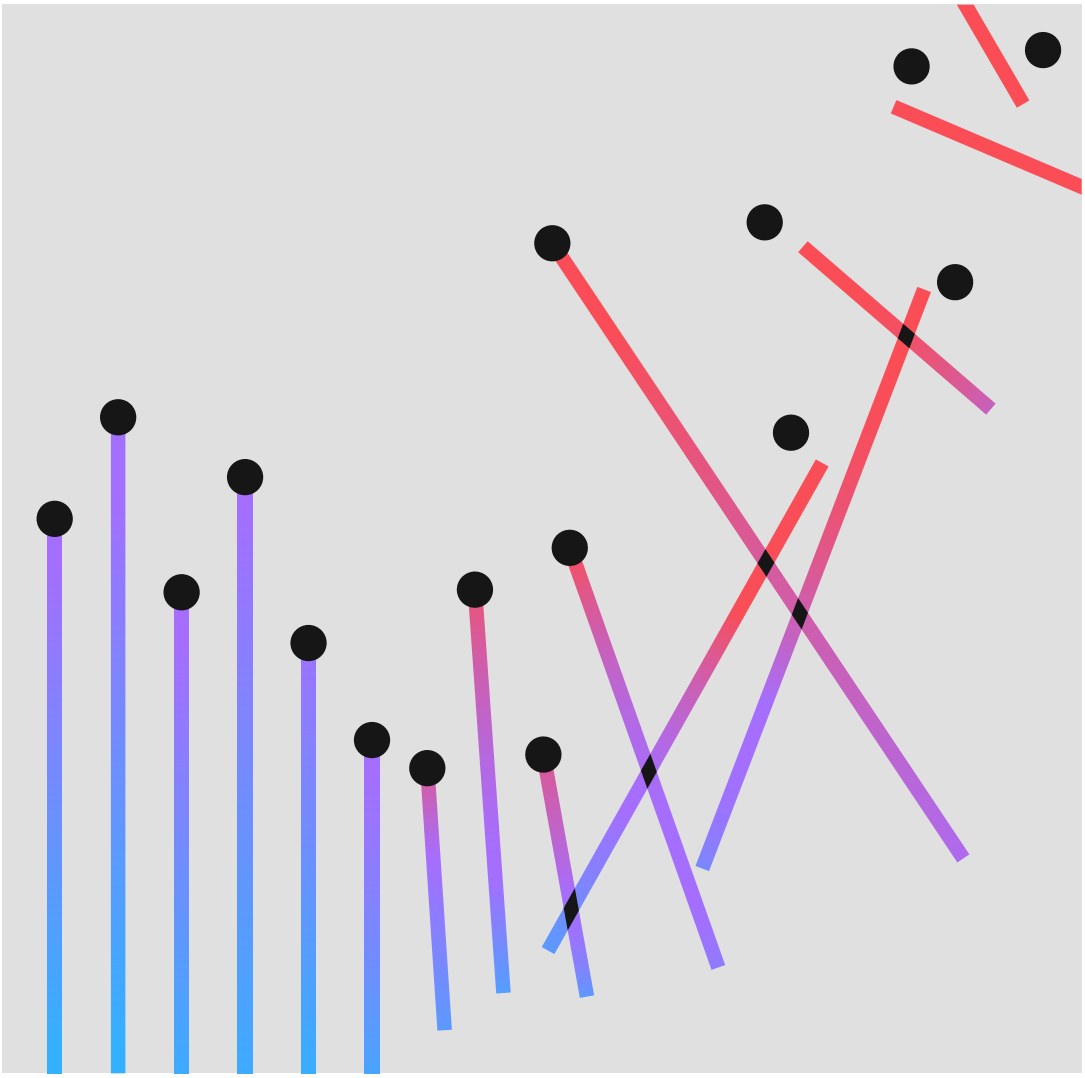
IBM **Security**

Cost of a Data Breach Report 2022: Il documento in sintesi



Sommario

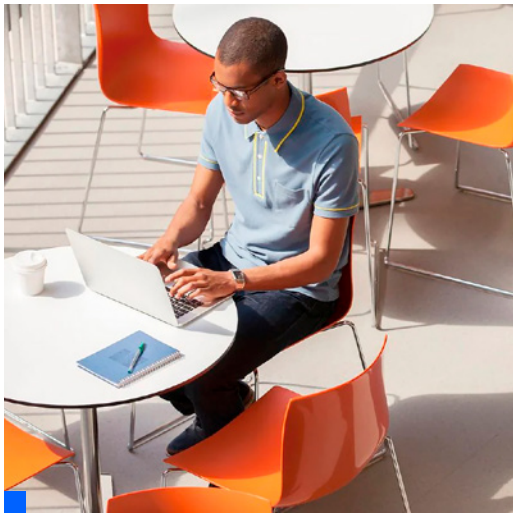
Il documento in sintesi

Il report Cost of a Data Breach offre ai responsabili IT, della gestione del rischio e della sicurezza una visione dei fattori che possono aumentare o contribuire a mitigare il costo crescente delle violazioni dei dati.

Giunta al 17° anno, questa ricerca - condotta in modo indipendente dal Ponemon Institute e sponsorizzata, analizzata e pubblicata da IBM Security® - ha preso in esame 550 organizzazioni colpite da violazioni di dati avvenute tra marzo 2021 e marzo 2022. Le violazioni si sono verificate in 17 Paesi e aree geografiche e in 17 settori diversi.

Abbiamo condotto più di 3.600 interviste con i rappresentanti di organizzazioni che hanno subito delle violazioni dei dati. Durante le interviste, abbiamo posto delle domande per determinare il costo subito dalle organizzazioni nelle diverse attività direttamente collegate alla risposta immediata e prolungata alle violazioni dei dati.

Come nei report degli anni precedenti, anche quest'anno i dati forniscono una visione di come decine di fattori incidano sui costi che continuano a sommarsi in seguito a una violazione dei dati. Inoltre, il report esamina le cause principali, le conseguenze a breve e a lungo termine delle violazioni dei dati e i fattori e le tecnologie di attenuazione che hanno permesso alle aziende di limitare le perdite.



Risultati principali

I risultati principali qui descritti si basano sull'analisi svolta da IBM Security sui dati di ricerca compilati dal Ponemon Institute.[1]

