Delinea

WHITEPAPER

# La sicurezza dell'identità è fondamentale per ottenere e preservare la cyber insurance

## Report della ricerca sulla cyber insurance 2024

# Prefazione

La cyber insurance è una componente fondamentale di un programma di gestione dei rischi informatici per garantire resilienza e recupero. Dal momento che stipulare una cyber insurance è diventata una prassi standard per le organizzazioni di tutti i tipi, l'attenzione si è spostata sul mantenimento dell'assicurabilità anche quando i fattori di rischio cambiano.

Poiché gli incidenti informatici hanno scosso il settore, le compagnie assicurative stanno effettuando valutazioni dei rischi dettagliate ed è sempre più difficile per i responsabili informatici dimostrare il valore del loro programma di sicurezza e ottenere una copertura solida. Le organizzazioni devono fornire prove pertinenti per garantire che la loro assicurazione continui a essere valida e venga aumentata o adeguata secondo necessità. Per le organizzazioni complesse ed ibride con profili di rischio mutevoli, raccogliere informazioni accurate e aggiornate può rivelarsi un compito estremamente laborioso e che richiede molto tempo.

In questa ricerca condotta su 300 decisori, analizziamo il modo in cui le aziende affrontano queste sfide per ottenere e preservare una cyber insurance. In particolare, esploreremo come le organizzazioni stanno adottando tecnologie più recenti, come l'intelligenza artificiale, per aumentare l'efficienza, crescere rapidamente e ridurre i costi.

## Punti chiave:

1. **Le lacune nella sicurezza dell'identità sono la causa più comune degli incidenti informatici che danno luogo a richieste di risarcimento assicurativo. La compromissione dell'identità e dei privilegi è responsabile del 47% degli attacchi che danno luogo a richieste di risarcimento assicurativo.**

2. **Le compagnie assicurative esigono la prova della sicurezza dell'identità prima di concedere una polizza. Oltre il 40% delle compagnie assicurative richiede controlli di accesso/autorizzazione basati sui privilegi minimi prima di concedere una polizza. Praticamente tutte le aziende statunitensi (95%) hanno dovuto investire in soluzioni di sicurezza dell'identità prima di ottenere una polizza.**

3. **Sebbene i costi complessivi delle cyber insurance siano in aumento, l'IA sta fornendo una leva finanziaria ai titolari delle polizze. Metà delle aziende statunitensi utilizza il rilevamento e il monitoraggio delle minacce supportati dall'IA per ridurre i premi delle cyber insurance.**

**47%**

La compromissione dell'identità e dei privilegi è responsabile del 47% degli attacchi che danno luogo a richieste di risarcimento assicurativo

Continua a leggere per confrontare le tue pratiche di sicurezza dell'identità e le tue strategie di cyber insurance. Ciò che scoprirai ti aiuterà a predisporre la tua prossima valutazione assicurativa informatica e a individuare modi innovativi per ridurre sforzi e costi.

# Punto chiave 1

## Le lacune nella sicurezza dell'identità sono la causa più comune degli incidenti informatici che danno luogo a richieste di risarcimento assicurativo.

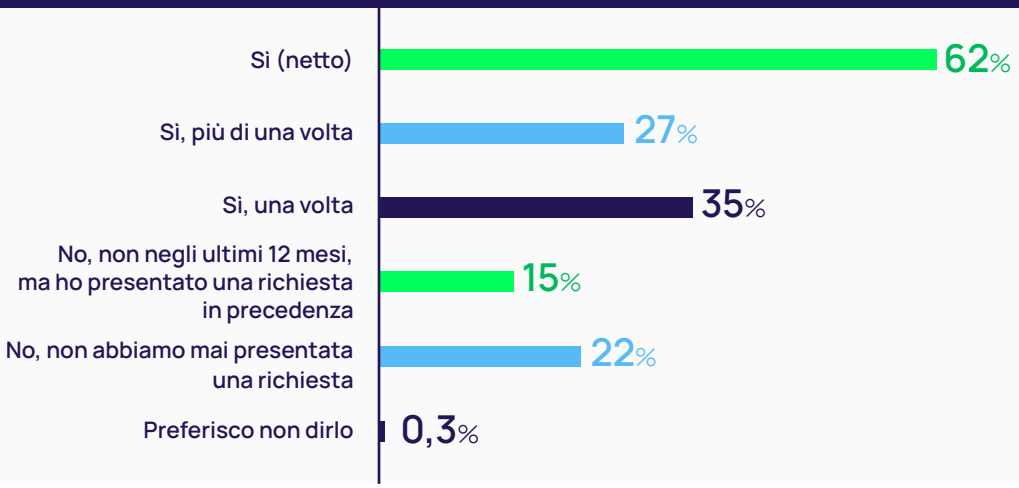
### La frequenza delle richieste di risarcimento da danni informatici rimane elevata.

Una volta che le aziende hanno una cyber insurance, la utilizzano.

I dati mostrano che il 77% delle aziende assicurate ha già presentato una richiesta di risarcimento. Ciò è in linea con i risultati del sondaggio Delinea del 2023, dove il 79% degli intervistati ha affermato di aver utilizzato una cyber insurance in passato.

Solo negli ultimi 12 mesi, il 62% delle aziende ha presentato una richiesta di risarcimento. È stato un anno particolarmente negativo per oltre il 27% delle aziende, che hanno presentato più di una richiesta nel corso dei 12 mesi precedenti.

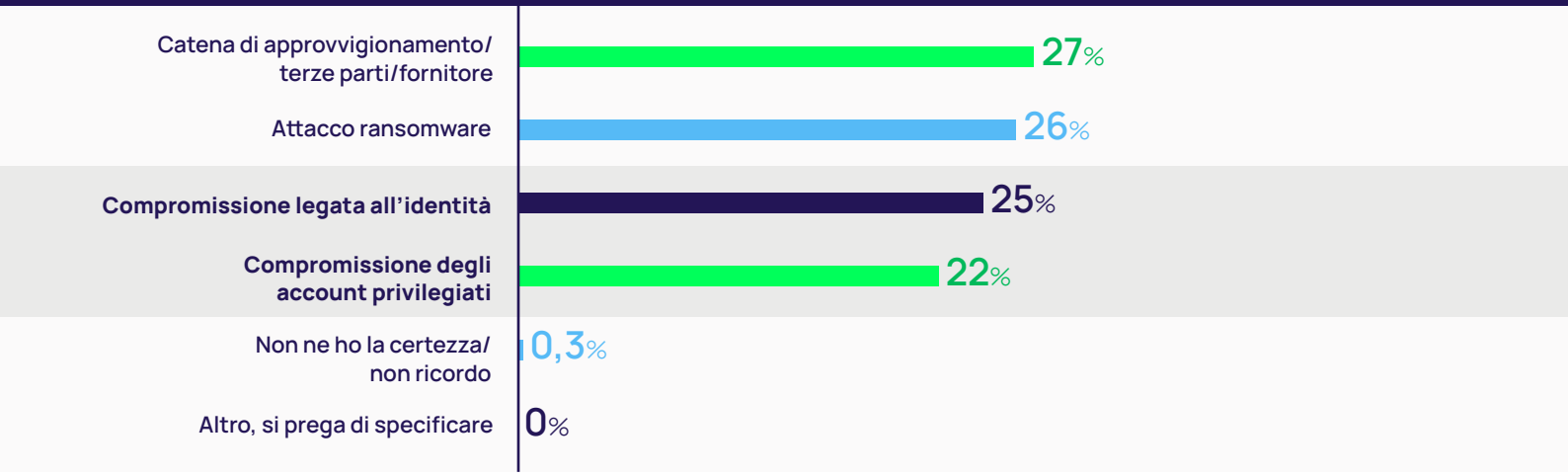
**Figura 1** | La tua organizzazione ha presentato una richiesta di risarcimento per danni informatici negli ultimi 12 mesi?




