SOPHOS

La Vera Storia Del Ransomware 2024

I risultati di uno studio indipendente a cui hanno partecipato 5.000 IT/ Cybersecurity Manager in 14 paesi del mondo, condotto nei mesi di gennaio e febbraio 2024.

Introduzione

Per il quinto anno consecutivo, Sophos ha svolto una ricerca che valuta le esperienze di vita reale delle organizzazioni in tutto il mondo. I risultati esplorano la storia completa delle vittime, dalla causa all'origine dell'attacco alla gravità degli incidenti, e dall'impatto finanziario ai tempi necessari per riprendere le normali attività operative. Queste nuove intuizioni e i concetti emersi dai nostri studi precedenti rivelano le realtà che le aziende si trovano ad affrontare al giorno d'oggi, mettendo in luce l'evoluzione dell'impatto del ransomware negli ultimi cinque anni.

Il report di quest'anno include anche nuovi ambiti di ricerca, incluso un confronto tra le richieste di riscatto e i pagamenti del riscatto, nonché una maggiore focalizzazione su quanto influisce il fatturato di un'organizzazione sull'esito di un attacco ransomware. Inoltre, per la prima volta, offre una prospettiva più nitida del ruolo delle forze dell'ordine nelle attività di riparazione dei danni causati dal ransomware.

Una nota sul periodo di riferimento del report

Per facilitare il confronto delle statistiche dei nostri sondaggi annuali, i nostri report vengono nominati in base all'anno in cui viene condotto il sondaggio, in questo caso il 2024. Siamo consci del fatto che i partecipanti condividono le loro esperienze nel corso dell'anno precedente, per cui molti degli attacchi menzionati si sono verificati nel 2023.

Informazioni sul sondaggio

Il report si basa sui risultati di un sondaggio indipendente e agnostico rispetto ai vendor, svolto per conto di Sophos intervistando 5.000 IT/Cybersecurity Manager in 14 paesi nelle aree geografiche di Nord e Sud America, EMEA (Europa, Medio Oriente e Africa) e Asia-Pacifico. Tutti i partecipanti rappresentano organizzazioni con un numero di dipendenti compreso tra 100 e 5.000. Il sondaggio è stato svolto da Vanson Bourne, un'azienda specializzata nell'ambito della ricerca, nei mesi di gennaio e febbraio 2024 e agli intervistati 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).

Tasso Di Attacchi Ransomware

L'anno scorso il 59% delle organizzazioni è stato colpito dal ransomware, una diminuzione minima, ma pur sempre ben accetta, rispetto al 66% registrato in entrambi i report dei due anni precedenti. Sebbene sia incoraggiante osservare un calo, il fatto che più della metà delle organizzazioni abbia subito un attacco ci fa capire che non è sicuramente il momento di abbassare la guardia.

2020	2021	2022	2023	2024
51%	37%	66%	66%	59%

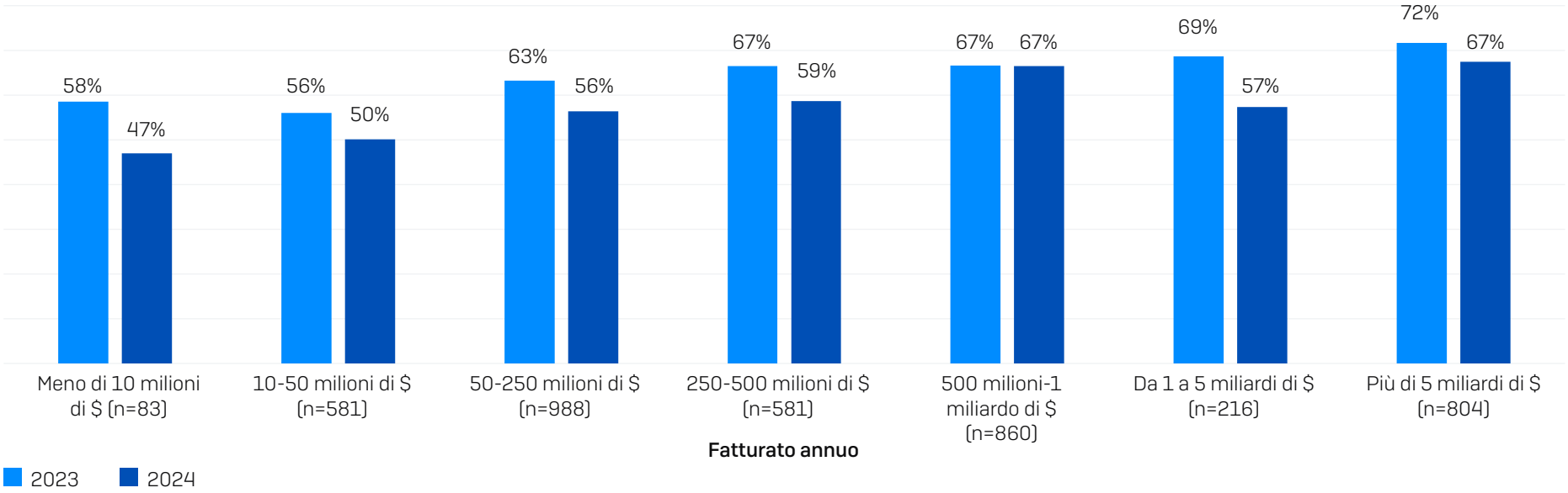
La tua organizzazione è stata colpita dal ransomware l'anno scorso?
Sì. n=5.000 (2024), 3.000 (2023), 5.600 (2022), 5.400 (2021), 5.000 (2020).

