SOPHOS

La Vera Storia Del Ransomware 2023

I risultati di uno studio indipendente a cui hanno partecipato 3.000 IT/ Cybersecurity Manager dislocati 14 paesi del mondo, da gennaio a marzo 2023.

Whitepaper Sophos. Maggio 2023

Introduzione

Come ogni anno, Sophos ha condotto una ricerca che valuta le esperienze di vita reale degli IT/Cybersecurity Manager in materia di ransomware. I risultati mettono in luce le realtà che le organizzazioni si trovano ad affrontare nel 2023. Rivelano le più comini cause all'origine degli attacchi e offrono nuove prospettive su come le esperienze in ambito ransomware variano a seconda del fatturato dell'organizzazione. Questo report svela inoltre l'impatto commerciale e operativo di quando, invece di servirsi dei backup, le organizzazioni pagano il riscatto per recuperare i dati.

Informazioni Sul Sondaggio

Sophos ha affidato a un'azienda esterna l'incarico di condurre un sondaggio agnostico rispetto ai vendor, coinvolgendo 3.000 IT/Cybersecurity Manager in organizzazioni con 100-5.000 dipendenti in 14 paesi nelle aree geografiche di Nord e Sud America, EMEA (Europa, Medio Oriente e Africa) e Asia-Pacifico. Il sondaggio è stato svolto da gennaio a marzo 2023 e ai partecipanti è stato chiesto di rispondere tenendo in considerazione le proprie esperienze durante l'anno precedente.

Nel settore dell'istruzione, i partecipanti sono stati suddivisi in istruzione scolastica (istituti con studenti fino ai 18 anni) e istruzione superiore (istituti con studenti di età maggiore di 18 anni).

Indice dei contenuti

Tasso Di Attacchi Ransomware

Dalla ricerca svolta, è emerso che il tasso di attacchi ransomware è rimasto invariato, con il 66% degli intervistati che sostiene che la propria organizzazione è stata colpita dal ransomware l'anno precedente: una percentuale identica a quella riscontrata nello studio del 2022. Con avversari informatici ora in grado di eseguire attacchi su vasta scala, oggi il ransomware è potenzialmente il più pericoloso rischio digitale che incombe sulle organizzazioni.

Sono diversi anni che i cybercriminali si adoperano per sviluppare e migliorare il modello del Ransomware as-a-Service: questo modello operativo rende l'uso del ransomware molto più accessibile per gli aspiranti hacker; allo stesso tempo, aiuta a conferire agli attacchi dinamiche sempre più sofisticate, in quanto permette ai malintenzionati di specializzarsi in fasi diverse di tali attacchi. Per maggiori informazioni sul Ransomware as-a-Service, leggi il Sophos 2023 Threat Report.

2020	2021	2022	2023
51%	37%	66%	66%

La tua organizzazione è stata colpita dal ransomware l'anno scorso?

Sì. n=3.000 (2023), 5.600 (2022), 5.400 (2021), 5.000 (2020)

Attacchi In Base Al Paese

Sebbene il tasso di attacchi ransomware registrato rimanga stabile rispetto al 2022, il sondaggio rivela alcune variazioni per quanto riguarda i paesi. Singapore ha segnalato il più alto tasso di attacchi ransomware nello studio di quest'anno, con l'84% delle organizzazioni che sostiene di avere subito un attacco l'anno precedente. Il Regno Unito ha invece riscontrato la più bassa percentuale di attacco (44%).

In Austria si è osservato il calo più significativo nel tasso di attacco: le organizzazioni colpite sono infatti scese dall'84% al 50%. Il Sud Africa ha registrato il più alto incremento nella percentuale di attacco, con il 78% di organizzazioni che sono state colpite dal malware nel sondaggio del 2023, rispetto al 51% nel 2022.

Per maggiori informazioni, vedi il paragrafo Tasso Di Attacchi Ransomware In Base Al Paese: Confronto Tra Il 2023 E Il 2022, a pagina 20.

Attacchi In Base Al Settore

Il settore dell'istruzione è quello che ha mostrato la più alta probabilità di subire un attacco ransomware l'anno scorso, con l'80% (istruzione scolastica) e il 79% (istruzione superiore) degli intervistati che dichiarano di essere stati colpiti. Storicamente, il settore dell'istruzione ha sempre affrontato difficoltà legate a una disponibilità di risorse e tecnologie molto più limitata, rispetto ad altri settori. I dati indicano che gli antagonisti informatici sfruttano proprio questi punti deboli.

Il settore IT, tecnologie e telecomunicazioni è quello che ha registrato la più bassa percentuale di attacco (50%): un risultato che indica un livello superiore di preparazione informatica e la presenza di difese digitali efficienti.

Per maggiori informazioni, vedi il paragrafo Tasso Di Attacchi Ransomware In Base Al Settore, a pagina 21.

66% percentuale di vittime del ransomware

Singapore ha la più alta percentuale di attacco (per paese)

Il Regno Unito mostra la più bassa percentuale di attacco (per paese)

L'istruzione è caratterizzata dalla maggiore quantità di attacchi (per settore)

IT, tecnologie e telecomunicazioni hanno la quantità più bassa di attacchi (per settore)

Attacchi In Base Alle Dimensioni Dell'Organizzazione: Confronto Tra Numero Di Dipendenti E Fatturato

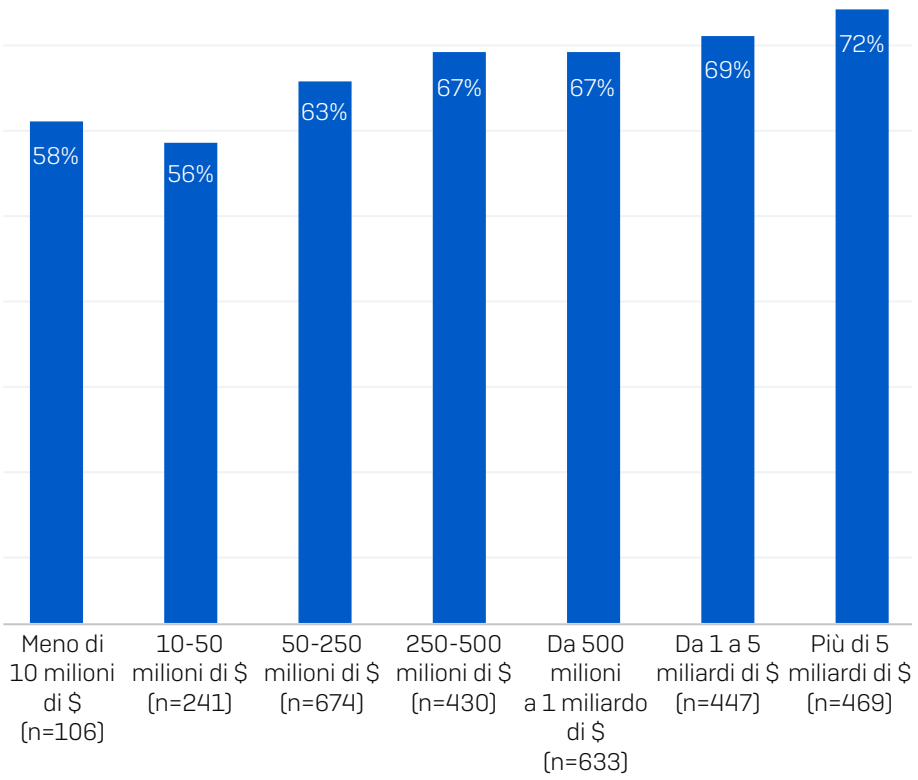
Dallo studio è emersa una netta correlazione tra fatturato annuo e propensione a cadere vittima di un attacco ransomware, con un aumento della percentuale di organizzazioni che sono state colpite dal ransomware che segue progressivamente l'aumento del fatturato. Gli attacchi ransomware l'anno scorso hanno colpito il 56% delle organizzazioni con fatturato pari a 10-50 milioni di $, ma la percentuale sale al 72% per le organizzazioni con fatturato superiore ai 5 miliardi di $.

Tuttavia, sembra non esserci una correlazione sufficientemente chiara tra gli attacchi ransomware subiti e il numero di dipendenti in un'organizzazione. Escludendo il segmento delle organizzazioni con 1.001-3.000 dipendenti, il tasso di attacchi ransomware è estremamente omogeneo:

- 100-250 dipendenti 62%
- 251-500 dipendenti 62%
- 501-1.000 dipendenti 62%
- 1.001-3.000 dipendenti 73%
- 3.001-5.000 dipendenti 63%

I dati indicano chiaramente che, nel contesto delle dimensioni di un'organizzazione, il fatturato annuo è un indicatore molto più attendibile del numero di dipendenti, per calcolare la probabilità di subire un attacco.

Percentuale Di Organizzazioni Colpite Dal Ransomware In Base Al Fatturato

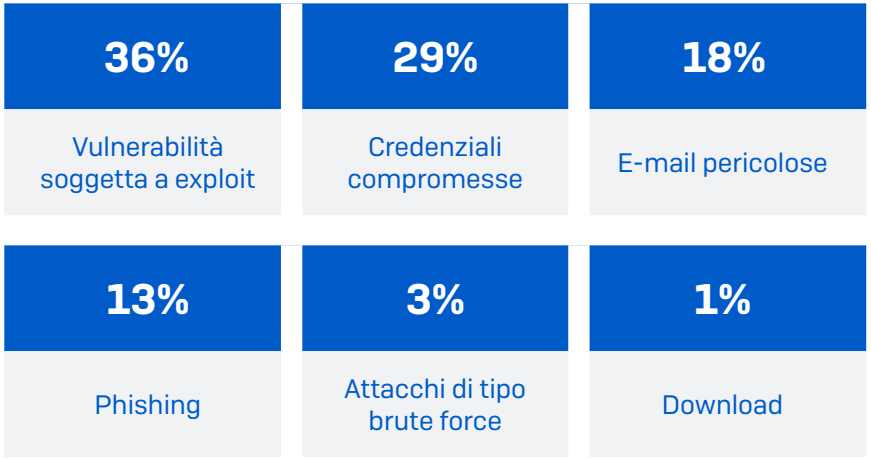


La tua organizzazione è stata colpita dal ransomware l'anno scorso? Sì. Base di partecipanti indicata nel grafico

Cause All'Origine Degli Attacchi Ransomware

I partecipanti al sondaggio indicano che la più comune causa all'origine degli attacchi ransomware è stata una vulnerabilità soggetta a exploit (36%), seguita da credenziali compromesse (29%). Questi risultati si allineano quasi perfettamente con l'ultima analisi retrospettiva condotta da Sophos su 152 attacchi per cui è stato richiesto l'intervento dei nostri team Incident Response e Managed Detection and Response (MDR): il 37% degli incidenti era stato infatti causato da una vulnerabilità soggetta a exploit e il 30% da credenziali compromesse.

