura 4, le sei minacce più comuni per l'IT vengono stabilite in base alla percezione del loro impatto economico, alle probabilità che accadano e all'impatto sulla reputazione, insieme alla frequenza con cui tali minacce hanno effettivamente causato interruzioni e danni alla reputazione negli ultimi 24 mesi. Ne consegue che l'errore umano e i guasti al sistema rappresentano le prime due minacce per l'IT. Allo stesso tempo, viene presentato l'elevato divario tra la percezione dell'impatto degli eventi disastrosi naturali e imputabili all'uomo sulla reputazione e l'effettivo peso di tali minacce.

L'avvento di terze parti

Recentemente sta aumentando il contributo di terze parti ad una serie di funzioni di business all'interno di un'organizzazione. Insieme ai contributi positivi, le attività di terze parti potrebbero comportare nuovi rischi per l'IT. Dal momento che le organizzazioni attuali stanno formando macrocosmi di partner, vendor, fornitori e consulenti sempre più grandi e connessi, è necessario che anche queste terze parti forniscano lo stesso livello di riduzione del rischio di IT, poiché ciò che l'organizzazione applicherà internamente diventerà sempre più rilevante.

Attualmente, i pericoli peggiori sono gli eventi disastrosi, ma le minacce più grandi sono rappresentate dagli eventi più comuni come l'errore umano e l'interruzione del sistema.

– Laurence Guihard-Joly, Global General Manager, IBM Business Continuity and Resiliency Services

I rischi per l'IT influiscono sulla reputazione

La reputazione del brand e dell'azienda è fondamentale in un'organizzazione e oggi l'IT può contribuire a proteggerla. Secondo l'IBM Global Study on the Economic Impact of IT Risk, i professionisti della continuity e resiliency affermano che negli ultimi 24 mesi, i guasti al sistema rappresentano la minaccia per l'IT che rappresenta l'impatto più elevato sulla reputazione. Ad amplificare questi dati si noti che, secondo le rilevazioni del 2012 IBM Global Study of Reputational Risk and IT, il danno di immagine è quello di durata più elevata tra quelli in cui un'organizzazione può incorrere, richiedendo oltre sei mesi per essere recuperato. La minaccia di guasti al sistema IT può essere ridotta attraverso un'adeguata pianificazione, frequenti attività di test e l'automazione di task quali il backup e l'aggiornamento dei sistemi operativi e del software.

Valutare le procedure legate al rischio per la reputazione

Quando si parla dell'impatto dei rischi di IT sull'immagine del brand e la reputazione, la vostra organizzazione è esposta, consapevole o capace? La soluzione IBM Reputational Risk Index può aiutarvi a scoprirlo. Rispondete ad alcune domande online e questo strumento vi fornirà in modo semplice e rapido una valutazione delle vostre attività di gestione del rischio per l'IT e la reputazione, i punteggi ottenuti nelle categorie di gestione del rischio e i consigli per migliorare.

La risorsa dell'outsourcing

L'outsourcing e la consulenza stanno diventando risorse sempre più importanti per una solida business continuity e resiliency. Il motivo per cui i reparti IT stanno cercando aiuto esterno è chiaro: hanno bisogno di maggiori competenze, larghezza di banda o di entrambe le cose. Ne è la prova il fatto che il 49 percento degli intervistati sulla continuity e resiliency ha affermato che la loro organizzazione non aveva superato una verifica interna o esterna. Nel periodo in cui veniva condotto questo studio, il 34 percento degli intervistati stava esternalizzando le proprie attività di gestione di business continuity e un ulteriore 18 percento affermava che probabilmente l'avrebbe fatto nei successivi 18 mesi. L'outsourcing e la consulenza sono ancora più interessanti, grazie alla disponibilità di una gamma di opzioni adattabili alle esigenze di ciascuna organizzazione che comprendono workshop di pianificazione e strategia, attività di valutazione e consulenza fino ad arrivare all'outsourcing completo.

Un piano di azione per i professionisti della business continuity

Dare voce alle conseguenze sia di tipo economico che di reputatione del rischio di IT è un'opportunità di successo per lei e per la sua organizzazione. L'organizzazione può avere un nuovo importante punto di vista tramite cui filtrare le strategie correlate al rischio di IT. Inoltre, le è possibile farsi conoscere come un esperto di tecnologia con una particolare attenzione alla produttività e di conseguenza con una maggiore visibilità.

Sulla base dei risultati ottenuti da questo studio, IBM offre sei procedure che aiutano a creare una casistica per spesa dedicata alla business continuity e alla resiliency e per conseguire risultati concreti. Alcune di queste procedure sono suggerimenti che abbiamo fornito negli ultimi cinque anni dedicati allo studio sui rischi per l'IT e alla pubblicazione dei report. Gli altri si basano sulle nuove informazioni e l'approfondimento dei dati emersi da questo studio. Con entrambi, speriamo di aiutare ad elevare la discussione sulla continuity e resiliency nelle organizzazioni e a fornire informazioni essenziali sul rischio per la reputazione e l'errore umano.

