observeIT | proofpoint.

REPORT 2020 SUL COSTO DELLE MINACCE INTERNE A LIVELLO MONDIALE

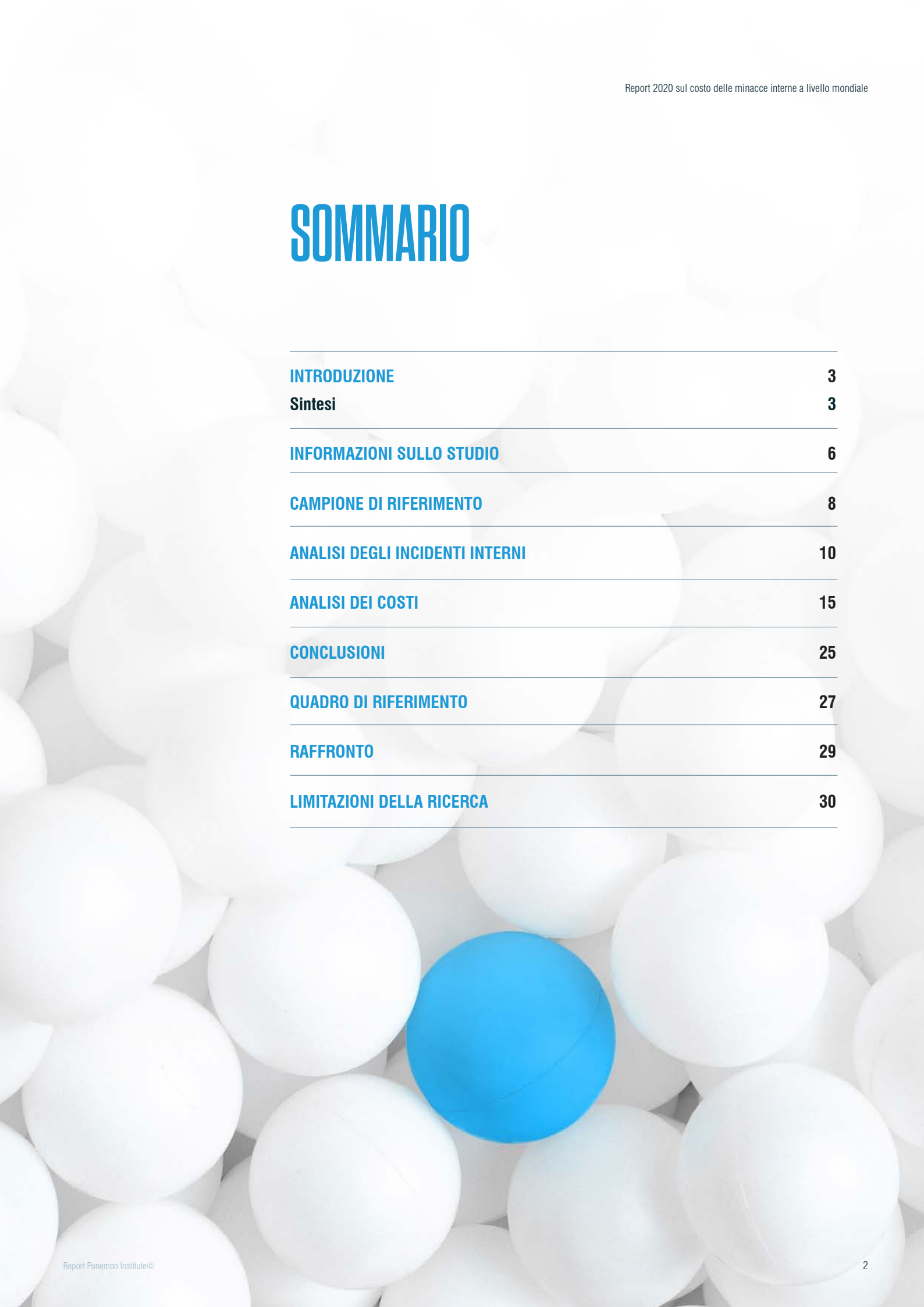
Realizzato in modo indipendente da:

Ponemon INSTITUTE

Sponsorizzato da:

observeIT IBM Security

SOMMARIO



INTRODUZIONE

Il Ponemon Institute è lieto di presentare i risultati del suo studio 2020 sul costo delle minacce interne a livello mondiale. Sponsorizzato da ObservelT e IBM, si tratta del terzo studio comparativo svolto per comprendere i costi diretti e indiretti associati alle minacce interne. Realizzato nel 2016, il primo studio era concentrato esclusivamente sulle aziende con sede negli Stati Uniti. Lo studio 2020 si concentra sulle aziende con sede in Nord America, Europa, Medio Oriente e Asia-Pacifico.

Ai fini di questa ricerca, le minacce interne sono definite come segue:

- Dipendente o sub-appaltatore negligente;
- Utente interno malintenzionato
- Ladro di credenziali d'accesso

Sintesi

La principale conclusione del report è che, il costo e la frequenza di tutti e tre i tipi di minaccia interna sopra delineati sono aumentati drasticamente in due anni. Per esempio, le minacce interne sono costate alle aziende 11,45 milioni di dollari nel 2020, un aumento del 31% dagli 8,76 milioni di dollari del 2018 (Ponemon). Inoltre, il numero di incidenti è aumentato del 47% in soli due anni, dai 3.200 del 2018 (Ponemon) ai 4.716 del 2020. Questi dati mostrano che le minacce interne sono un rischio per la sicurezza informatica ancora attuale, anche se spesso non adeguatamente affrontato dalle aziende rispetto alle minacce esterne.

Abbiamo intervistato 964 persone fra professionisti dell'IT e addetti della sicurezza informatica in 204 aziende con sede in Nord America (Stati Uniti e Canada), Europa, Medio Oriente Africa e Asia-Pacifico. Le interviste si sono concluse nel settembre 2019. Ogni azienda aveva subito uno o più incidenti gravi causati da una minaccia interna. Le aziende interessate erano imprese con una forza lavoro di 1.000 o più dipendenti a livello globale. Negli ultimi 12 mesi, queste aziende hanno subito complessivamente 4.716 incidenti interni.

Di seguito alcune importanti statistiche sul costo delle minacce di origine interna in un periodo di 12 mesi:

Numero totale di aziende intervistate
204

Numero totale di incidenti interni
4.716

Costo totale medio
11,45 M$

Incidenti dovuti a negligenza
62%

Incidenti imputabili a utenti interni malintenzionati
23%

Incidenti legati al furto delle credenziali di accesso
14%

Costo annuo per negligenza
4,58 M$

Costo annuo per gli utenti interni malintenzionati
4,08 M$

Costo annuo per i furti delle credenziali di accesso
2,79 M$

QUESTI TIPI DI INCIDENTI COSTANO A OGNI AZIENDA **UNA MEDIA DI 2,79 MILIONI DI DOLLARI ALL'ANNO.**

OGNI SINGOLO INCIDENTE ATTRIBUIBILE A UTENTI INTERNI MALINTENZIONATI COSTA ALLE AZIENDE CHE HANNO PARTECIPATO ALLA RICERCA **UNA MEDIA DI 755.760 DOLLARI.**

La maggior parte degli incidenti è dovuta alla negligenza degli utenti interni, ma il furto delle credenziali di accesso è quello più costoso.

Il costo delle minacce interne varia notevolmente in base al tipo di incidente. Se coinvolge un dipendente o un appaltatore negligente, ogni incidente costa in media 307.111 dollari. Tuttavia, dato che si tratta della casistica più frequente (62%), i costi totali per le aziende possono raggiungere in media a 4,58 milioni di dollari all'anno.

Il costo medio per ogni incidente può quasi triplicare se è imputabile a un impostore (furto d'identità) o a un ladro di credenziali d'accesso (871.686 dollari), Di tutti i tipi di furto di credenziali d'accesso, il più costoso è quello che coinvolge gli utenti con privilegi. In questa ricerca, il 14% dei furti era proprio di tale tipologia. Questi tipi di incidente costano a ogni azienda una media di 2,79 milioni di dollari all'anno.

Ogni singolo incidente attribuibile a utenti interni malintenzionati costa alle aziende che hanno partecipato alla ricerca una media di 755.760 dollari. Nonostante gli incidenti di origine dolosa siano spesso quelli più clamorosi, questi rappresentano solo il 23% del totale. Tuttavia, poiché possono avere delle ripercussioni durante tutto l'anno, il loro costo medio annuo per azienda è pari a 4,08 milioni di dollari.

Le indagini sono i centri di costo in più rapida crescita

Le attività che generano costi sono: il monitoraggio, le indagini, l'escalation dei problemi, la risposta agli incidenti, il contenimento, l'analisi a posteriori e le azioni correttive. Fra queste attività il centro di costo dalla crescita più rapida è quello delle indagini, aumentato per tutte le casistiche mediamente dell'86% in soli due anni, raggiungendo 103.798 dollari.

Sono necessari oltre due mesi in media per contenere un incidente interno

Occorrono in media 77 giorni per contenere ogni singolo incidente interno. Solo il 13% degli incidenti è stato arginato in meno di 30 giorni.

Le dimensioni e il settore di un'azienda influiscono sul costo per singolo incidente

I danni economici variano in base alle dimensioni di un'azienda. Nell'ultimo anno, le grandi aziende (25.001-75.000 dipendenti) hanno speso una media di 17,92 milioni di dollari per risolvere gli incidenti legati al personale interno. Dal canto loro, per affrontare le conseguenze di questi incidenti le aziende più piccole (meno di 500 dipendenti) hanno speso in media 7,68 milioni di dollari. I settori interessati dalla maggiore crescita di questo problema sono il commercio al dettaglio (38,2% di aumento in due anni) e i servizi finanziari (20,3% di aumento).

Tutti i tipi di minacce interne sono in aumento

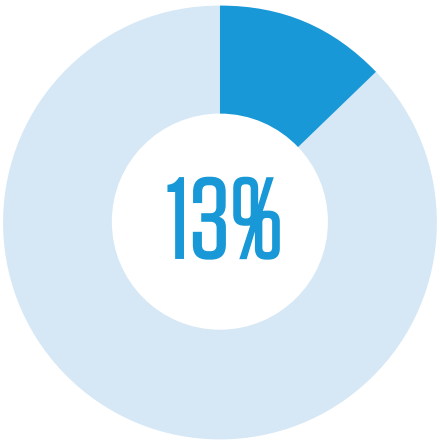
Dal 2018, il numero medio di incidenti dovuti alla negligenza di un dipendente o di un sub-appaltatore è aumentato da 13,2 a 14,5 per azienda , mentre il numero medio di furti delle credenziali è quasi triplicato, passando da 1,0 a 2,7. Ciò detto, il 60% delle aziende ha subito più di 30 incidenti all'anno.

Cinque indicatori di un'azienda a rischio

1. Dipendenti che non ricevono formazione atta a comprendere e applicare appieno leggi, obblighi o i requisiti normativi inerenti al loro lavoro e che influiscono sulla sicurezza dell'azienda.
2. Dipendenti inconsapevoli delle misure da adottare in modo sistematico per assicurare la protezione costante dei dispositivi che utilizzano, siano essi forniti dall'azienda o personali ma usati sul lavoro (BYOD).
3. Dipendenti che inviano dati altamente riservati verso un luogo non protetto nel cloud, mettendo a rischio l'azienda.
4. Dipendenti che violano le policy di sicurezza dell'azienda per semplificare i loro compiti.
5. Dipendenti che mettono a rischio l'azienda quando non installano sistematicamente le patch e gli ultimi aggiornamenti a dispositivi e servizi.