Le e-mail sono state la causa che ha scatenato il 30% (cifra arrotondata) degli attacchi: il 18% degli attacchi ha avuto inizio con un'e-mail pericolosa e il 13% con il phishing. Infine, il 3% dei casi ha avuto inizio in seguito a un attacco di tipo brute force e appena l'1% in seguito a un download.



Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? Se l'organizzazione è stata colpita più di una volta, pensa all'attacco più grave (n=1.974 organizzazioni colpite dal ransomware l'anno scorso).

Cause All'Origine Degli Attacchi In Base Al Settore

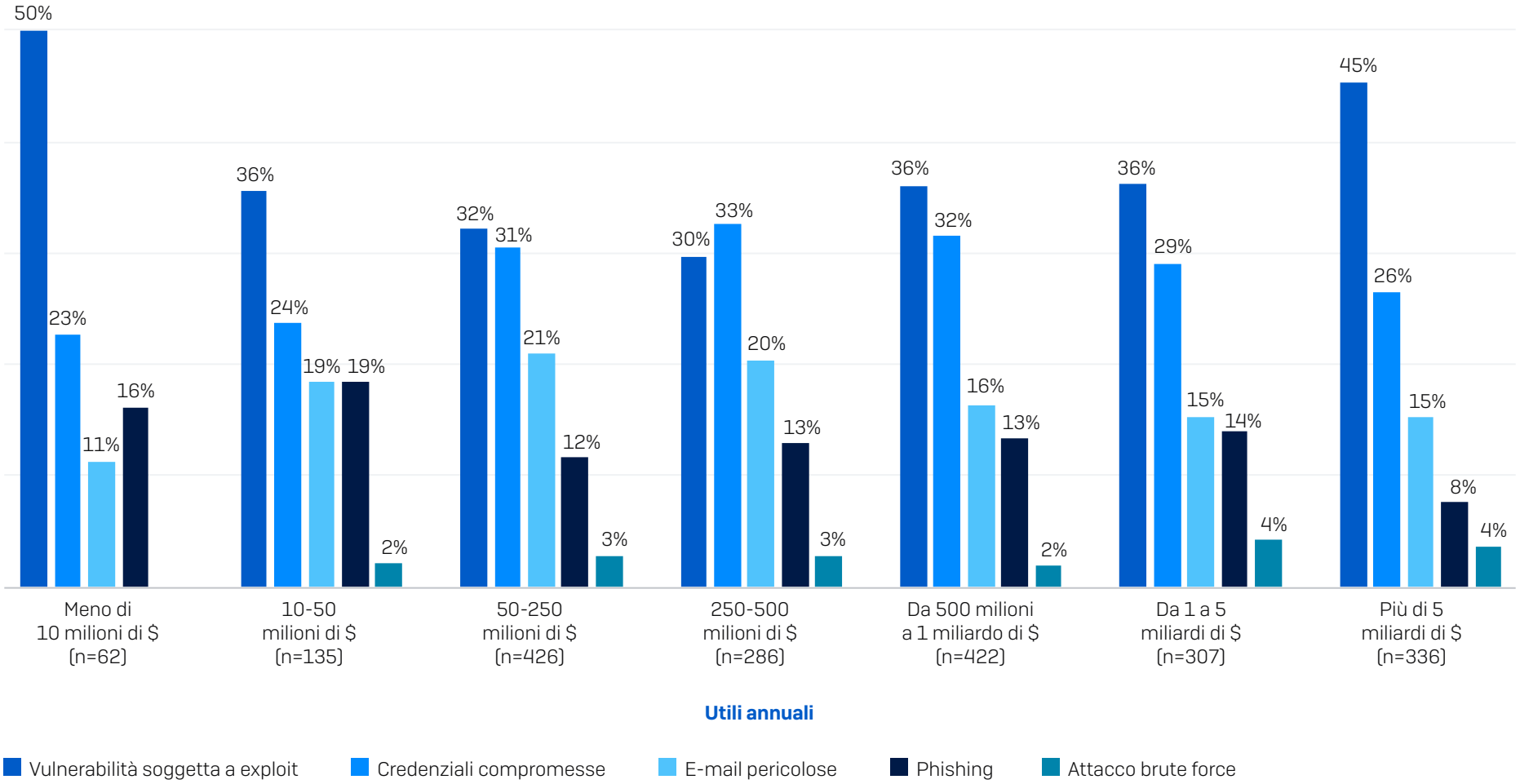
Il settore dei mass media, tempo libero e intrattenimento è quello che ha registrato il tasso più alto di attacchi in cui la causa originaria è stata una vulnerabilità soggetta a exploit (55%), il che indica che sono presenti lacune di sicurezza molto diffuse in questo ambito. Gli intervistati che lavorano nel governo centrale e federale hanno riscontrato la percentuale più alta di attacchi che hanno avuto inizio da credenziali compromesse (41%). Questo potrebbe essere dovuto all'alto tasso di furto di credenziali in questo settore, a una capacità limitata di prevenire gli exploit di credenziali rubate, oppure a una combinazione di entrambi i fattori.

IT, tecnologie e telecomunicazioni hanno le percentuali più basse sia in termini di vulnerabilità soggette a exploit (22%), sia di credenziali compromesse (22%); con molta probabilità, queste statistiche riflettono gli elevati livelli di protezione informatica implementati in questo settore. Tuttavia, i partecipanti al sondaggio di queste organizzazioni hanno anche registrato la percentuale più alta di attacchi basati su e-mail, in quanto le caselle di posta degli utenti sono state identificate come il punto di inizio di oltre la metà (51%) degli incidenti.

Per maggiori informazioni, vedi il paragrafo Cause All'Origine Degli Attacchi In Base Al Settore, a pagina 22.

Cause All'Origine Degli Attacchi In Base Al Fatturato

Analizzando le cause all'origine degli attacchi in base al fatturato annuale delle organizzazioni, si scopre che le vulnerabilità soggette a exploit e le credenziali compromesse seguono curve di propensione opposte. Le percentuali più alte di attacchi che hanno avuto inizio a causa di una vulnerabilità soggetta a exploit sono state riscontrate nelle coorti con fatturato più basso (meno di 10 milioni di $: 50%) e più alto (oltre i 5 miliardi di $: 45%), diminuendo drasticamente al 30% nella coorte mediana (250-500 milioni di $). Si osserva invece una tendenza opposta per quanto riguarda le credenziali compromesse, che raggiungono un picco nella coorte mediana (33%), e presentano tassi inferiori nelle coorti con fatturato più basso (23%) e più alto (26%).

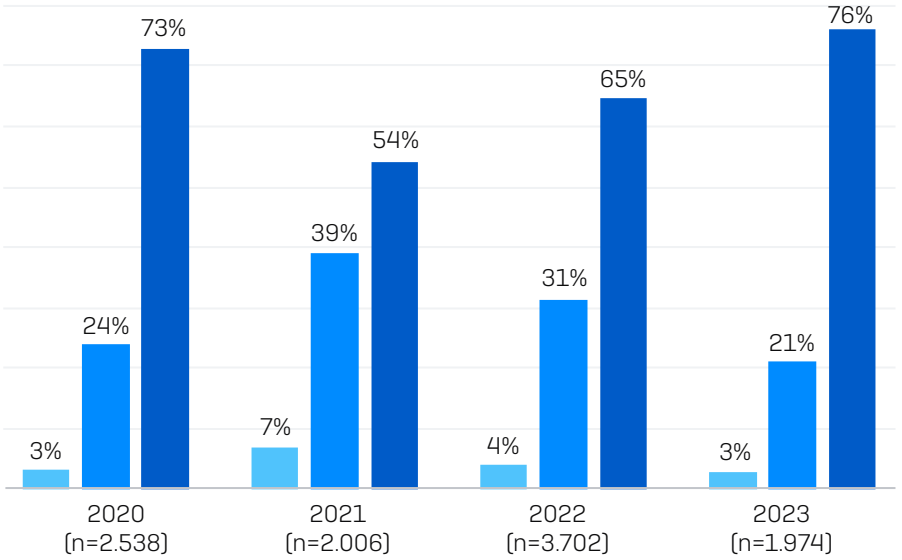


Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? Selezione delle opzioni di risposta. Base di partecipanti indicata nel grafico

Tasso Di Cifratura Non Autorizzata Dei Dati

Si è notato un aumento costante in termini di cifratura non autorizzata dei dati, con cybercriminali che riescono a cifrare i dati delle vittime in più di tre quarti (76%) degli attacchi ransomware. Di fatto, i livelli di cifratura non autorizzata hanno ora raggiunto il picco più alto degli ultimi quattro anni. Molto probabilmente, queste statistiche riflettono le sempre maggiori capacità tecniche degli antagonisti informatici, che continuano a introdurre innovazioni e ad affinare i propri approcci.

Durante l'attacco ransomware, i cybercriminali sono riusciti a cifrare i dati della tua organizzazione?



No, non sono stati cifrati dati ma abbiamo ricevuto una richiesta di riscatto (estorsione)

No, l'attacco è stato bloccato prima che fossero cifrati dei dati

Sì, sono stati cifrati dei dati

Cifratura Non Autorizzata Dei Dati In Base Al Settore

Quasi tutti i settori fanno fatica a bloccare gli attacchi prima che vengano cifrati i dati: in ogni settore (tranne uno), più di due terzi degli attacchi hanno portato alla cifratura non autorizzata dei dati. Il tasso più alto di cifratura non autorizzata (92%) è stato registrato dai servizi commerciali e professionali.

IT, tecnologie e telecomunicazioni è il settore in controtendenza, con meno di metà degli attacchi (47%) che includevano la cifratura non autorizzata delle informazioni. Questo dimostra ulteriormente l'efficacia del livello delle difese informatiche, nonché l'ottimo grado di preparazione ad avviare una risposta tempestiva in questo settore.

Per maggiori informazioni, vedi il paragrafo Cifratura Non Autorizzata Dei Dati In Base Al Settore, a pagina 23.

