



Acronis Global Disaster Recovery Index 2011

Classifica internazionale annuale relativa alla fiducia delle aziende rispetto a preparazione, capacità e procedure di backup e ripristino. In collaborazione con Ponemon Institute.

DR Index 2011

Copyright © Acronis, Inc., 2000 – 2011



Sommario

Riepilogo esecutivo	3
Cos'è la classifica Acronis Global DR Index?	4
Formato dell'indagine	4
Le classifiche: i livelli di fiducia in tutto il mondo	5
Principali risultati per regione: alla conquista dell'Oro	6
I più fiduciosi: Germania e Paesi Bassi (e la Svizzera)	6
Livello di fiducia successivo ai leader: Singapore, Hong Kong e Giappone	6
La nordica terra di mezzo	7
Chi resta indietro: Regno Unito, Australia e Stati Uniti.....	7
Spazio per crescere: Francia e Italia.....	8
Principali risultati globali: le tendenze a sostegno della fiducia	9
Primo risultato - La fiducia nel ripristino d'emergenza inizia dall'alto: i primi in classifica hanno il maggiore sostegno da parte dei team dirigenziali	9
Secondo risultato - La scarsità di investimenti in strumenti e risorse diminuisce la fiducia.....	10
Terzo risultato - I leader della classifica sono organizzati meglio e subiscono in misura inferiore le conseguenze dell'inattività	11
Quarto risultato - In testa alla classifica si trovano i paesi che dichiarano il maggior numero di server virtuali; sono anche quelli che eseguono con maggiore frequenza il backup di tali server.....	12
Quinto risultato - Nel 2011 l'impiego del cloud raddoppierà, ma i dubbi restano	14
Sesto risultato - Tutte le aziende ritengono complessa l'esecuzione del backup e del ripristino d'emergenza in un ambiente ibrido	16
Consigli per il backup e il ripristino d'emergenza: il punto di vista dello sponsor della ricerca	18
Appendice 1: Grafico: Livello nell'azienda e canale di riferimento dell'intervistato.....	19
Appendice 2: Suddivisione degli intervistati per paese	19
Appendice 3: Grafico: Comparti di appartenenza degli intervistati	19
Appendice 4: Domande utilizzate nel sondaggio.....	20

Riepilogo esecutivo

Cenni preliminari

La capacità di adattamento è un aspetto essenziale per tutti i paesi che prendono parte a un'economia internazionale altamente competitiva. Le organizzazioni di tutto il mondo traducono questo nella capacità di rimanere operativi anche in seguito a un guasto IT o a un'emergenza di grave entità, sia essa provocata dall'uomo o naturale.

Indipendentemente dal luogo in cui si trovano, i responsabili IT condividono una sfida: mantenere al sicuro e funzionali i dati e i sistemi aziendali strategici. Sono poche le aziende che possono oggi superare una grave perdita di dati senza aver previsto una strategia di backup e ripristino d'emergenza completa.

Intanto, la quantità di dati creati dalle aziende supera la loro capacità di immagazzinarli. The Economist stima che la quantità di informazioni create cresce ogni anno di un valore complessivo pari al 60%. Questa visione è supportata dagli analisti di IDC: secondo le loro previsioni, 'l'universo digitale' raggiungerà gli 1,8 zettabyte (1,8 miliardi di terabyte) nel 2011, con un aumento del 47% a partire dal 2010, e punterà ai 7 ZB entro il 2015.

Con l'adozione della virtualizzazione e con la tendenza crescente verso il cloud, le strategie di ripristino d'emergenza diventano sempre più complesse. Dai responsabili IT ci si aspetta ormai che i dati vengano conservati al sicuro anche negli ambienti ibridi costituiti da infrastrutture fisiche, virtuali e cloud. La tendenza ha fatto sì che le aziende adottassero svariate soluzioni di backup in diversi momenti del tempo. Sebbene sia normale che esistano in un'azienda due o tre soluzioni di backup differenti, non è raro che ce ne siano addirittura cinque o sei. Evidentemente, un mondo ibrido è anche un mondo molto complicato.

Al di là delle complesse problematiche a cui questo porterebbe, non esiste uno standard globale per il backup e il ripristino d'emergenza. Il rapporto Acronis Disaster Recovery Index dimostra che i paesi del mondo hanno diversi livelli di fiducia verso il ripristino d'emergenza, a seconda della loro cultura, dell'adozione di nuove tecnologie, della fiducia nelle procedure di backup e del sostegno e comprensione da parte del team dirigenziale. Lo studio ha identificato che le caratteristiche richieste a un'azienda affinché mostri fiducia nell'eccellenza delle proprie procedure di backup e ripristino sono estremamente variegata.

Tuttavia, su un punto tutti i paesi concordano: desiderano una singola soluzione di backup e ripristino d'emergenza che possa facilmente e in modo affidabile coprire tutte le esigenze dei loro ambienti ibridi.

L'economia globale è entrata in un periodo di crescita dei dati senza precedenti che sollecita in modo anch'esso senza precedenti l'infrastruttura IT. Grazie a una comprensione più dettagliata di ciò che fa eccellere le nazioni nella classifica Acronis Global Disaster Recovery Index, gli altri paesi dell'elenco potranno identificare le tendenze delle best practice e adottare percorsi simili per migliorare la propria strategia di ripristino d'emergenza. Potranno altresì confrontarsi coi propri pari nel paese di appartenenza.

Cos'è la classifica Acronis Global DR Index?

Acronis Global DR Index è un barometro annuale che genera una classifica dei paesi rispetto ai livelli di fiducia e alle capacità di backup e ripristino d'emergenza delle aziende di tutto il mondo. Lo scopo della classifica è di offrire a tutte le aziende una migliore comprensione del modo in cui le proprie fiducia e capacità si confrontano con quelle di aziende di pari livello in altri paesi. Sebbene l'atteggiamento e le percezioni rispetto alla fiducia varino da paese a paese, la classifica fornisce a tutte le aziende un modello di tendenze e strategie in grado di migliorare la fiducia e le capacità delle strategie di backup e ripristino d'emergenza.

La classifica si fonda su uno studio commissionato da Acronis ed eseguito da Ponemon Institute, una società di ricerca internazionale nonché affermato think-tank sulle tendenze relative alla protezione dei dati. La ricerca si basa sulle risposte di oltre 3.000 professionisti IT in Australia, Francia, Germania, Hong Kong, Italia, Giappone, Paesi Bassi, Norvegia, Singapore, Svezia, Svizzera, Regno Unito e Stati Uniti. È stata realizzata su una vasta gamma di aziende. (Appendice 1, 2 e 3).

Formato dell'indagine

Per l'indagine è stata impiegata una combinazione di metodi di campionamento online, complessivi e personalizzati, con modelli proprietari che hanno incluso professionisti IT qualificati di aziende di piccole e medie dimensioni (società della fascia media di mercato che non superano i 1.000 lavoratori). Tutte le fasi della ricerca – condotta tra il settembre e l'ottobre del 2010 - sono state portate a termine dal Ponemon Institute.

Per creare la classifica, a ciascun paese è stata assegnata una posizione basata sulle risposte complessive a 11 domande relative a preparazione, capacità e pratiche di backup e ripristino d'emergenza (Appendice 4). Le domande miravano a valutare la fiducia dei responsabili IT rispetto alle strategie di ripristino d'emergenza in base alla loro abilità e volontà di adottare nuove tecnologie; fiducia nelle procedure e nelle politiche applicate; livello di sostegno da parte del team dirigenziale; capacità di ripristino in tempi rapidi dopo un periodo di inattività.

Ad ogni partecipante è stato assegnato un punteggio ponderato per ciascuna risposta:

Completamente d'accordo con un'affermazione	5
D'accordo con un'affermazione	2.5
Neutrale	0
In disaccordo con un'affermazione	-2.5
Completamente in disaccordo con un'affermazione	-5

Il punteggio medio di tutte le regioni è risultato 1 mentre i punteggi dei singoli paesi variano considerevolmente da un punteggio massimo pari a 2,08 (molta fiducia) e un punteggio basso e negativo pari a -0,92 (fiducia totalmente assente).

* Non oltre 500 in Asia.

Le classifiche: i livelli di fiducia in tutto il mondo

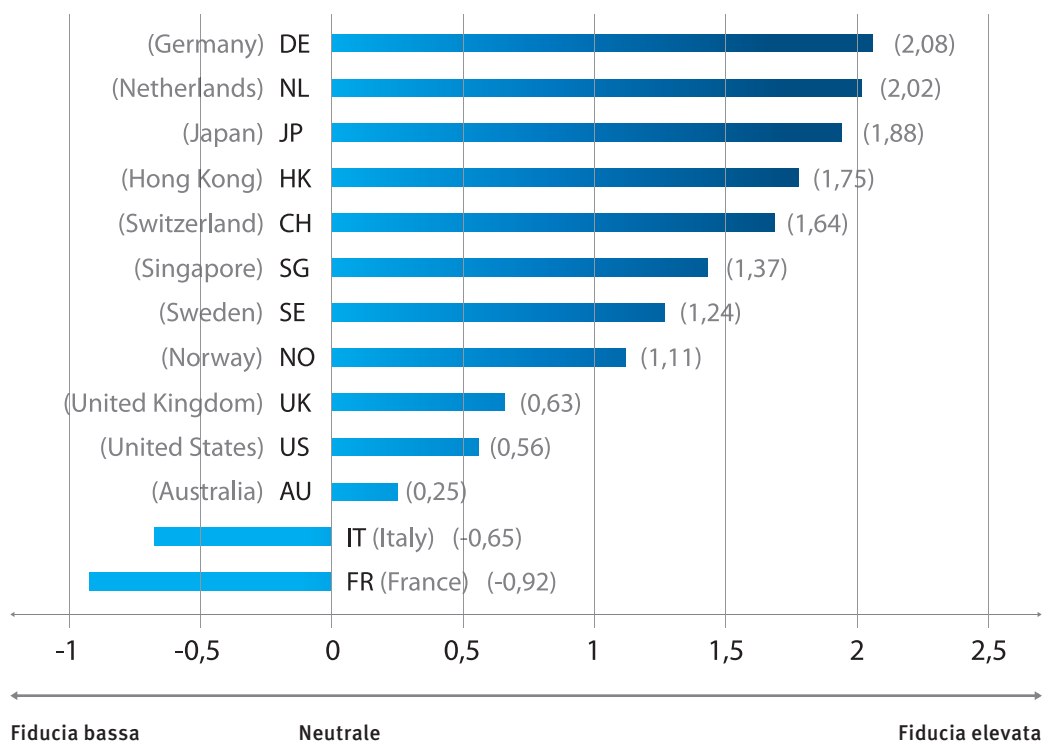
I posti più alti risultano contesi da Germania (2,08) e Paesi Bassi (2,02), ma è la Germania che alla fine conquista il miglior punteggio rispetto alla fiducia nelle procedure e nei processi di backup e ripristino d'emergenza. Entrambi i paesi hanno ottenuto il doppio della media internazionale (1).