### Le tecniche di attacco sfruttano identità e account privilegiati.

Nell'insieme, i due vettori di attacco all'identità, ovvero la compromissione dell'identità e la compromissione degli account privilegiati, causano oltre il 47% degli attacchi che portano a richieste di risarcimento assicurativo.

**Figura 2** | Cosa ha causato l'incidente informatico a cui è collegata la richiesta di risarcimento assicurativo?



Oggigiorno, la maggior parte degli aggressori informatici non ha bisogno di entrare nel sistema: basta semplicemente effettuare il login. Gli attacchi basati sull'identità solitamente iniziano quando un aggressore utilizza credenziali valide rubate o acquistate. Possono utilizzare tali credenziali per fingersi un'identità autorizzata o utilizzare un account privilegiato per sbloccare l'accesso a risorse protette. A seconda del livello di accesso associato a tale identità o account privilegiato, l'aggressore potrebbe essere in grado di scaricare malware, manipolare dati, arrestare sistemi o altro, tutte azioni che potrebbero portare ad una potenziale richiesta di risarcimento alla compagnia assicurativa.

Nell'ambito della catena di approvvigionamento, terze parti quali appaltatori, fornitori e partner hanno spesso accesso a dati sensibili e sistemi IT. Ad esempio, i team addetti alle operazioni IT spesso esternalizzano attività come la risoluzione dei problemi, mentre i team di ingegneria solitamente si avvalgono di sviluppatori esterni. Questi utenti possono accedere alle risorse utilizzando un account privilegiato condiviso o un'identità singola. Troppo spesso, queste tipologie di utenti operano senza un'adeguata supervisione e l'accesso resta attivo molto tempo dopo il completamento dei progetti, lasciando vulnerabilità che i malintenzionati sfrutteranno, con conseguenti potenziali risarcimenti per gli assicuratori.

Spesso il ransomware si diffonde tramite tecniche di ingegneria sociale o phishing, incoraggiando gli utenti con privilegi locali a fare clic su un link con cui scaricare malware. Una volta che ha messo piede nel sistema, un aggressore può crittografare i dati e chiedere un riscatto per la chiave di crittografia, oppure esfiltrare i dati e minacciare di pubblicarli se non viene pagato un riscatto.

## Le aziende stipulano una copertura assicurativa contro i rischi informatici per supportare i requisiti di conformità e garantire la continuità aziendale.

Abbiamo chiesto alle aziende perché cercavano una copertura assicurativa *al momento in cui l'hanno stipulata*. Tra i fattori scatenanti rientrano la conformità ai requisiti normativi, le direttive della dirigenza o del consiglio di amministrazione e le risposte a recenti attacchi informatici, sia all'interno del settore sia che interessano direttamente l'organizzazione.

Gli intervistati segnalano che i requisiti di conformità/normativi sono i *fattori n. 1* per ottenere una cyber insurance. Il punto in questo caso non è che normative come PCI, HIPAA e altri quadri normativi di conformità richiedano che le entità interessate abbiano una cyber insurance. E non è neppure il caso che la cyber insurance sia una strategia efficace per pagare le sanzioni per non conformità, almeno per la maggior parte delle aziende; la realtà è che le sanzioni normative sono la spesa ***meno comune*** che la cyber insurance pagherà.

**Figura 3 A** | Quali erano i motivi principali per cui hai richiesto una cyber insurance all'epoca?

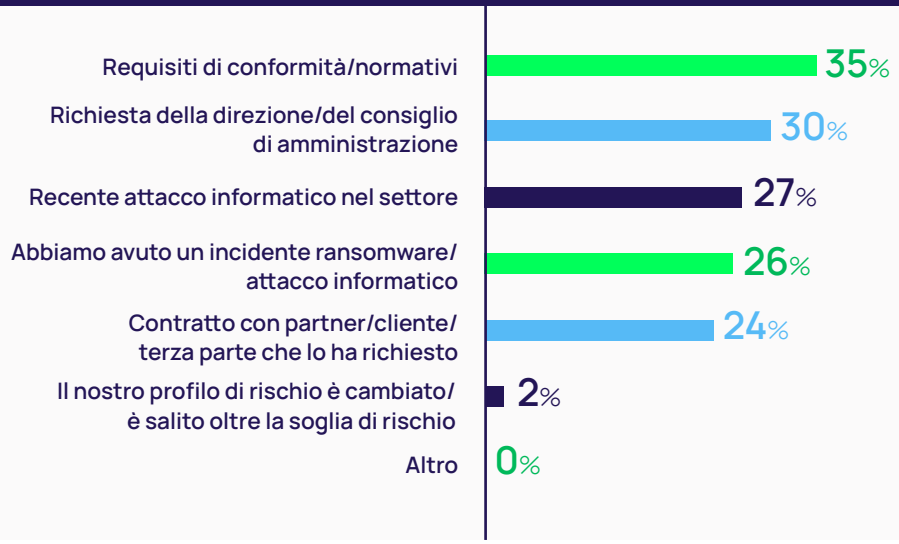
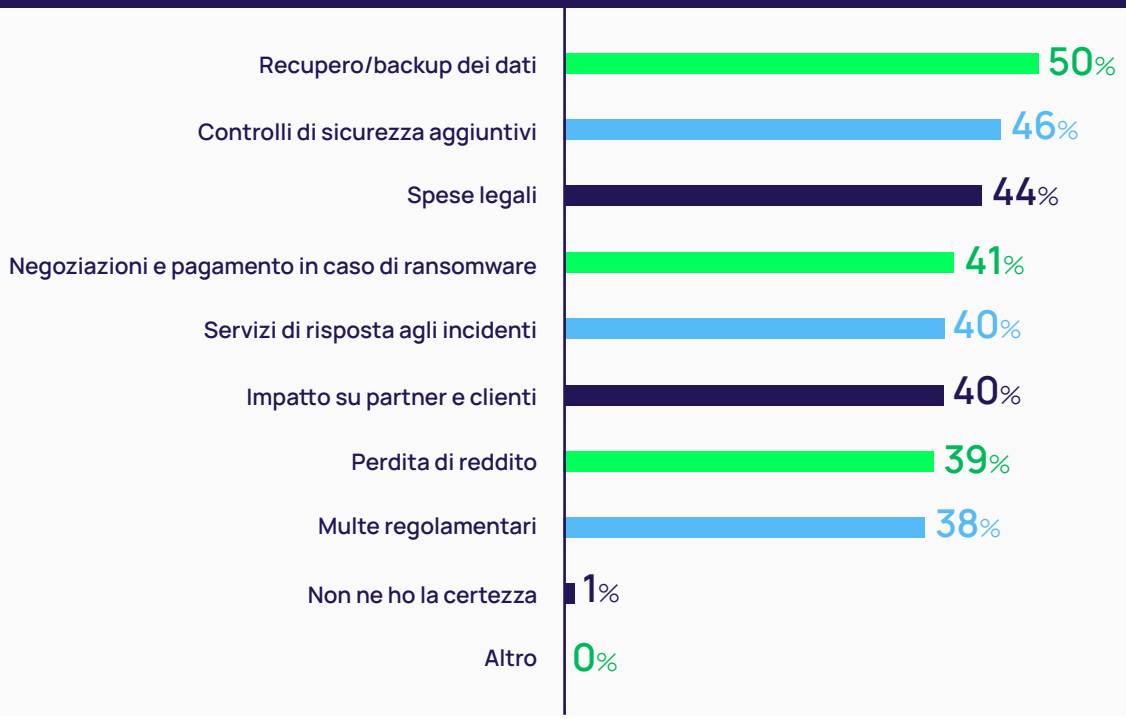


**Figura 3 B** | Cosa coprirebbe la tua polizza di cyber insurance?




Più probabilmente, le aziende soggette a normative di settore dovranno affrontare sanzioni severe per inosservanza delle norme sulla protezione dei dati. Un rapido ripristino e backup possono aiutare ad evitare multe e altri costi associati alla non conformità in seguito a una violazione dei dati, perché consentono di recuperare e proteggere rapidamente i dati.