77 GIORNI

per contenere un incidente interno



degli incidenti è stato contenuto in meno di

30 GIORNI

30

delle aziende ha subito più di 30 incidenti all'anno

INFORMAZIONI SULLO STUDIO

La nostra ricerca si concentra sugli incidenti di origine interna che hanno avuto un impatto sui costi delle aziende negli ultimi 12 mesi. La nostra metodologia cerca di tenere conto dei costi sia diretti sia di quelli indiretti tra cui, a mero titolo esemplificativo, le seguenti minacce per le aziende:

- Furto o perdita di dati strategici o proprietà intellettuale;
- Impatto dei tempi di inattività sulla produttività dell'azienda;
- Danni ad attrezzature e altre risorse;
- Costi per il rilevamento e il risanamento dei sistemi e dei processi aziendali fondamentali;
- Implicazioni legali e normative, compresi i costi di difesa nelle controversie;
- Perdita di fiducia delle principali parti interessate;
- Danneggiamento del marchio e della reputazione sul mercato.

Questa ricerca utilizza un metodo per il calcolo dei costi in base alle attività. La nostra indagine sul campo, condotta nell'arco di due mesi, si è conclusa nel settembre 2019. Il nostro campione di riferimento finale era costituito di 204 diverse aziende. In totale sono state condotte 964 interviste in totale con alcuni dipendenti chiave di tali aziende. I costi delle attività per il presente studio sono stati calcolati sulla base delle informazioni raccolte in stretta riservatezza dai partecipanti durante riunioni o visite in loco. Le aziende prescelte rispondevano ai seguenti criteri:

- Aziende commerciali e del settore pubblico;
- Forza lavoro globale di 1.000 o più dipendenti a livello globale
- Presenza nelle seguenti regioni: Nord America, Europa, Medio Oriente Africa e Asia-Pacifico
- Ruolo IT centrale, con controllo sull'ambiente in sede e/o nel cloud
- Vittima di uno o più incidenti gravi causati da persone interne negligenti o malintenzionate

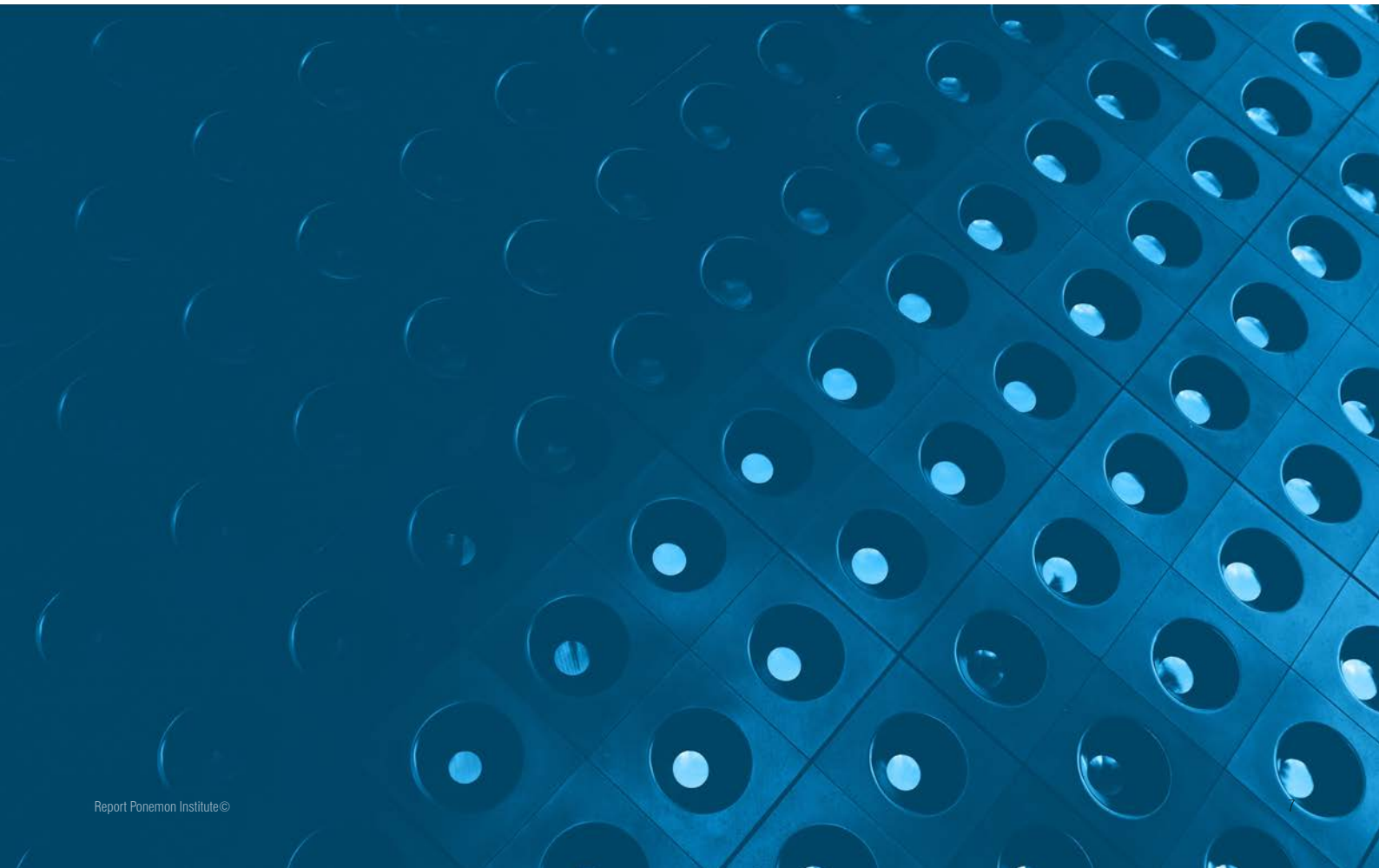
PER RACCOGLIERE ED ESTRAPOLARE I DATI, I RICERCATORI HANNO CONDOTTO INTERVISTE DIAGNOSTICHE E **CALCOLATO I COSTI IN BASE ALLE ATTIVITÀ.**

Questo report presenta un quadro obiettivo che misura l'impatto economico totale degli incidenti di origine interna. Sono stati utilizzati tre profili per categorizzare e analizzare i costi relativi agli incidenti interni per 204 aziende:

- Dipendente o sub-appaltatore negligente
- Utente interno (incluso collaboratore o sub-appaltatore) malintenzionato
- Ladro delle credenziali di accesso di dipendenti/utenti

Il primo passo della ricerca è stato il reclutamento di aziende internazionali. Per raccogliere ed estrapolare i dati, i ricercatori hanno condotto interviste diagnostiche e calcolato i costi in base alle attività. Il Ponemon Institute ha svolto tutte le fasi di questo progetto di ricerca, che includeva le seguenti fasi:

- Sessioni di lavoro con ObserveIT e IBM per stabilire le aree di ricerca
- Reclutamento delle aziende di riferimento
- Sviluppo di un metodo di calcolo dei costi in base alle attività
- Amministrazione del programma di ricerca
- Analisi di tutti i risultati mediante appropriate verifiche di affidabilità
- Preparazione di un report che riassume tutti i risultati salienti della ricerca



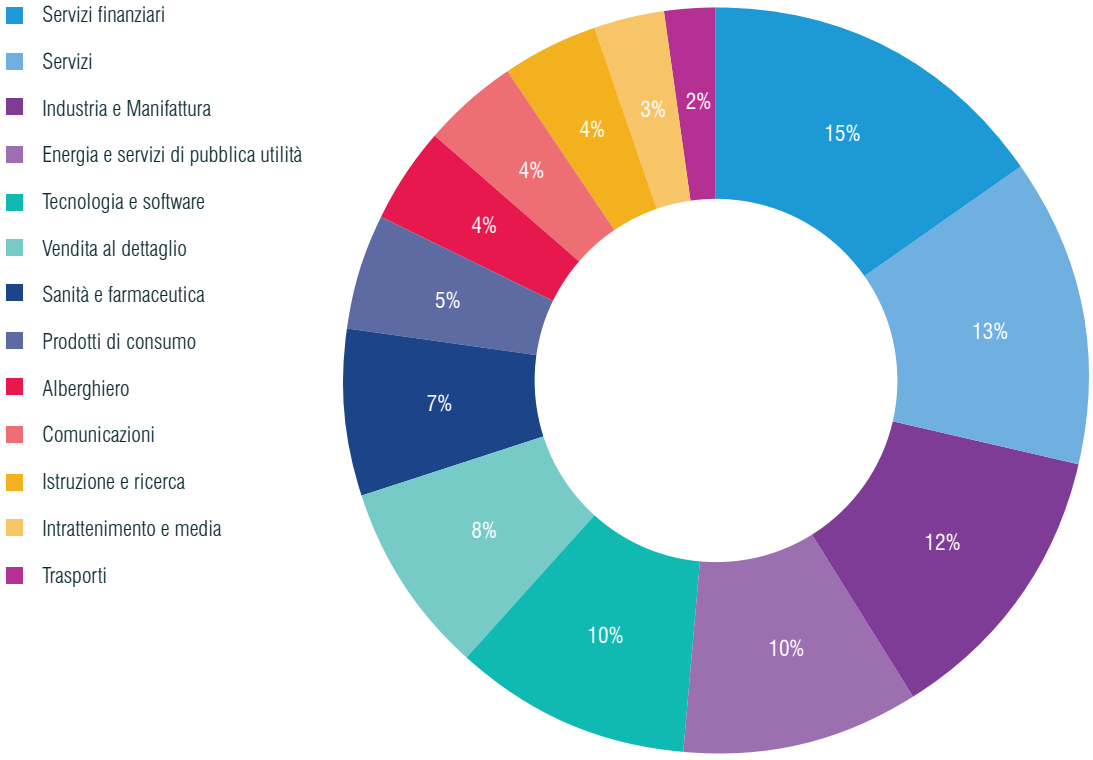
CAMPIONE DI RIFERIMENTO

Nella ricerca comparativa l'unità dell'analisi è l'azienda. Il seguente grafico a torta mostra la distribuzione percentuale delle aziende in 13 settori di attività. I tre settori principali sono i servizi finanziari, i servizi e il settore industriale e manifatturiero. Le società di servizi finanziari includono banche, assicurazioni, società di gestione degli investimenti e di intermediazione. Il settore servizi rappresenta un'ampia gamma di aziende, comprese quelle dei servizi professionali.

Figura 1.

Settori di attività delle aziende partecipanti

n=204 aziende

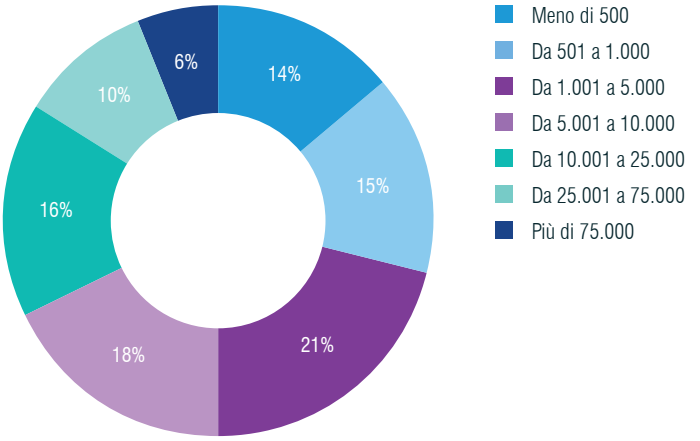


La figura 2 mostra la distribuzione percentuale delle aziende in base al numero totale di dipendenti, che è un indicatore delle dimensioni dell'azienda. Come si può vedere, il 50% del campione include le aziende più grandi, con oltre 5.000 dipendenti equivalenti a tempo pieno.

Figura 2.