4,35 milioni di dollari

Costo totale medio di una violazione dei dati

Raggiungendo il suo massimo storico, nel 2022 il costo di una violazione dei dati è stato in media di 4,35 milioni di dollari. Questa cifra rappresenta un aumento del 2,6% rispetto allo scorso anno, quando il costo medio di una violazione era di 4,24 milioni di dollari. Il costo medio è aumentato del 12,7% rispetto ai 3,86 milioni di dollari del report del 2020.

83%

Percentuale di organizzazioni che hanno subito più di una violazione

L'83% delle organizzazioni interessate dallo studio ha subito più di una violazione dei dati e solo il 17% ha dichiarato che si è trattato del primo episodio. Il 60% delle organizzazioni ha dichiarato di aver aumentato il prezzo dei propri servizi o prodotti a causa della violazione dei dati.

4,82 milioni di dollari

Costo medio di una violazione dei dati di un'infrastruttura critica

Il costo medio di una violazione dei dati per le organizzazioni che si occupano di infrastrutture critiche interessate dallo studio è stato di 4,82 milioni di dollari, un milione di dollari in più rispetto al costo medio delle organizzazioni di altri settori. Le organizzazioni che si occupano di infrastrutture critiche sono quelle che operano nei settori dei servizi finanziari, industriali, tecnologici, energetici, dei trasporti, delle comunicazioni, della sanità, dell'istruzione e della pubblica amministrazione. Il 28% ha subito un attacco distruttivo o ransomware, mentre il 17% ha subito una violazione a causa della compromissione di un partner aziendale.