Attacchi In Base Al Fatturato

Un dato incoraggiante è che l'anno scorso tutte le fasce di fatturato hanno registrato una diminuzione nel tasso di attacchi ransomware (sebbene per la fascia da 500 milioni a 1 miliardo di $ il calo sia stato di meno dell'1%).

Generalmente, la propensione a cadere vittima del ransomware aumenta in maniera direttamente proporzionale al fatturato: le organizzazioni con oltre 5 miliardi di $ di fatturato sono a pari merito una delle due fasce con la percentuale più alta (67%). Tuttavia, anche le organizzazioni più piccole (meno di 10 milioni di $ di fatturato) vengono colpite regolarmente da questi attacchi, con poco meno della metà (47%) degli intervistati che dichiara di avere subito un attacco ransomware l'anno scorso. Anche se molti attacchi ransomware vengono sferrati da gang molto sofisticate e con ampia disponibilità finanziaria, si è riscontrato un aumento dell'utilizzo di ransomware rudimentale a basso costo, da parte di hacker molto meno abili.

Percentuale delle organizzazioni colpite dal ransomware negli ultimi 12 mesi



La tua organizzazione è stata colpita dal ransomware l'anno scorso? Sì. n=5.000 (2024), 3.000 (2023). Base di partecipanti in base alla fascia di fatturato per l'anno 2024 indicata nel grafico.

Attacchi In Base Al Settore

Ad eccezione di alcuni casi, i tassi di attacchi ransomware sono stati generalmente omogenei tra i vari settori, con una percentuale compresa tra il 60% e il 68% di organizzazioni colpite dal ransomware in 11 dei 15 settori analizzati. Nello studio di quest'anno, i settori con i migliori risultati sono stati *amministrazione locale/pubblica* (34%) e *retail* (45%), nei quali meno della metà degli intervistati ha dichiarato di essere caduta vittima del ransomware.

È interessante osservare che i due settori governativi occupano posizioni opposte, in quanto le organizzazioni che operano nell'ambito del *governo centrale/federale* hanno registrato il tasso di attacchi più alto tra tutti i settori (68%), ovvero il doppio di quello segnalato dall'*amministrazione locale/pubblica* (34%). Allo stesso tempo, in linea con la tendenza generale verso un calo della percentuale di attacchi, il tasso del *governo centrale/federale* è più basso, rispetto al 70% registrato nel 2023.

Esistono vari motivi che possono giustificare questa variazione negli enti governativi. In un anno di instabilità diffusa, potrebbe darsi che gli enti nel settore del governo centrale abbiano subito un incremento nel numero di attacchi a sfondo politico. I risultati potrebbero anche riflettere l'impegno delle organizzazioni nell'amministrazione locale/pubblica a migliorare la propria resilienza agli attacchi negli ultimi 12 mesi. In alternativa, potrebbero rappresentare un cambiamento nell'approccio dei cybercriminali, dovuto alla capacità limitata del settore dell'amministrazione locale/pubblica di pagare un riscatto.

Altre novità interessanti osservate nei settori quest'anno includono:

- Un calo della più alta percentuale individuale di attacchi segnalati, che è scesa dall'80% (*istruzione scolastica*) al 69% (*governo centrale/federale*)
- Quest'anno il settore dell'istruzione non ha più registrato i due tassi massimi di attacco, con il 66% per l'*istruzione superiore* e il 63% per l'*istruzione scolastica*, a differenza (rispettivamente) del 79% e dell'80% dell'anno scorso
- Quello della *sanità* è stato uno dei cinque settori che hanno riportato un incremento della percentuale di attacchi nell'ultimo anno, passando dal 60% al 67%
- *IT, telecomunicazioni e tecnologie* non è più il settore che detiene il primato del minore tasso di attacchi, in quanto l'anno scorso è stato colpito il 55% delle organizzazioni che ne fanno parte, una statistica in aumento rispetto al 50% del 2023

Vedi l'appendice per un'analisi dettagliata del tasso di attacchi ransomware in base al settore.