Numero di dipendenti delle aziende partecipanti

n=204 aziende

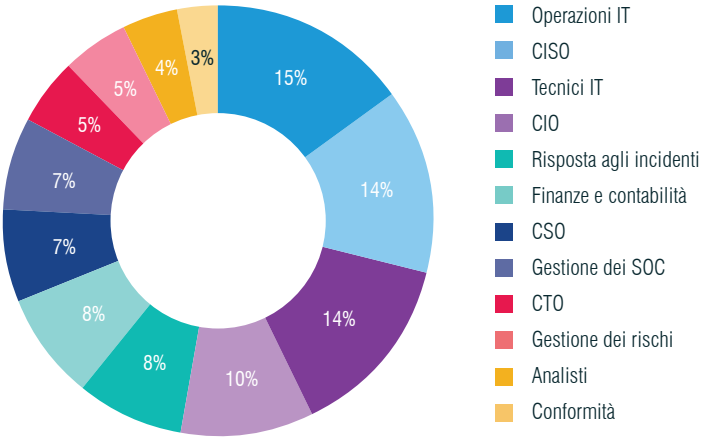


Secondo la figura 3, 964 persone hanno partecipato alle interviste sul campo. Ogni caso di studio ha coinvolto in media 4,7 persone. I tre segmenti più grandi sono: operazioni IT (15%), CISO (14%) e tecnici IT (14%).

Figura 3.

Intervistati per posizione o funzione

n=964 persone

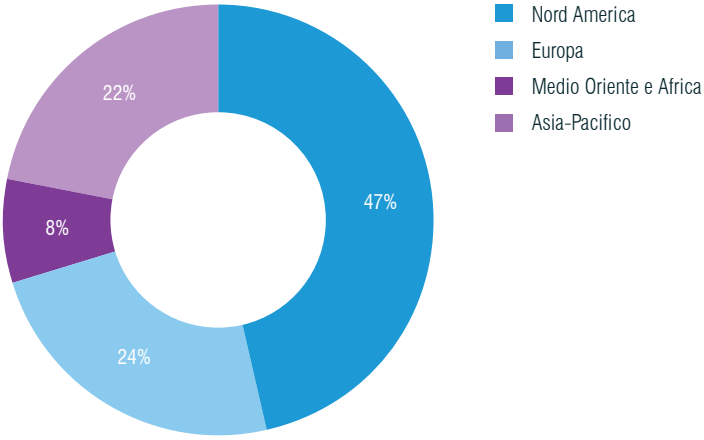


La figura 4 mostra le aree del mondo incluse nella ricerca. Il Nord America rappresenta il segmento più grande (47% delle aziende), mentre il Medio Oriente è il più piccolo (8%). Date le dimensioni ridotte del campione, abbiamo accorpato Europa e Medio Oriente nel segmento EMEA.

Figura 4.

Distribuzione regionale delle aziende internazionali

n=204 aziende



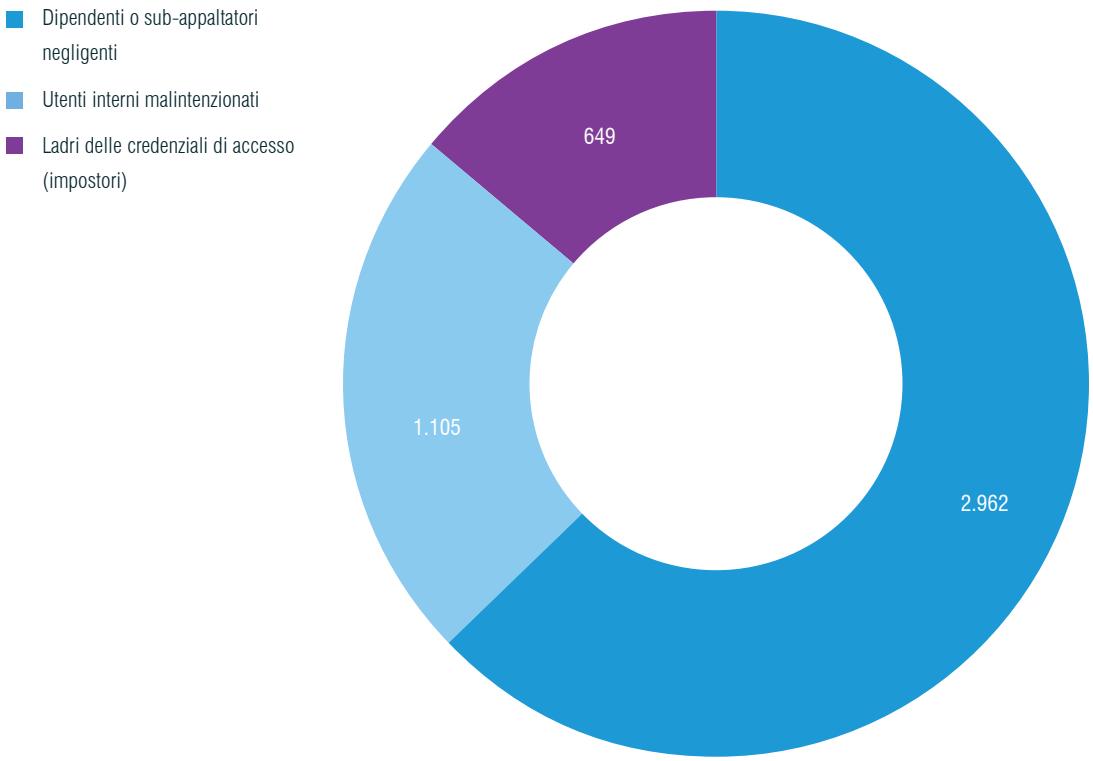
ANALISI DEGLI INCIDENTI INTERNI

La figura 5 mostra la distribuzione dei 4.716 attacchi denunciati e analizzati nel nostro campione. Un totale di 2.962 attacchi (62%) è risultato imputabile alla negligenza di un dipendente o di un sub-appaltatore. Gli utenti interni malintenzionati hanno causato 1.105 attacchi (23%).

649 attacchi (14%) sono risultati al furto delle credenziali. Di questi, 191 hanno avuto origine dal furto delle credenziali di accesso degli utenti con privilegi.
Il numero più elevato di incidenti segnalati da una data azienda è di 45 e il numero più basso è pari a 1.

Figura 5.

Frequenza dei 4.716 eventi per i tre profili di utenti interni

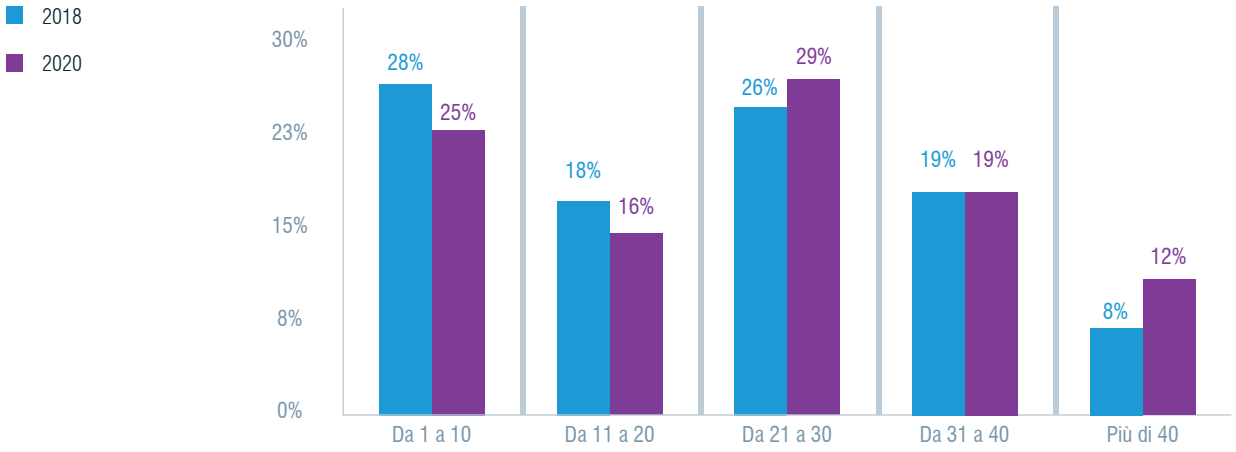


La figura 6 presenta un istogramma degli incidenti interni per il nostro campione di 204 aziende negli ultimi 12 mesi. Come si può evincere, il 60% delle aziende ha registrato in media più di 30 incidenti all'anno.

Figura 6.

Frequenza percentuale degli incidenti legati al personale interno per azienda

Dati raggruppati per i tre profili

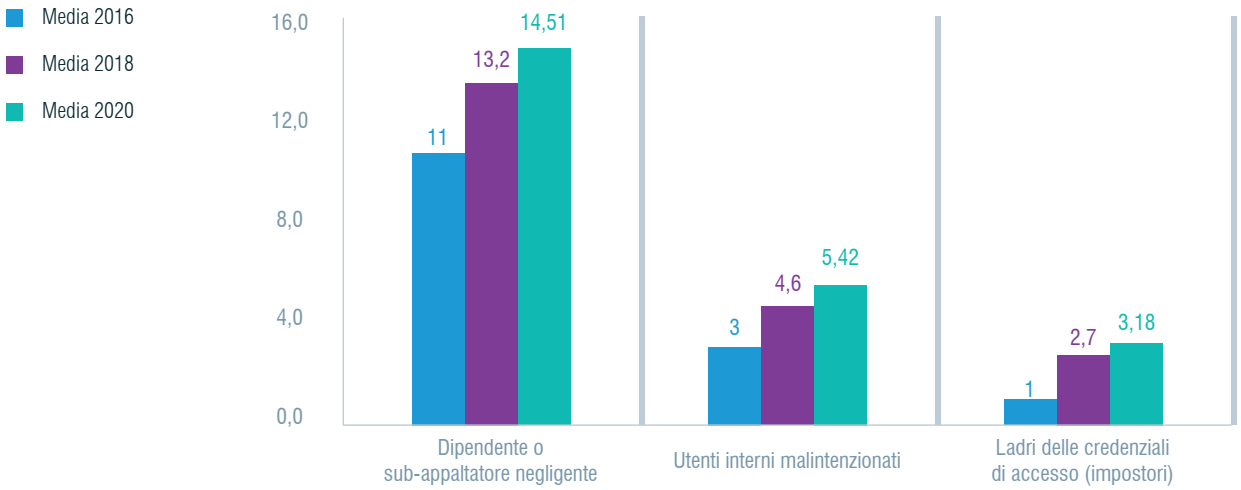


Tutti i tipi di minacce interne sono in crescita costante

Come mostrato nella figura 7, dal 2016 il numero medio di incidenti dovuti alla negligenza di un dipendente o sub-appaltatore è aumentato da 10,5 a 14,5 nel 2020. Il numero medio di incidenti legati a furti delle credenziali di accesso per ogni azienda è aumentato passando da 1 nel 2016 a 3,2 nel 2020.[1]

Figura 7.

Frequenza per i tre profili di utenti interni



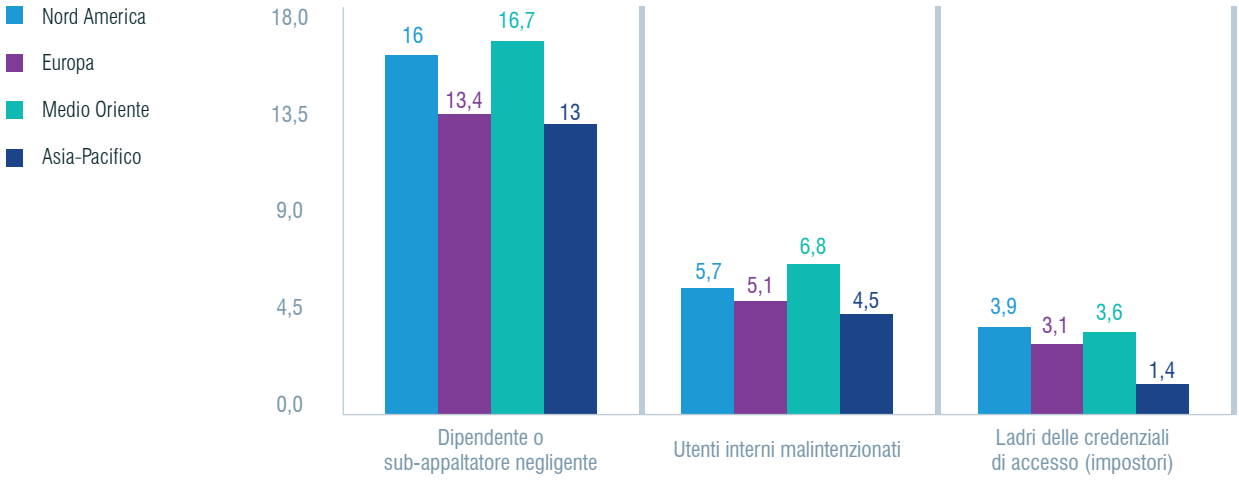
1 I dati del 2016 sono relativi solo alle aziende con sede negli Stati Uniti. I dati del 2020 includono Nord America, Europa, Medio Oriente Africa e Asia-Pacifico. Riteniamo che i dati siano comparabili perché le aziende statunitensi rappresentate nel report 2016 sono multinazionali.