A differenza del notevole impegno di questi due paesi europei, il resto dell'Europa resta molto indietro. Gli altri mercati europei ottengono le peggiori performance e si posizionano all'estremità inferiore della classifica. Tra di loro si piazzano Regno Unito, con un valore sotto la media di 0,63, Italia (-0,65) e Francia (-0,92), con una mancanza generalizzata di fiducia. A metà classifica, notevolmente sopra il livello medio, si trovano Svizzera (1,64), Svezia (1,24) e Norvegia (1,11).

Dopo la Germania e i Paesi Bassi si trova la regione APJ (Asia Pacifica e Giappone). Il Giappone ottiene il maggior punteggio (1,88) seguito da vicino da Hong Kong (1,75) e Singapore (1,37). Sebbene questi paesi ottengano buoni punteggi in generale rispetto a processi e procedure, superano quasi tutte le altre regioni per quel che riguarda la disponibilità della tecnologia necessaria e di abbondanti risorse per garantire operazioni di backup e ripristino d'emergenza valide.

La sorpresa principale è rappresentata dagli Stati Uniti (0,56), che si colloca poco al di sotto del livello medio per quel che riguarda tecnologia e risorse. Il risultato appare in linea con il basso punteggio ottenuto tanto dal Regno Unito (0,63) quanto dall'Australia (0,25).

Grafico: Acronis Global Disaster Recovery Index 2011



Principali risultati per regione: alla conquista dell'Oro

Oltre ad offrire delle prospettive globali, questa ricerca è stata ideata per fornire una panoramica su ciascun paese, al fine di aiutare le aziende locali a comprendere ciò che stanno facendo nel modo corretto, a individuare spazi di miglioramento, e a confrontarsi con i pari.

Senza un contesto globale, le aziende sono portate ad adottare gli stessi processi, tecnologie e stili aziendali di quelle a loro più vicine. Sebbene ciò possa garantire che, in media, tutte le aziende locali possano seguire strategie di backup e ripristino d'emergenza simili, è solo quando si inizia a confrontare i risultati a livello globale che emergono i veri leader. Per dirla in termini atletici, è la differenza che intercorre tra l'essere un campione nazionale sui 100 m o salire sul podio perché si è conquistata la medaglia d'oro sui 100 m ai giochi olimpici.

I più fiduciosi: Germania e Paesi Bassi (e la Svizzera)

Come leader della classifica globale, le aziende tedesche e olandesi dimostrano le basi più solide per le attività di backup e ripristino d'emergenza. Ecco i risultati principali:

Risultano avere il miglior supporto e comprensione da parte del team dirigenziale (73%/69%), i migliori controlli e procedure (85%/77%) e le politiche meglio documentate (85%/78%). Di conseguenza, ottengono i migliori punteggi rispetto alla fiducia nelle proprie capacità di ripristinare rapidamente i sistemi in caso di inattività (77%/85%), entrambi superiori di oltre il 50% rispetto alla media.

Con la sola eccezione di Svizzera (13%), Norvegia (17%) e Svezia (16%), i tedeschi e gli olandesi registrano la percentuale di spesa più elevata del proprio budget IT rispetto a backup e ripristino d'emergenza, con il 13% e il 14% rispettivamente.

La ricerca suggerisce che tedeschi e olandesi hanno individuato un livello di assegnazione delle priorità rispetto a backup e ripristino d'emergenza che li soddisfa pienamente. Quando si chiede loro perché non assegnano una priorità ancora maggiore a backup e ripristino d'emergenza, citano come ragione principale il fatto

che non hanno mai avuto esperienza di una perdita di dati, e pertanto non la percepiscono come una minaccia (41%/42%).

Livello di fiducia successivo ai leader: Singapore, Hong Kong e Giappone

Malgrado alcune sostanziali differenze rispetto ai paesi che occupano i primi posti, Singapore, Hong Kong e il Giappone hanno ottenuto punteggi elevati, posizionandosi ragionevolmente vicini ai posti più alti in classifica. Indubbiamente sono le regioni con la maggiore fiducia per quel che riguarda il credere che le proprie attività di backup e ripristino d'emergenza funzioneranno in caso di evento grave (68%/71%/74%). Ecco i risultati principali:

Malgrado il supporto e la comprensione da parte del team dirigenziale siano approssimativamente vicini alla media (48%/60%/57%), questi paesi dichiarano di avere risorse (49%/55%/54%) e tecnologie (46%/62%/56%) simili rispetto ai leader della classifica.

Singapore, Hong Kong e il Giappone affermano, in media, di avere il personale più qualificato per eseguire operazioni di backup e ripristino d'emergenza in caso di evento di grave entità.

Tuttavia, c'è un'area con differenze notevoli tra Singapore, Hong Kong, Giappone e i leader della classifica. La differenza sta nella quota complessiva di budget IT spesa in attività di backup e ripristino d'emergenza. Abbiamo già visto che tedeschi (13%) e olandesi (14%) destinano oltre il doppio del loro budget IT complessivo al backup e al ripristino d'emergenza rispetto a Singapore (6%), Hong Kong (5%) e al Giappone (7%). Questa equa scarsità di budget destinato al backup e al ripristino d'emergenza è in apparente conflitto con l'iniziale elevata fiducia nelle capacità di rapido ripristino dopo un evento di grave entità.

Come nota finale, Singapore, Hong Kong e il Giappone sono i paesi che con maggiore probabilità (67%/66%/70%) utilizzano soluzioni di backup distinte per ambienti fisici

e virtuali rispetto a qualsiasi altra regione. Circa la metà delle aziende in questi paesi utilizza più di tre differenti soluzioni e tra un quinto e un terzo (22%/25%/33%) ne impiegano più di cinque, dato sorprendente perché l'impiego di una soluzione singola che possa gestire sia ambienti fisici che virtuali consente un notevole risparmio di costi amministrativi.

La nordica terra di mezzo

La ricerca rileva che le aziende svedesi e norvegesi hanno atteggiamenti molto simili rispetto al backup e al ripristino d'emergenza. Sebbene in genere ottengano un punteggio di poco superiore alla media nella ricerca, numerosi aspetti differenziano i due paesi.

Le aziende svedesi (16%) e norvegesi (17%) investono una parte più consistente del proprio budget IT complessivo in backup e ripristino d'emergenza rispetto a qualsiasi altro paese partecipante all'indagine e quasi tre volte ciò che spendono le aziende di Singapore, Hong Kong e Giappone.

Paragonate al resto del mondo, tuttavia, le aziende svedesi e norvegesi sono quelle che con meno probabilità passeranno al cloud computing, e un numero molto ridotto utilizza il cloud in modo significativo sin da oggi. Mentre la maggior parte dei paesi avranno un aumento medio dell'87% nell'IT basato su cloud nei prossimi 12 mesi, l'utilizzo del cloud da parte di Svezia e Norvegia crescerà di poco più del 20% (dal 7% all'8%/dal 7% al 9%) durante lo stesso periodo.

Insieme a quelle francesi e italiane, le aziende svedesi e norvegesi citano una mancanza di fiducia nei fornitori di servizi cloud come principale preoccupazione, e con buone ragioni, poiché nessuna azienda dovrebbe affidare con estrema fiducia a chiunque i propri dati. È invece importante selezionare un fornitore con una storia consolidata di protezione dei dati, in grado di fornire il livello di sicurezza richiesto per far sì che i dati siano al sicuro, protetti e accessibili solo al legittimo proprietario.

Chi resta indietro: Regno Unito, Australia e Stati Uniti

Le aziende di Regno Unito, Australia e Stati Uniti hanno ottenuto un basso punteggio per quel che riguarda la loro capacità di evitare i periodi di inattività in caso di eventi gravi (27%/44%/38%). Molto indietro rispetto ai leader della classifica - Germania (77%) e Paesi Bassi (85%) - anche la fiducia nella rapidità di ripristino (56%/36%/40%).

Questo gruppo resta indietro per quel che riguarda il sostegno e la comprensione da parte del team dirigenziale, e all'abbondanza delle risorse e delle tecnologie necessarie per eseguire le operazioni. Per quel che riguarda la capacità di eseguire il ripristino dopo un evento di grave entità, gli australiani dimostrano il livello di fiducia minore. Solo il 22% delle aziende australiane ritiene di poter tornare funzionale rapidamente in caso di inattività, rispetto a una media globale del 50%.

Approssimativamente, circa un terzo delle aziende di Regno Unito (36%), Australia (36%) e Stati Uniti (32%) non ha approntato una strategia di backup e ripristino d'emergenza. Questi paesi sono quelli che dichiarano in generale che alle attività di backup e ripristino d'emergenza non viene attribuita la necessaria priorità, citando una mancanza di budget e risorse come ragione primaria che sottende a questo. Ma la teoria entra in gioco solo parzialmente. Come proporzione di tutta la spesa IT, Regno Unito, Australia e Stati Uniti spendono molto meno in backup e ripristino d'emergenza (10%/11%/10%) rispetto a Germania (13%) e Paesi Bassi (14%) ma di un margine non eccessivamente ampio.

Spazio per crescere: Francia e Italia

Le aziende in Francia e in Italia assegnano la priorità più bassa a backup e ripristino d'emergenza, come mostra il fatto che il 39% dei francesi e il 53% delle aziende italiane afferma di non investire nulla in tali attività.

Sono inoltre quelle che ammettono di non avere una strategia ad hoc (41%/45%) e quelle che con meno probabilità si ritengono in grado di eseguire un ripristino rapido in caso di inattività, con rispettivamente il 27% e il 30%, confrontato con un valore medio della classifica pari al 50%. La loro spesa rappresenta la percentuale più bassa del budget IT complessivo di tutti i paesi che hanno partecipato al sondaggio, con rispettivamente il 5% (Francia) e il 4% (Italia).