Furto Di Dati

Il 30% degli attacchi in cui sono state cifrate informazioni è stato caratterizzato anche dal furto di dati. Questo approccio "a doppio impatto" degli antagonisti informatici sta diventando sempre più diffuso, poiché aiuta i malintenzionati a incrementare le loro possibilità di monetizzazione degli attacchi. La minaccia di divulgare pubblicamente i dati rubati può essere sfruttata per estorcere pagamenti alle vittime; inoltre, queste informazioni possono anche essere vendute a terzi. L'elevata frequenza dei casi di furto dei dati rende ancora più fondamentale la necessità di bloccare gli attacchi tempestivamente, prima che possano essere esfiltrate informazioni importanti.

30%

Percentuale di attacchi ransomware in cui sono state cifrate informazioni e in cui c'è anche stato un furto di dati

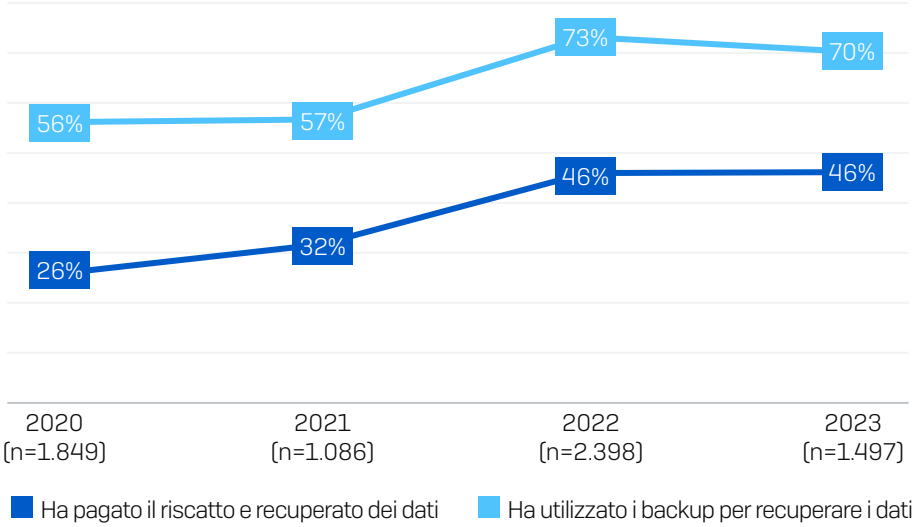
Durante l'attacco ransomware, i cybercriminali sono riusciti a cifrare i dati della tua organizzazione? Sì; Sì, e sono anche stati rubati dati n=1.497

Recupero Dei Dati

Il 97% delle organizzazioni che sono cadute vittima della cifratura non autorizzata dei dati è riuscito a recuperare le informazioni. I backup sono stati l'approccio più comune per il recupero dei dati, in quanto hanno svolto un ruolo essenziale nel 70% degli incidenti. Il 46% delle vittime ha pagato il riscatto e ha recuperato i dati, mentre il 2% ha adottato altri metodi. Complessivamente, una vittima su cinque (21%) ha scelto più di un solo metodo per recuperare i dati. L'1% delle organizzazioni che avevano subito la cifratura dei dati ha pagato il riscatto ma i dati sottratti non sono stati restituiti.

Ha utilizzato i backup per recuperare i dati	Ha pagato il riscatto e recuperato dei dati	Ha utilizzato altri metodi per recuperare i dati
70%	46%	2%

Preoccupa molto il fatto che l'utilizzo dei backup per recuperare i dati sia in calo rispetto all'anno scorso, quando era stato impiegato come metodo di recupero nel 73% dei casi. Il tasso di pagamento del riscatto non ha subito variazioni rispetto all'anno precedente.



La tua organizzazione è riuscita a recuperare almeno parte dei dati? Sì, abbiamo pagato il riscatto e recuperato dei dati; Sì, abbiamo utilizzato i backup per recuperare i dati. Base di partecipanti indicata nel grafico

Recupero Dei Dati In Base Al Paese

Complessivamente, gli intervistati nell'area EMEA hanno registrato livelli aggregati più alti di utilizzo di backup (75%) e livelli aggregati più bassi di pagamento del riscatto (40%), rispetto ai partecipanti al sondaggio con sede in Nord e Sud America (65%/55%) e Asia-Pacifico (67%/49%). A livello dei singoli paesi, la Francia presenta il tasso più alto di utilizzo di backup (87%), seguita a distanza ravvicinata dalla Svizzera (84%).

L'importanza dei backup è ancora più evidente se consideriamo che i due paesi con la percentuale più bassa di utilizzo dei backup per il ripristino dei dati, Italia (55%) e Singapore (57%), sono anche quelli caratterizzati dai minori tassi complessivi di recupero dei dati (rispettivamente 93% e 90%). L'Italia è anche il paese con la maggiore propensione a pagare il riscatto (56%), seguita a ruota da U.S.A. e Brasile (entrambi al 55%).

Nella maggior parte dei casi, le organizzazioni che hanno pagato il riscatto sono riuscite a recuperare dei dati. Tuttavia, in Francia e nel Regno Unito, circa un'organizzazione su dieci tra quelle che hanno pagato il riscatto non ha riavuto neppure parte dei dati.

Per maggiori informazioni, vedi il paragrafo Recupero Dei Dati In Base Al Paese, a pagina 24.

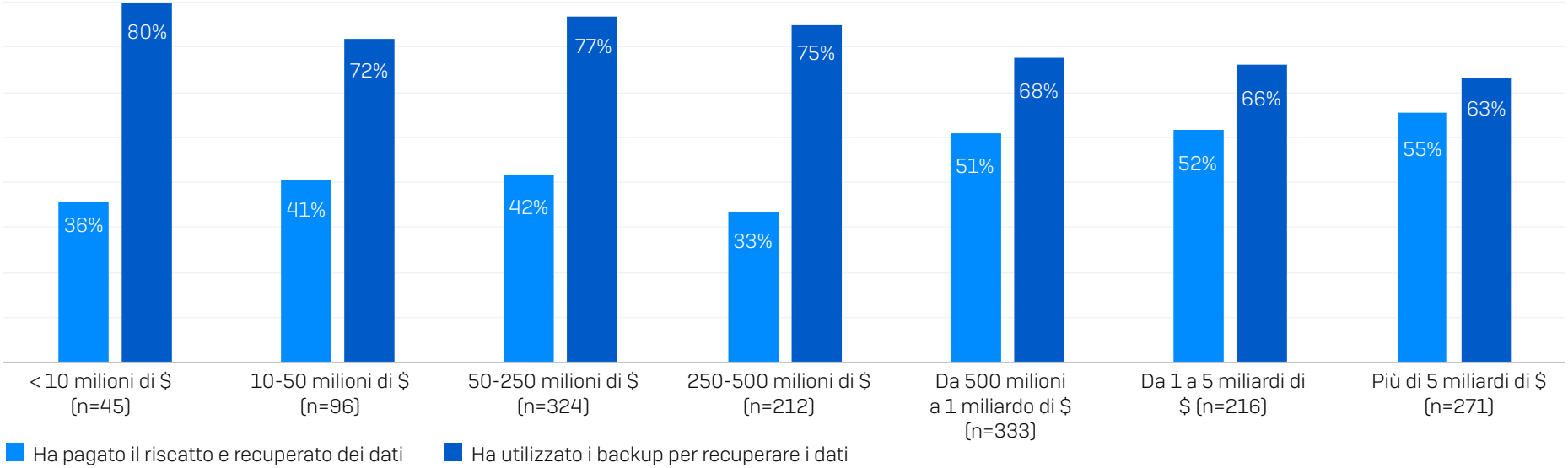
Pagamento Del Riscatto E Utilizzo Dei Backup In Base Al Fatturato

Generalmente, a un aumento del fatturato annuo corrisponde una maggiore propensione delle organizzazioni a recuperare i dati pagando il riscatto. Contemporaneamente, il tasso di utilizzo dei backup invece scende.

Tra le organizzazioni con un fatturato superiore ai 5 miliardi di $, il 55% sostiene di avere recuperato i dati pagando il riscatto, mentre il 63% ha utilizzato i backup. Parallelamente, il 36% delle organizzazioni con un fatturato inferiore ai 10 milioni di $ ha recuperato i dati pagando il riscatto, mentre l'80% ha utilizzato i backup: il tasso di uso dei backup più alto tra tutte le coorti (in base al fatturato).

Le organizzazioni con fatturato annuo più basso hanno a disposizione meno fondi da dedicare ai pagamenti del riscatto e questo le costringe ad affidarsi principalmente ai backup per recuperare i dati. Allo stesso tempo, le organizzazioni con fatturati più elevati di solito sono caratterizzate da infrastrutture informatiche complesse, il che complica l'utilizzo dei backup per poter recuperare i dati in maniera tempestiva. Sono anche aziende dotate di risorse economiche adeguate per risolvere questi tipi di situazioni con un pagamento.

Pagamento Del Riscatto E Utilizzo Dei Backup In Base Al Fatturato



La tua organizzazione è riuscita a recuperare almeno parte dei dati? Sì, abbiamo pagato il riscatto e recuperato dei dati; Sì, abbiamo utilizzato i backup per recuperare i dati. Base di partecipanti indicata nel grafico

L'Impatto Delle Cyberassicurazioni Sul Recupero Dei Dati

Le organizzazioni con una polizza cyberassicurativa presentano una maggiore probabilità di recuperare i dati cifrati, rispetto a quelle che non hanno stipulato alcuna assicurazione. Tuttavia, il tipo di cyberassicurazione non sembra costituire una differenza significativa: a recuperare i dati sono stati il 98% delle organizzazioni con una polizza indipendente e il 97% dei partecipanti al sondaggio con una copertura più completa che include l'ambito informatico. Come termine di confronto, l'84% di tutte le organizzazioni che non avevano stipulato una polizza è riuscito a recuperare i dati cifrati.

Percentuale di vittime del ransomware che sono riuscite a recuperare i dati cifrati

La tua organizzazione è riuscita a recuperare almeno parte dei dati? n=1.497 organizzazioni colpite l'anno scorso da un attacco ransomware che ne ha cifrato i dati

Questa differenza è probabilmente dovuta a diversi fattori. Prima di tutto, uno dei requisiti obbligatori per stipulare una cyberassicurazione è la presenza di piani di backup e di recupero dei dati. Le cyberassicurazioni sono anche in grado di fornire alle vittime del ransomware consulenza pratica durante il processo di recupero, per ottimizzare i risultati. Inoltre, rispetto alle organizzazioni senza assicurazione, gli intervistati con una polizza cyberassicurativa sono caratterizzati da una maggiore probabilità di pagare il riscatto per recuperare i dati.