Le aziende del Medio Oriente sono quelle che riscontrano il maggior numero di incidenti interni, mentre quelle dell'Asia-Pacifico è quella con il numero minore.

La figura 8 mostra la frequenza degli incidenti interni nelle quattro regioni rappresentate dalla ricerca. In tutte le regioni la negligenza da parte di dipendenti o sub-appaltatori è la circostanza più frequente. Le aziende di Nord America e Medio Oriente sono l'obiettivo più probabile dei furti delle credenziali di connessione.

Figura 8.

Frequenza media degli incidenti per i tre profili

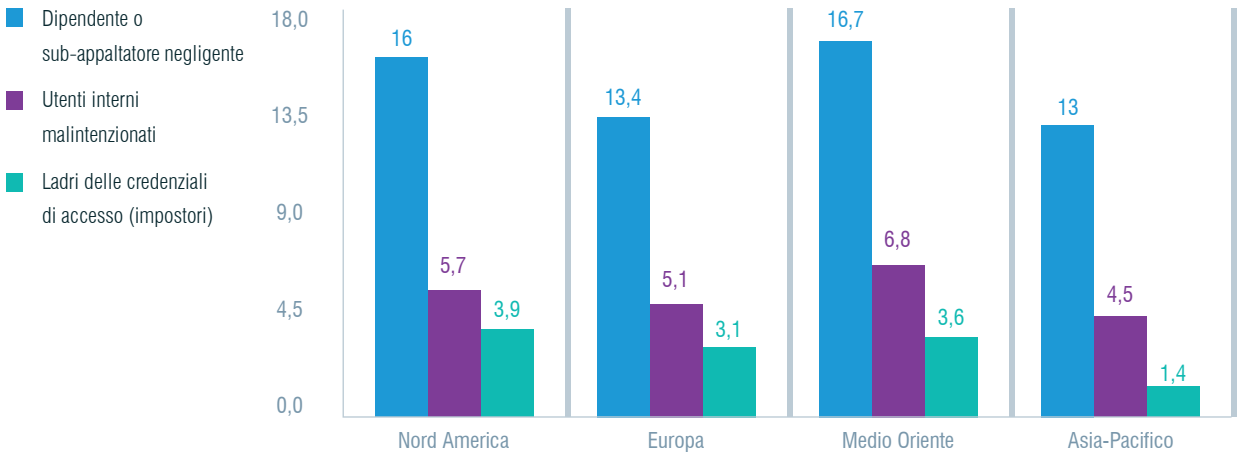


La frequenza delle minacce interne varia in base alla regione

Come illustrato nella figura 9, le aziende nordamericane e mediorientali sono quelle che hanno subito il maggior numero di incidenti legati al personale interno negli ultimi 12 mesi. Per contro, le aziende dell'Asia-Pacifico sono state quelle con il minor numero di casi.

Figura 9.

Frequenza per regione per i tre profili di utenti interni



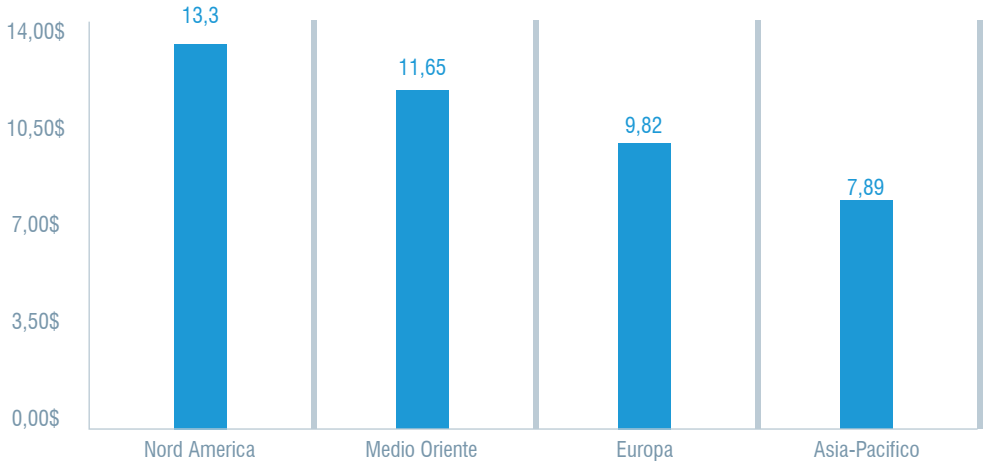
Le aziende nordamericane hanno registrato un costo medio annuo superiore al costo medio generale

La figura 10 riporta il costo totale annualizzato per le quattro regioni. Le imprese nordamericane hanno registrato il costo totale più elevato pari a 13,3 milioni di dollari. Il secondo costo più elevato è stato a carico delle aziende mediorientali con 11,65 milioni di dollari. Europa e Asia-Pacifico hanno registrato un costo medio molto inferiore al costo medio totale di tutte le 204 imprese.

Figura 10.

Costo medio delle attività per regione

Media = 11,45 (milioni di dollari)



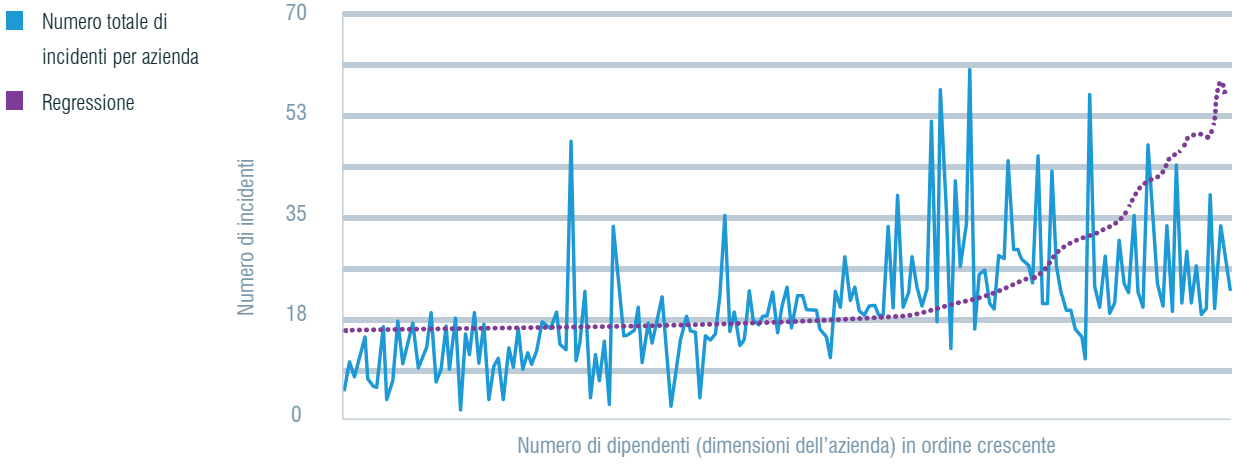
Più grande è l'azienda, maggiore è il numero di incidenti interni

La figura 11 mostra la distribuzione degli incidenti interni in ordine crescente per numero di dipendenti o dimensioni delle aziende partecipanti. La curva ascendente suggerisce che la frequenza degli incidenti interni è positivamente correlata alle dimensioni dell'azienda. La correlazione è ancora più marcata per le aziende più grandi.

Figura 11.

Incidenti interni per numero di dipendenti (dimensioni dell'azienda) in ordine crescente

Media = 11,45 (milioni di dollari)

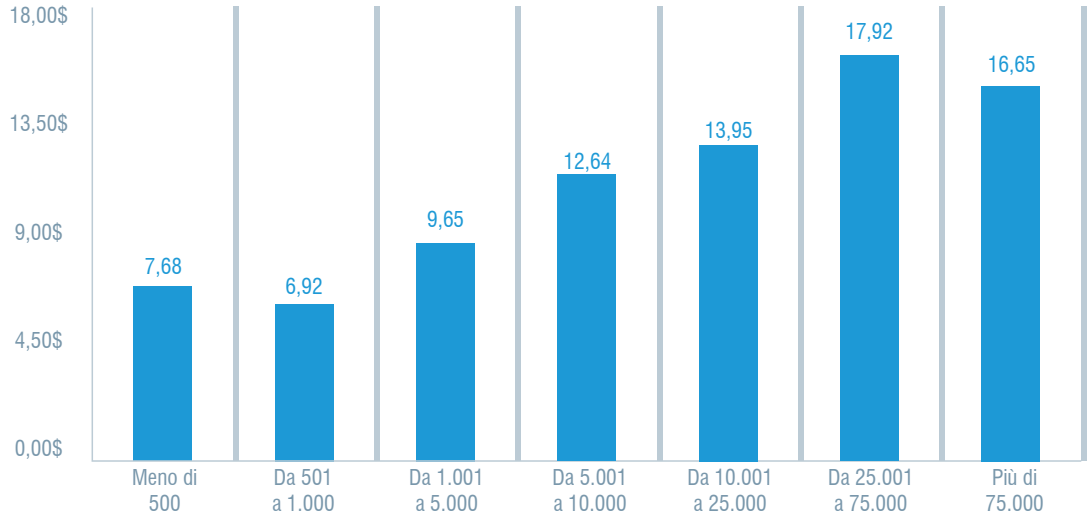


La figura 12 riporta il costo totale annualizzato per numero globale di dipendenti delle aziende. Le aziende con un numero di dipendenti compreso fra 25.001 e 75.000 hanno avuto il costo totale più elevato, pari a 17,92 milioni di dollari, mentre quelle con 500-1.000 dipendenti hanno avuto il costo annualizzato più basso a 6,92 milioni.

Figura 12.

Costo medio delle attività per numero di dipendenti

Media = 11,45 (milioni di dollari)



ANALISI DEI COSTI

Questo studio ha preso in esame le attività principali relative ai processi che generano una serie di spese associate alla risposta di un'azienda agli incidenti di origine interna. Nel nostro report abbiamo definito sette centri di costo interni:[2]

Monitoraggio e sorveglianza
Attività che consentono a un'azienda di rilevare ragionevolmente e possibilmente scoraggiare le minacce o gli attacchi interni. Ciò include i costi (spese generali) associati a determinate tecnologie che permettono di potenziare la mitigazione o il rilevamento precoce delle minacce.

Indagini
Attività necessarie per identificare accuratamente la fonte, la portata e la rilevanza di uno o più incidenti.

Escalation dei problemi
Attività svolte per generare consapevolezza degli incidenti effettivi fra le principali parti interessate all'interno dell'azienda. Le attività di escalation includono anche i passi compiuti per organizzare una risposta iniziale della direzione.

Risposta agli incidenti
Attività relative alla formazione e al coinvolgimento del team di risposta agli incidenti, compresi i passi compiuti per formulare la risposta finale da parte della direzione.