La cyber insurance si concentra principalmente sui servizi di backup e recupero dati, perché sono essenziali per ridurre al minimo i tempi di inattività e le perdite finanziarie dopo un incidente informatico. Coprendo questi servizi, gli assicuratori favoriscono una rapida ripresa e la resilienza aziendale, con vantaggi sia per la società assicurata sia per le compagnie assicurative.

Bisogna inoltre tenere presente che l'assicurazione è una strategia di gestione del rischio, non una strategia di cyber security. Molte aziende utilizzano quadri normativi di conformità o di cyber security come il NIST per orientare i propri programmi di sicurezza, anche se non sono entità interessate. Questi quadri normativi richiedono la prova dei controlli di sicurezza, così come faranno le compagnie assicurative, poiché è dimostrato che riducono i rischi. Se adotterai questi controlli, riuscirai a soddisfare sia gli enti regolatori sia le compagnie assicurative. Anche se non hai vincoli di normative che comportano potenziali sanzioni, non puoi semplicemente saltare questa parte ed aspettarti di superare il prossimo audit o la successiva valutazione assicurativa.

Metà delle aziende statunitensi utilizza il rilevamento e il monitoraggio delle minacce supportati dall'IA per ridurre i premi delle cyber insurance

# Punto chiave 2

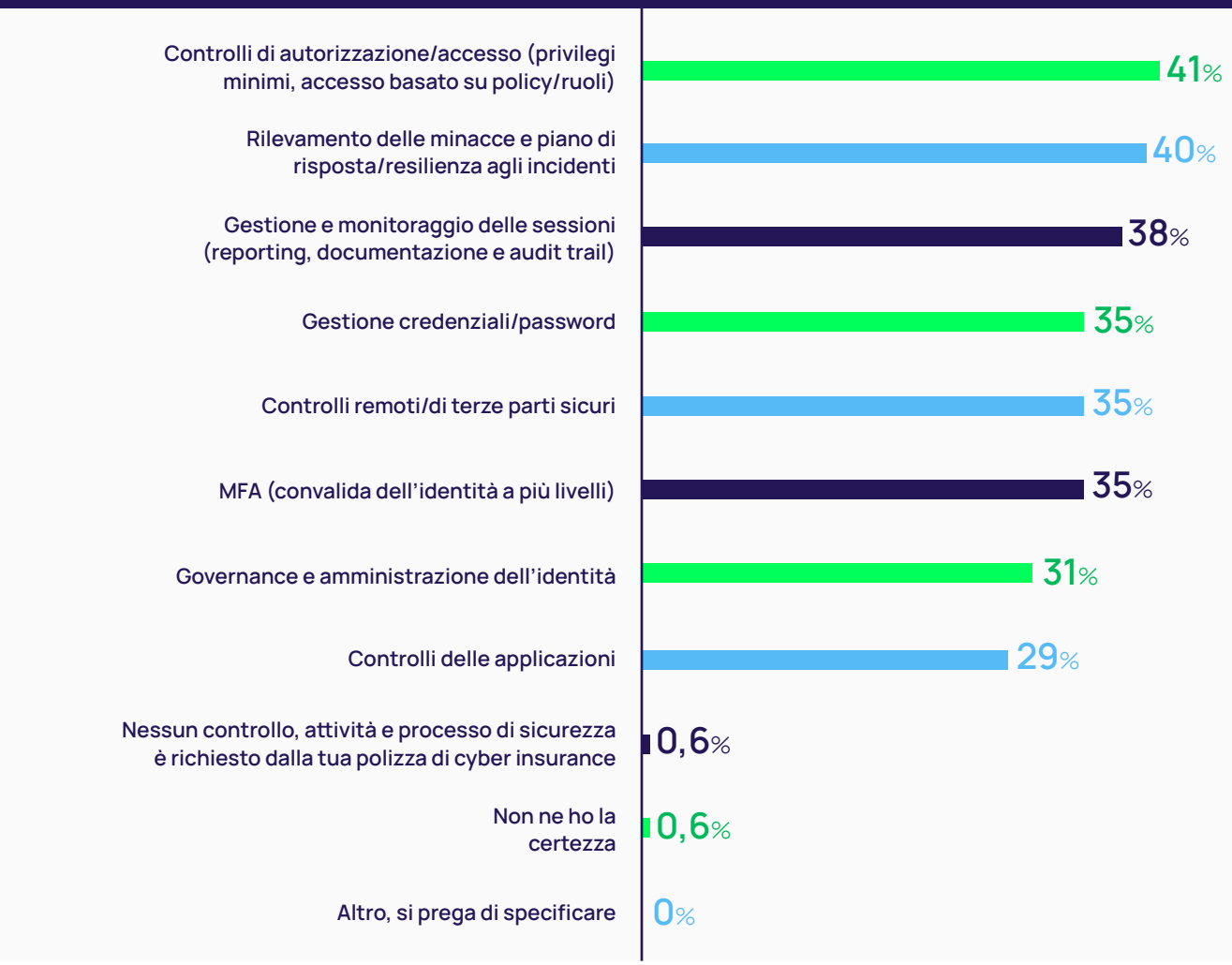
## Le compagnie assicurative richiedono la prova della sicurezza dell'identità prima di concedere una polizza: il 41% richiede controlli di autorizzazione.

### Le compagnie assicurative esigono controlli, attività e processi di sicurezza dell'identità.

Ora che dispongono di più dati storici che indicano la causa degli attacchi informatici, molte compagnie assicurative hanno imposto ai propri assicurati di ridurre al minimo la probabilità e l'impatto degli incidenti informatici, riducendo così i potenziali risarcimenti per le richieste. Quasi tutti gli intervistati hanno una qualche forma di requisito di sicurezza dell'identità imposto dalla loro compagnia di cyber insurance. La maggior parte degli intervistati afferma che le polizze di cyber insurance richiedono molteplici controlli di sicurezza dell'identità.

Le compagnie assicurative solitamente richiedono ai titolari delle polizze di definire controlli relativi all'autorizzazione/accesso con privilegi minimi, seguiti da vicino dal rilevamento delle minacce e dalla risposta.

**Figura 4** | Quali controlli, attività e processi di sicurezza sono richiesti dalla tua polizza di cyber insurance?




Questi controlli sono conformi alle migliori pratiche del settore e ai requisiti normativi. Controlli di sicurezza efficaci non solo aiutano a prevenire gli incidenti, ma garantiscono anche che le organizzazioni possano rispondere in modo rapido ed efficace, riducendo i tempi di inattività e le perdite finanziarie. Grazie all'obbligo di controlli di sicurezza completi, le compagnie assicurative possono gestire e prevedere meglio le potenziali perdite, ottenendo così premi più stabili e prevedibili per i titolari delle polizze.

# Richiesta di definizione dei di sicurezza dell'identità

## Controlli di accesso/ autorizzazione

I controlli di accesso autorizzano i sistemi e i dati a cui un'identità può accedere e le azioni che può intraprendere con tale accesso. Le aziende solitamente gestiscono l'autorizzazione tramite policy quali controlli di accesso basati sui ruoli o controlli di accesso basati sugli attributi. Le best practice basate sui privilegi minimi richiedono che le identità abbiano solo le autorizzazioni necessarie per svolgere le proprie funzioni lavorative, solo quando ne hanno bisogno.

## Controlli delle applicazioni

I controlli delle applicazioni aiutano a bilanciare le best practice basate sui privilegi minimi e la produttività degli utenti. Le applicazioni attendibili vengono aggiunte agli elenchi di applicazioni consentite per l'installazione o l'esecuzione automatica, mentre le applicazioni dannose note (malware) vengono aggiunte agli elenchi di applicazioni vietate e bloccate. Le applicazioni sconosciute possono essere collocate in una sandbox finché non vengono esaminate e approvate.