I due paesi dichiarano di avere anche il personale meno qualificato (29%/32%) e sono quelli che con maggiore probabilità subiranno una sostanziale inattività in caso di eventi di grave entità (68%/64%). Dichiarano inoltre alcuni tra i livelli di risorse (26%/28%), tecnologie (32%/33%), controlli e procedure (36%/38%) più bassi e le politiche meno documentate (33%/45%).

Le previsioni per il backup e il ripristino d'emergenza in questi paesi restano prevalentemente deboli. Il ritmo di adozione della virtualizzazione dei server da parte dei francesi e degli italiani è tra i più bassi tra quelli dei paesi partecipanti, ed entrambi i paesi restano indietro anche per quel che riguarda i tassi di utilizzo della virtualizzazione attuali (14%/7%) e futuri (25%/8%). Dopo il Regno Unito (60%), le aziende in Francia (56%) e in Italia (53%) sono quelle che più ammettono di non eseguire il backup dei server virtuali alla stessa stregua di quelli fisici, con una frequenza quasi tre volte maggiore rispetto a quella delle aziende tedesche (21%) e olandesi (20%).

Ma forse la soluzione potenziale arriva dal cloud. In linea con il resto dei paesi inclusi nello studio, la maggior parte delle aziende francesi (68%) e italiane (58%) prevede che il cloud diventi parte della propria strategia di backup e ripristino d'emergenza nel corso del prossimo anno.

Questi paesi potrebbero trarre vantaggio da una soluzione di backup e ripristino d'emergenza che sia caratterizzata da facilità d'utilizzo e che supporti ambienti fisici, virtuali e nel cloud da una singola interfaccia, riducendo così l'impatto delle risorse limitate e la necessità di formazione. Le soluzioni con macchine virtuali senza agente sono quelle più efficienti, poiché consentono di eseguire i backup virtuali con la stessa frequenza di quelli fisici

Principali risultati globali: le tendenze a sostegno della fiducia

Nella sezione che segue vengono identificati sei risultati chiave relativi alla classifica e alcuni dati di riferimento incrociati che identificano quelle tendenze più strettamente

connesse all'avere il livello di fiducia simile a quello dei leader della classifica.

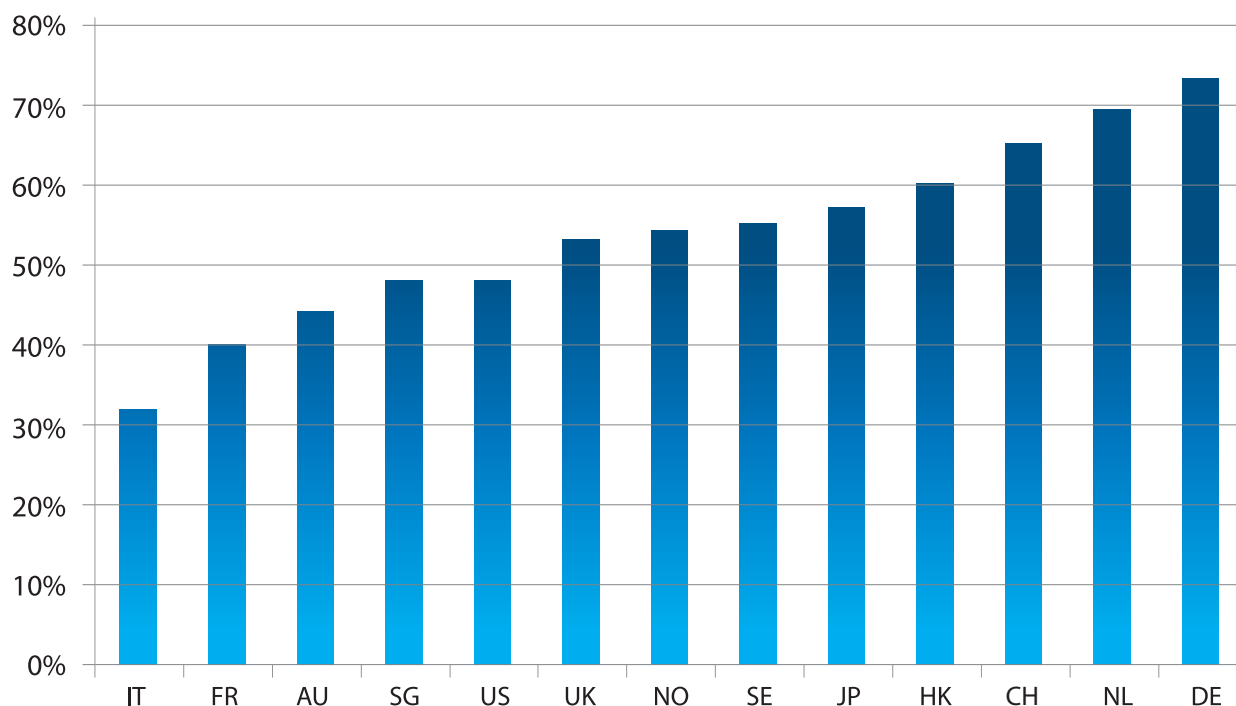
Primo risultato - La fiducia nel ripristino d'emergenza inizia dall'alto: i primi in classifica hanno il maggiore sostegno da parte dei team dirigenziali

Quando si tratta di avere un elevato livello di fiducia nel backup e nel ripristino d'emergenza, l'avere il supporto dei consigli di amministrazione, con i dirigenti senior che sostengono le attività di backup e ripristino d'emergenza è cruciale.

L'indagine ha individuato delle correlazioni tra coloro che

hanno attività di backup e ripristino d'emergenza ben gestite (52%), coloro che sono fiduciosi nel fatto che il backup e il ripristino d'emergenza funziona e coloro che hanno il sostegno dei dirigenti dell'azienda (54%). Le aziende tedesche detengono il più alto (73%) livello di supporto da parte del team dirigenziale, mentre quelle italiane registrano il valore inferiore (32%).

Grafico: percentuale dei responsabili IT che ritengono che il team dirigenziale offra il giusto supporto alle attività di backup e ripristino d'emergenza aziendali.



Il supporto da parte del consiglio di amministrazione, che poi decide le assegnazioni del budget IT, è evidentemente un requisito di base affinché i manager IT abbiano a loro volta fiducia nelle attività di backup e ripristino

d'emergenza. La ricerca mostra anche che le aziende con il più elevato livello di supporto da parte dei dirigenti risentono anche di meno in termini di periodi di inattività in caso di evento di grave entità.

Secondo risultato - La scarsità di investimenti in strumenti e risorse diminuisce la fiducia

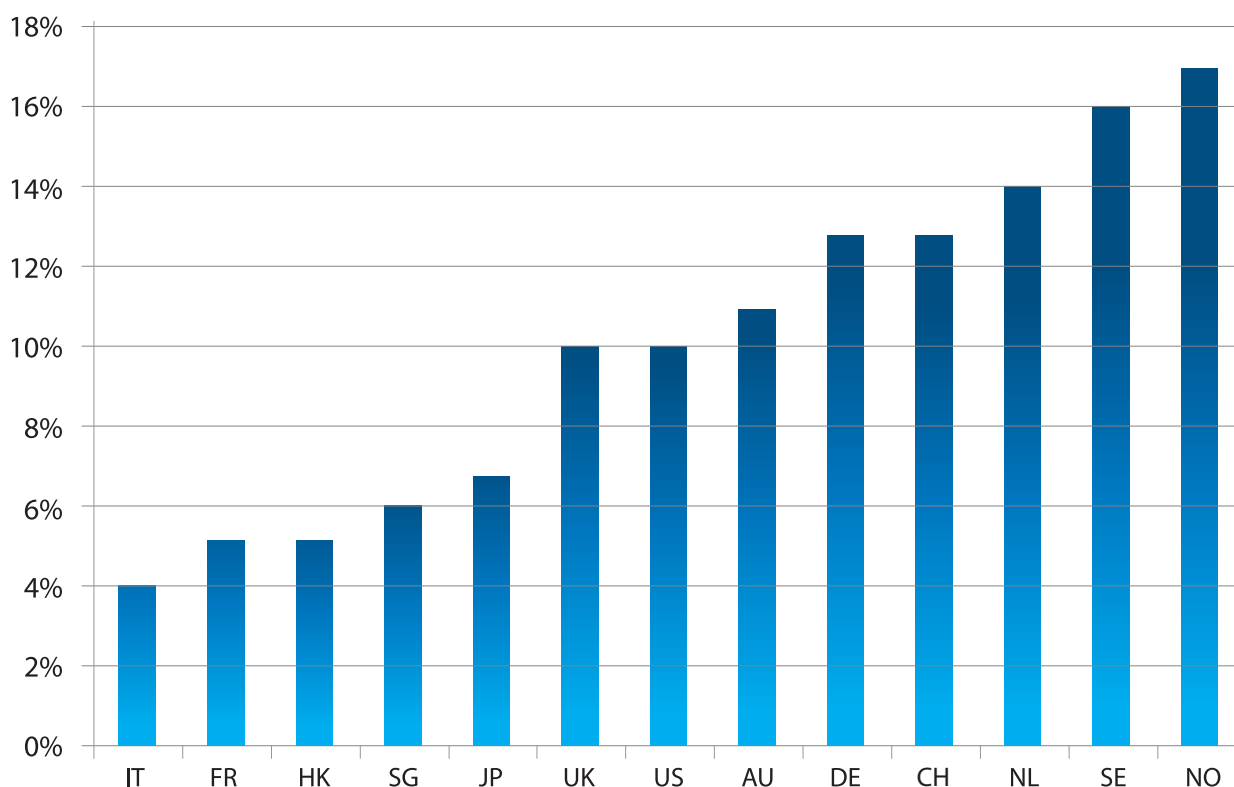
Il sostegno e la comprensione da parte dei team dirigenziali si traduce in investimenti sufficienti per l'acquisto delle risorse e tecnologie necessarie affinché le attività di backup e ripristino d'emergenza siano efficienti. I dirigenti comprendono che maggiori investimenti in backup e ripristino d'emergenza possono aiutare a ridurre i tempi di inattività in caso di emergenza. Malgrado ciò, meno della metà (46%) delle aziende globali intervistate ritiene di avere risorse o tecnologie adeguate a consentire operazioni di backup e ripristino d'emergenza complete.