Portare il messaggio sul rischio per la reputazione ai leader aziendali

Fino a due terzi degli intervistati crede che i propri leader non abbiano compreso che le interruzioni al business e all'IT possono danneggiare seriamente la reputazione e l'immagine del brand e comportare un aggravio dei costi. E' quindi importante aiutare questi leader a conoscere le conseguenze sulla reputazione dei guasti all'IT e diventare con i propri colleghi i professionisti di IT in grado proteggere questo importante asset aziendale.

Realizzare un business case per gli investimenti di IT

Dato che il 75 percento dei costi legati ai guasti dell'IT sono da attribuire al danno sulla reputazione e alle performance di business, è evidente che si hanno a disposizione dei fatti concreti su cui costruire un business case in grado di finanziare la business continuity e resiliency. Ai CFO e agli executive delle business unit vengono solitamente presentate richieste di budget in termini di progetti e costi. E' necessario avere un approccio diverso. Bisogna associare la spesa richiesta dalla continuity ad obiettivi di business quantificabili quali l'incremento della produttività e del fatturato e la protezione della reputazione e del valore del brand.

E' necessario sviluppare dei parametri per la riduzione dei rischi per l'IT

Per supportare un business case, è necessario sviluppare parametri in grado di correlare i risultati delle iniziative di riduzione dei rischi al miglioramento dei risultati di business. In verità, è più difficile di quanto sembri perché non è facile misurare un risultato di un'azione preventiva o di un'attivtà fatta meglio e più rapidamente. Una strategia vincente potrebbe essere quella di assumere un approccio"outside in" individuando innanzitutto gli obiettivi di business che la leadership vuole conseguire e poi determinando cosa misurare e come, in modo da poter vedere i risultati delle attività di riduzione del rischio.

Ridurre le possibilità di errore umano

L'errore umano è la causa principale delle interruzioni al business e all'IT. E' preferibile valutare soluzioni di automazione in un contesto di riduzione delle possibilità di errore umano piuttosto che tagliare i costi per l'IT. Per esempio, rendere automatico il backup di tutte le piattaforme utente e server potrebbe risolvere una serie di errori umani che possono comportare la perdita dei dati, quali ad esempio configurare in modo non corretto il backup del software, dimenticare di eseguire il backup o persino perdere un notebook.

Gestire la collaborazione

Il 41 percento dei professionisti impegnati nella business continuity e resiliency che sono stati intervistati afferma che la collaborazione tra le diverse funzioni nell'organizzazione di supporto alla gestione della business continuity è insufficiente o addirittura inesistente. Dato che le tecnologie diventano sempre più complesse e i rischi per l'IT tendono a sovrapporsi, la collaborazione è particolarmente importante.

Cercare un aiuto esterno

Collaborare con esperti esterni che hanno un diverso punto di vista può aiutare ad affrontare in modo nuovo vecchi problemi e ad identificare i nuovi problemi che stanno emergendo insieme alle nuove tecnologie. I consulenti di IT possono aiutare a determinare una strategia per la riduzione dei rischi di IT, sviluppare un piano di implementazione e creare un business case. Possono aiutare inoltre le organizzazioni a determinare quali componenti della business continuity e resiliency possono essere gestite in modo più efficace da un service provider di IT dotato delle competenze, risorse o tecnologie più elevate. Per le organizzazioni più piccole che hanno difficoltà assicurarsi specialisti esperti o in settori come quello sanitario dove i reparti IT sono relativamente più compatti, utilizzare servizi gestiti per la gestione di tutta la business continuity può essere una buona scelta.

In che modo IBM può essere di aiuto

La strategia e la gestione della business continuity possono diventare uno straordinario vantaggio competitivo quando sono pianificate e implementate in maniera efficace. Mentre ci si protegge e si riducono i rischi, si può anche migliorare il valore del brand di fronte a clienti, partner e analisti. Inoltre, l'organizzazione può attrarre nuovi clienti, conservare i clienti attuali e generare maggiore fatturato.

Per avere un quadro completo dei rischi per il proprio business, occorre iniziare un IT Risk Management Workshop. I consulenti IBM collaboreranno per fornire una valutazione esaustiva dei rischi ai diversi livelli del proprio business: processi, tecnologie, applicazioni, dati ed anche infrastruttura e strutture fisiche dell'IT. Un workshop Continuous Operations Risk Evaluation (CORE) aiuta ad individuare le funzionalità di un'organizzazione che possono assicurarle operazioni di business senza interruzioni. Per gestire la resilienza in tutta l'azienda, i nostri IBM SmartCloud Resilience Service offrono servizi gestiti on-demand, basati sul cloud e in grado di proteggere senza ulteriori costi i dati, le applicazioni e le operazioni dall'inattività e a ripristinare rapidamente i dati e le operazioni, nel caso in cui si verifichi un'interruzione.