Contenimento
Attività volte a prevenire gli incidenti o gli attacchi interni o a limitarne la gravità. Includono la disattivazione di applicazioni e di endpoint vulnerabili.

Risposta a posteriori
Attività che aiutano l'azienda a ridurre al minimo il potenziale di incidenti futuri o attacchi di origine interna. Includono inoltre i passi compiuti per comunicare con le principali parti interessate, sia all'interno che all'esterno dell'azienda, compresa l'elaborazione di raccomandazioni per ridurre al minimo i potenziali danni.

Applicazione di misure correttive
Attività associate alla riparazione e alle azioni correttive dei sistemi e dei processi fondamentali dell'azienda. Includono il ripristino delle risorse di informazioni e delle infrastrutture IT che hanno subito danni.

2 I costi interni sono stati estrapolati utilizzando il tempo di manodopera come indicatore dei costi diretti e indiretti. Questo metodo è stato inoltre usato per attribuire un componente di spese generali ai costi fissi, come gli investimenti pluriennali in tecnologie.

Per ogni singolo incidente le aziende spendono in media 644.852 dollari

La tabella 1 riepiloga il costo medio delle tre tipologie di incidenti di origine interna e i sette centri di attività. Come riportato, il contenimento e le azioni correttive rappresentano le attività più costose. Quelli meno costosi sono invece l'analisi a posteriori e l'escalation.

Tabella 1. Centri di costo (per incidente)	Dipendente o sub-appaltatore negligente	Utenti interni malintenzionati	Furto delle credenziali di accesso	Costo medio
Monitoraggio e sorveglianza	21.538$	21.857$	22.977$	22.124$
Indagini	49.441$	114.524$	147.429$	103.798$
Escalation dei problemi	9.282$	29.513$	26.619$	21.805$
Risposta agli incidenti	62.877$	159.398$	132.677$	118.317$
Contenimento	75.903$	175.962$	382.794$	211.553$
Analisi a posteriori	21.035$	19.282$	18.121$	19.480$
Applicazione di misure correttive	67.036$	235.223$	141.069$	147.776$
Totale	307.111$	755.760$	871.686$	644.852$

Le aziende spendono di più per le indagini e per l'escalation dei problemi. La Tabella 2 mostra l'aumento percentuale dei costi per ciascuna attività. Il costo dell'applicazione delle misure correttive non è aumentato così nettamente come quello delle altre attività

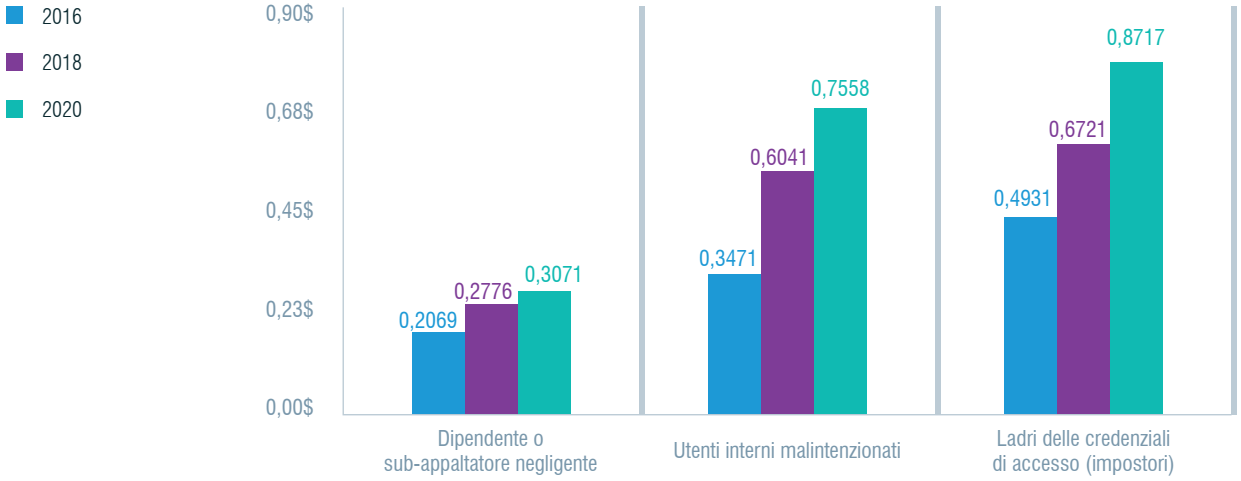
Tabella 2. Centri di costo	2016	2018	2020	Aumento netto su tre anni
Monitoraggio e sorveglianza	9.610$	12.634$	22.124$	79%
Indagini	41.461$	78.398$	103.798$	86%
Escalation dei problemi	8.919$	12.542$	21.805$	84%
Risposta agli incidenti	66.370$	91.263$	118.317$	56%
Contenimento	122.796$	173.060$	211.553$	53%
Analisi a posteriori	8.498$	11.491$	19.480$	78%
Applicazione di misure correttive	91.397$	138.532$	147.776$	47%
Totale	349.052$	517.920$	644.852$	60%

Come mostrato nella figura 13, il furto delle credenziali d'accesso è l'incidente interno più costoso: oltre 2,5 volte superiore a quello degli incidenti imputabili alla negligenza di un dipendente o di un sub-appaltatore.

Figura 13.

Costo medio per incidente per i tre profili

In milioni di dollari



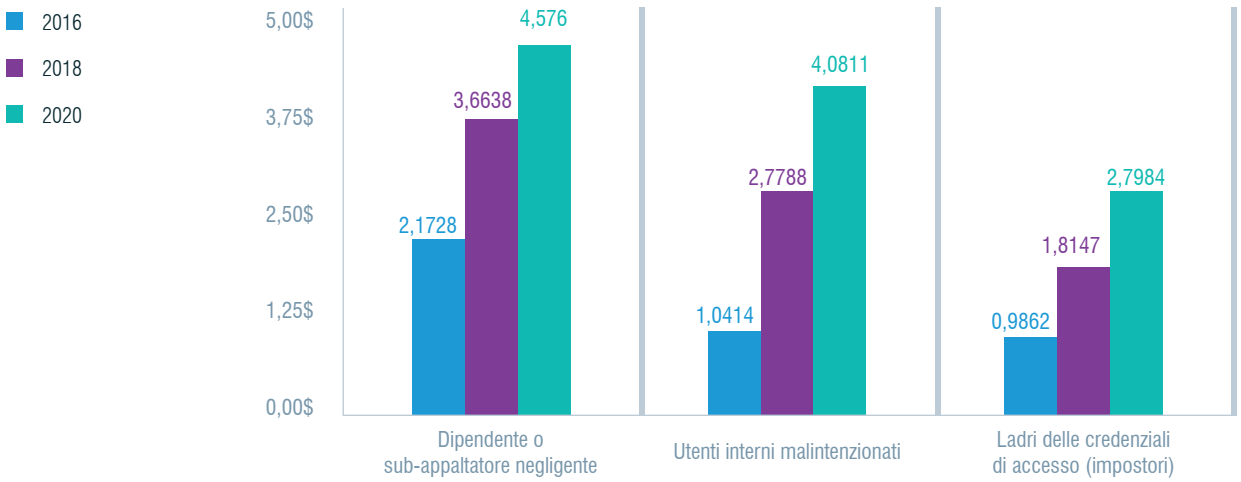
La negligenza di dipendenti e sub-appaltatori è la più costosa su base annua

La figura 14 mostra i costi annualizzati relativi agli incidenti interni per i tre profili. In termini di costi annuali totali, è chiaro che un dipendente o un sub-appaltatore negligente sia il profilo di utente interno più costoso. Sebbene il furto delle credenziali di accesso sia il tipo di incidente più costoso su base unitaria, rappresenta il profilo meno oneroso su base annualizzata.

Figura 14.

Costo annualizzato medio per i tre profili

In milioni di dollari

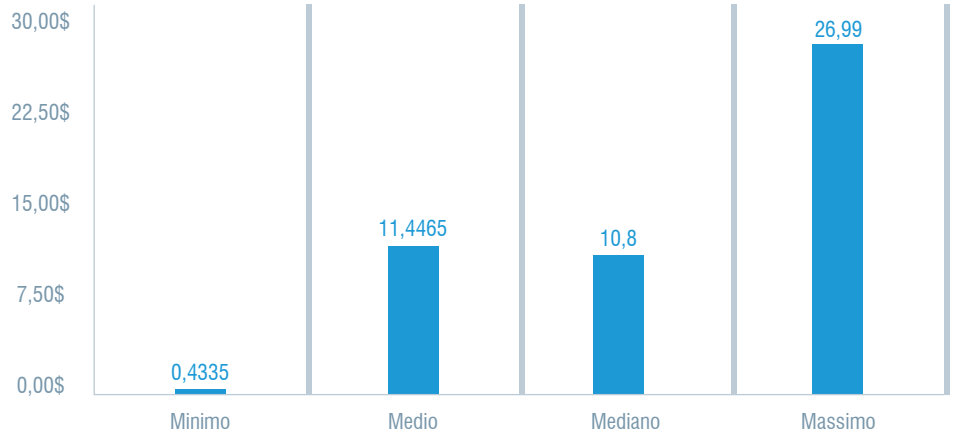


La figura 15 riporta i costi mediani, medi, minimi e massimi degli incidenti interni (combinando i tre profili) negli ultimi 12 mesi. I costi medi e mediani sono rispettivamente di 11,45 e 10,80 milioni di dollari. Il costo minimo è pari a 0,43 milioni di dollari, mentre il costo massimo è pari a 26,99 milioni di dollari.

Figura 15.

Statistiche del campione sul costo degli incidenti interni negli ultimi 12 mesi

Dati raggruppati per i tre profili | In milioni di dollari



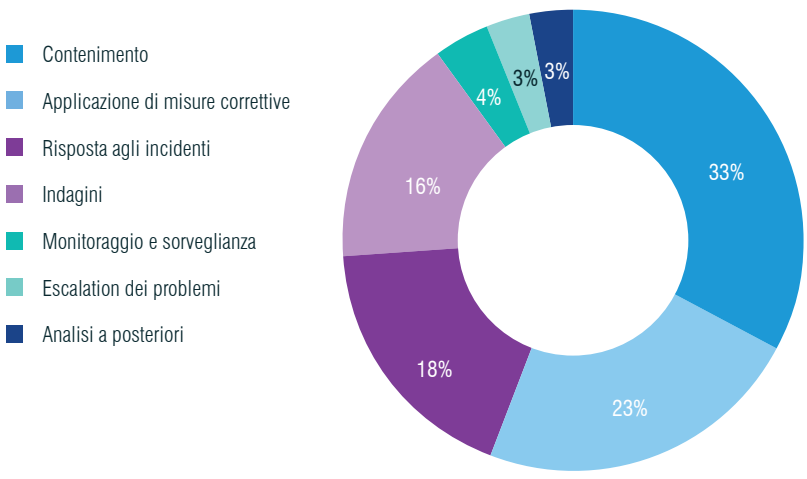
Il contenimento costituisce un terzo di tutti i costi

Il seguente grafico a torta mostra i costi percentuali delle sette attività. Secondo la figura 16, il contenimento costituisce il 33% dei costi annualizzati totali degli incidenti causati dal personale interno. Le attività relative all'applicazione di misure correttive e alla risposta agli incidenti rappresentano rispettivamente il 23% e il 18% del costo totale.

Figura 16.