Per quel che riguarda i paesi con i maggiori investimenti in backup e ripristino d'emergenza, la Svizzera e Hong Kong ottengono il punteggio più elevato per quel che riguarda il disporre di abbondanti risorse (63%) e tecnologie (60%). A livello complessivo, la regione con le risorse migliori è quella Asiatico-Pacifica con il Giappone, Hong Kong e Singapore che ottengono un punteggio medio regionale pari al 53% per l'abbondanza di risorse e al 54% per le tecnologie.

Anche per quel che riguarda questi aspetti, Stati Uniti, Regno Unito e Australia restano indietro. Le aziende statunitensi ottengono un basso punteggio in entrambi i casi, con appena il 44% delle aziende che dichiarano di disporre di abbondanti risorse e solo il 33% che ritiene di avere tecnologie sufficienti a consentire operazioni di backup e ripristino d'emergenza complete. Più indietro ancora il Regno Unito, con punteggi rispettivamente del 31% e del 32%. L'Australia appare un gradino più avanti, con punteggi rispettivamente del 41% e del 33%.

La situazione si ripete in modo simile anche per quel che riguarda la spesa complessiva relativa a backup e ripristino d'emergenza. I leader europei della classifica (Germania, Svizzera e Olanda) tendono a investire in media circa il 14% del proprio budget IT in backup e ripristino d'emergenza. Al contrario i leader asiatici (Giappone, Hong Kong e Singapore) ottengono in media il 6%.

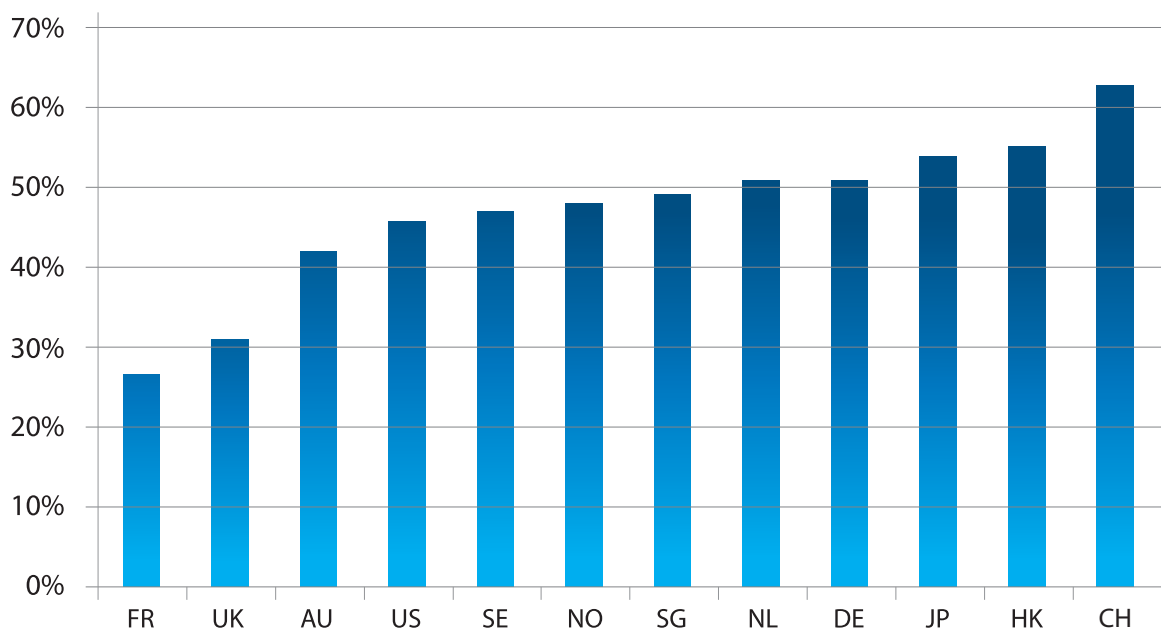
Grafico: percentuale di budget IT dedicato a backup e ripristino d'emergenza



Le aziende di tutto il mondo creano nuovi dati a un ritmo prolifico, in media oltre 100 GB ogni giorno, secondo lo studio. Malgrado questa crescita dei dati, e sebbene la maggioranza delle aziende spenda circa il 10% del budget IT in backup e ripristino d'emergenza, oltre un quinto (21%) dichiara di non spendere nulla. L'Italia registra il punteggio peggiore, con il 53% delle aziende italiane intervistate che dichiara di non spendere nulla in backup e ripristino d'emergenza.

Circa la metà (44%) di tutte le aziende intervistate concorda sul fatto che le strategie di backup e ripristino d'emergenza in essere nelle proprie organizzazioni non hanno la priorità sufficiente, citando scarsità di budget e risorse IT tra i motivi principali.

Grafico: percentuale di responsabili IT che concordano sul fatto di disporre di abbondanti risorse per consentire attività di backup e ripristino d'emergenza complete



Terzo risultato - I leader della classifica sono organizzati meglio e subiscono in misura inferiore le conseguenze dell'inattività

Non si tratta semplicemente di avere risorse e tecnologie sufficienti: occorre anche che vengano utilizzate in maniera efficace. Alcune domande dell'indagine consentono di comprendere in che modo le aziende riescono a gestire in modo funzionale le politiche e le procedure di backup e ripristino d'emergenza.

Sotto questo aspetto, il paese meglio organizzato appare essere la Germania, che dichiara i controlli e le procedure più abbondanti (85%) e le politiche meglio documentate (85%). Ciò si collega direttamente al fatto che la maggior parte delle aziende tedesche (69%) ritiene di poter evitare periodi di inattività consistenti in caso di eventi di grave entità. La Svizzera si colloca al secondo posto con un punteggio pari al 77% per i controlli e all'80% per le politiche, e oltre la metà (51%) ritiene di poter evitare periodi di inattività consistenti in caso di eventi di grave entità.

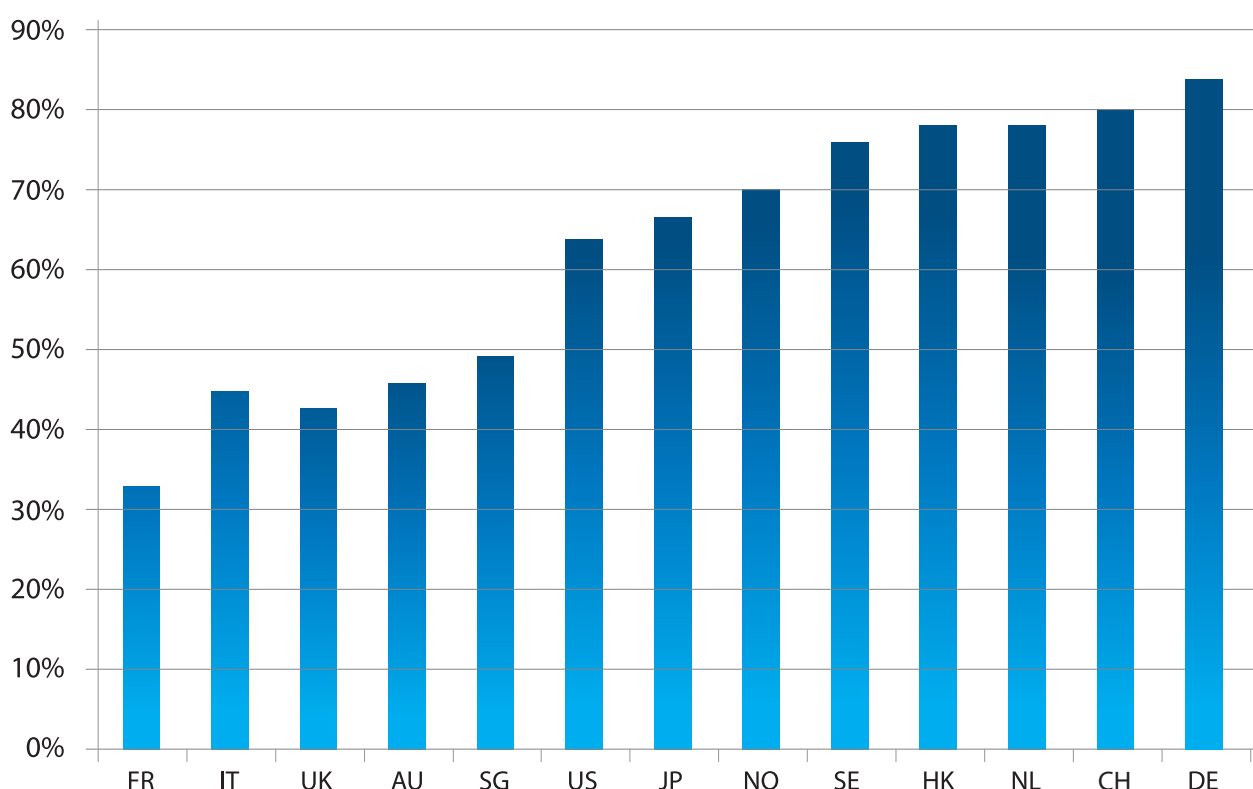
Sebbene non possa paragonarsi a Germania o Svizzera per quel che riguarda l'organizzazione, la regione Asiatico Pacifica conserva i propri standard tendenzialmente elevati. Hong Kong in particolare registra il 66% per i controlli e il 78% per le politiche, mentre un numero

corrispondente (73%) delle aziende di Hong Kong ritiene di poter evitare periodi di inattività consistenti in caso di eventi di grave entità.

Per una volta gli Stati Uniti ottengono punteggi notevolmente superiori rispetto al Regno Unito e all'Australia, con il 60% di aziende (valore superiore alla media) che ritiene di disporre di controlli e procedure di vasta portata e il 65% che afferma di avere politiche ben documentate. L'Australia ottiene appena il 48% rispetto ai controlli e alle procedure, e il 46% rispetto alle politiche ben documentate, mentre il Regno Unito resta indietro, con risultati rispettivamente del 32% e del 44%. Inoltre, solo il 27% delle aziende britanniche ritiene di poter evitare periodi di inattività consistenti in caso di eventi di grave entità.

Il paese ad ottenere il punteggio più basso in questa categoria è la Francia, con il 36% di aziende che ritiene di disporre di controlli e procedure di vasta portata e il 33% che afferma di avere politiche ben documentate. Non sorprende pertanto che solo il 32% delle aziende francesi ritiene di poter evitare periodi di inattività consistenti in caso di eventi di grave entità.