## Gestione credenziali/ password

Le credenziali includono nomi utente, password, token e altri segreti che sbloccano l'accesso ai tuoi sistemi e dati. Gli aggressori informatici utilizzano metodi quali il credential stuffing e il password cracking per rubare le credenziali. Possono anche acquistare credenziali da broker di accesso sul dark web. Per prevenire i furti, le credenziali devono essere difficili da indovinare e sempre protette. È possibile conservare le credenziali in un vault crittografato di livello militare. La gestione continua delle credenziali, attraverso meccanismi quali rotazione e scadenza, garantisce una durata limitata.

## Governance e amministrazione dell'identità (IGA)

L'IGA controlla le autorizzazioni per le identità durante tutto il loro ciclo di vita, incluso quando gli utenti entrano, si trasferiscono o lasciano il proprio ruolo, e consente la supervisione di tutte le identità nella tua organizzazione (umane e automatiche), semplificando la dimostrazione di tale supervisione a auditor, compagnie di cyber insurance e organismi di conformità.

## Autenticazione a più fattori (MFA)

L'autenticazione a più fattori convalida le identità umane chiedendo alle persone di fornire qualcosa in loro possesso (ad esempio un codice su un telefono o un'impronta digitale) o qualcosa che conoscono (ad esempio domande di verifica). Le best practice prevedono la convalida dell'identità a ogni interazione che comporti un rischio elevato, tra cui l'accesso iniziale e l'elevazione dei privilegi.

## Controlli remoti/di terze parti sicuri

Questi controlli consentono ai dipendenti da remoto e a terze parti di accedere in modo sicuro alle risorse di cui hanno bisogno per completare il loro lavoro, continuando comunque a essere attentamente monitorati per una supervisione continua.

## Gestione e monitoraggio delle sessioni

La gestione e il monitoraggio continuo delle sessioni rilevano anomalie nelle attività e negli eventi di identità, favorendo la prevenzione proattiva degli incidenti e una risposta rapida. Gli audit trail consentono di identificare schemi utili per prevedere i rischi e accelerare l'analisi forense post-evento. Inoltre, i resoconti granulari consentono di monitorare i miglioramenti nella sicurezza dell'identità, garantire la responsabilità e dimostrare l'efficacia dei controlli alle compagnie di cyber insurance.

## Rilevamento delle minacce e risposta agli incidenti

Un rilevamento delle minacce e una risposta agli incidenti che siano efficaci sono essenziali per la cyber resilience e la continuità aziendale. I controlli includono meccanismi per rilevare le minacce e un piano di risposta strutturato per mitigare proattivamente i rischi e contenere e porre rimedio agli incidenti in corso. Ciò include ridondanze per garantire interruzioni minime o nulle durante un incidente.

## L'importanza della sicurezza dell'identità è ribadita dagli esperti di sicurezza e di cyber insurance

**CJ Dietzman**
Vicepresidente Senior di Alliant Insurance Service

Quando penso alle aspettative delle compagnie assicurative e dei sottoscrittori, la sicurezza dell'identità è diventata una posta in gioco fondamentale. Il modo in cui le compagnie di cyber insurance misurano il rischio si basa su incidenti, leggi e richieste di risarcimento. Quando eseguiamo il reverse engineering degli attacchi informatici, spesso abbiamo riscontrato punti deboli nella gestione delle identità. È necessario disporre di una buona narrazione di controlli integrati e di una storia olistica su come si mitiga il rischio di accesso non autorizzato e si proteggono le identità."

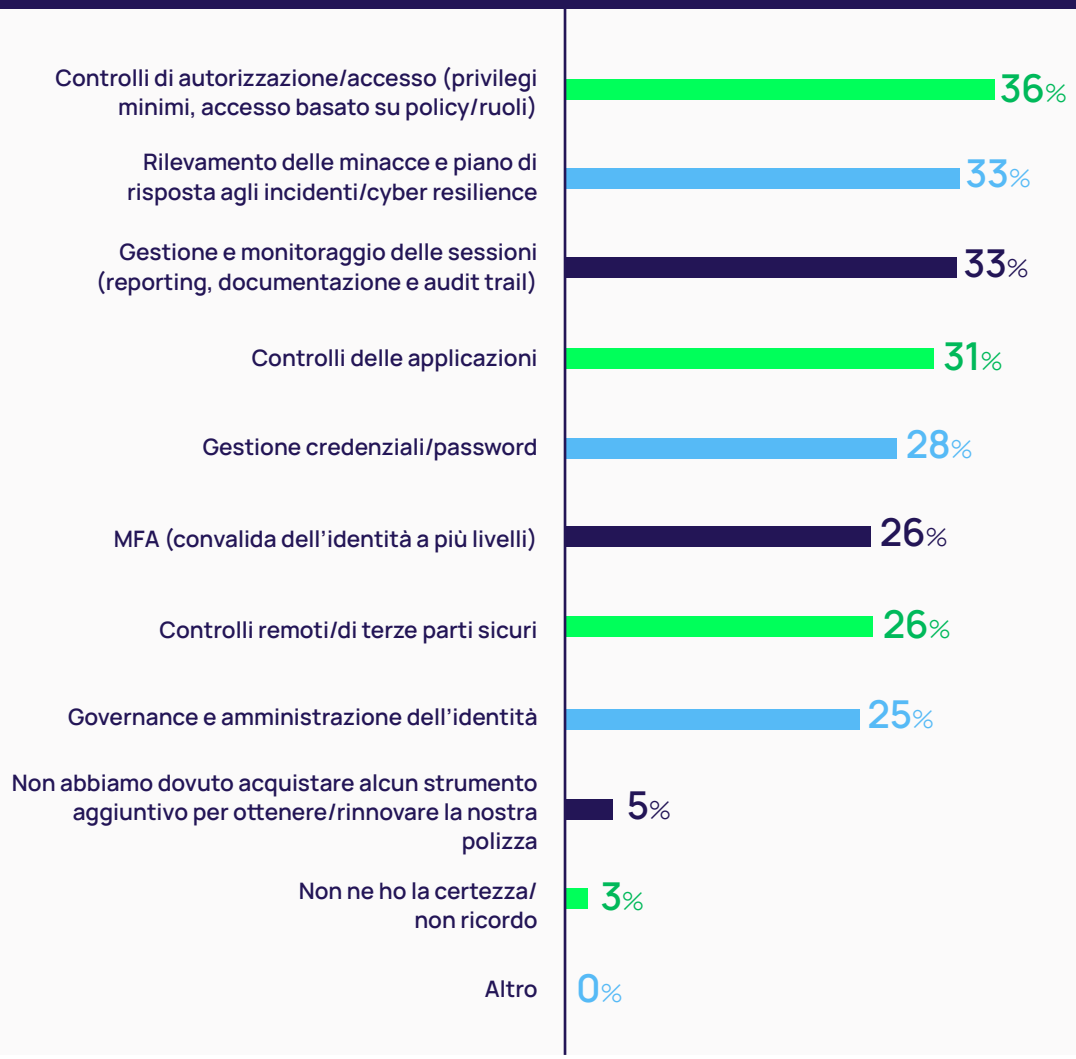
La maggior parte degli incidenti di cyber security che ha raggiunto il livello di una richiesta di risarcimento è causata dalla raccolta di credenziali, dalla compromissione di un insider, dall'utilizzo di una terza parte che ha avuto accesso ai sistemi, ecc., quindi quando le organizzazioni vengono valutate per i rinnovi, queste sono le domande che vengono poste".

**Mirna Soto**
CEO di Apogee Executive Advisors ed esperta in cyber security e gestione dei rischi

## La maggior parte delle aziende intervistate ha dovuto investire in soluzioni di sicurezza dell'identità prima di sottoscrivere o rinnovare la propria polizza.