Costo percentuale degli incidenti interni per attività

n=204 aziende



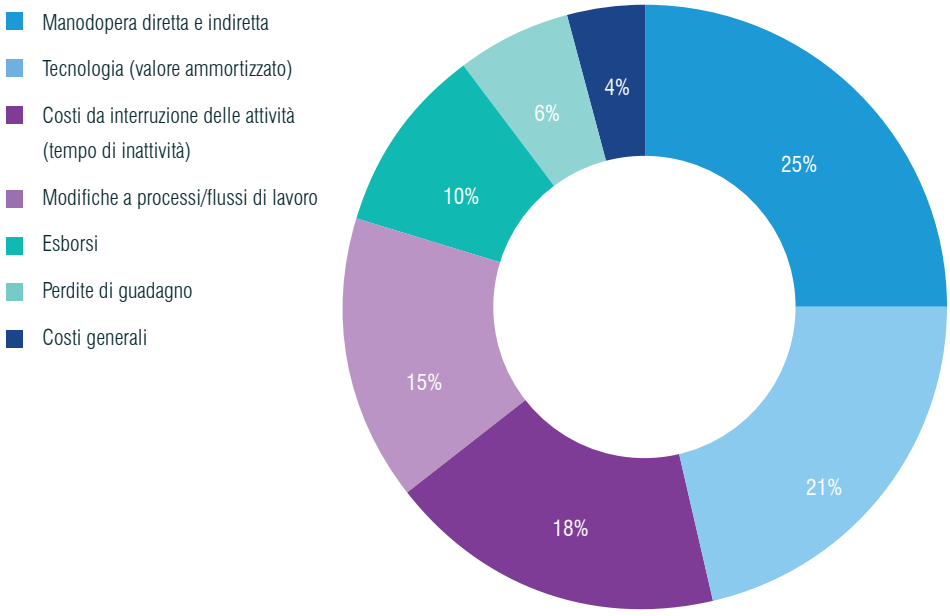
Le persone e le tecnologie rappresentano la maggiore spesa delle aziende per risolvere gli incidenti interni

La figura 17 mostra la ripartizione percentuale dei costi relativi agli incidenti interni imputabili a dipendenti disattenti o negligenti, utenti interni malintenzionati e ladri delle credenziali d'accesso, secondo sette categorie di costi. La categoria di costo più ampia (manodopera diretta e indiretta) include i costi diretti e indiretti associati al personale interno, ai lavoratori temporanei e a contratto. La categoria seguente è la tecnologia, che include il valore ammortizzato e le licenze per il software e l'hardware utilizzati in risposta alle minacce interne (21%).

I costi legati ai processi includono le attività dei sistemi di governance e di controllo necessari in risposta a minacce e attacchi. Il costo delle interruzioni delle attività include la ridotta produttività di dipendenti o utenti risultante da incidenti interni. Le spese generali includono un'ampia gamma di costi in cui si incorre a sostegno del personale e dell'infrastruttura di sicurezza informatica.

Figura 17.

Costo in percentuale degli incidenti interni per categorie standard

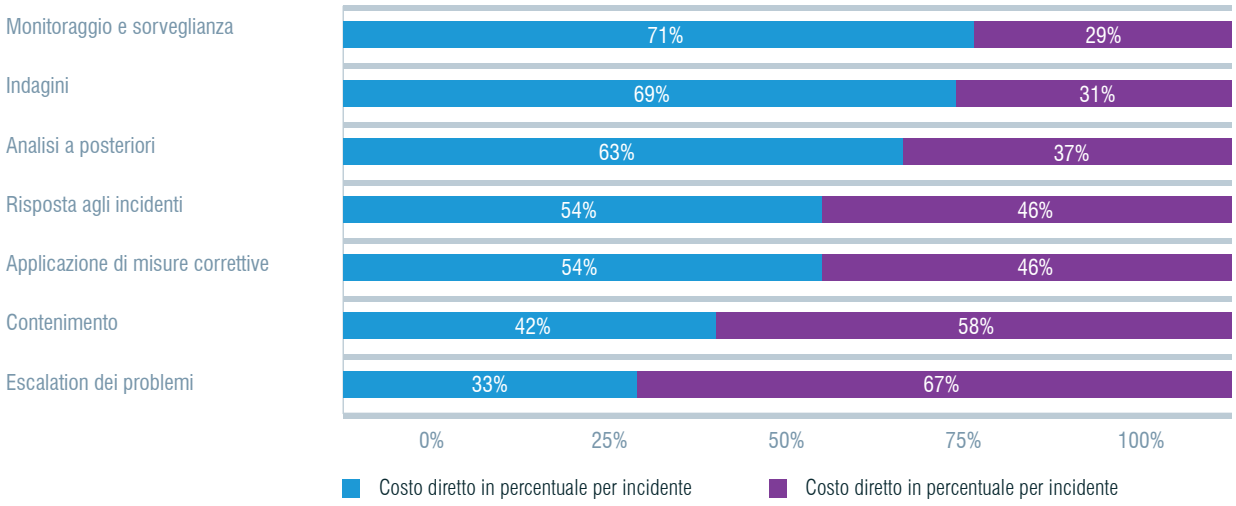


Alle aziende è stato chiesto di stimare i costi diretti sostenuti per compiere una data attività nonché il tempo, l'impegno e le altre risorse necessarie, ma non in termini di esborsi di cassa diretti (vale a dire i costi indiretti). La figura 18 mostra la percentuale dei costi diretti e indiretti per i sette centri di costo relativi alle attività interne. Come si può evincere, la percentuale più alta di costi diretti è costituita da monitoraggio e sorveglianza, mentre la percentuale più alta di costi indiretti va all'escalation dei problemi.

Figura 18

Percentuali di costi diretti e indiretti per i centri di attività

Dati raggruppati per i tre profili



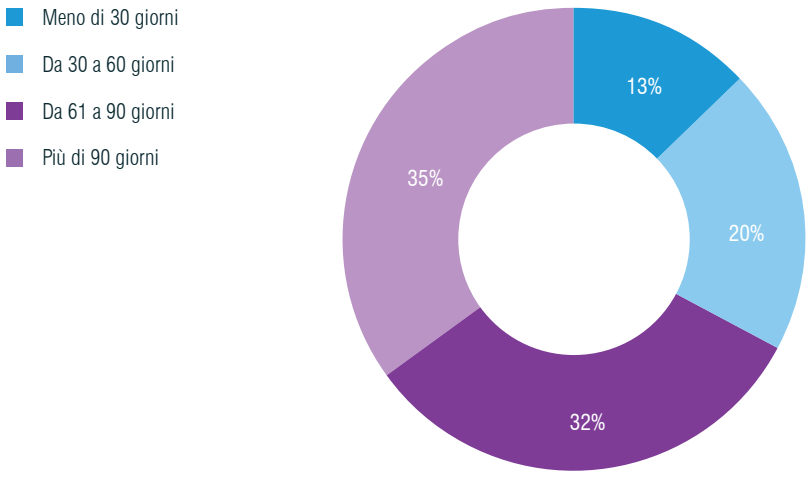
Le aziende impiegano in media oltre due mesi per contenere un incidente

Come mostrato nella figura 19, il tempo medio di contenimento degli incidenti di origine interna nel nostro campione di riferimento è di 77 giorni. Solo il 13% degli incidenti è stato arginato in meno di 30 giorni.

Figura 19.

Distribuzione percentuale degli incidenti interni in base al tempo necessario per il contenimento

Media = 77 giorni



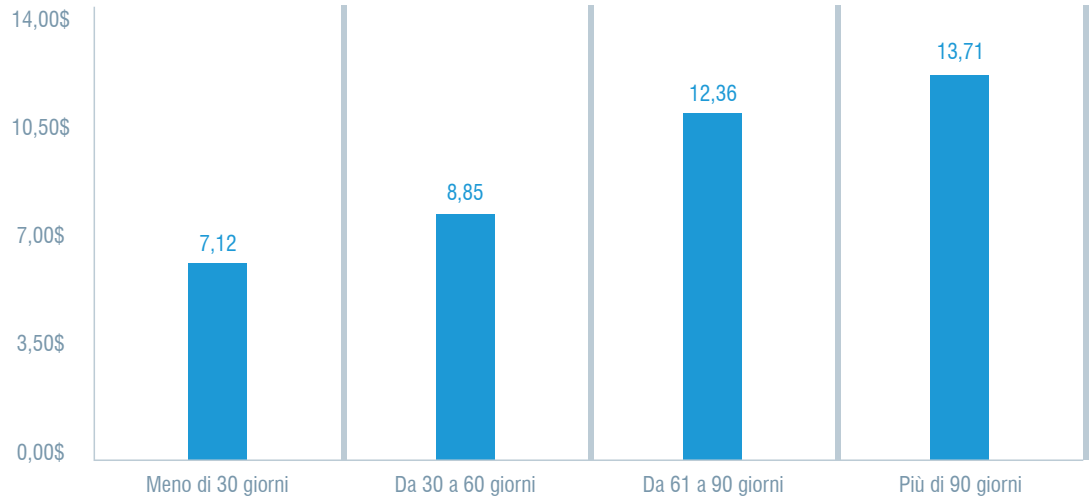
Più veloce è il contenimento, meno costoso è l'incidente

Il costo totale annualizzato degli incidenti di origine interna sembra essere positivamente correlato al tempo necessario per contenerli. Come mostrato nella figura 20, gli incidenti che richiedono più di 90 giorni per il contenimento hanno avuto il costo totale medio annuo più elevato (13,71 milioni di dollari). Per contro, i casi per i quali occorrono meno di 30 giorni hanno i costi totali più bassi (7,12 milioni di dollari). Il costo medio annuo è di 11,45 milioni di dollari.

Figura 20.

Costo medio delle attività in funzione del tempo di contenimento degli incidenti

Media = 11,45 (milioni di dollari)



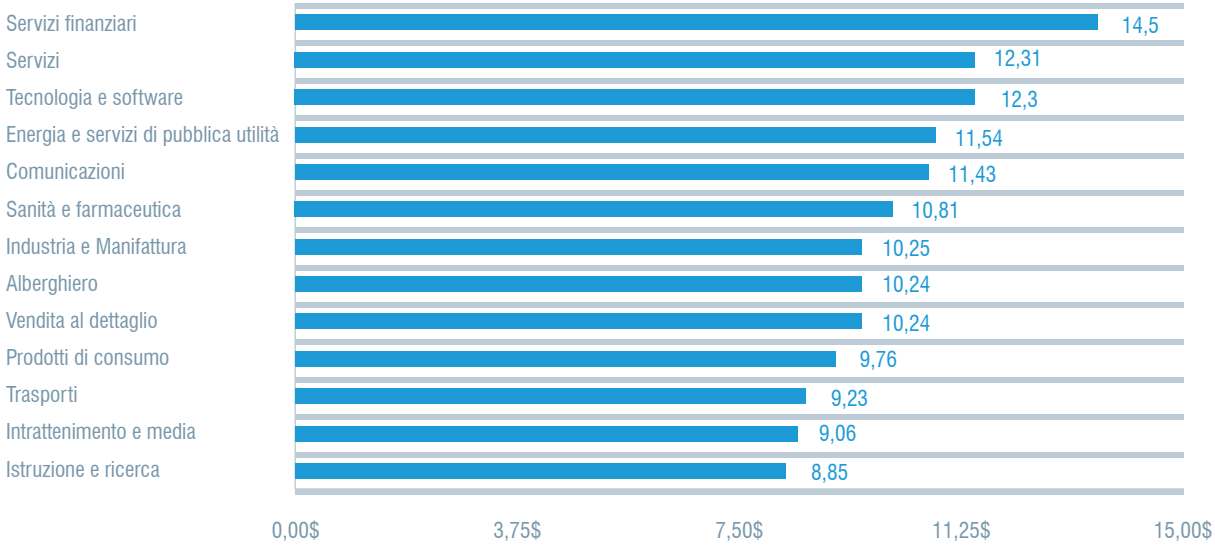
La figura 21 riporta il costo totale annualizzato per 13 settori d'attività[3]. Con 14,5 milioni di dollari, sono le aziende di servizi finanziari ad aver registrato il costo totale più elevato. Seguono i settori di servizi e di tecnologia e software, rispettivamente con 12,31 milioni e 12,3 milioni di dollari. Per contro le aziende del settore istruzione e ricerca hanno riportato il costo totale annualizzato più basso con 8,85 milioni di dollari.