L'impatto delle cyberassicurazioni sulla propensione a pagare il riscatto

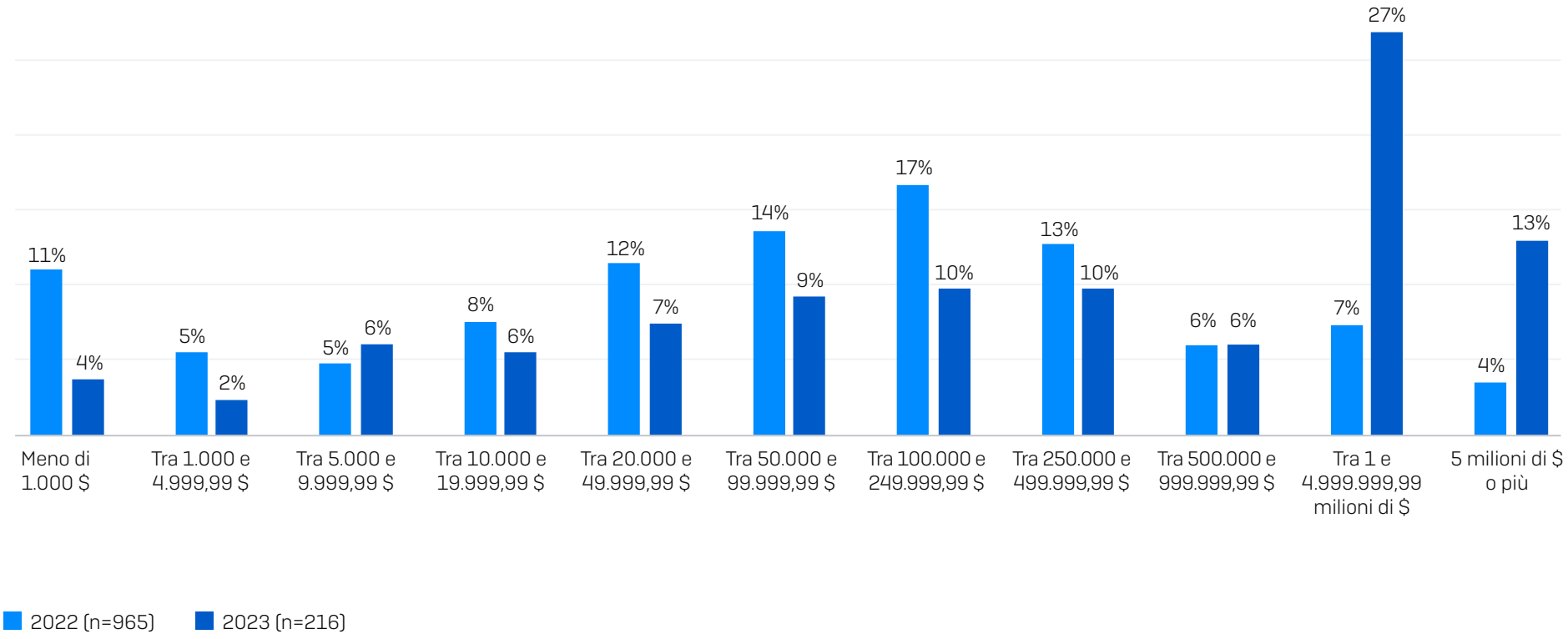
La tua organizzazione è riuscita a recuperare almeno parte dei dati? Sì, abbiamo pagato il riscatto e recuperato dei dati. n=1.497 organizzazioni colpite l'anno scorso da un attacco ransomware che ne ha cifrato i dati (771 con polizza indipendente, 658 con una copertura più completa che include l'ambito informatico, 67 senza cyberassicurazione)

Pagamenti del riscatto

Sebbene generalmente la propensione a pagare il riscatto sia rimasta invariata rispetto al sondaggio dell'anno scorso, i pagamenti hanno subito un'impennata, con pagamenti medi per il riscatto che sono quasi raddoppiati, passando da 812.380 $ nel 2022 a 1.542.333 $ nel 2023. Il pagamento mediano registrato quest'anno ha raggiunto i 400.000 $.

Dallo studio è emersa una distribuzione estesa dei pagamenti; tuttavia, la percentuale di organizzazioni che hanno pagato riscatti più alti è salita rispetto al nostro sondaggio del 2022, con il 40% degli intervistati che confessa di avere effettuato pagamenti pari o superiori a 1 milione di $. L'anno scorso questa percentuale ammontava all'11%. Solo il 34% dei partecipanti dichiara invece di avere pagato meno di 100.000 $, in calo rispetto al 54% dell'anno scorso.

Pagamenti Del Riscatto: Confronto Tra Il 2023 E Il 2022



A quanto ammonta la somma di riscatto pagata ai cybercriminali? Le risposte "Non lo so" sono state omesse.

Pagamenti Del Riscatto In Base Al Fatturato

Probabilmente non sorprende che le organizzazioni con il fatturato più alto siano quelle più propense a pagare le somme di riscatto più elevate. Questa statistica dimostra che i cybercriminali modificano la somma che sono disposti ad accettare, in base al potenziale di pagamento della vittima. Nello studio non è stata fatta distinzione tra i pagamenti effettuati con fondi interni e quelli a carico delle cyberassicurazioni.

È interessante osservare che sembra esserci poca differenza tra i pagamenti del riscatto medi e mediani per le organizzazioni con un fatturato di 250-500 milioni di $ e per le organizzazioni con un fatturato che ammonta a 500 milioni-1 miliardo di $.

	50-250 MILIONI DI $ (N=37)	250-500 MILIONI DI $ (N=33)	DA 500 MILIONI A 1 MILIARDO DI $ (N=72)	1-5 MILIARDI DI $ (N=45)	PIÙ DI 5 MILIARDI DI $ (N=21)
Pagamento del riscatto medio	690.996 $	1.523.652 $	1.466.240 $	2.049.817 $	2.464.339 $
Pagamento del riscatto mediano	145.000 $	428.000 $	425.000 $	1.000.000 $	3.000.000 $

A quanto ammonta la somma di riscatto pagata ai cybercriminali? Le risposte "Non lo so" sono state omesse. Le organizzazioni con fatturato annuo inferiore ai 50 milioni di $ sono state escluse, per via della limitata base di partecipanti. Base di partecipanti indicata nel grafico. I dati per i segmenti con meno di 30 risposte sono da considerarsi puramente indicativi.

Costi Di Riparazione Dei Danni

I pagamenti del riscatto sono solo uno dei vari tipi di costi di riparazione dei danni da sostenere quando si viene colpiti dal ransomware. Escludendo le somme di riscatto versate, le organizzazioni hanno dovuto affrontare un costo medio di riparazione dei danni causati dal ransomware pari a 1,82 milioni di $: un aumento rispetto agli 1,4 milioni di $ del 2022 e agli 1,85 milioni di $ del 2021.

Nota: la domanda del sondaggio nel 2021 e nel 2022 includeva nei costi stimati anche le somme di riscatto pagate, che sono state tuttavia escluse dalla formulazione della domanda nel 2023. Di conseguenza, il confronto annuale è da considerarsi puramente indicativo.

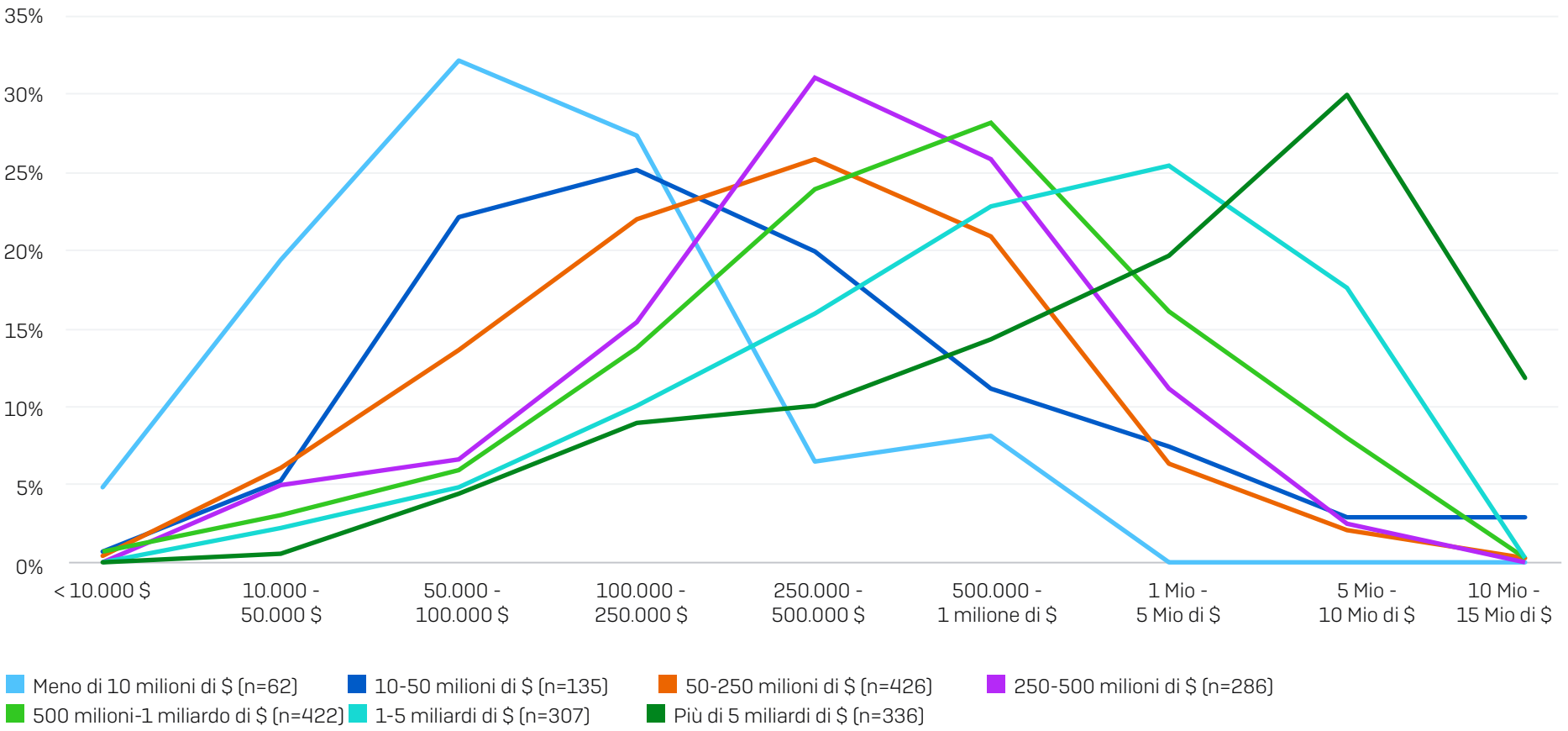
Costo Medio Di Riparazione Dei Danni

2021	2022	2023
1,85 Mio di $	1,4 Mio di $	1,82 Mio di $

Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.)? n=1.974 (2023)/3.702 (2022)/2.006 (2021). Nota: la domanda formulata per il sondaggio del 2022 e del 2021 includeva anche "pagamento del riscatto".