Per soddisfare i requisiti di sicurezza sopra indicati, le organizzazioni affermano che non possono semplicemente presentare processi manuali ai potenziali fornitori di assicurazioni e aspettarsi di ricevere una polizza. Invece, hanno bisogno di acquistare soluzioni di sicurezza dell'identità come parte del loro stack tecnologico di sicurezza.

**Figura 5** | Quali strumenti aggiuntivi hai dovuto acquistare per ottenere/rinnovare la tua polizza?

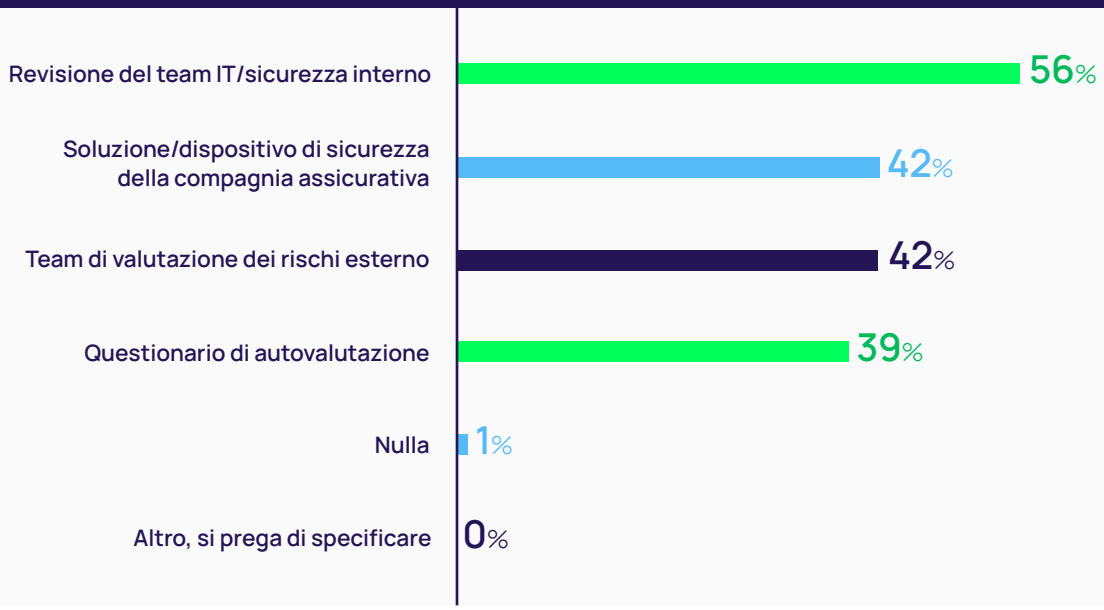



Questi risultati evidenziano le diverse esigenze di sicurezza delle organizzazioni e i diversi livelli di preparazione per quanto riguarda l'infrastruttura di cyber security.

## Le valutazioni verificano lo stato di sicurezza prima che le polizze vengano concesse.

A fronte della crescente maturità del settore della cyber insurance, le compagnie assicurative richiedono ora valutazioni dettagliate del livello di sicurezza. La maggior parte degli intervistati sceglie di effettuare queste valutazioni autonomamente. Altri si avvalgono di un team di valutazione dei rischi esterno per integrare le proprie competenze interne e fornire una visione imparziale dello stato di sicurezza di un'azienda.

**Figura 6** | Che tipo di valutazioni hai dovuto effettuare per ottenere la tua polizza di cyber insurance?




Che tu esegua queste valutazioni autonomamente o ti affidi a una terza parte, si prevede che allontanerà il personale più qualificato dei team IT e di sicurezza dal loro lavoro quotidiano e li dedicherà a progetti più strategici.

**41%**

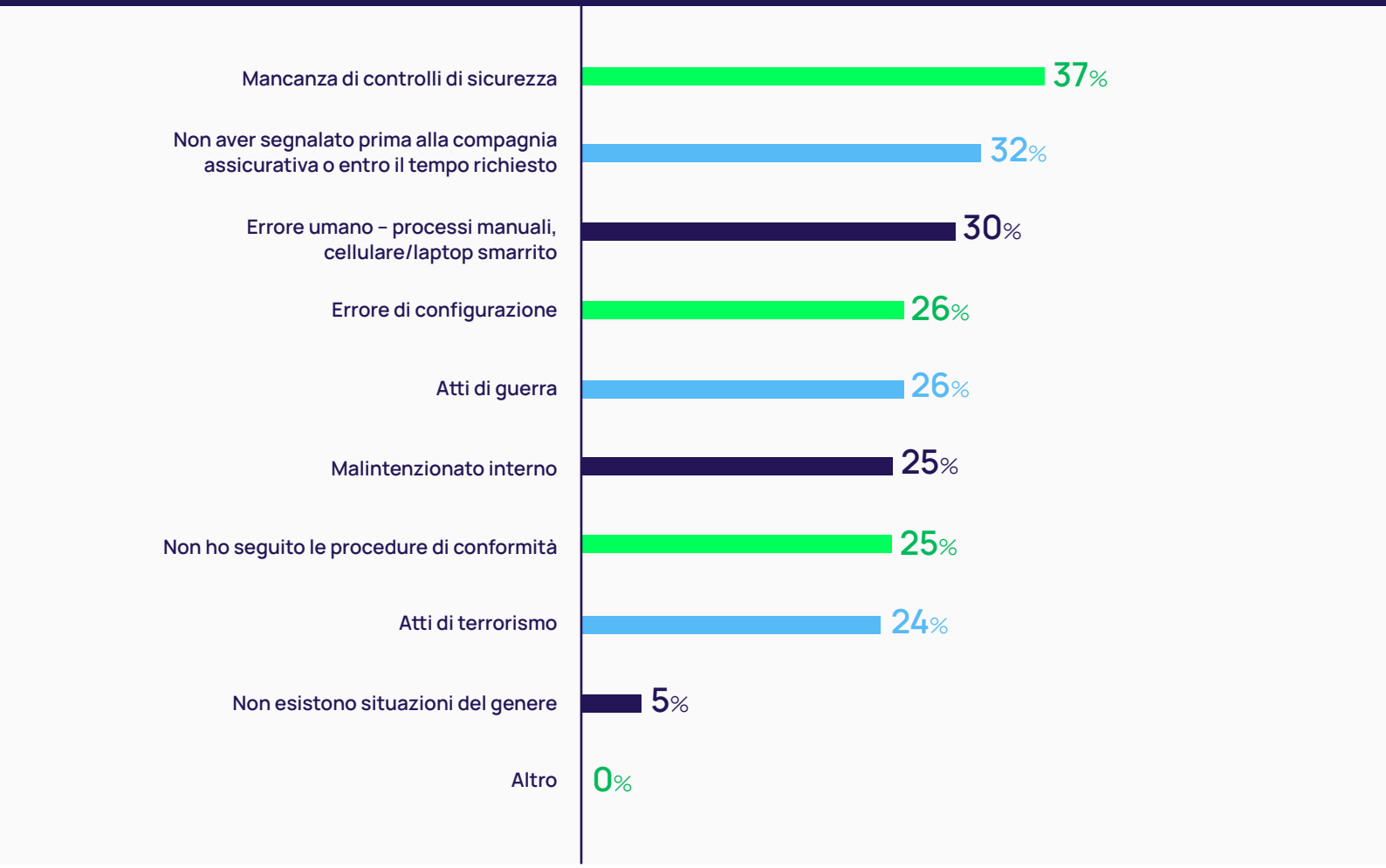
Il 41% delle compagnie assicurative richiede controlli di accesso/ autorizzazione basati sui privilegi minimi prima di concedere una polizza

## I requisiti non finiscono una volta concesse le polizze. Per far si che i risarcimenti vengano pagati, è necessario mantenere efficaci controlli di sicurezza.