3,05 milioni di dollari

Risparmi medi sui costi associati all'implementazione completa dell'AI e dell'automazione della sicurezza

Le violazioni nelle organizzazioni dotate di un'implementazione completa dell'AI e dell'automazione della sicurezza hanno registrato un costo di 3,05 milioni di dollari in meno rispetto alle violazioni nelle organizzazioni prive di un'implementazione completa dell'AI e dell'automazione della sicurezza. Questa differenza del 65,2% nel costo medio di violazione (compreso tra 3,15 milioni di dollari per l'implementazione completa e 6,20 milioni di dollari per la mancata implementazione) rappresenta il più grande risparmio di costi riportato nello studio. Le aziende che hanno scelto un'implementazione completa dell'AI e dell'automazione della sicurezza hanno anche registrato una riduzione media di 74 giorni nel tempo medio necessario per identificare e contenere la violazione, noto come ciclo di vita della violazione, rispetto a quelle che non dispongono di AI e automazione della sicurezza: 249 giorni rispetto a 323 giorni. L'utilizzo dell'AI e dell'automazione della sicurezza è aumentato di quasi un quinto in due anni, passando dal 59% del 2020 al 70% del 2022.

1. Gli importi dei costi riportati nel presente report sono espressi in dollari USA.

4,54 milioni di dollari

Costo medio di un attacco ransomware, escluso il costo del riscatto

L'11% delle violazioni incluse nello studio è stato costituito da attacchi ransomware, con un tasso di crescita del 41% rispetto al 2021, anno in cui il ransomware rappresentava il 7,8% delle violazioni. Il costo medio di un attacco ransomware è leggermente diminuito, passando dai 4,62 milioni di dollari del 2021 ai 4,54 milioni di dollari del 2022. Questo costo è stato leggermente superiore al costo totale medio di una violazione dei dati, pari a 4,35 milioni di dollari.

19%

Frequenza delle violazioni causate da credenziali rubate o compromesse

L'uso di credenziali rubate o compromesse rimane la causa più comune delle violazioni dei dati. Le credenziali rubate o compromesse hanno rappresentato il principale vettore di attacco sia nello studio del 2022 (19% delle violazioni) che nello studio del 2021 (20% delle violazioni). Le violazioni causate da credenziali rubate o compromesse hanno registrato un costo medio di 4,50 milioni di dollari. Queste violazioni hanno avuto il ciclo di vita più lungo: 243 giorni per individuare la violazione e altri 84 giorni per contenerla. Il phishing ha costituito la seconda causa più comune di violazione, con il 16%, e anche la più costosa, con una media di 4,91 milioni di dollari di costi di violazione.

59%

Percentuale di organizzazioni che non implementano un approccio Zero Trust

Solo il 41% delle organizzazioni coinvolte nello studio ha dichiarato di adottare un'architettura di sicurezza Zero Trust. Il restante 59% delle organizzazioni che non adottano il framework Zero Trust incorre in un aumento medio dei costi di violazione di 1 milione di dollari rispetto a quelle che lo adottano. Tra le organizzazioni che si occupano di infrastrutture critiche, una percentuale ancora più alta, pari al 79%, non adotta l'approccio Zero Trust. Queste organizzazioni hanno registrato in media costi di violazione pari a 5,40 milioni di dollari, oltre un milione di dollari in più rispetto alla media globale.

1 milione di dollari

Differenza media dei costi nei casi in cui lo smart working è stato il fattore responsabile della violazione rispetto a quando non lo è stato

Quando lo smart working è stato un fattore responsabile della violazione, i costi sono stati in media superiori di quasi 1 milione di dollari rispetto alle violazioni in cui lo smart working non è stato un fattore: 4,99 milioni di dollari rispetto a 4,02 milioni di dollari. Le violazioni legate al lavoro a distanza costano in media circa 600.000 dollari in più rispetto alla media globale.