I costi medi di riparazione dei danni partono da 165.520 $ per le organizzazioni con fatturato annuo inferiore ai 10 milioni di $ e raggiungono i 4.496.086 $ nella coorte con fatturato superiore ai 5 miliardi di $. Sebbene queste cifre includano un'ampia selezione di tipi di costi di riparazione diversi, si nota una tendenza ricorrente ben definita che associa l'aumento dei costi di riparazione a un maggiore fatturato annuo, come dimostra il diagramma nella pagina seguente.

Costi Di Riparazione Dei Danni In Base Al Fatturato



Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.)? Base di partecipanti indicata nel grafico

Costi Di Riparazione Dei Danni In Base Al Metodo Di Recupero Dei Dati

Comunque si scelga di analizzare i dati, l'utilizzo dei backup per rimediare ai danni provocati da un attacco ransomware implica costi molto minori rispetto al pagamento del riscatto. Il costo di riparazione mediano per le organizzazioni che hanno utilizzato i backup (375.000 $) è pari alla metà della cifra mediana versata dalle organizzazioni che hanno pagato il riscatto (750.000 $). Analogamente, il costo medio è quasi 1 milione di $ più basso per i partecipanti che hanno usato i backup. Se ci dovesse essere bisogno di ulteriore prova a dimostrazione dei vantaggi finanziari derivati dall'investimento in una strategia di backup efficace, le statistiche parlano chiaro.

Ha pagato il riscatto e recuperato dei dati	Ha utilizzato i backup per recuperare i dati
750.000 $	**375.000 $**
Cifra mediana	Cifra mediana
2,6 Mio di $	**1,62 Mio di $**
Cifra media	Cifra media

Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.)? n=694 organizzazioni che hanno pagato il riscatto e recuperato dei dati e 1.053 organizzazioni che hanno utilizzato i backup per recuperare i dati.

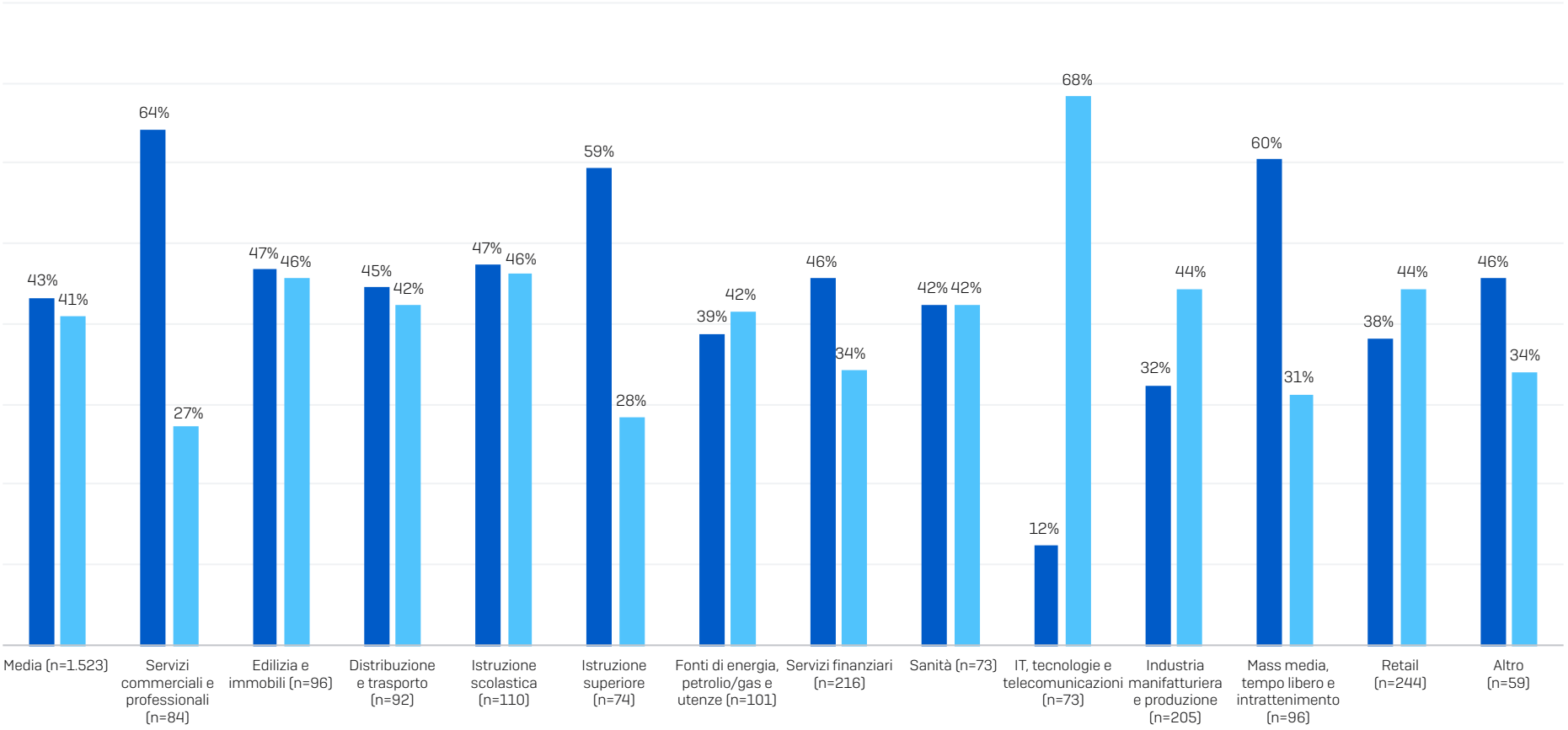
Impatto Commerciale

L'84% delle organizzazioni del settore privato che sono state colpite dal ransomware dichiara che l'attacco ha provocato perdite commerciali/di fatturato. Il fatturato annuo influisce solo in minima parte sulle perdite commerciali, con la percentuale più bassa (79%) riscontrata nella coorte con fatturato pari a 250-500 milioni di $; il tasso più elevato (88%) è stato invece osservato nelle organizzazioni con fatturato inferiore ai 10 milioni di $ e in quelle con fatturato superiore ai 5 miliardi di $.

Il tipo di settore svolge un ruolo molto più significativo nella propensione a subire perdite commerciali/di fatturato. Complessivamente, i settori dell'istruzione scolastica (94%) e dell'edilizia e immobili (93%) sono stati quelli con la più alta probabilità di subire una perdita commerciale/di fatturato in seguito a un attacco, mentre il settore dell'industria manifatturiera e della produzione è stato quello con la probabilità minore (77%).

Approfondendo ulteriormente, si osserva una variazione significativa nei settori che dichiarano di avere perso "molto" in termini commerciali/di fatturato: nel settore dei servizi commerciali e professionali (64%) è stata riscontrata una probabilità più di cinque volte superiore di subire questo livello di impatto, rispetto alle organizzazioni che operano nell'ambito di IT, tecnologie e telecomunicazioni (12%).

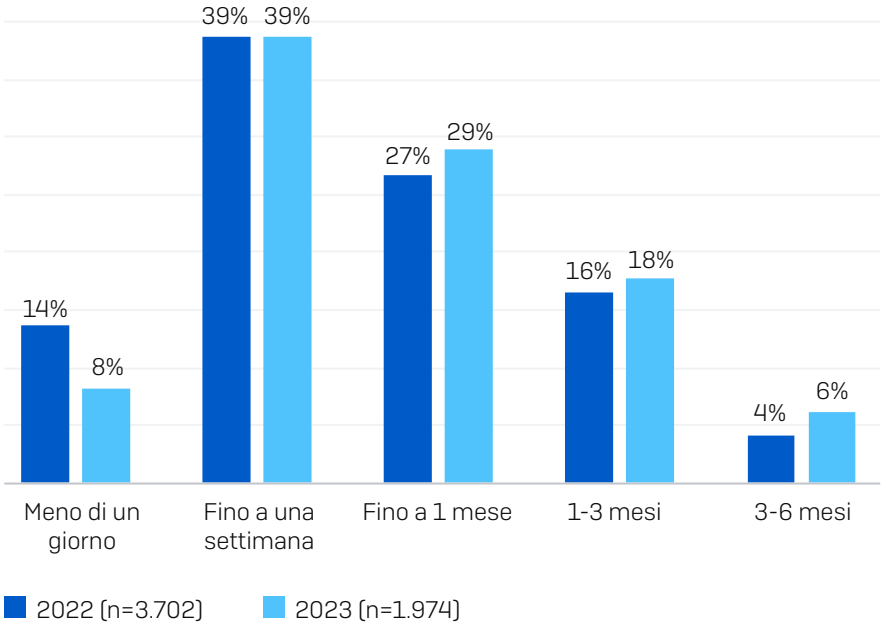
Perdite Commerciali/Di Fatturato In Base Al Settore



L'attacco ransomware è risultato in perdite commerciali/di fatturato per la tua organizzazione? Sì, abbiamo perso molto in termini commerciali/di fatturato;
Sì, abbiamo subito perdite parziali in termini commerciali/di fatturato. Organizzazioni del settore privato che sono state colpite dal ransomware, base di partecipanti indicata nel grafico