Grafico: Aziende che sono d'accordo o completamente d'accordo con l'affermazione che le proprie politiche e procedure sono ben documentate

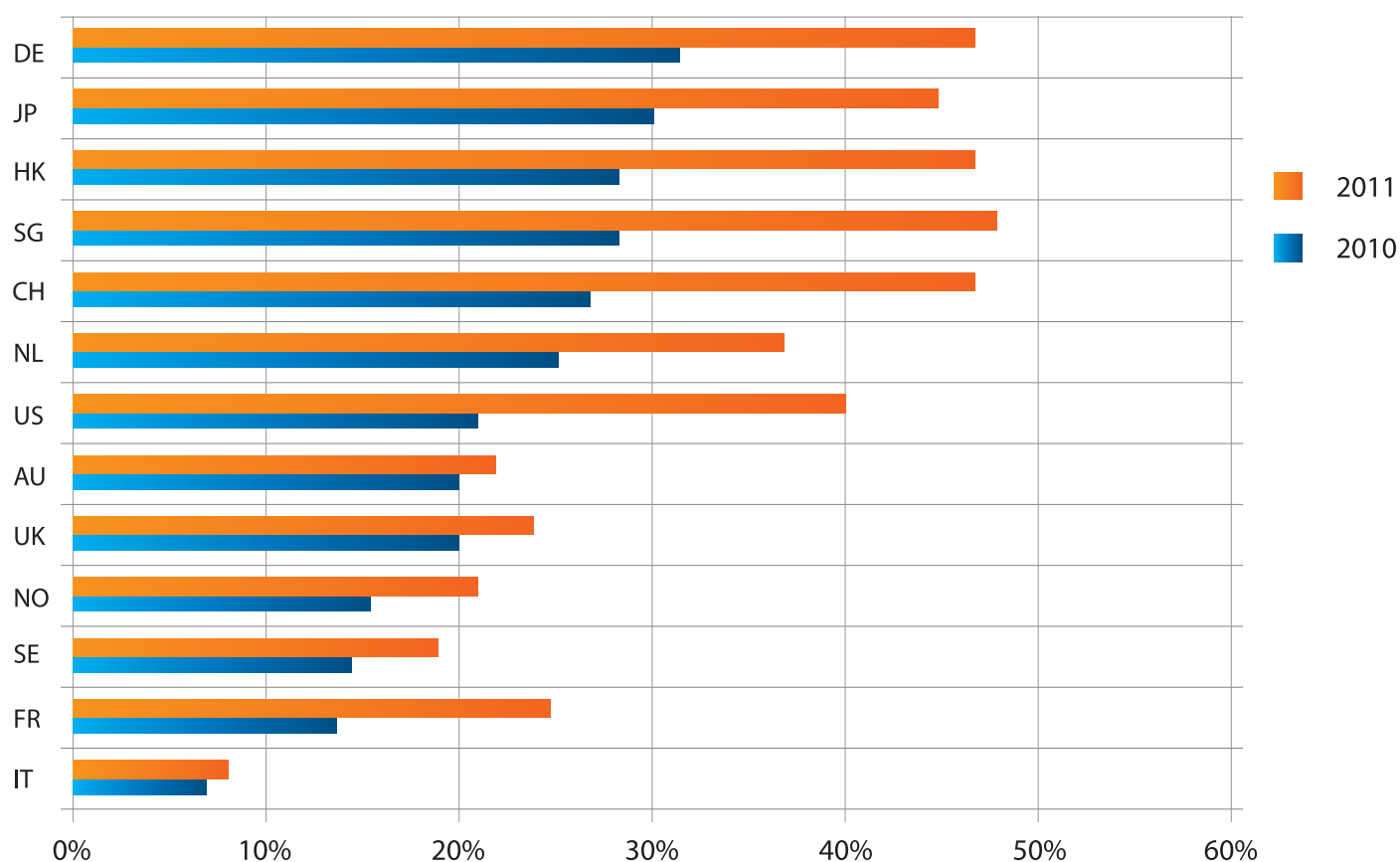


Quarto risultato - In testa alla classifica si trovano i paesi che dichiarano il maggior numero di server virtuali; sono anche quelli che eseguono con maggiore frequenza il backup di tali server

I paesi con il più elevato tasso di adozione delle tecnologie di virtualizzazione dei server occupano i posti più elevati nella classifica Global DR Index. Oltre alle posizioni di testa complessive dell'indice, le aziende di Germania, Olanda e

Svizzera, insieme a quelle di Singapore, Hong Kong e del Giappone, registrano anche le percentuali di adozione di server virtuali più elevate per il 2010 e per il 2011.

Grafico: percentuale di aziende che impiegano server di produzione virtualizzati attualmente e di quelle che li adotteranno nel 2011

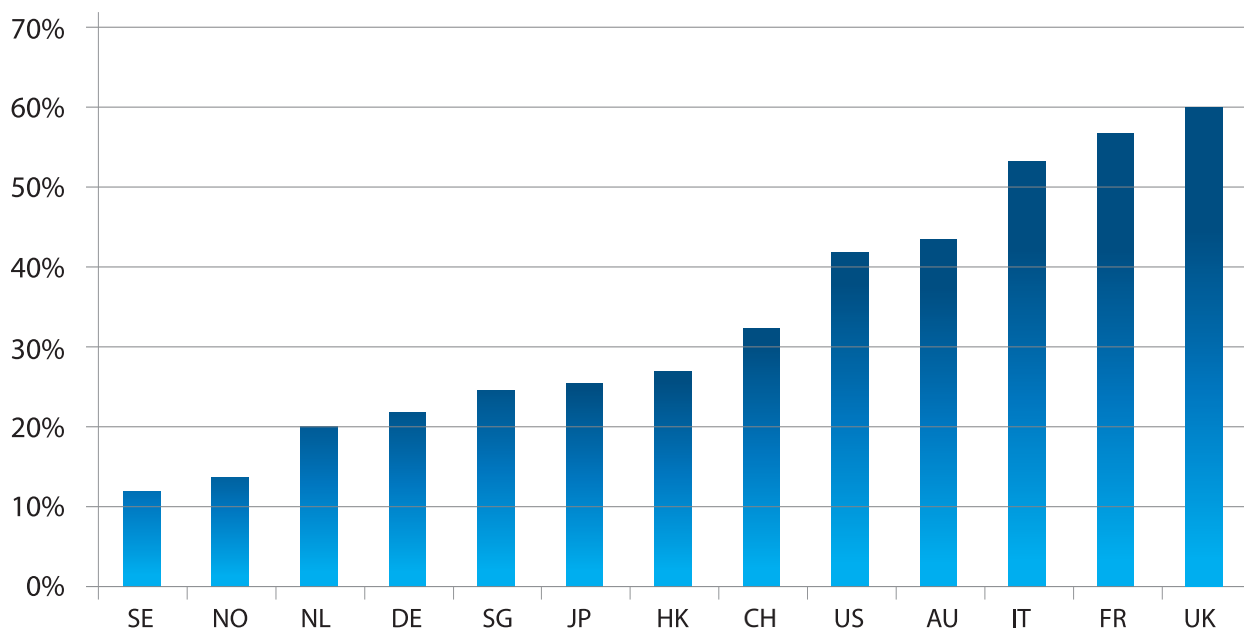


In generale, la maggior parte dei paesi prevede di aumentare l'impiego dei server virtuali di circa il 50% nei prossimi 12 mesi (dal 22% al 33%).

Mano a mano che le aziende del mondo adottano la virtualizzazione dei server, emergono domande sulle politiche e le pratiche di backup di sistemi e file in

ambienti ibridi tra fisico e virtuale. Questa ricerca rileva che la maggior parte delle aziende che occupano le prime posizioni della classifica attribuiscono un'eguale importanza ai regolari backup fisici e virtuali. Senza alcuna eccezione, le aziende dei paesi che ottengono punteggi bassi attribuiscono un'importanza significativamente inferiore alla regolarità dei propri backup virtuali.

Grafico: percentuale di responsabili IT che non eseguono il backup dei server virtualizzati con la stessa frequenza rispetto ai server fisici



Appare ovvia la correlazione tra questo risultato e il dato precedente che indicava i paesi che hanno un approccio organizzativo strutturato e che investono in modo sufficiente nelle attività di backup e ripristino d'emergenza. I paesi con un punteggio basso in generale rispetto agli investimenti e all'approccio organizzativo risultano essere anche quelli che eseguono il backup dei propri server virtuali con una frequenza inferiore rispetto ai server fisici, a dispetto del fatto che in tutte le regioni si prevede un aumento medio del 50% nell'adozione dei server virtuali durante il corso del prossimo anno. Il considerare in maniera distinta il backup di server virtuali

e fisici può probabilmente essere attribuito alla scarsità di risorse e tecnologie.