45%

Quota di violazioni avvenute nel cloud

Il 45% delle violazioni registrate nello studio si è verificato nel cloud. Tuttavia, le violazioni avvenute in un ambiente di cloud ibrido sono costate in media 3,80 milioni di dollari, in controtendenza rispetto ai 4,24 milioni di dollari delle violazioni avvenute nei cloud privati e ai 5,02 milioni di dollari delle violazioni avvenute nei cloud pubblici. La differenza di costo tra le violazioni del cloud ibrido e quelle del cloud pubblico è stata del 27,6%. Le organizzazioni con un modello di cloud ibrido hanno anche sperimentato cicli di vita delle violazioni più brevi rispetto alle organizzazioni che hanno adottato esclusivamente un modello di cloud pubblico o privato.

2,66 milioni di dollari

Risparmi medi sui costi associati a un team di risposta agli incidenti (IR) e a un piano IR verificato regolarmente

Quasi tre quarti delle organizzazioni interessate dallo studio hanno dichiarato di disporre di un piano IR, mentre il 63% ha affermato di verificarlo regolarmente. La presenza di un team IR e di un piano IR verificato regolarmente ha portato a significativi risparmi sui costi. Le aziende con un team IR che hanno verificato il proprio piano IR hanno registrato una riduzione media dei costi di violazione di 2,66 milioni di dollari rispetto alle organizzazioni prive di un team IR e che non verificano il piano IR. La differenza di 3,26 milioni di dollari rispetto ai 5,92 milioni di dollari rappresenta un risparmio del 58%.

29 giorni

Riduzione dei tempi di risposta per chi dispone di tecnologie di rilevamento e risposta estese (XDR)

Le tecnologie XDR (Xtended Detection and Response) sono state implementate dal 44% delle organizzazioni. Le organizzazioni dotate di tecnologie XDR hanno registrato notevoli vantaggi nei tempi di risposta. Le organizzazioni che hanno implementato le tecnologie XDR hanno ridotto il ciclo di vita delle violazioni di circa un mese, in media, rispetto alle organizzazioni che non le hanno implementate. In particolare, le organizzazioni dotate di tecnologie XDR hanno impiegato 275 giorni per identificare e contenere una violazione contro i 304 giorni delle organizzazioni prive di tecnologie XDR. Questa cifra rappresenta una differenza del 10% nei tempi di risposta.

12 anni

Anni consecutivi in cui il settore sanitario ha registrato il costo medio di una violazione più alto

I costi delle violazioni nel settore sanitario hanno raggiunto un nuovo record. La violazione media nel settore sanitario è aumentata di quasi 1 milione di dollari, raggiungendo i 10,10 milioni di dollari. I costi delle violazioni nel settore sanitario hanno reso questo settore il più costoso per 12 anni consecutivi, con un aumento del 41,6% rispetto al report del 2020. Le organizzazioni finanziarie hanno ottenuto il secondo costo più elevato, con una media di 5,97 milioni di dollari, seguite dai prodotti farmaceutici con 5,01 milioni di dollari, dalla tecnologia con 4,97 milioni di dollari e dall'energia con 4,72 milioni di dollari.

9,44 milioni di dollari

Costo medio di una violazione negli Stati Uniti, il più alto di tutti i Paesi

Le cinque nazioni/regioni con il costo medio di violazione dei dati più elevato sono stati gli Stati Uniti con 9,44 milioni di dollari, il Medio Oriente con 7,46 milioni di dollari, il Canada con 5,64 milioni di dollari, il Regno Unito con 5,05 milioni di dollari e la Germania con 4,85 milioni di dollari. Gli Stati Uniti guidano la classifica da 12 anni consecutivi. Nel frattempo, il Paese con il tasso di crescita più rapido rispetto all'anno precedente è stato il Brasile, con un aumento del 27,8%: da 1,08 milioni di dollari a 1,38 milioni di dollari.

Consigli per ridurre al minimo l’impatto finanziario di una violazione dei dati

In questa sezione, IBM Security illustra le misure che le organizzazioni possono adottare per ridurre i costi finanziari e le conseguenze sulla reputazione di una violazione dei dati. Queste raccomandazioni includono gli approcci alla sicurezza adottati con successo dalle organizzazioni che hanno partecipato allo studio.