Tempo Necessario Per Riprendere Le Normali Attività

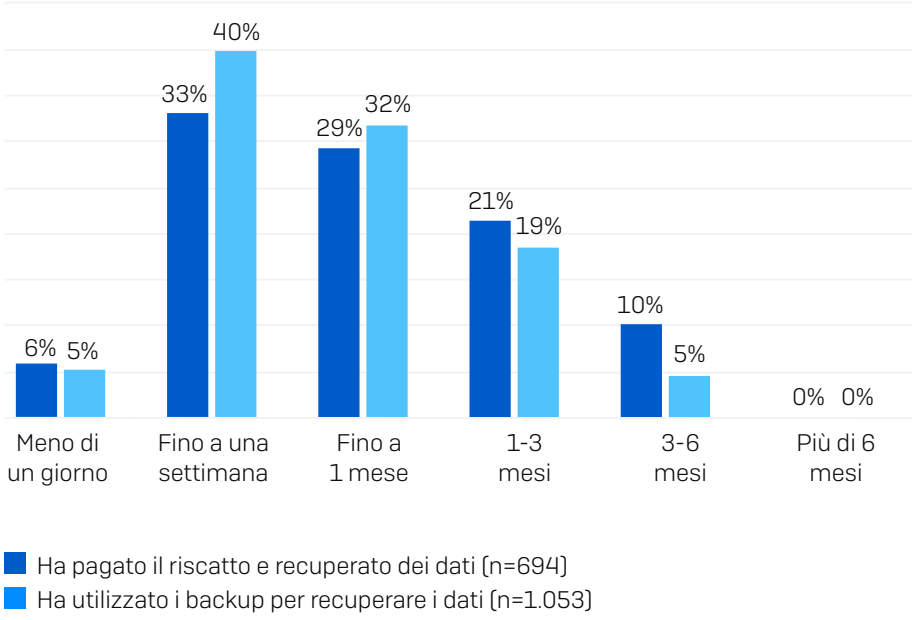
Sebbene il tempo necessario per riprendersi da un attacco ransomware rimanga generalmente in linea con il report del 2022, la percentuale delle organizzazioni che sono state in grado di riprendere le normali attività in meno di un giorno è scesa dal 14% all'8%.



Di quanto tempo ha avuto bisogno la tua organizzazione per riprendere completamente le normali attività operative dopo l'attacco ransomware? Base di partecipanti indicata nel grafico

Tempo Necessario Per Riprendere Le Normali Attività In Base Al Metodo Di Recupero Dei Dati

Dal sondaggio è emerso che le organizzazioni che utilizzano i backup per recuperare i dati sono in grado di riprendersi dalle conseguenze dell'attacco più rapidamente, rispetto alle organizzazioni che pagano il riscatto. Il 45% degli intervistati che sostengono di avere utilizzato i backup è riuscito a riprendersi entro una settimana, a differenza del 39% dei partecipanti che dichiarano di avere pagato il riscatto. Quasi un terzo (32%) delle organizzazioni che hanno pagato il riscatto ha avuto bisogno di più di un mese per riprendere le normali attività, mentre per chi ha utilizzato il backup questa statistica scende al 23% (cifra arrotondata). Anche se queste due opzioni di risposta non si escludono reciprocamente (alcuni intervistati hanno sia pagato il riscatto, sia utilizzato i backup), i vantaggi dei backup in termini di tempi di ripresa delle attività sono evidenti.



Di quanto tempo ha avuto bisogno la tua organizzazione per riprendere completamente le normali attività operative dopo l'attacco ransomware?
Organizzazioni che hanno pagato il riscatto e/o utilizzato backup per recuperare i dati. Base di partecipanti indicata nel grafico

Conclusione

Indipendentemente dal fatturato che generano, dall'area geografica in cui sono situate o dal settore in cui operano, le organizzazioni si trovano continuamente ad affrontare il problema del ransomware: una minaccia che diventa ogni giorno sempre più devastante. Man mano che i cybercriminali affinano progressivamente le loro tattiche, tecniche e procedure (TTP), i team di sicurezza fanno fatica a tenere testa ad attacchi sempre più evoluti. Di conseguenza, i tassi di cifratura non autorizzata sono in aumento.

La diminuzione dell'uso dei backup per il recupero dei dati cifrati è abbastanza preoccupante. Se ci dovesse essere bisogno di ulteriore prova a dimostrazione dei vantaggi finanziari e operativi derivati dall'investimento in una strategia di backup efficace, i risultati di questo report parlano chiaro.

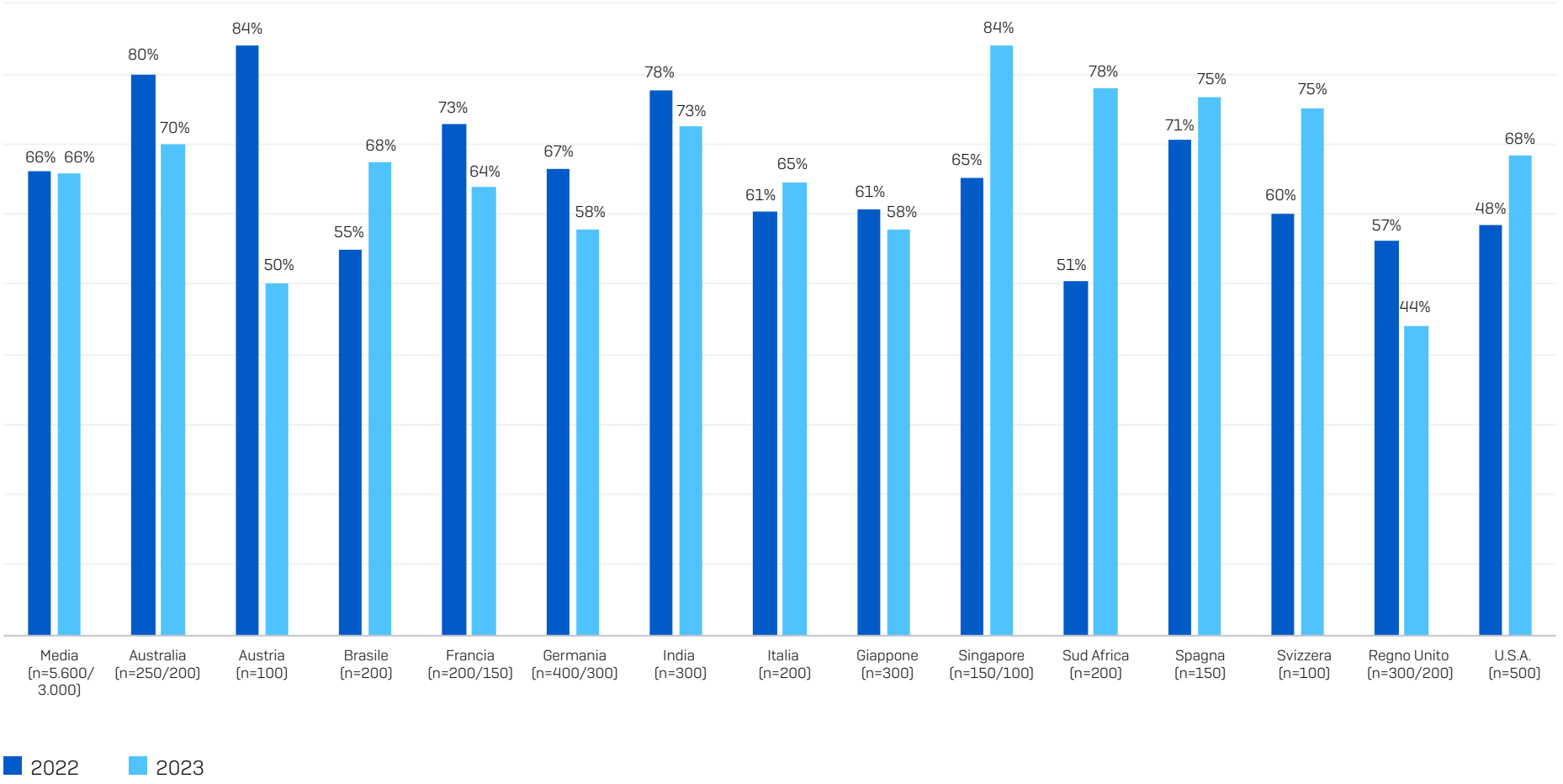
Con la crescita del business model del ransomware as-a-Service, prevediamo che quest'anno gli attacchi saranno tutt'altro che in calo. Il nostro consiglio per le organizzazioni è di concentrarsi su quanto segue:

- Potenziamento delle difese, con l'uso di:
  - Strumenti di sicurezza che proteggono i sistemi dai più comuni vettori di attacco (inclusa una protezione endpoint con potenti funzionalità antiexploit per prevenire gli exploit delle vulnerabilità), più Zero Trust Network Access (ZTNA) per sventare i tentativi di utilizzo improprio di credenziali compromesse
  - Tecnologie adattive che rispondono automaticamente agli attacchi, bloccando così gli hacker e regalando ai team di sicurezza tempo prezioso per avviare una risposta adeguata
  - Rilevamento, indagine e risposta alle minacce 24/7, da svolgere internamente oppure in collaborazione con un fornitore di servizi specializzato in Managed Detection and Response (MDR).
- Ottimizzazione della strategia di preparazione per gli attacchi, inclusi backup svolti a intervalli regolari, esercitazioni che prevedono il recupero dei dati dai backup, e compilazione e continuo aggiornamento di un piano di incident response
- Implementazione di una strategia efficace per garantire l'integrità della sicurezza, che deve includere l'applicazione tempestiva delle patch e la revisione a intervalli regolari delle configurazioni degli strumenti di sicurezza