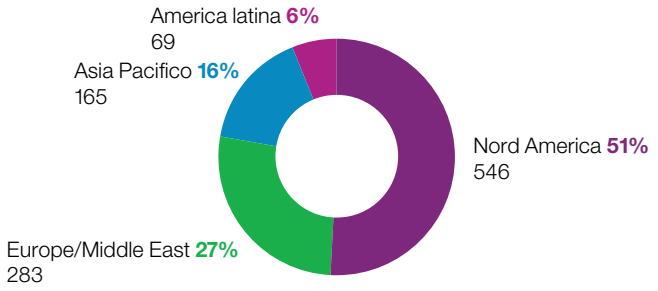
Informazioni sullo studio

L'IBM Global Study on the Economic Impact of IT Risk è uno dei più importanti studi indipendenti finora condotti per valutare le conseguenze finanziarie e di reputazione dovute a interruzioni IT causate da un problema alla business continuity o da violazioni della sicurezza dell'IT. Lo studio, un supplemento al 2013 IBM Reputational Risk and IT Study, è stato sponsorizzato da IBM e condotto in modo indipendente dal Ponemon Institute®, nel luglio 2013.

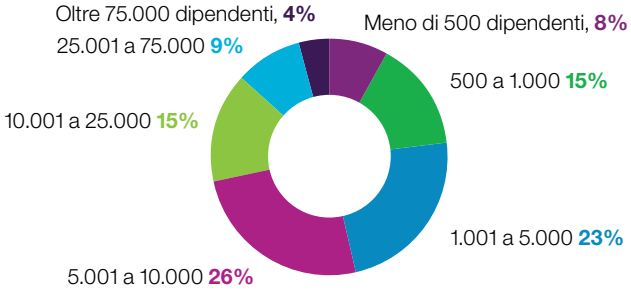
La partecipazione è stata limitata ai professionisti IT il cui lavoro si incentra sulla business continuity, la sicurezza IT o su entrambe le aree, con responsabilità decisionali o correlate alle performance. Per questa specifica analisi della ricerca, sono state incluse nei dati soltanto le risposte dei professionisti di business continuity.

Totale degli intervistati sulla business continuity: 1.069

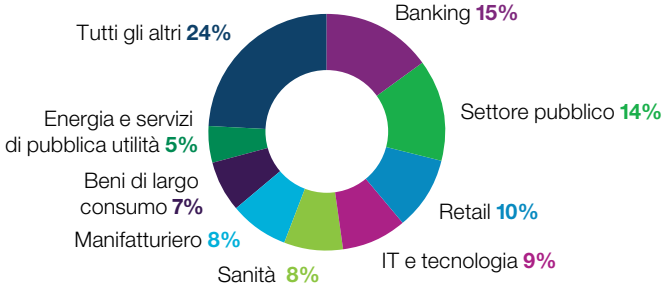
Sede (35 Paesi)



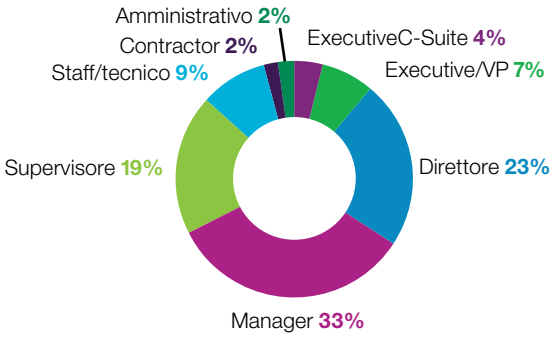
Dimensioni azienda (dipendenti)



Settori



Qualifiche professionali



Lo studio "IBM Global Study on the Economic Impact of IT Risk", condotto in modo indipendente da Ponemon Institute, ha raccolto informazioni da 1.069 professionisti impegnati nella business continuity e nella resiliency provenienti da tutto il mondo.

Ulteriori informazioni

Per ulteriori informazioni su come IBM può aiutare a proteggere un'organizzazione potenziando la business continuity e resiliency, contattare il responsabile commerciale IBM o il Business Partner IBM (BP), oppure visitare il sito web al seguente indirizzo: **ibm.com**/services/continuity

Partecipate alla discussione sulla business continuity

Per approfondimenti sullo studio "IBM Global Study on the Economic Impact of IT Risk", visitare: **ibm.com**/services/riskstudy

IBM Business Continuity Index
ibmbusinesscontinuityindex.com

IBM Reputational Risk Index
ibmriskindex.com

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

RLW03026-ITIT-01