Adottare un modello di sicurezza Zero Trust per evitare l’accesso non autorizzato ai dati sensibili.
I risultati dello studio hanno mostrato che, mentre solo il 41% delle organizzazioni ha implementato un approccio di sicurezza Zero Trust, con un’implementazione matura si può ottenere un potenziale risparmio sui costi di violazione pari a 1,5 milioni di dollari. Man mano che le organizzazioni incorporano lo smart working e gli ambienti ibridi multicloud, una strategia Zero Trust può aiutare a proteggere i dati e le risorse limitandone l’accessibilità e richiedendo un contesto.

Gli strumenti di sicurezza in grado di condividere dati tra sistemi diversi e di centralizzare le operazioni di sicurezza dei dati possono aiutare i team dedicati alla sicurezza a rilevare gli incidenti in ambienti ibridi multicloud complessi. È possibile ottenere insight più dettagliati, ridurre i rischi e accelerare la risposta grazie a una piattaforma di sicurezza aperta in grado di far progredire la strategia Zero Trust. Allo stesso tempo, è possibile utilizzare gli investimenti esistenti lasciando i dati dove sono, aiutando così il team a diventare più efficiente e collaborativo.

Proteggere i dati sensibili in ambienti cloud utilizzando le policy e la crittografia.
Negli ambienti cloud vengono ospitati quantitativi e valori sempre maggiori di dati: le aziende devono quindi provvedere a proteggere i database su cloud. Pratiche di sicurezza del cloud mature sono state associate a un risparmio sui costi di violazione pari a 720.000 dollari rispetto alla mancanza di pratiche di sicurezza del cloud. È opportuno utilizzare lo schema di classificazione dei dati e i programmi di conservazione per contribuire a dare visibilità e a ridurre il volume di informazioni sensibili che sono vulnerabili a una violazione. È consigliabile proteggere le informazioni sensibili mediante la crittografia dei dati e la crittografia con omomorfia totale. L'utilizzo di un framework interno per gli audit, la valutazione del rischio in tutta l'azienda e il monitoraggio della conformità ai requisiti di governance possono contribuire a migliorare la capacità di rilevare una violazione dei dati e a intensificare gli sforzi di contenimento.

Investire in orchestrazione, automazione e risposta della sicurezza (SOAR, Security Orchestration, Automation and Response) e XDR per migliorare i tempi di rilevamento e risposta.
Insieme all'intelligenza artificiale e all'automazione della sicurezza, le funzionalità XDR possono contribuire a ridurre significativamente i costi medi delle violazioni dei dati e i cicli di vita delle violazioni. Secondo lo studio, le organizzazioni che hanno implementato le tecnologie XDR hanno ridotto il ciclo di vita delle violazioni di una media di 29 giorni rispetto alle organizzazioni che non le hanno implementato, con un risparmio sui costi pari a 400.000 dollari. I software SOAR e SIEM (Security Information and Event Management), i servizi di rilevamento e risposta gestiti e le tecnologie XDR possono aiutare un'organizzazione ad accelerare la risposta agli incidenti mediante l'automazione, la standardizzazione dei processi e l'integrazione con gli strumenti di sicurezza esistenti.

Utilizzare strumenti che aiutino a proteggere e monitorare gli endpoint e i dipendenti a distanza.
Nello studio, le violazioni in cui lo smart working è stato un fattore responsabile della violazione sono costate quasi un milione di dollari in più rispetto a quelle in cui lo smart working non è stato un fattore. I prodotti e i servizi di gestione unificata degli endpoint (UEM, Unified Endpoint Management), di rilevamento e risposta degli endpoint (EDR, Endpoint Detection and Response) e di gestione delle identità e degli accessi (IAM, Identity and Access Management) possono contribuire a fornire ai team dedicati alla sicurezza una visibilità più approfondita sulle attività sospette. Questa sorveglianza coinvolge i dispositivi BYOD (Bring Your Own Device) e i laptop, i desktop, i tablet, i dispositivi mobili e l'IoT dell'azienda, compresi gli endpoint a cui l'organizzazione non ha accesso fisico. Le soluzioni UEM, EDR e IAM accelerano le indagini e i tempi di risposta per isolare e contenere i danni delle violazioni per cui lo smart working è stato un fattore responsabile.