Ottime notizie: se hai acquistato soluzioni di sicurezza dell'identità, hai dimostrato di avere controlli adeguati ed hai superato la valutazione. La tua polizza di cyber insurance è stata accettata!

Tuttavia, i risultati di questo sondaggio dimostrano che se non si adottano tali controlli di sicurezza e non li si utilizza correttamente, è probabile che la richiesta di risarcimento assicurativo venga respinta. Come hanno affermato gli intervistati, è necessario assicurarsi di verificare che i controlli di sicurezza siano applicati alla propria organizzazione in evoluzione, che siano configurati correttamente e che funzionino come previsto.

**Figura 7** | In quali situazioni, se presenti, la tua copertura di cyber insurance sarebbe nulla?



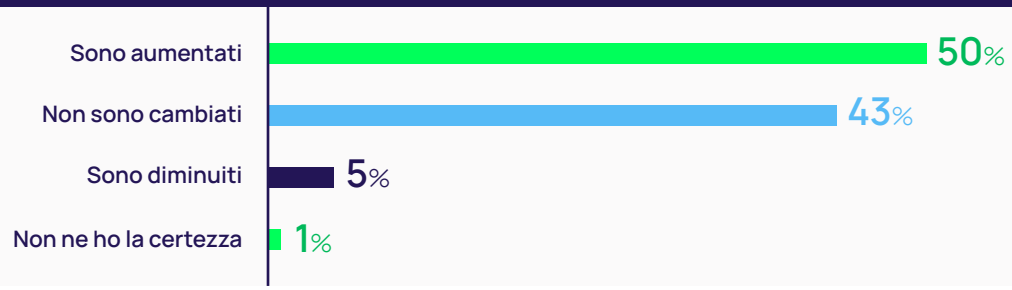

Il tuo stato di sicurezza non è del tipo "imposta e dimentica". Il rischio è in continua evoluzione man mano che l'ambiente IT diventa più complesso e le persone entrano, cambiano ruolo e lasciano l'organizzazione. La verità è che le aziende non sempre rispettano le polizze che orgogliosamente condividono con la compagnia assicurativa nella loro domanda.

# Punto chiave 3

## Sebbene i costi complessivi delle cyber insurance siano in aumento, le nuove tecnologie come l'IA stanno riducendo i premi.

### I costi assicurativi continuano ad aumentare per molte organizzazioni.

**Figura 8** | Come sono cambiati, se lo sono, i costi della tua cyber insurance da quando ne hai fatto domanda o dall'ultima volta che l'hai rinnovata?




Sebbene più della metà segnali un aumento, un confronto annuale mostra che l'incremento sta rallentando. L'anno scorso, il 79% delle aziende ha dichiarato che i costi assicurativi sono aumentati dall'ultima domanda o rinnovo.

Perché questo aumento per alcuni?

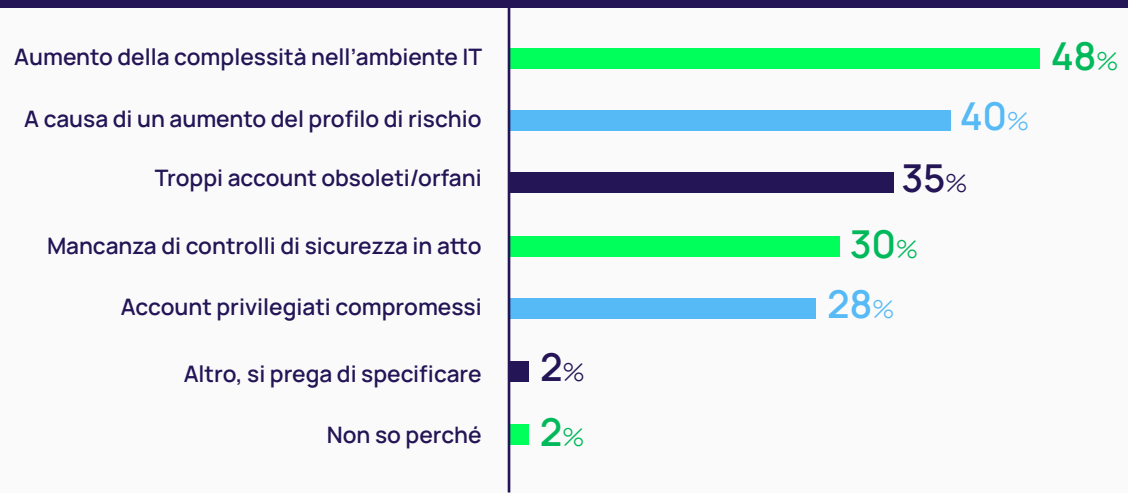
Considera il costo totale delle risorse necessarie per completare le valutazioni assicurative, colmare le lacune e dimostrare l'efficacia della cyber security in un moderno ambiente IT ibrido.

Gli intervistati indicano la complessità dell'IT come fattore determinante nell'aumento dei costi. Con l'aumentare del numero di identità, sono necessarie più risorse per portare a termine queste attività. La complessità dell'ambiente IT rende più arduo completare le valutazioni di sicurezza delle cyber insurance, con soluzioni di audit e resoconti scollegate che complicano l'aggregazione di dettagli e la misurazione del rischio.

L'aumento dei costi potrebbe indurre i titolari di polizze a richiedere limiti di copertura più elevati a causa di un profilo di rischio più elevato. Sono consapevoli dell'impatto aziendale che dovranno sostenere se dovessero subire un attacco informatico e vogliono trasferire tale rischio.

In base alla complessità informatica e al profilo di rischio, le compagnie assicurative potrebbero aumentare i prezzi per tutti gli assicurati per garantire sufficiente liquidità nel caso in cui si verifichino più richieste di risarcimento contemporaneamente.

**Figura 9** | Perché i costi sono aumentati?



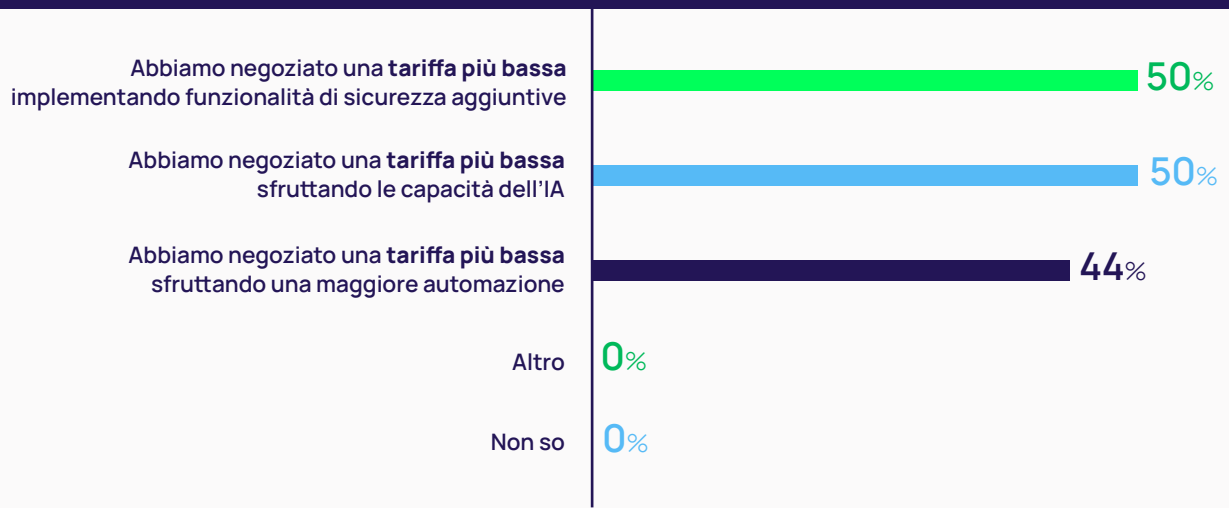

Le soluzioni di cyber security che valutano in modo rapido e completo un ambiente IT complesso e forniscono report basati sui rischi che puoi condividere con le compagnie assicurative sono mezzi efficaci per ridurre i costi della tua cyber insurance.