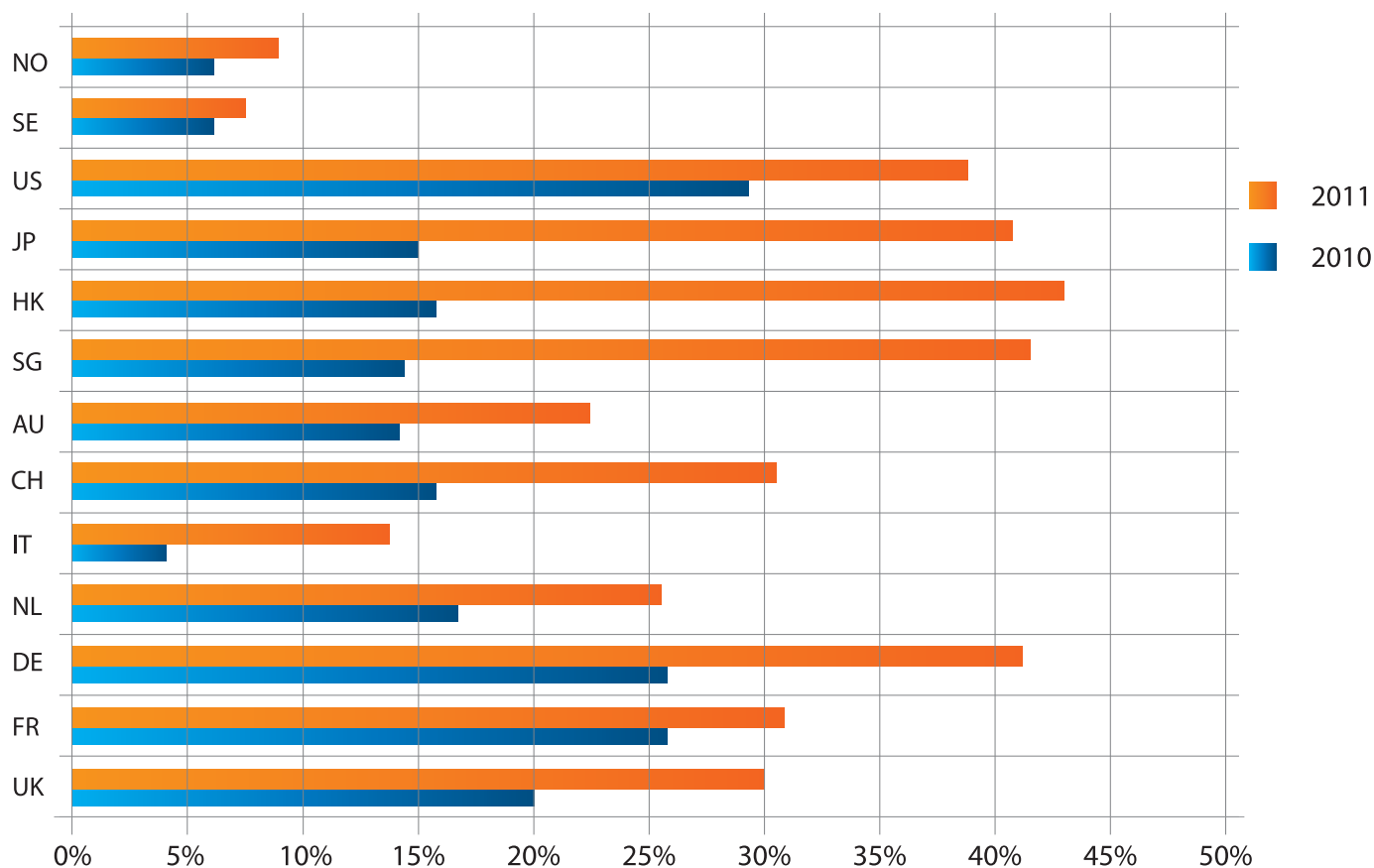
Se mancano il personale e gli strumenti adeguati, è più probabile che i responsabili IT subiscano una maggiore pressione. La conseguenza è che meno probabilmente metteranno in atto controlli dettagliati o avranno tempo di implementare procedure o politiche ben documentate. Se combinati, questi fattori offrono senz'altro un potenziale modello fallimentare di strategia di backup e ripristino d'emergenza.

Quinto risultato - Nel 2011 l'impiego del cloud raddoppierà, ma i dubbi restano

Delle oltre 3.000 aziende intervistate, circa tre quarti (74%) dichiarano di voler implementare una qualche forma di infrastruttura IT basata su cloud entro la fine del 2010. Sebbene questa percentuale di adozione sembri a prima vista

notevole, il cloud attualmente rappresenta solo circa il 16% delle infrastrutture IT di tali aziende. Tuttavia, nei prossimi 12 mesi, ed entro la fine del 2011, si prevede un picco dell'87% di questa cifra (dal 16% al 30%), in tutte le regioni.

Grafico: percentuale di utilizzo di infrastrutture IT basate su cloud e percentuale di crescita stimata in un anno



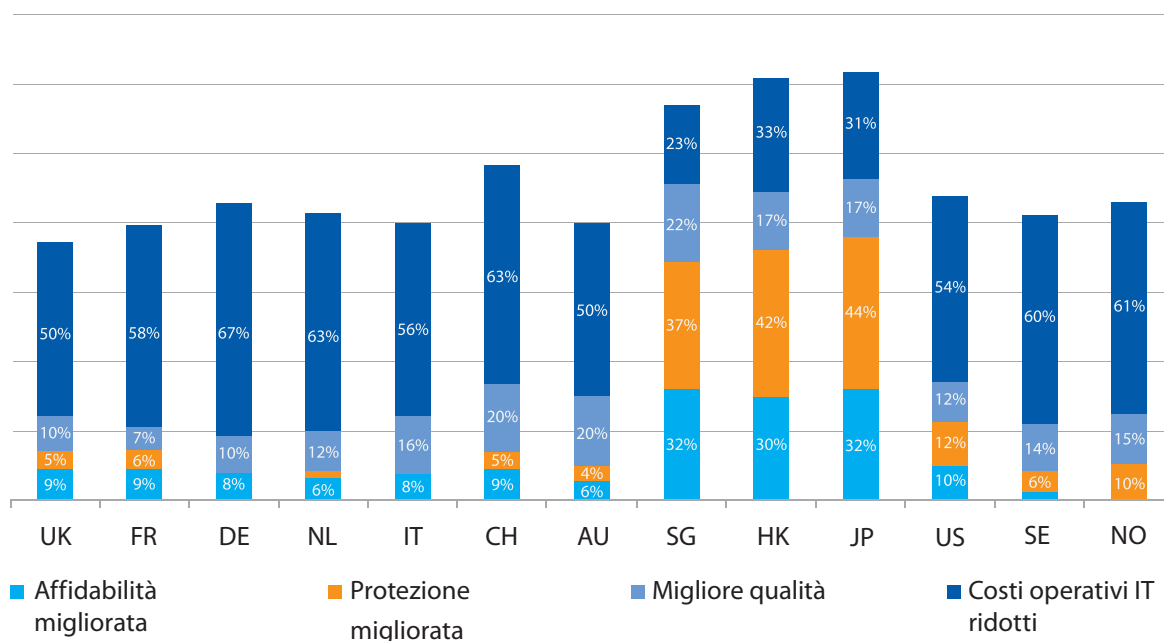
Il cloud non è ancora una delle scelte di preferenza per le strategie di backup e ripristino d'emergenza. Oltre il 50% delle aziende preferisce tuttora eseguire la replica dei dati su una connessione privata protetta piuttosto che nel cloud (21% contro 33%). Ci sono tuttavia alcune deviazioni di tendenza. Oltre due terzi (71%) di tutte le aziende intervistate prevedono di includere il cloud computing nella propria strategia di backup e ripristino d'emergenza entro la fine del 2011.

Malgrado l'imminente aumento nell'adozione del cloud per il backup e il ripristino d'emergenza fuori sede, le aziende hanno ancora profonde riserve rispetto ai rischi di impiego di tale tecnologia. Citano la velocità di recupero dei dati (54%), la mancanza di sicurezza (39%) e l'ulteriore complessità del lavoro (33%) come tre delle motivazioni

principali. Prevedibilmente, le aziende continueranno a eseguire backup e ripristino in locale per la velocità, e impiegheranno il cloud come ulteriore livello di protezione, per la conservazione a lungo termine (per sostituire i backup su nastro) e per i potenziali guasti in sede.

Il fatto che il costo non sia elencato come motivo di preoccupazione per le aziende che intendono adottare il cloud computing mostra che per molti il cloud è considerato una tecnologia importante per la riduzione dei costi. Il dato appare supportato dal fatto che solo l'8% degli intervistati teme che il costo del cloud computing possa aumentare in futuro, mentre la maggior parte delle aziende (51%) cita la possibilità di ridurre i costi operativi IT come maggior vantaggio percepito dal passaggio al cloud.

Grafico: vantaggi principali derivanti dall'impiego del cloud computing per il backup e il ripristino d'emergenza



Gli intervistati hanno selezionato tutte le risposte ritenute valide tra le otto opzioni proposte

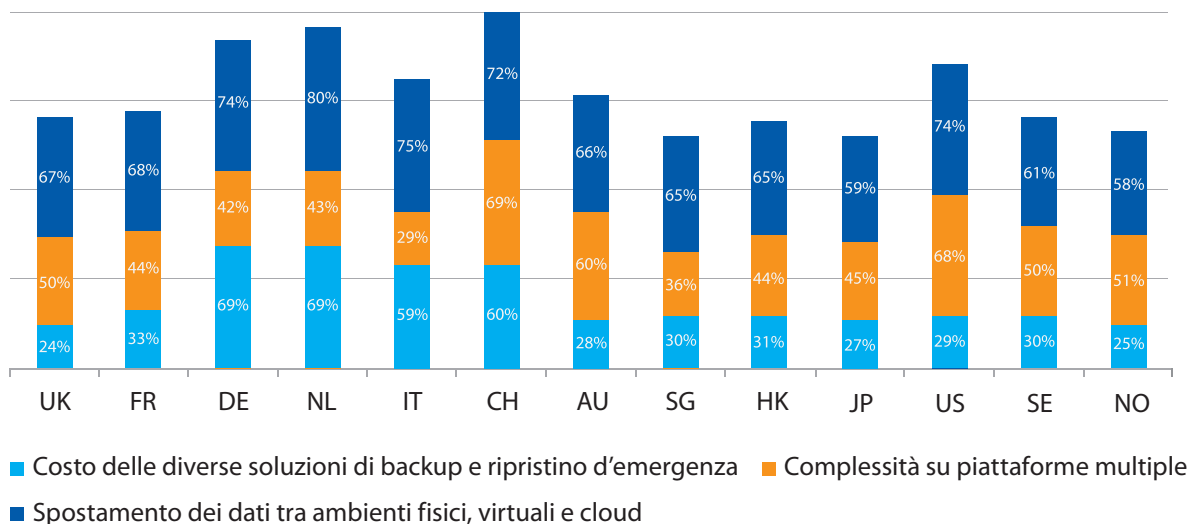
Sesto risultato - Tutte le aziende ritengono complessa l'esecuzione del backup e del ripristino d'emergenza in un ambiente ibrido

La ricerca ha già accertato che praticamente ogni azienda del mondo dispone di qualche infrastruttura virtuale (75%) o basata su cloud (74%), e che in tutta probabilità queste percentuali cresceranno nel prossimo futuro.

In ogni regione, lo spostamento dei dati tra ambienti

fisici, virtuali e cloud viene citato come ostacolo principale (68%) per quel che riguarda l'esecuzione di backup in un ambiente ibrido. Dato che ogni azienda utilizza in media due o tre diverse applicazioni di backup e ripristino d'emergenza, è chiara la ragione per la quale la complessità (48%) viene citata come secondo ostacolo.