Ulteriori Grafici

Tasso Di Attacchi Ransomware In Base Al Paese: Confronto Tra Il 2023 E Il 2022

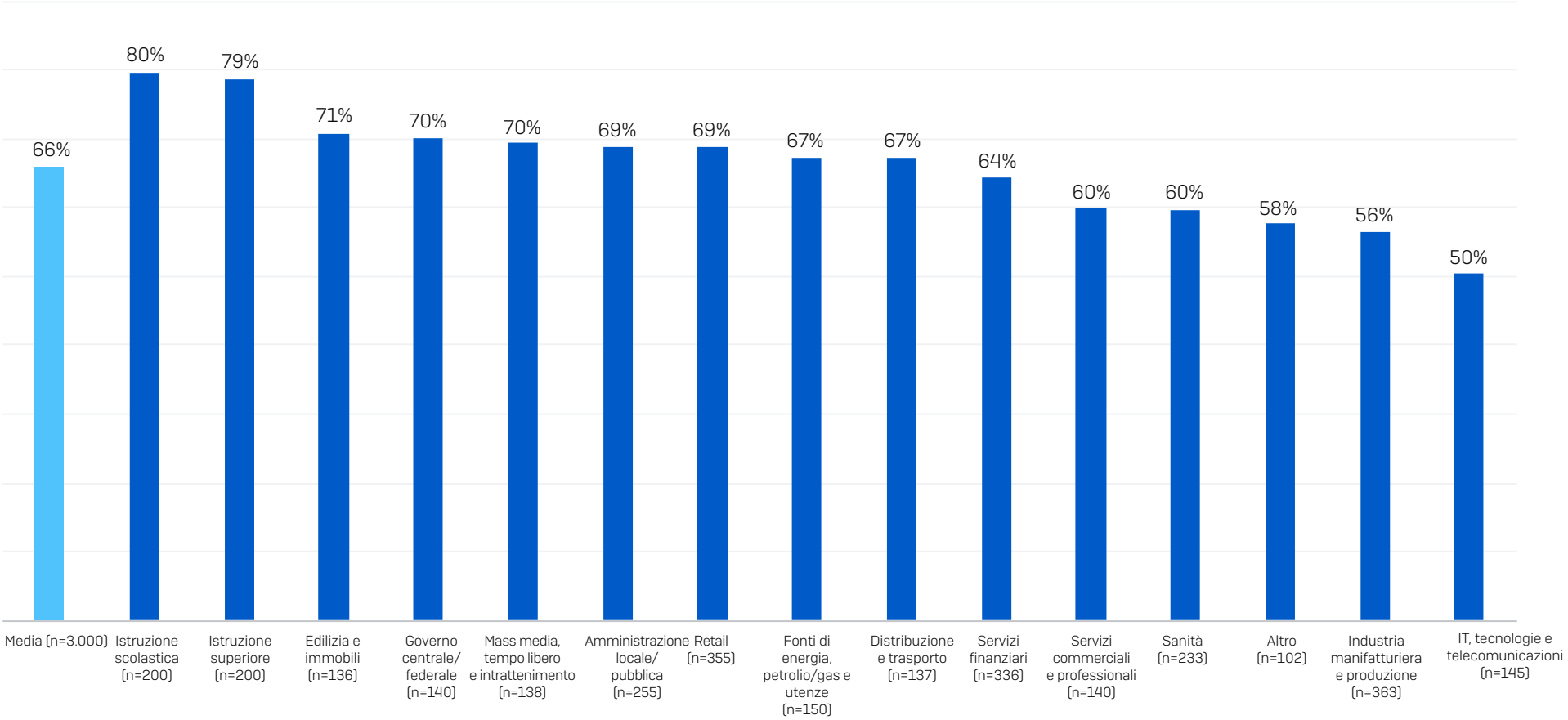
Percentuale Di Organizzazioni Colpite Dal Ransomware



La tua organizzazione è stata colpita dal ransomware l'anno scorso? Base di partecipanti indicata nel grafico

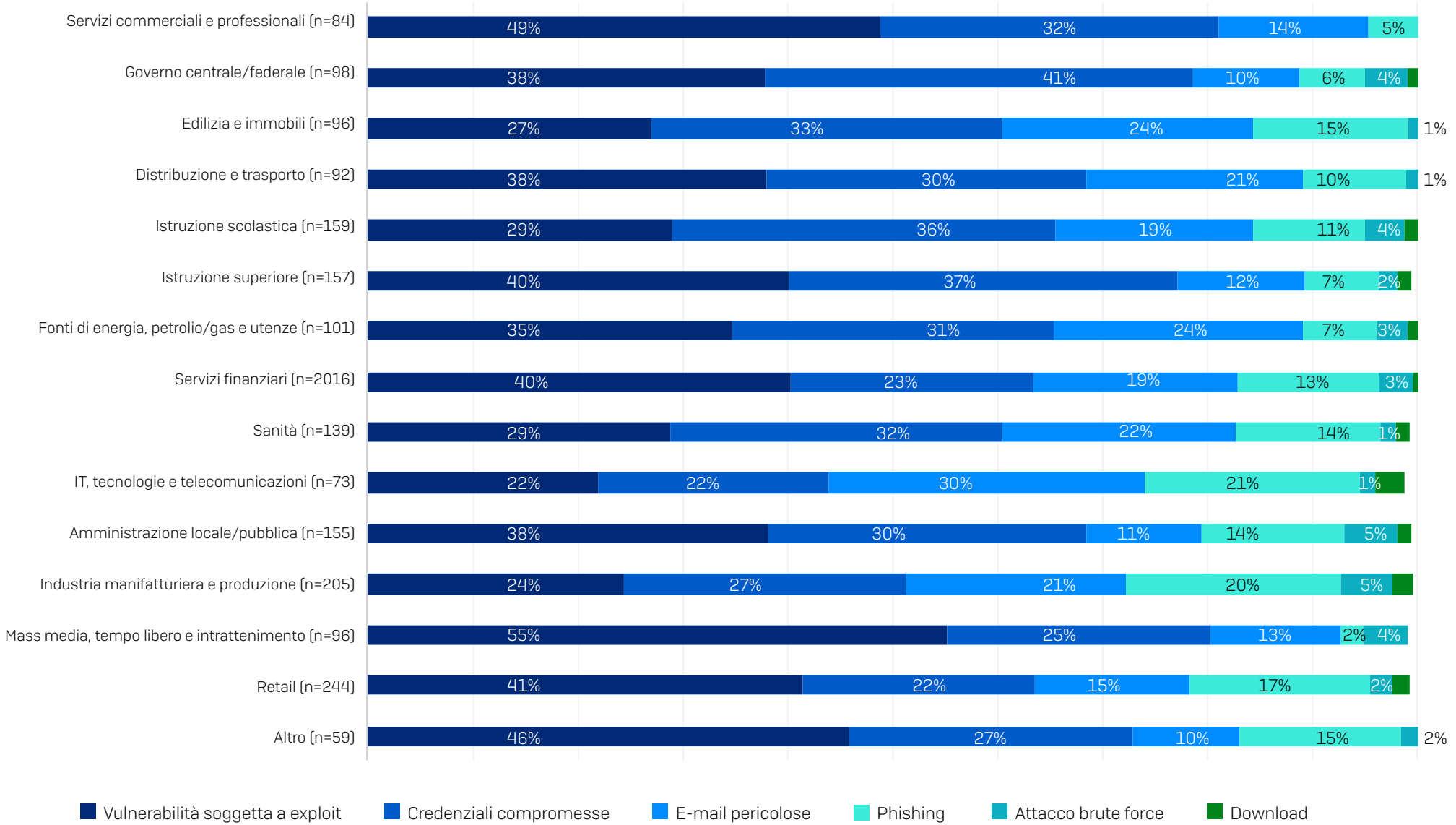
Tasso Di Attacchi Ransomware In Base Al Settore

Percentuale Di Organizzazioni Colpite Dal Ransomware



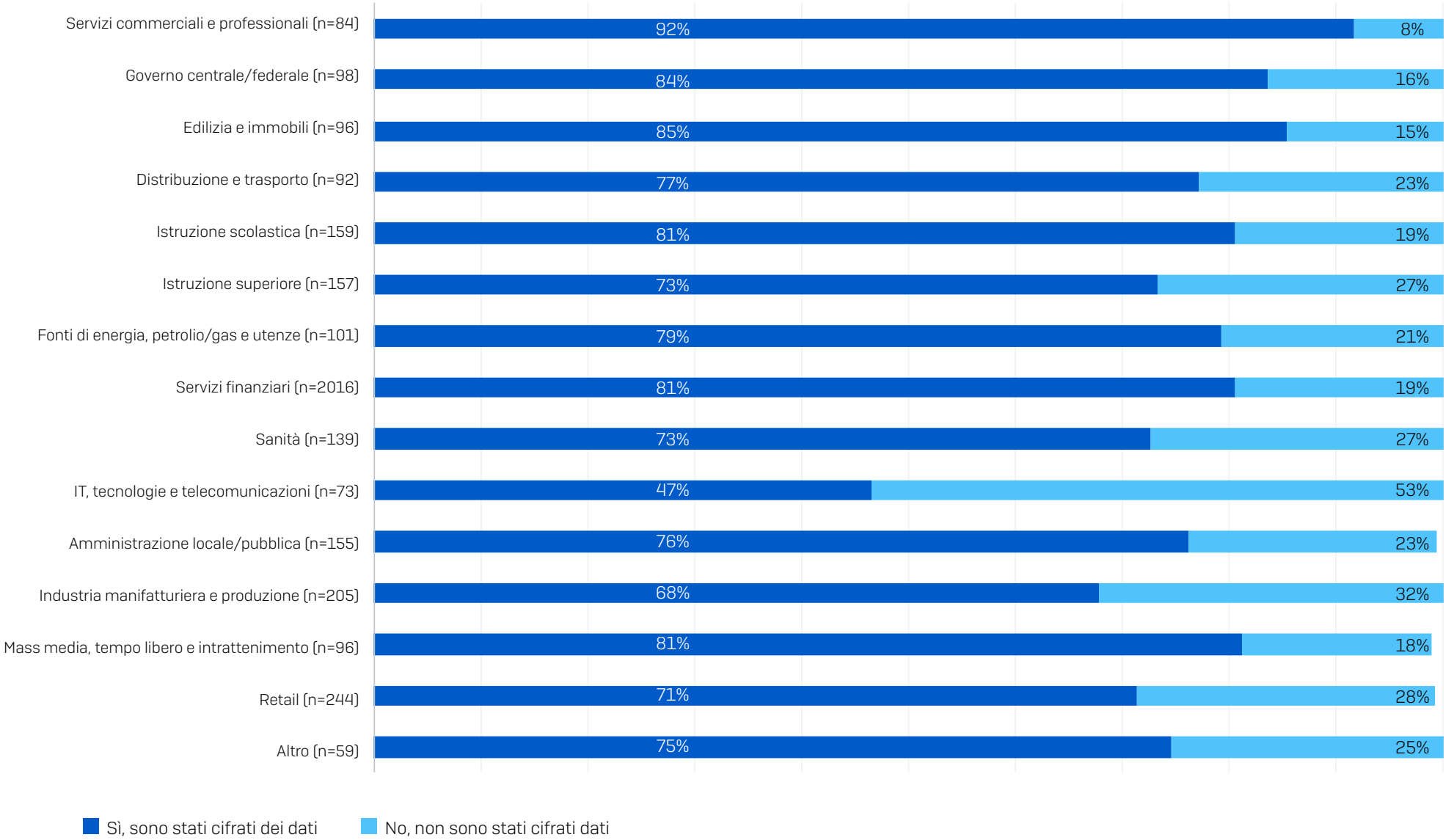
La tua organizzazione è stata colpita dal ransomware l'anno scorso? Base di partecipanti indicata nel grafico