## L'IA e i controlli di sicurezza hanno aiutato le aziende lungimiranti a ridurre le tariffe assicurative.

Non tutti hanno la stessa tariffa assicurativa. La tua tariffa viene determinata in base al livello di rischio che la compagnia assicurativa considera per te, ovvero in base al tuo profilo di rischio. Nel caso della cyber insurance, il rischio è influenzato da fattori quali il tuo stack tecnologico, i controlli di sicurezza e lo storico. Se riesci a dimostrare visibilità e controlli che ti rendono meno a rischio, potresti riuscire ad abbassare con successo le tue tariffe e, di conseguenza, i tuoi costi.

I risultati del sondaggio dimostrano che le aziende lungimiranti stanno sfruttando i vantaggi dell'IA per negoziare tariffe più basse e, di conseguenza, costi più bassi. La maggior parte, tuttavia, deve ancora concentrarsi sull'adozione e sull'implementazione delle basi di una solida sicurezza dell'identità.

**Figura 10** | Perché i costi della tua assicurazione sono diminuiti?

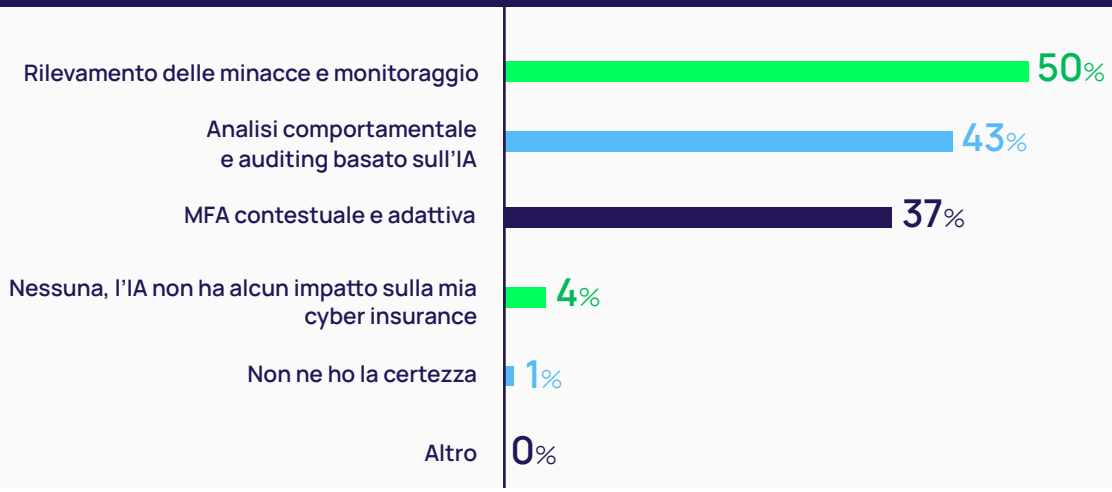



## L'intelligenza artificiale, in particolare per il rilevamento e il monitoraggio delle minacce, è efficace per la riduzione dei premi della cyber insurance

I premi, ovvero l'importo di denaro che un'azienda paga per mantenere attiva una polizza assicurativa, sono determinati dal tipo di assicurazione stipulata, dai limiti della polizza e dalla franchigia, tra gli altri fattori. Maggiore è la fiducia che riponi nella tua sicurezza e nei tuoi controlli, tanto più potrai scegliere l'assicurazione giusta per te e negoziare premi più bassi.

Le aziende stanno adottando l'intelligenza artificiale (IA) per garantire che le soluzioni e le polizze di cyber insurance funzionino come previsto e per contenere gli incidenti in corso, in modo da ridurre il tempo di permanenza degli agenti della minaccia e il raggio di esplosione degli attacchi, il che a sua volta può ridurre il profilo di rischio.

**Figura 11** | Quali funzionalità di IA, se presenti, stai adottando per ridurre i premi della tua cyber insurance?



# Conclusione

La maggior parte delle aziende statunitensi intervistate ha dovuto investire in soluzioni di sicurezza dell'identità prima di ottenere una polizza

Sebbene l'assicurazione sia uno strumento essenziale per la cyber resilience, non sarà mai possibile trasferire tutti i rischi. La cyber insurance deve funzionare in concomitanza con controlli e processi di cyber security solidi, ragionevoli e difendibili.

In particolare, le compagnie assicurative si aspettano di vedere policy di sicurezza dell'identità e soluzioni efficaci prima di concedere una polizza. Dovrai condividere le prove dei controlli di sicurezza dell'identità in azione e assicurarti di mantenere tali controlli man mano che la superficie di attacco cambia e il profilo di rischio aumenta.

L'IA aiuta le organizzazioni ad acquisire le conoscenze degli esperti in materia e ad agire come "assistenti SOC" per individuare più rapidamente le minacce legate all'identità, riducendo in definitiva i tempi di permanenza, limitando il raggio di esplosione di un attacco e riducendo il rischio. Sulla base dei risultati di questo sondaggio, l'IA è destinata a offrire vantaggi ancora maggiori man mano che le aziende negoziano le polizze con le compagnie assicurative

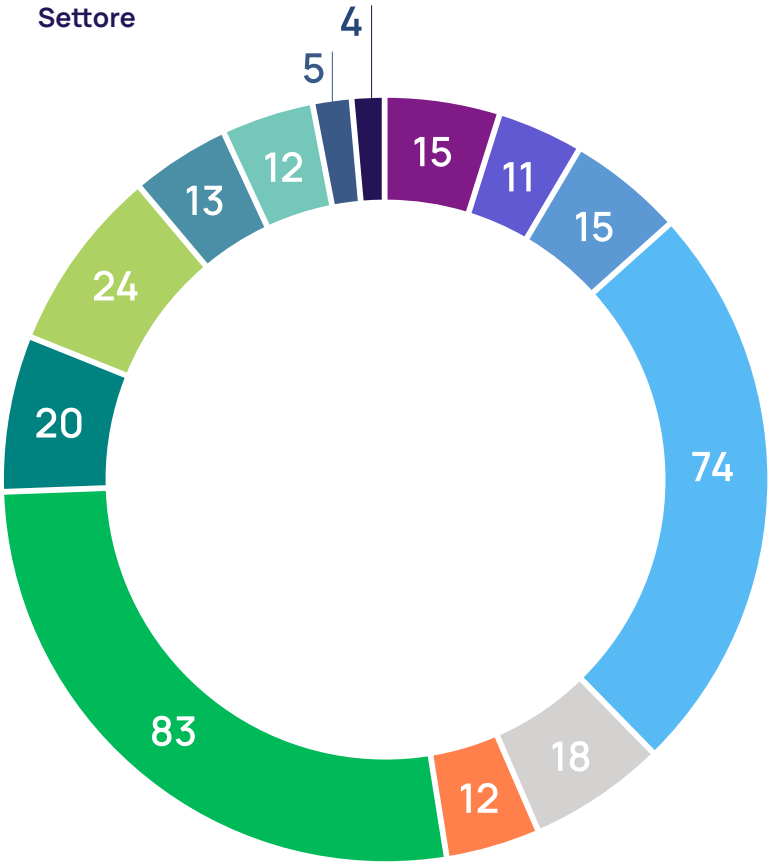
Come parte della valutazione del rischio, le compagnie assicurative vorranno sapere in che modo stai integrando l'IA nei tuoi sforzi di trasformazione digitale, tra cui sviluppo del prodotto, codifica, sviluppo, test di controllo qualità, ecc. Dovresti anche aspettarti domande che analizzino attentamente il modo in cui il tuo team addetto alla sicurezza utilizza l'IA per aspetti quali gestione dell'identità, autorizzazione, rilevamento e risposta. Tutti i controlli basati sull'IA devono essere facilmente spiegabili, in modo che il tuo team, gli auditor e le compagnie assicurative siano sicuri del modo in cui lavorano per ridurre i rischi.