3 Le differenze tra i vari settori industriali devono essere interpretate con cautela date le ridotte dimensioni dei sottocampioni.

Figura 21.

Costo annualizzato delle attività per settore

Media = 11,45 (milioni di dollari)

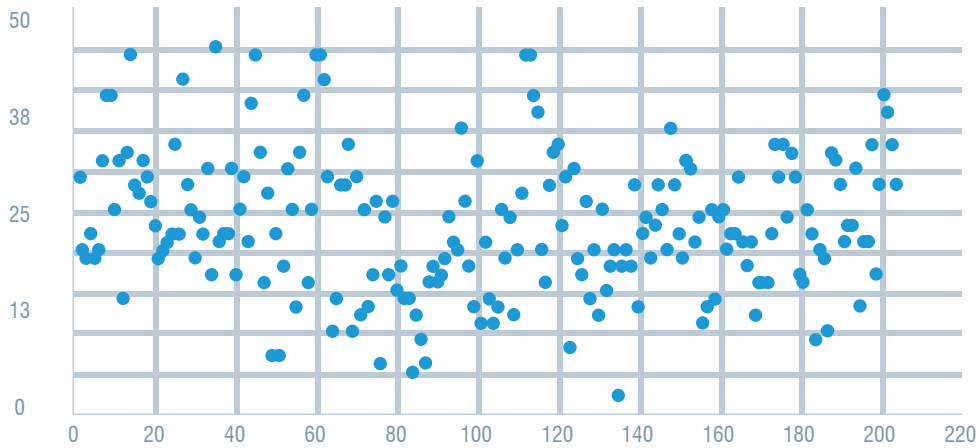


La figura 22 mostra un grafico a dispersione dei costi totali annualizzati relativi agli incidenti interni per azienda. Delle 204 imprese partecipanti, 124 (il 61%) hanno registrato un costo totale medio pari o inferiore alla media di 11,45 milioni di dollari negli ultimi 12 mesi. Per le restanti 80 aziende (39%) il costo è stato superiore alla media. Il risultato suggerisce che la ripartizione è disomogenea.

Figura 22.

Grafico a dispersione degli incidenti interni per azienda

Media = 11,45 (milioni di dollari)



Come mostrato nella tabella 3, per prevenire le minacce interne la maggior parte delle aziende ha implementato corsi di sensibilizzazione degli utenti (55%), misure di prevenzione delle fughe di dati (54%) e analisi del comportamento degli utenti (50%),

Tabella 3. **Strumenti e attività per ridurre le minacce interne** Strumenti di sicurezza e attività	Numero di aziende	Percentuale di aziende
Formazione e sensibilizzazione degli utenti	112	55%
Prevenzione della fuga di dati (DLP)	110	54%
Analisi del comportamento degli utenti	102	50%
Monitoraggio e sorveglianza dei dipendenti	96	47%
Gestione degli incidenti e degli eventi di sicurezza (SIEM)	91	45%
Gestione della risposta agli incidenti	89	44%
Rigorose procedure di verifica di terze parti	87	43%
Condivisione delle informazioni sulle minacce	85	42%
Gestione degli accessi con privilegi	80	39%
Informazioni sul traffico di rete	77	38%

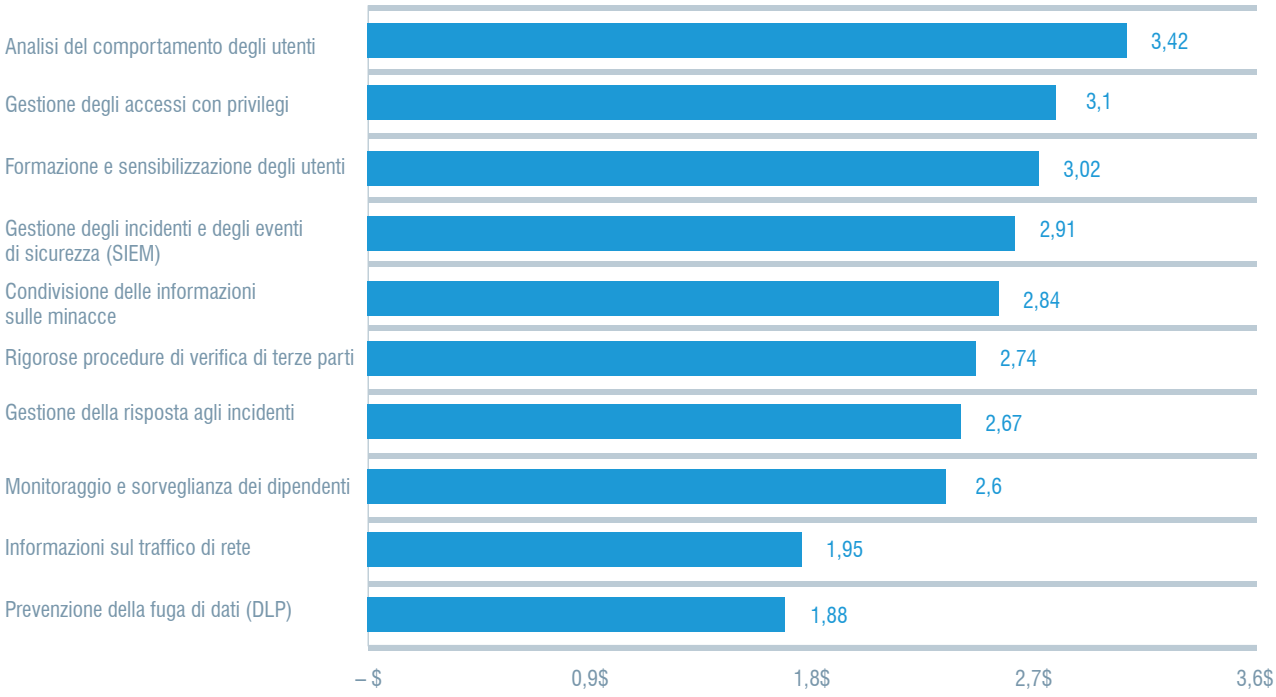
L'analisi del comportamento degli utenti, la gestione degli accessi con privilegi e la formazione e sensibilizzazione degli utenti sono gli strumenti e le attività più efficaci e convenienti

Secondo la figura 23, le aziende possono risparmiare una media di 3,4 milioni e di 3,1 milioni di dollari, rispettivamente, implementando una soluzione di analisi del comportamento degli utenti e di gestione degli accessi con privilegi. La figura 23 riporta gli strumenti e le attività utilizzati più di frequente. Ne risulta che 112 aziende hanno implementato programmi di formazione per sensibilizzare i dipendenti sulle minacce interne. Sono 110 le aziende che hanno adottato soluzioni per la prevenzione della fuga di dati, mentre sono 102 quelle che si avvalgono dell'analisi del comportamento degli utenti per individuare le attività di rete sospette.

Figura 23.

Risparmi risultanti dall'impiego di strumenti e attività per la riduzione del rischio informatico

Media = 11,45 (milioni di dollari)



CONCLUSIONI - GESTIONE DELLE MINACCE INTERNE

Con l'aumento delle minacce interne, l'incremento del costo medio per incidente da 8,76 milioni di dollari nel 2018 (Ponemon) a 11,45 milioni nel 2020 e l'aumento da 73 a 77 giorni (Ponemon) del tempo di contenimento degli incidenti, le aziende devono implementare un efficace programma di gestione delle minacce interne. L'obiettivo del programma è di rispondere rapidamente agli incidenti e di ridurne al minimo l'impatto complessivo.

Che siano di natura accidentale o dolosa, gli incidenti interni non possono essere eliminati con la sola tecnologia. Le aziende hanno bisogno di un programma di gestione delle minacce interne che includa persone, processi e tecnologie per identificare e prevenire gli eventi all'interno dell'azienda.

Risorse umane

- Il rilevamento e la prevenzione delle minacce interne è un lavoro di squadra. Assicurati di coinvolgere i gruppi e le parti interessate nelle attività del centro operazioni di sicurezza dell'azienda.
- Limita l'accesso degli utenti ai dati non essenziali oppure cerca di ridurre il tempo per il quale gli utenti privilegiati possono accedere alle informazioni necessarie per completare un'attività.
- Cerca i principali indicatori comportamentali per scoprire una potenziale minaccia interna.

Processi

- Valuta i rischi a cui è esposta l'azienda e sviluppa una funzione specificamente dedicata alle minacce interne, soprattutto se i dati sono particolarmente sensibili o preziosi.
- Stabilisci processi coerenti, ripetibili ed equi per tutti i dipendenti, utilizzando una tecnologia che possa ottimizzare e sostenere tali processi.
- Investi nella formazione degli utenti, per fornire loro conoscenze in aree quali la gestione sicura dei dati, la sensibilizzazione alla sicurezza e la vigilanza.

Tecnologia

- Valuta l'impatto sulle prestazioni di ogni soluzione di protezione contro le minacce interne nonché la sua facilità di gestione e distribuzione, stabilità e flessibilità.
- Scegli una soluzione che possa evolvere di pari passo con la crescita dell'azienda.
- Tieni a mente le diverse competenze di ciascun fornitore in materia di minacce interne nonché di rilevamento e prevenzione delle minacce esterne.
- Determina se la soluzione fornisce visibilità sull'attività degli utenti, in particolare quelli con privilegi.

QUESTO STUDIO SUI COSTI È L'UNICO CHE PRENDE IN ESAME **LE ATTIVITÀ RELATIVE AI PROCESSI** E **AI SISTEMI AZIENDALI FONDAMENTALI,** CHE GENERANO VARIE SPESE.

QUADRO DI RIFERIMENTO

Lo scopo della presente ricerca è di fornire indicazioni sul potenziale costo delle minacce interne per un'azienda. Questo studio è l'unico che prende in esame le attività relative ai processi e ai sistemi aziendali fondamentali, che generano una serie di spese associate alla risposta di un'azienda agli incidenti causati da dolo o negligenza degli utenti interni. Nello studio definiamo come incidente causato dal personale interno il danneggiamento di dati, reti o sistemi fondamentali di un'azienda. Questa definizione include anche gli attacchi perpetrati da attori esterni (noti anche come impostori) che rubano le credenziali di accesso di dipendenti o utenti legittimi.

Le nostre metodologie di raffronto sono concepite per far luce sulle effettive esperienze e conseguenze degli incidenti di origine interna. In base alle interviste condotte con svariati dipendenti di alto livello in ciascuna azienda, abbiamo classificato i costi secondo due flussi distinti:

- I costi associati alla lotta contro le minacce interne, che noi definiamo centri di costo interni;
- I costi relativi alle conseguenze degli incidenti, che definiamo effetti esterni dell'evento o dell'attacco.

Analizziamo i centri di costo interni in modo sequenziale, partendo dal monitoraggio e sorveglianza del panorama delle minacce interne per giungere all'applicazione di misure correttive. Abbiamo inoltre incluso i costi relativi alle opportunità commerciali perse e ai tempi di inattività. Per ogni centro di costo abbiamo chiesto agli intervistati di stimare i costi diretti, indiretti e, se pertinenti, i costi in termini di opportunità, definiti come segue:

- Costo diretto: l'esborso diretto per intraprendere una determinata attività
- Costo indiretto: tempo, impegno e altre risorse coinvolte, ma non in termini di esborsi diretti
- Costo in termini di opportunità: il costo risultante dalla perdita di opportunità commerciali a causa del danno alla reputazione dopo il verificarsi di un incidente.

I costi esterni quali perdita delle risorse di informazioni, inattività, danni alle attrezzature e perdite di ricavi, sono stati calcolati utilizzando metodi di sistema dei costi. I costi totali sono stati distribuiti fra sette distinti vettori di costo.[4]

4 Siamo consapevoli del fatto che queste sette categorie di costo non sono indipendenti l'una dall'altra e che non rappresentino un elenco esaustivo di tutti i centri di costo aziendali.