Grafico: Ostacoli al backup in un ambiente IT ibrido

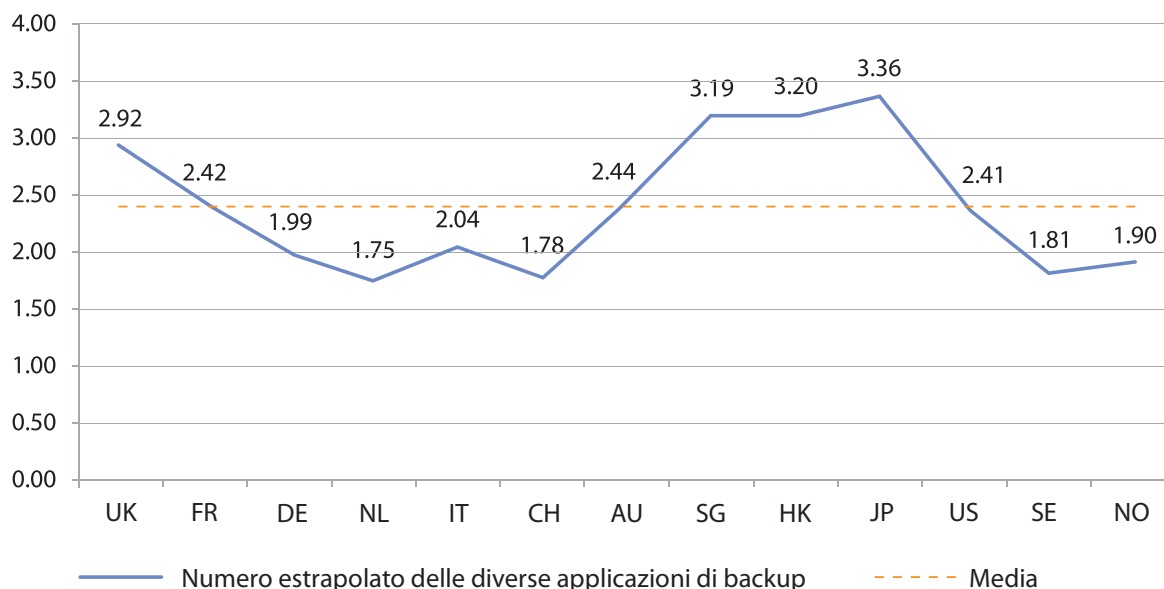


Agli intervistati è stato chiesto di selezionare tre risposte ritenute valide tra le cinque opzioni proposte

In Asia viene utilizzato il maggior numero di applicazioni di backup e ripristino d'emergenza; oltre un quarto (27%) degli intervistati nella regione afferma di avere cinque o più applicazioni per eseguire il backup e recuperare i dati. Al contrario, i paesi in cima alla classifica, Germania e Paesi

Bassi, utilizzano il minor numero di applicazini diverse. Le aziende in Germania e in Olanda mostrano una percentuale di utilizzo doppia di una sola applicazione rispetto a quel che accade nella regione Asiatico Pacifica.

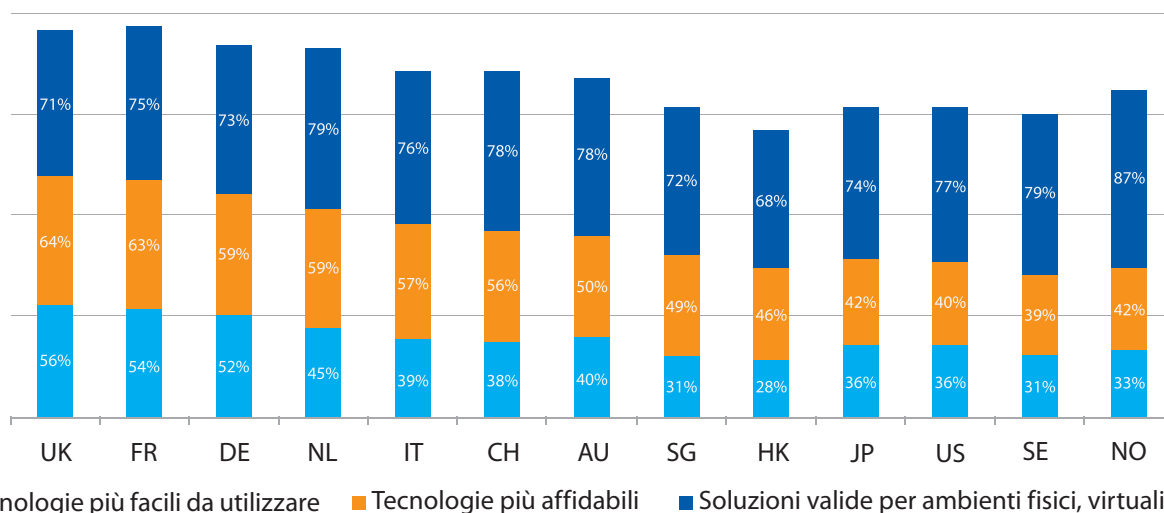
Grafico: numero di applicazioni di backup differenti utilizzato dalle aziende intervistate



Malgrado le grandi differenze nel numero di applicazioni utilizzate, le aziende di tutto il mondo concordano su una cosa rispetto al backup e al ripristino d'emergenza: un'unica soluzione completa semplificherebbe le cose. Oltre i tre quarti (76%) delle aziende intervistate afferma che l'elemento più vantaggioso e che potrebbe migliorare la propria strategia di backup e ripristino d'emergenza

è un'unica soluzione capace di offrire protezione nell'ambiente fisico, virtuale e nel cloud. Questa esigenza viene considerata prioritaria rispetto alla disponibilità e alla conoscenza di best practice relative al ripristino d'emergenza, di strumenti che consentano di ottenere il sostegno del team dirigenziale e dell'impiego di tecnologie che siano al contempo più facili da utilizzare e più affidabili.

Grafico: Tre consigli per migliorare le procedure di backup e ripristino



Agli intervistati è stato chiesto di selezionare le tre esigenze principali tra le sei opzioni proposte

Consigli per il backup e il ripristino d'emergenza: il punto di vista dello sponsor della ricerca

Nel mondo d'oggi, il backup e il ripristino d'emergenza sono ancora una materia che molte PMI devono affrontare. Ci vengono chieste spesso le ragioni. Questo studio guarda al futuro offrendoci una risposta.

È chiaro che le organizzazioni in tutto il mondo stanno ancora cercando di attuare queste strategie nel modo migliore. Hanno ancora bisogno di supporto nell'ottenere il sostegno dei dirigenti, nella gestione delle risorse e nell'implementazione di tecnologie di facile utilizzo e affidabili. In qualche misura, c'è ancora una carenza di best practice offerte dai fornitori e molte PMI si affidano fortemente ai propri partner di canale affinché siano questi i loro consulenti sulle best practice e le sostengano nel fare le giuste scelte.

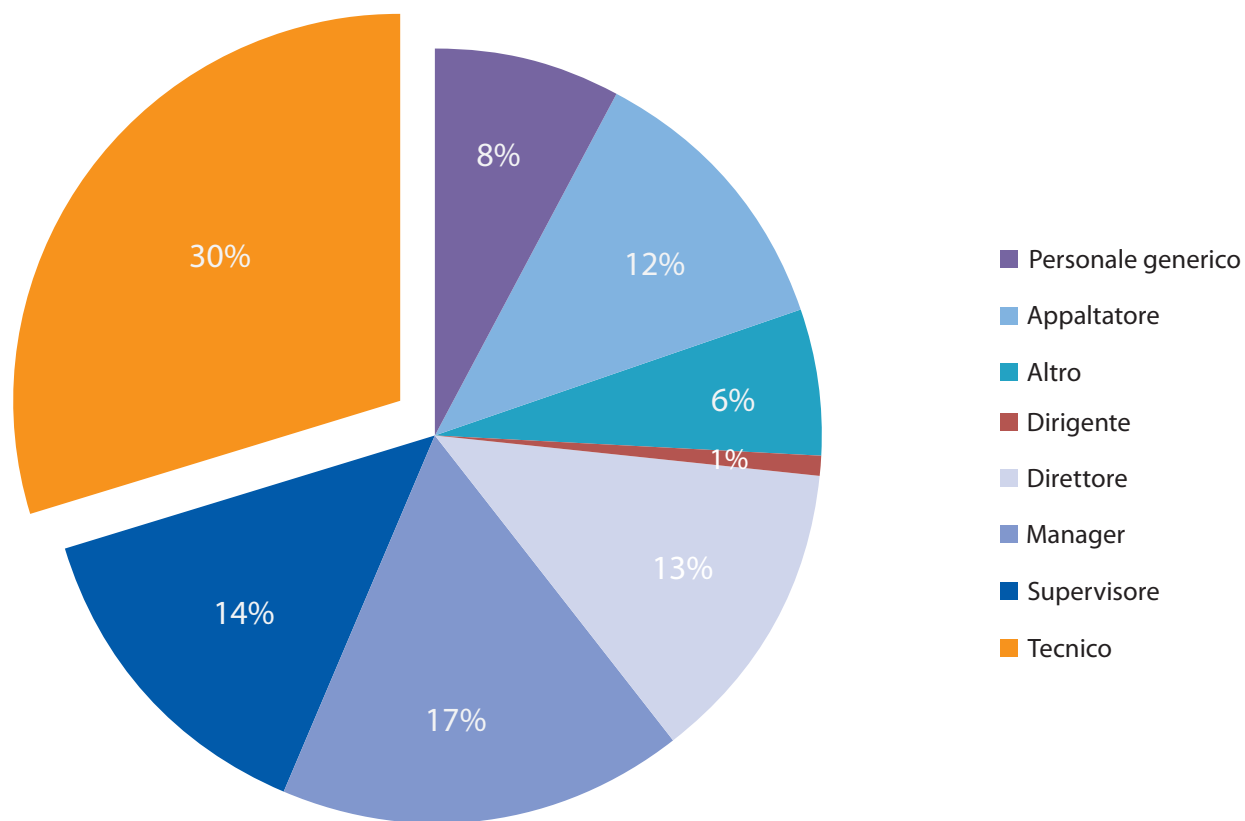
Tuttavia, la complessità è aumentata dal fatto che alle organizzazioni si presentano tre differenti piattaforme nelle quali implementare le strategie di disaster recovery: fisico, virtuale e cloud. Ognuna di esse mostra vantaggi e svantaggi tipici. Alcune organizzazioni sceglieranno di restare in ambito puramente fisico, altre accoglieranno la virtualizzazione, mentre quelle più predisposte al rischio opteranno per una combinazione di fisico, virtuale e cloud.