# Metodologia

Questo sondaggio online è stato condotto per conto di Delinea da Censuswide, che, a giugno 2024, ha intervistato 306 dirigenti con visibilità sul processo di domanda o rinnovo della cyber insurance della propria organizzazione. A tutti gli intervistati è stata posta la stessa serie di domande e le opzioni di risposta sono state casuali. I risultati non sono stati ponderati.

## Ripartizione dei 306 intervistati per conteggi

### Settore

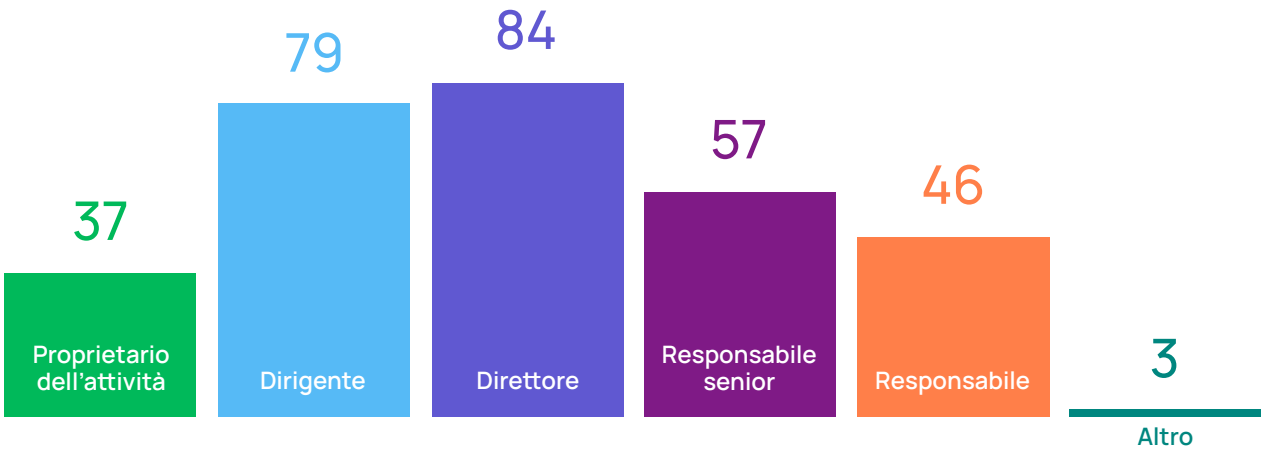



- Architettura, ingegneria e pianificazione residenziale
- Arti e cultura
- Istruzione
- Finanza
- Sanità
- Risorse umane
- IT e telecomunicazioni
- Dipartimento legale
- Produzione e servizi di pubblica utilità
- Vendita al dettaglio, ristorazione e tempo libero
- Vendite, media e marketing
- Viaggi e trasporti
- Altro

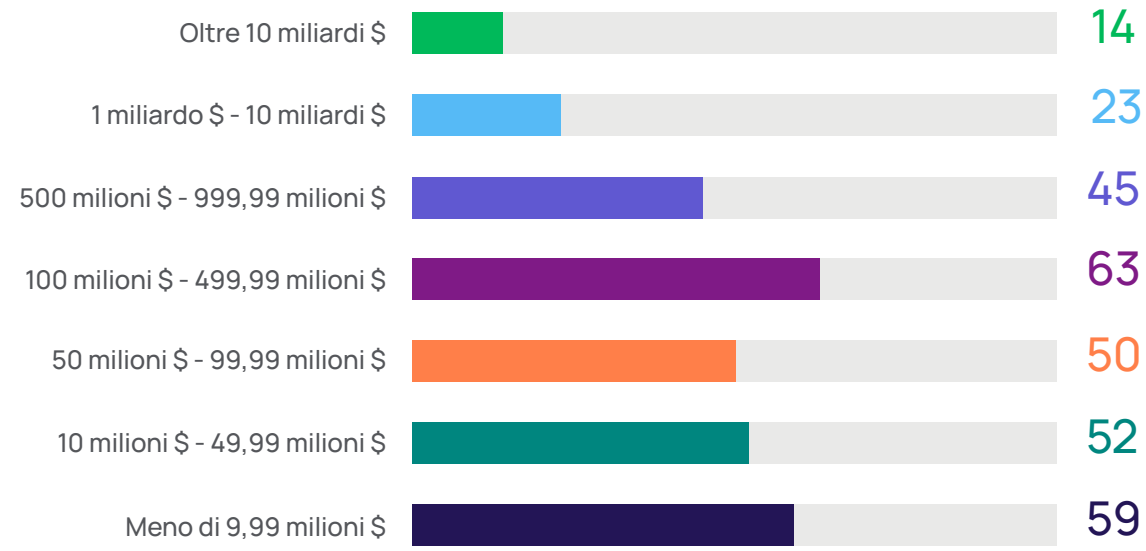
### Ruoli

Dipartimento finanziario | Dipartimento legale | IT | Sicurezza/rischio | Conformità

## Posizioni




## Dimensioni aziendali



# Risorse correlate

## WEBINAR

**The Future of Cyber Insurance: Navigating the Impact of AI on Policy Holders**

Ascolta cosa dicono gli esperti di cyber security e cyber insurance sulla valutazione del linguaggio delle polizze per assicurarti di comprendere la copertura, le esclusioni e il supporto che il tuo fornitore ti fornirà in caso di incidente.

Guarda il video (EN)

## WHITEPAPER

**Approfondimenti sui requisiti di sicurezza informatica rafforzati**

Questo report raccoglie i questionari delle principali compagnie assicurative e mette in evidenza le domande più comuni. Nello specifico, esamina i requisiti sempre più severi delle compagnie assicurative in materia di sicurezza dell'identità, tra cui l'autenticazione a più fattori (MFA), un sistema di gestione delle password, controllo degli accessi, elevazione dei privilegi, gestione delle sessioni, privilegi minimi e politiche zero trust.

Scarica ora

## PODCAST

**Cyber Insurance Trends for Risk Management with Joe Carson of Delinea and Dara Gibson of Optiv**

Scopri come affrontare il tema della cyber insurance con il tuo consiglio di amministrazione.

Ascolta ora (EN)

Delinea

Securing identities at every interaction

Delinea, azienda pioniera nella protezione delle identità attraverso l'autorizzazione centralizzata, rende le organizzazioni più sicure governando senza soluzione di continuità le loro interazioni in tutta l'azienda moderna. Delinea consente alle organizzazioni di applicare il contesto e l'intelligenza in tutto il ciclo di vita dell'identità attraverso l'infrastruttura cloud e tradizionale, i dati e le applicazioni SaaS per eliminare le minacce legate all'identità. Grazie all'autorizzazione intelligente, Delinea è l'unica piattaforma che consente di scoprire tutte le identità, assegnare i livelli di accesso appropriati, rilevare le irregolarità e rispondere immediatamente alle minacce all'identità in tempo reale. Delinea accelera l'adozione da parte dei vostri team, con un'implementazione in settimane, non in mesi, e li rende inoltre più produttivi, richiedendo il 90% in meno delle risorse da gestire rispetto al concorrente più prossimo. Con un tempo di attività garantito del 99,99%, la Delinea Platform è la soluzione di sicurezza delle identità più affidabile sul mercato. Per saperne di più su Delinea, visita **delinea.com**, **LinkedIn**, **X** e **YouTube**.

© Delinea CISR2024-WP-0824-IT