Attacchi In Base Al Paese

La Francia ha registrato la percentuale più alta di attacchi ransomware nel 2024, con il 74% degli intervistati che dichiara di esserne caduta vittima l'anno scorso, seguita da Sud Africa (69%) e Italia (68%). All'estremo opposto, il tasso di attacchi più basso è stato segnalato in Brasile (44%), Giappone (51%) e Australia (54%).

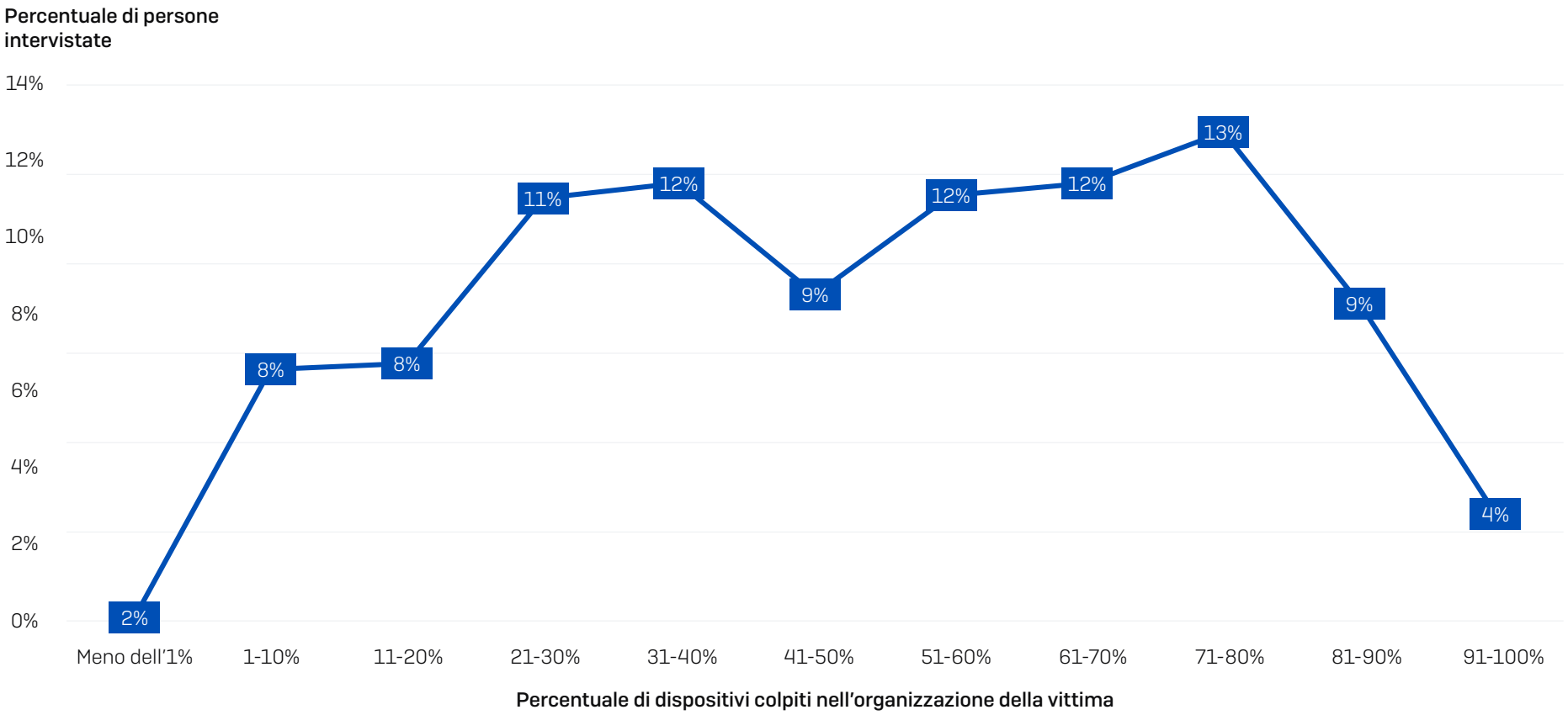
Nel complesso, nove paesi hanno registrato una percentuale di attacchi inferiore rispetto al 2023. I cinque paesi caratterizzati da un aumento della percentuale di attacchi rispetto al 2023 si trovano tutti in Europa: Austria, Francia, Germania, Italia e Regno Unito (l'aumento della Germania è stato di meno dell'1%). Queste statistiche potrebbero riflettere un'intensificazione degli attacchi contro le organizzazioni europee. In alternativa, potrebbero essere dovute al fatto che i sistemi di difesa in Europa non sono stati in grado di tenere il passo con comportamenti cybercriminali che si sono evoluti maggiormente rispetto ad altre aree geografiche.