Creare e verificare dei playbook di risposta agli incidenti per aumentare la resilienza informatica.
Due tra i modi più efficaci per mitigare i costi di una violazione dei dati sono la formazione di un team di risposta agli incidenti (IR) e la verifica approfondita del piano IR. Le violazioni rilevate nelle organizzazioni dotate di team IR che verificano regolarmente il proprio piano hanno registrato un risparmio di 2,66 milioni di dollari rispetto alle violazioni registrate nelle organizzazioni prive di team IR o di verifica del piano IR. Le organizzazioni possono reagire rapidamente per contenere le conseguenze di una violazione, stabilendo un playbook dettagliato sugli incidenti informatici. Verificare regolarmente il piano attraverso esercitazioni o eseguendo uno scenario di violazione in un ambiente simulato, ad esempio un cyber range.

Le esercitazioni di simulazione degli avversari, note anche come Red Teaming, possono migliorare l'efficacia dei team IR scoprendo percorsi e tecniche di attacco che potrebbero sfuggire e identificando le lacune nelle loro capacità di rilevamento e risposta. Una soluzione di Attack Surface Management (ASM) può aiutare le organizzazioni a migliorare la propria efficacia nella sicurezza individuando punti di esposizione precedentemente sconosciuti mediante simulazioni di un'esperienza di attacco autentica.

Le raccomandazioni sulle pratiche di sicurezza hanno esclusivamente scopo didattico e non sono garanzia di risultati.

Informazioni sul Ponemon Institute e su IBM Security

Ponemon Institute

Il Ponemon Institute si dedica alla ricerca e alla didattica indipendente con lo scopo di far progredire le pratiche di gestione responsabile delle informazioni e della privacy nelle aziende e nelle amministrazioni pubbliche. La nostra missione è condurre studi empirici di alta qualità su questioni critiche che riguardano la gestione e la sicurezza di informazioni sensibili relative a persone e organizzazioni.

Il Ponemon Institute si attiene a rigorosi standard di riservatezza dei dati, privacy ed etica della ricerca e non raccoglie informazioni di identificazione personale dalle persone o informazioni di identificazione aziendale nell'ambito delle ricerche aziendali. Inoltre, i rigorosi standard di qualità garantiscono che ai soggetti non vengano poste domande non pertinenti, irrilevanti o improprie.

IBM Security

IBM Security offre uno dei portafogli più avanzati e integrati di prodotti e servizi per la sicurezza aziendale. Il portafoglio, supportato dalla ricerca di fama mondiale IBM Security X-Force®, offre soluzioni di sicurezza per aiutare le organizzazioni a integrare la sicurezza nel tessuto aziendale, in modo da poter prosperare anche in uno scenario di incertezza.

IBM gestisce una delle più ampie e preparate organizzazioni di ricerca, sviluppo e fornitura di soluzioni di sicurezza. IBM, che monitora oltre 4,7 bilioni di eventi al mese in più di 130 Paesi, detiene oltre 10.000 brevetti in materia di sicurezza. Per saperne di più, visita ibm.com/it-it/security. Partecipa alla discussione nella IBM Security Community.