Cause All'Origine Degli Attacchi In Base Al Settore



Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? Selezione delle opzioni di risposta. Base di partecipanti indicata nel grafico

Cifratura Non Autorizzata Dei Dati In Base Al Settore



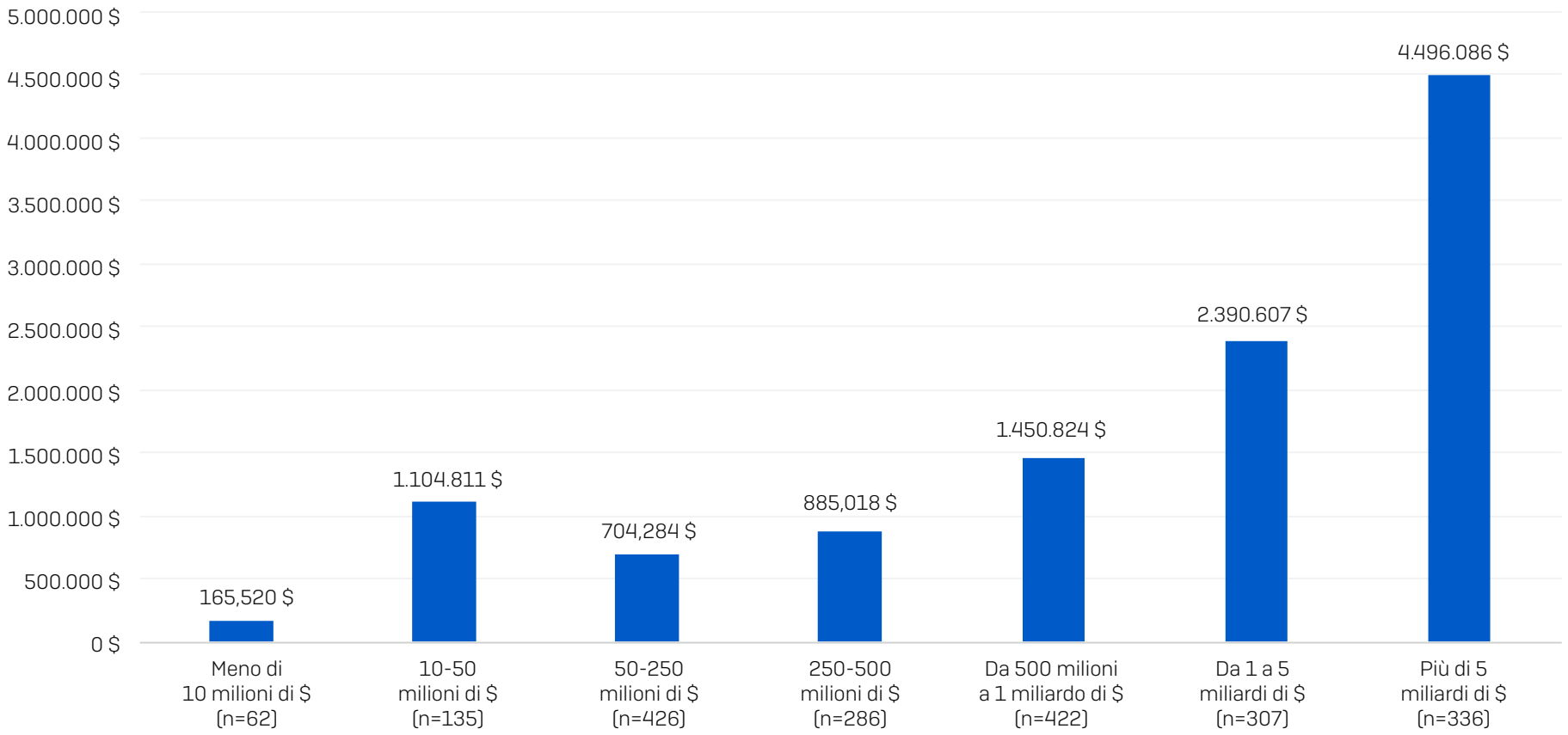
Durante l'attacco ransomware, i cybercriminali sono riusciti a cifrare i dati della tua organizzazione? Alcune opzioni di risposta sono state accorpate. Base di partecipanti indicata nel grafico

Recupero Dei Dati In Base Al Paese

La tua organizzazione è riuscita a recuperare almeno parte dei dati?

	USA (N=274)	BRASILE (N=98)	GERMANIA (N=122)	AUSTRIA (N=48)	SVIZ-ZERA (N=68)	REGNO UNITO (N=66)	ITALIA (N=82)	SPAGNA (N=93)	FRANCIA (N=68)	SUD AFRICA (N=139)	INDIA (N=167)	AUSTRALIA (N=96)	GIAPPONE (N=125)	SINGA-PORE (N=51)
Sì, abbiamo pagato il riscatto e recuperato dei dati	54%	55%	44%	42%	38%	44%	54%	29%	22%	45%	43%	53%	52%	53%
Sì, abbiamo utilizzato i backup per recuperare i dati	66%	61%	78%	73%	84%	68%	55%	81%	87%	76%	73%	73%	60%	57%
Sì, abbiamo utilizzato altri metodi per recuperare i dati	1%	4%	1%	0%	3%	0%	0%	0%	3%	3%	3%	3%	6%	0%
No, anche se abbiamo pagato il riscatto	1%	0%	0%	0%	0%	5%	2%	0%	3%	0%	1%	0%	0%	0%
No, non abbiamo pagato il riscatto	0%	1%	2%	2%	1%	2%	5%	2%	0%	0%	1%	1%	5%	10%
Non lo so	0%	0%	2%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Abbiamo recuperato i dati con un altro metodo	99%	99%	95%	98%	99%	94%	93%	98%	97%	100%	98%	99%	95%	90%
Abbiamo utilizzato più di un metodo per recuperare i dati	22%	21%	27%	17%	26%	18%	16%	12%	12%	24%	20%	29%	22%	20%
Ha pagato il riscatto	55%	55%	44%	42%	38%	48%	56%	29%	25%	45%	44%	53%	52%	53%
Percentuale di organizzazioni che hanno pagato il riscatto ma non non hanno recuperato i dati	1%	0%	0%	0%	0%	9%	4%	0%	12%	0%	3%	0%	0%	0%

Costo Medio Di Riparazione Dei Danni In Base Al Fatturato



Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.)? Base di partecipanti indicata nel grafico.

Metodologia Di Ricerca

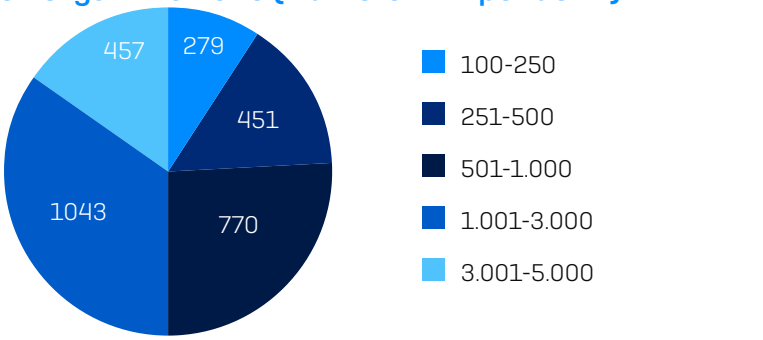
Sophos ha affidato a un'azienda esterna l'incarico di condurre un sondaggio agnostico rispetto ai vendor, coinvolgendo 3.000 Cybersecurity/IT Manager nei mesi di gennaio-marzo 2023. Le persone che hanno partecipato al sondaggio si trovavano in 14 paesi nelle aree geografiche di Nord e Sud America, EMEA (Europa, Medio Oriente e Africa) e Asia-Pacifico.

Tutti gli intervistati lavoravano in organizzazioni con un numero di dipendenti compreso tra 100 e 5.000 (50% in organizzazioni con 100-1.000 dipendenti, 50% in organizzazioni con 1.001-5.000 dipendenti). Nella coorte di ricerca, il fatturato annuo varia da meno di 10 milioni di $ a oltre 5 miliardi di $.

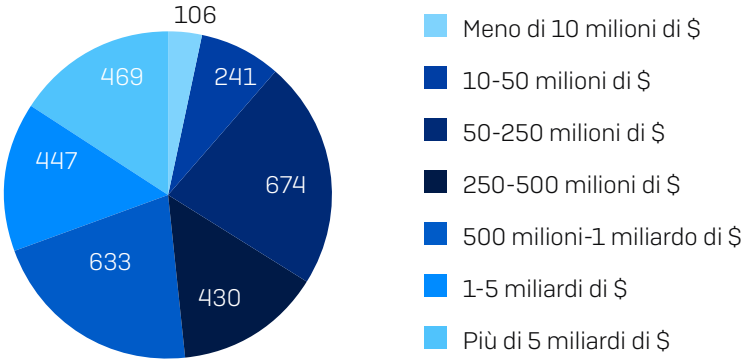
Partecipanti per paese

PAESE	NUMERO DI PARTECIPANTI	PAESE	NUMERO DI PARTECIPANTI
Stati Uniti	500	Regno Unito	200
Germania	300	Sud Africa	200
India	300	Francia	150
Giappone	300	Spagna	150
Australia	200	Austria	100
Brasile	200	Singapore	100
Italia	200	Svizzera	100

Numero Di Intervistati In Base Alle Dimensioni Dell'Organizzazione (Numero Di Dipendenti)



Numero Di Intervistati In Base Alle Dimensioni Dell'Organizzazione (Fatturato Annuo)



Sophos offre soluzioni di cybersecurity leader di settore, ideali per le aziende di tutte le dimensioni; inoltre, protegge i sistemi in tempo reale contro minacce avanzate quali malware, ransomware e phishing. Grazie alle funzionalità Next-Gen dall'efficacia comprovata, garantisce una protezione efficace per i dati aziendali, con prodotti basati su tecnologie di Intelligenza Artificiale e Machine Learning.

2023-05-05 (WP-DD)

SOPHOS