Questo studio prende in esame le attività principali relative ai processi che generano una serie di spese associate alla risposta di un'azienda agli incidenti di origine interna.

I sette centri di costi interni inclusi nel quadro di riferimento sono i seguenti:[5]

- **Monitoraggio e sorveglianza:** attività che consentono a un'azienda di rilevare ragionevolmente e possibilmente scoraggiare le minacce o gli attacchi interni. Ciò include i costi (spese generali) associati a determinate tecnologie che permettono di potenziare la mitigazione o il rilevamento precoce delle minacce.
- **Indagini:** attività necessarie per identificare accuratamente la fonte, la portata e la rilevanza di uno o più incidenti.
- **Escalation dei problemi:** attività svolte per generare consapevolezza sugli incidenti effettivi fra le principali parti interessate all'interno dell'azienda. Le attività di escalation includono anche i passi compiuti per organizzare una risposta iniziale della dirigenza.
- **Risposta agli incidenti:** attività relative alla formazione e al coinvolgimento del team di risposta agli incidenti, compresi i passi compiuti per formulare la risposta finale da parte della direzione.
- **Contenimento:** attività volte a prevenire gli incidenti o gli attacchi interni o a limitarne la gravità. Includono la disattivazione di applicazioni e di endpoint vulnerabili.
- **Risposta a posteriori:** attività che aiutano l'azienda a ridurre al minimo il potenziale di incidenti futuri o attacchi di origine interna. Includono inoltre i passi compiuti per comunicare con le principali parti interessate, sia all'interno sia all'esterno dell'azienda, compresa l'elaborazione di raccomandazioni per ridurre al minimo i potenziali danni.
- **Applicazione di misure correttive:** attività associate alla riparazione e alle azioni correttive dei sistemi e dei processi fondamentali dell'azienda. Includono il ripristino delle risorse di informazione e delle infrastrutture IT che hanno subito danni.

Oltre alle attività relative ai processi di cui sopra, le aziende spesso incorrono in costi o in conseguenze esterne a seguito di un incidente. La nostra ricerca rivela che i quattro centri di costi generali associati a tali conseguenze esterne sono i seguenti

- **Costo legato a perdita o furto di informazioni:** perdita o furto di informazioni sensibili e riservate a seguito di un attacco interno. Tali informazioni includono segreti commerciali, proprietà intellettuali (fra cui il codice sorgente), informazioni sui clienti e registri del personale. Questa categoria include inoltre il costo della notifica di violazione dei dati nel caso di acquisizione illecita di dati personali.
- **Costo da inattività:** l'impatto economico di tempi di fermo o arrestio non programmati che impediscono all'azienda di adempiere ai propri obblighi di trattamento dei dati.
- **Costo da danni alle attrezzature:** il costo per risanare attrezzature e altre risorse IT a seguito di attacchi interni alle risorse di informazioni e all'infrastruttura critica.
- **Perdita di ricavi:** perdita di clienti (abbandono) e di altre parti interessate a causa di ritardi o arresto dei sistemi a causa di un attacco interno. Per estrapolare questo costo, abbiamo utilizzato una metodologia di stima dei costi, che si basa sull'"indice di valore economico" di un cliente medio definito per ogni azienda partecipante.

5 I costi interni sono stati estrapolati utilizzando il tempo di manodopera come indicatore dei costi diretti e indiretti. Questo metodo è stato inoltre usato per attribuire un componente di spese generali ai costi fissi, come gli investimenti pluriennali in tecnologie.

IL NOSTRO STRUMENTO DI RAFFRONTO (O BENCHMARKING) È CONCEPITO PER **RACCOGLIERE INFORMAZIONI DESCRITTIVE** DAL REPARTO IT.

RAFFRONTO

Il nostro strumento di raffronto (benchmarking) è concepito per raccogliere informazioni descrittive da professionisti informatici, addetti alla sicurezza delle Informazioni e altre figure chiave, in merito ai costi effettivi sostenuti, direttamente o indirettamente, a seguito del rilevamento di un attacco o di un incidente di origine interna all'azienda. La nostra metodologia di calcolo dei costi non richiede la raccolta dei risultati contabili effettivi dei partecipanti allo studio, ma si basa piuttosto sulle stime e sull'estrapolazione dei dati raccolti durante le interviste condotte nell'arco di quattro settimane.

La stima dei costi si basa su interviste diagnostiche riservate con il personale chiave di ciascuna azienda presa in esame. Le metodologie di raccolta dei dati non includono informazioni contabili, ma si affidano invece a stime numeriche basate sulle conoscenze e l'esperienza di ciascun partecipante. All'interno di ogni categoria la stima dei costi è stata effettuata in due fasi. Innanzitutto, lo strumento di raffronto ha chiesto ai partecipanti di stimare il costo diretto per ogni categoria di costo, utilizzando un intervallo variabile definito in base al formato di asse numerico.

Utilizzo dell'asse numerico

L'asse numerico fornito sotto ciascuna categoria di costi associati alle violazioni dei dati fornisce la migliore stima possibile della somma degli esborsi, dei costi di manodopera e delle spese generali sostenuti. Contrassegnare un solo punto fra i limiti inferiore e superiore definiti sopra. Durante l'intervista, si possono ripristinare i limiti inferiore e superiore dell'asse numerico in qualsiasi momento.

Inserire qui la stima dei costi diretti per [relativa categoria di costo]

Limite inferiore

Limite superiore

Il valore numerico ottenuto con questo asse numerico (piuttosto che una stima precisa per ciascuna categoria di costo presentata) ha contribuito a preservare l'anonimato dei partecipanti e un tasso di risposte più elevato. Lo strumento di raffronto chiedeva inoltre ai professionisti di fornire, separatamente, una seconda stima dei costi indiretti e in termini di opportunità.

Le stime dei costi sono state poi raggruppate per ciascuna azienda in base all'importanza relativa di tali costi rispetto al costo diretto in una data categoria. Infine, ai partecipanti sono state poste domande di carattere generale per ottenere informazioni aggiuntive, come ad esempio una stima delle perdite di fatturato a causa di un incidente o un attacco legato al personale interno.

Le domande del sondaggio sono state limitate alle categorie di costo comuni a differenti settori economici. In base alla nostra esperienza, un sondaggio concentrato sui processi ottiene un tasso di risposte più elevato e risultati di maggiore qualità. Abbiamo utilizzato anche uno strumento cartaceo, anziché un sondaggio elettronico, per garantire una maggiore riservatezza.

Per mantenere il completo anonimato, lo strumento del sondaggio non ha acquisito alcun genere di informazioni specifiche sulle aziende. I documenti del sondaggio non contenevano codici di tracciamento né altri metodi che potessero collegare le risposte alle aziende partecipanti.

Al fine di mantenere lo strumento di raffronto gestibile in termini di dimensioni, abbiamo limitato l'indagine solo ai centri di costo considerati cruciali per la misurazione dei costi. Sulla base di alcune discussioni con gli esperti, è stato deciso di concentrare la serie finale di elementi su un insieme limitato di attività che generano costi diretti o indiretti. Dopo aver raccolto le informazioni di raffronto, ogni strumento è stato attentamente esaminato per confermarne coerenza e completezza. Sono state escluse dallo studio le aziende che hanno fornito risposte incomplete, incoerenti o che non ne hanno fornite.

L'indagine sul campo è iniziata a marzo 2019. Per garantire coerenza fra tutte le aziende studiate, la raccolta di informazioni sulla loro esperienza è stata limitata a un periodo di quattro settimane consecutive. Questo arco di tempo non è stato necessariamente lo stesso per tutte le aziende partecipanti allo studio. I costi estrapolati, diretti e indiretti, sono stati annualizzati dividendo il costo totale calcolato su quattro settimane (rapporto = 4/52 settimane).

LIMITAZIONI DELLA RICERCA

Il nostro studio utilizza un metodo di raffronto riservato e proprietario, utilizzato con successo in ricerche precedenti. Tuttavia, questa ricerca ha presentato delle limitazioni intrinseche da considerare attentamente prima di trarre conclusioni dai suoi risultati.

- **Risultati non statistici:** il nostro studio si basa su un campione rappresentativo, non statistico, delle aziende che hanno subito uno o più incidenti legati al personale interno negli ultimi 12 mesi. Poiché le nostre metodologie di campionamento non sono scientifiche, non è possibile applicare ai dati raccolti le inferenze statistiche, i margini di errore e gli intervalli di confidenza.
- **Mancanza di risposta:** i risultati attuali si basano su un piccolo campione rappresentativo di riferimento. In questo studio, 159 aziende hanno completato il processo di benchmarking. Non abbiamo testato la mancata risposta, perciò è sempre possibile che i costi soggiacenti alle violazioni dei dati nelle aziende non partecipanti siano sostanzialmente differenti.
- **Errore da quadro di campionamento:** dato che il nostro quadro di campionamento è soggettivo, la qualità dei risultati dipende da quanto sono rappresentative le aziende del campione preso in esame. Riteniamo che l'attuale quadro di campionamento sia più incentrato sulle aziende dotate di programmi di privacy o di sicurezza delle informazioni più maturi.
- **Informazioni specifiche sulle aziende:** le informazioni di riferimento sono sensibili e riservate, pertanto lo strumento utilizzato non acquisisce alcuna informazione che possa identificare le aziende che hanno partecipato. Inoltre, permette ai partecipanti di usare variabili di risposta categoriche per divulgare informazioni demografiche sull'azienda e sul settore di attività.
- **Fattori non misurati:** per mantenere i testi del questionario concisi e mirati, abbiamo deciso di omettere dalle nostre analisi altre variabili importanti, come le principali tendenze e le caratteristiche organizzative. Non è possibile determinare la misura in cui le variabili omesse possono spiegare i risultati di raffronto.
- **Risultati sui costi estrapolati:** la qualità di una ricerca di raffronto si fonda sull'integrità delle risposte riservate fornite dagli intervistati delle aziende partecipanti. Anche se determinate verifiche ed equilibri possono essere integrati nel processo stesso, c'è sempre la possibilità che alcune delle risposte fornite non siano accurate o veritiere. Inoltre, l'uso delle metodologie di estrapolazione dei costi, piuttosto che dei dati effettivi, potrebbe inavvertitamente introdurre errori e imprecisioni.

observe IT

INFORMAZIONI SU OBSERVEIT

In qualità di soluzione leader per la gestione delle minacce interne, Proofpoint | ObserveIT protegge contro fughe di dati, atti dolosi e danni al marchio causati dalle azioni dannose, negligenti o inconsapevoli degli utenti interni. ObserveIT correla attività e spostamenti dei dati, permettendo agli addetti alla sicurezza di identificare i rischi legati agli utenti, rilevare e contrastare le violazioni di dati causate da personale interno e accelerare la risposta agli incidenti di sicurezza. Per maggiori informazioni visita: www.observeIT.com

Ponemon INSTITUTE

INFORMAZIONI SUL PONEMON INSTITUTE

Il Ponemon Institute è un istituto di ricerca e formazione indipendente dedicato alla promozione di pratiche responsabili in materia di gestione delle informazioni e della privacy nel settore pubblico e privato. La sua missione è quella di condurre studi empirici di alta qualità sulle problematiche critiche che influiscono sulla gestione e la protezione dei dati sensibili personali e aziendali.

A tal fine, vengono applicati rigorosi standard di protezione dei dati, privacy e ricerca etica. Il Ponemon Institute non raccoglie alcun dato di identificazione personale da singoli individui (né acquisisce informazioni che possano identificare le aziende coinvolte nelle ricerche). Inoltre, applica rigorosi standard di qualità per garantire che agli intervistati non vengano poste domande inutili, irrilevanti o improprie.