Per domande o commenti sul presente report, compresa l'autorizzazione a citarlo o riprodurlo, contatta via posta tradizionale, telefono o e-mail:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City
Michigan 49686 USA

1.800.887.3118
research@ponemon.org

Fasi successive

Soluzioni di sicurezza Zero Trust
Applica la sicurezza a ogni utente, dispositivo e connessione.
Scopri di più

Gestione delle identità e degli accessi (IAM)
Collega ogni utente, API e dispositivo a ogni app in modo sicuro.
Scopri di più

Sicurezza dei dati
Scopri, classifica e proteggi i dati aziendali sensibili.
Scopri di più

Orchestrazione, automazione e risposta della sicurezza (SOAR)
Accelera la risposta agli incidenti mediante l'orchestrazione e l'automazione.
Scopri di più

Gestione delle informazioni e degli eventi di sicurezza (SIEM)
Ottieni visibilità per rilevare, indagare e rispondere alle minacce.
Scopri di più

Sicurezza del cloud
Integra la sicurezza nel tuo percorso verso il multicloud ibrido.
Scopri di più

Sicurezza degli endpoint
Proteggi dispositivi, utenti e organizzazioni da attacchi sofisticati.
Scopri di più

Servizi di sicurezza informatica
Riduci i rischi mediante servizi di consulenza, cloud e sicurezza gestita.
Scopri di più

Risposta agli incidenti e intelligence relativa alle minacce
Gestisci e rispondi in modo proattivo alle minacce alla sicurezza.
Scopri di più

Prenota una consulenza individuale con un esperto di IBM Security X-Force
Prenota ora

IBM Italia S.p.A.
Circonvallazione Idroscalo
20054 Segrate (Milano)
Italia

Prodotto negli Stati Uniti d'America
Luglio 2022

Le informazioni contenute nel presente documento sono aggiornate alla data della prima pubblicazione e potrebbero essere modificate da IBM senza alcun preavviso. Non tutte le offerte sono disponibili in tutti i Paesi in cui IBM opera.

I dati sulle prestazioni e gli esempi di clienti citati sono presentati solo a scopo illustrativo. Le prestazioni effettive possono variare a seconda delle configurazioni e delle condizioni operative specifiche. LE INFORMAZIONI FORNITE NEL PRESENTE DOCUMENTO SONO DA CONSIDERARSI "NELLO STATO IN CUI SI TROVANO", SENZA GARANZIE, ESPLICITE O IMPLICITE, IVI INCLUSE GARANZIE DI COMMERCIABILITÀ, DI IDONEITÀ PER UN PARTICOLARE SCOPO E GARANZIE O CONDIZIONI DI NON VIOLAZIONE. I prodotti IBM sono coperti da garanzia in accordo con termini e condizioni dei contratti sulla base dei quali vengono forniti.

Dichiarazione di conformità alle procedure di sicurezza: la sicurezza dei sistemi IT implica la protezione di sistemi e dati mediante prevenzione, rilevamento e risposta ad accessi impropri all'interno e all'esterno dell'azienda. L'accesso improprio può causare l'alterazione, la distruzione, l'appropriazione indebita o l'uso improprio delle informazioni; può inoltre provocare danni e uso improprio dei sistemi, che possono essere utilizzati per attaccare altri sistemi. Nessun prodotto o sistema IT può essere considerato completamente sicuro e nessun prodotto, servizio o misura di sicurezza è del tutto efficace nel prevenire l'uso o l'accesso improprio. Sistemi, prodotti e servizi IBM sono progettati come elementi di un approccio di sicurezza completo, nel rispetto delle normative, che richiederà necessariamente procedure operative aggiuntive e il probabile impiego di altri sistemi, prodotti o servizi per raggiungere la massima efficienza. IBM NON GARANTISCE CHE SISTEMI, PRODOTTI O SERVIZI SIANO ESENTI DA O RENDERANNO L'AZIENDA ESENTE DA, CONDOTTA MALEVOLA O ILLEGALE DI UNA QUALSIASI TERZA PARTE.

È responsabilità del cliente assicurare la conformità a normative e regolamenti applicabili. IBM non fornisce consulenza legale né dichiara o garantisce che i propri servizi o prodotti assicurino al cliente la conformità con qualsivoglia legge o regolamento. Le dichiarazioni riguardanti la direzione e le intenzioni future di IBM sono soggette a modifiche o revoche senza preavviso e rappresentano solo obiettivi e finalità.