In definitiva la riuscita delle procedure di backup e ripristino si basa sulla disponibilità costante dei sistemi e dei dati e sull'impatto che i tempi di inattività a questi associati hanno verso l'esterno e in termini di perdita di profitto e di clienti, indipendentemente dall'ambiente in cui dati e sistemi sono contenuti. L'impiego di più soluzioni diverse per gestire i dati in ambienti fisici, virtuali e nel cloud rende questo processo inutilmente complicato e rischioso, implicando altresì perdite di tempo e risorse.

Nel caso delle PMI, le basi della riuscita di un servizio stanno nella capacità di garantire agli utenti facilità d'uso, efficacia dal punto di vista dei costi e flessibilità, oltre alla possibilità di attuare rapidamente le misure previste così da ottenere il minimo impatto possibile sulle attività aziendali. Tanto i servizi di clouding quanto la virtualizzazione offrono questi vantaggi, pertanto il futuro appare roseo. Gestite nel modo giusto, da una soluzione centralizzata e di facile impiego, possono offrire alle aziende una protezione definitiva per il backup e il ripristino d'emergenza, garantendo una maggiore facilità di gestione della continuità aziendale.

Auguriamo ai responsabili IT di tutto il mondo di trovare utile questa indagine, e speriamo che li incoraggi a completare il questionario online per poter confrontare le proprie procedure di backup e ripristino d'emergenza con quelle delle controparti nel proprio paese e con i punti di riferimento internazionali definiti negli altri paesi.

Appendice 1: Grafico: Livello nell'azienda e canale di riferimento dell'intervistato

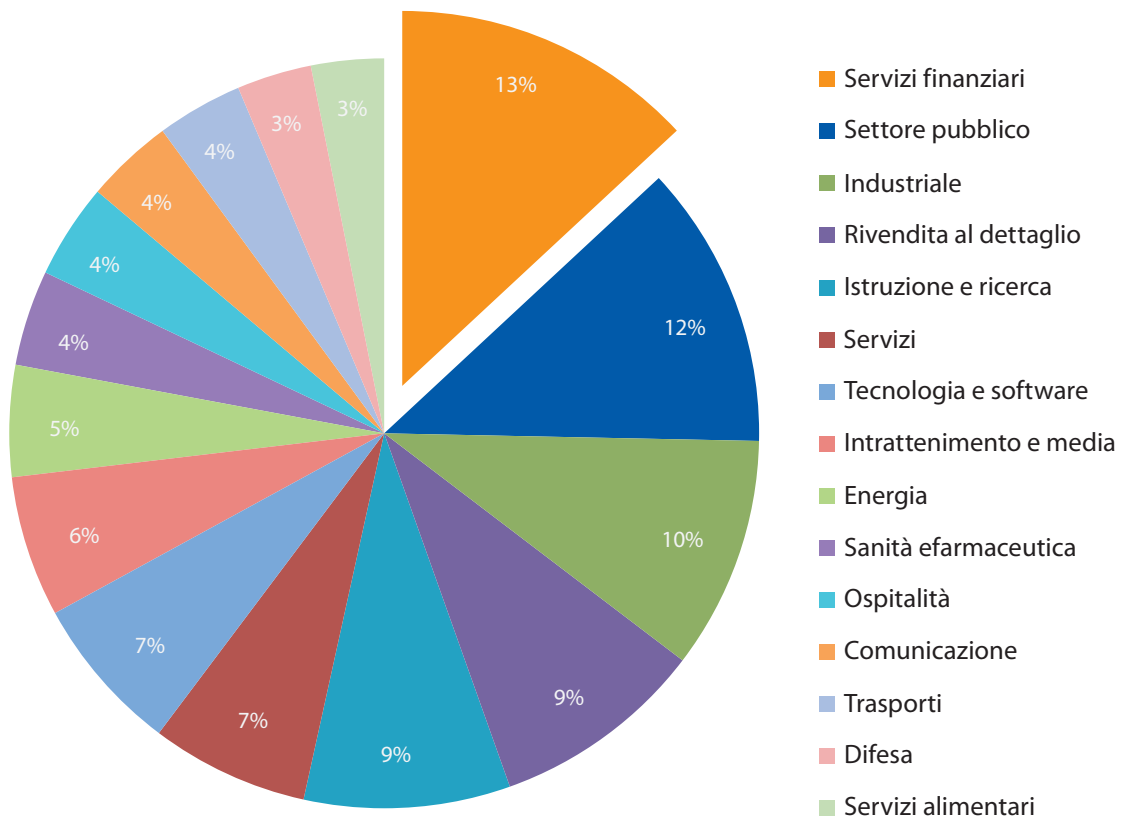


* Tutti gli intervistati sono stati filtrati per garantire che il campione fosse coinvolto nelle attività di backup e ripristino d'emergenza dell'azienda.

Appendice 2: Suddivisione degli intervistati per paese

Paese	Totale intervistati
Australia	259
Francia	231
Germania	483
Hong Kong	132
Italia	128
Giappone	231
Paesi Bassi	268
Norvegia	90
Singapore	102
Svizzera	113
Svezia	87
Regno Unito	411
Stati Uniti	516

Appendice 3: Grafico: Comparti di appartenenza degli intervistati



Appendice 4: Domande utilizzate nel sondaggio

Classifichi la sua opinione rispetto alle seguenti 11 affermazioni utilizzando le indicazioni fornite sotto ciascuna affermazione.

Le operazioni di backup e ripristino di emergenza della nostra azienda sono ben gestite.

Completamente d'accordo D'accordo Neutrale In disaccordo Completamente in disaccordo

La nostra azienda non ha timori rispetto al funzionamento corretto delle attività di backup e ripristino d'emergenza nel caso di un evento o incidente di grave entità.

Completamente d'accordo D'accordo Neutrale In disaccordo Completamente in disaccordo

I dirigenti aziendali sostengono pienamente le nostre attività di protezione e di backup e ripristino d'emergenza.

Completamente d'accordo D'accordo Neutrale In disaccordo Completamente in disaccordo

Disponiamo di abbondanti risorse che consentono attività di backup e ripristino d'emergenza complete.

Completamente d'accordo D'accordo Neutrale In disaccordo Completamente in disaccordo

Disponiamo di un gran numero di tecnologie che consentono attività di backup e ripristino d'emergenza complete.

Completamente d'accordo D'accordo Neutrale In disaccordo Completamente in disaccordo

Disponiamo di procedure e controlli di ampia portata che consentono attività di backup e ripristino d'emergenza complete.

Completamente d'accordo D'accordo Neutrale In disaccordo Completamente in disaccordo

Le procedure e le politiche di backup e ripristino d'emergenza della nostra azienda sono ben documentate.

Completamente d'accordo D'accordo Neutrale In disaccordo Completamente in disaccordo

La nostra azienda non subirebbe periodi di inattività critici nel caso in cui si verificasse un evento o un incidente di grave entità (ad esempio un evento climatico estremo, un attacco informatico e così via).

Completamente d'accordo D'accordo Neutrale In disaccordo Completamente in disaccordo

Il nostro personale della sicurezza e IT è qualificato per eseguire attività di backup e ripristino d'emergenza nel caso in cui si verificasse un evento o un incidente di grave entità (ad esempio un evento climatico estremo, un attacco informatico e così via).

Completamente d'accordo D'accordo Neutrale In disaccordo Completamente in disaccordo

La migrazione verso nuove tecnologie, quali il cloud computing e la virtualizzazione renderà ancora più facile garantire l'efficiente gestione delle attività di backup e ripristino d'emergenza.

Completamente d'accordo D'accordo Neutrale In disaccordo Completamente in disaccordo

La nostra azienda è in grado di eseguire un ripristino rapido in caso di inattività o guasto dei sistemi.

Completamente d'accordo D'accordo Neutrale In disaccordo Completamente in disaccordo

Informazioni su Ponemon Institute LLC

Ponemon Institute si occupa di ricerca e di formazione indipendenti che mirano a promuovere pratiche di gestione responsabile delle informazioni e della privacy all'interno di aziende e amministrazioni pubbliche. Il nostro obiettivo è condurre studi empirici di qualità elevata volti a migliorare la gestione e la sicurezza delle informazioni riservate e sensibili relative a persone e organizzazioni. In qualità di membri del Council of American Survey Research Organizations (CASRO),

ci atteniamo a standard severi di riservatezza dei dati, privacy e ricerca etica. Nelle nostre ricerche non vengono raccolte informazioni personali che consentano l'identificazione dei soggetti intervistati o delle aziende partecipanti agli studi. Inoltre, abbiamo adottato elevati standard di qualità per garantire che non vengano poste domande non pertinenti, irrilevanti o non adeguate. Per ulteriori informazioni, visitare il sito www.ponemon.org.

Informazioni su Acronis

Acronis è leader nella produzione di soluzioni per il backup, il ripristino e la sicurezza di ambienti fisici, virtuali e cloud, caratterizzate da elevate prestazioni e facilità d'uso. La brevettata tecnologia di disk imaging consente ad aziende di ogni dimensione come ad utenti privati di proteggere le proprie risorse digitali. Grazie ai prodotti software di Acronis per il ripristino, la distribuzione e

la migrazione, gli utenti possono proteggere le proprie informazioni digitali, garantire la continuità nei processi aziendali e ridurre i tempi di inattività. I prodotti e le soluzioni Acronis sono distribuiti in oltre 90 paesi e disponibili in 14 lingue. Per ulteriori informazioni, visitare www.acronis.it. Acronis è presente anche su Twitter: <http://twitter.com/acronis>.

Per ulteriori informazioni, visitare l'indirizzo <http://www.acronis.it>



Per acquistare i prodotti Acronis, visitare l'indirizzo www.acronis.it o cercare online un rivenditore autorizzato.

Altre informazioni sulle sedi Acronis sono reperibili all'indirizzo: <http://www.acronis.it/company/worldwide.html>

Copyright © 2000-2011 Acronis, Inc. Tutti i diritti riservati. "Acronis" e il logo Acronis sono marchi Acronis, Inc. Windows è un marchio registrato di Microsoft Corporation. Gli altri nomi menzionati possono essere marchi o marchi registrati dei rispettivi titolari. Soggetto a modifiche tecniche. Le immagini potrebbero non corrispondere al prodotto reale. Si declina qualsiasi responsabilità per possibili errori. 2011-01