Vedi l'appendice per un'analisi dettagliata del tasso di attacchi ransomware in base al paese.

Percentuale Di Computer Colpiti

In media, in un attacco ransomware viene colpita poco meno della metà (49%) dei computer di un'organizzazione. La crittografia completa dell'intero ambiente avviene molto raramente, con appena il 4% delle organizzazioni che sostiene che il 91% o più dei propri dispositivi è stato colpito dall'attacco. All'estremo opposto, esistono attacchi che riguardano solo una quantità esigua di dispositivi, sebbene questo scenario sia molto improbabile: infatti, solo il 2% delle organizzazioni interessate afferma che è stato colpito meno dell'1% dei propri dispositivi.

Percentuale di dispositivi colpiti nell'organizzazione della vittima



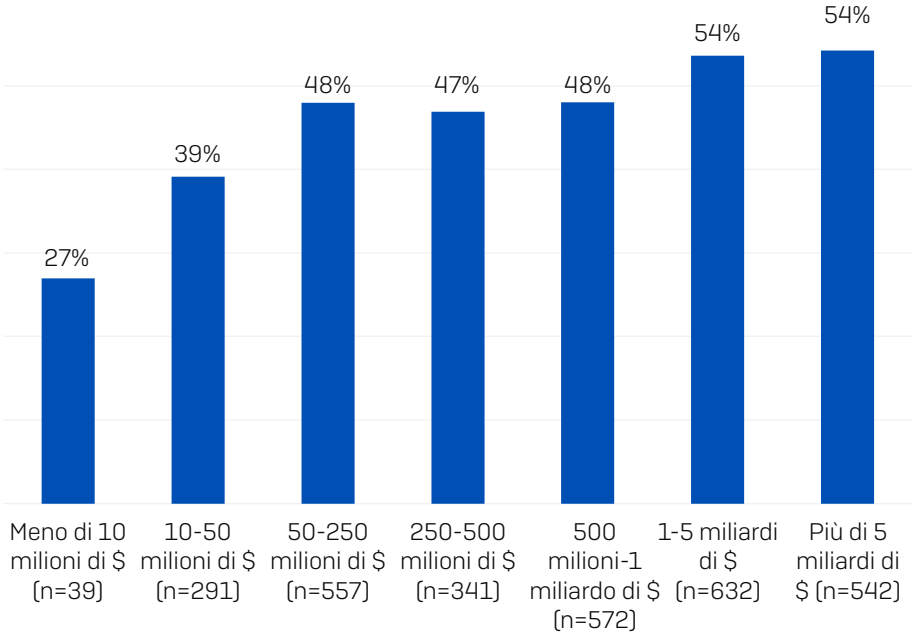
Qual è la percentuale di computer della tua organizzazione che sono stati colpiti ransomware l'anno scorso? n=2.974 organizzazioni colpite dal ransomware.

Percentuale Di Computer Colpiti In Base Al Fatturato

Anche se a livello globale, tra tutti i partecipanti al sondaggio, la distribuzione è stata ampia, si nota una variazione notevole nel numero di dispositivi colpiti sia in base alle dimensioni dell'organizzazione che in base al fatturato.

Parallelamente al fatturato, aumenta anche la proporzione dell'ambiente informatico coinvolto nell'attacco ransomware, con le organizzazioni di piccole dimensioni (meno di 10 milioni di $ di fatturato) che indicano che i loro dispositivi sono stati colpiti in una percentuale di casi pari alla metà di quella delle aziende con oltre 1 miliardo di $ di fatturato (27% vs 54%).

Con molta probabilità, questo risultato è dovuto a diversi fattori. Le organizzazioni più piccole sono meno propense a gestire centralmente tutti i dispositivi, riducendo così le opportunità per gli hacker di accedere all'intero ambiente informatico. Inoltre, nella maggior parte dei casi le piccole aziende e le startup utilizzano principalmente piattaforme SaaS, limitando così il rischio di interruzione del servizio per via di minacce come il ransomware.



Qual è la percentuale di computer della tua organizzazione che sono stati colpiti ransomware l'anno scorso? n=2.974 organizzazioni colpite dal ransomware.

Percentuale Di Computer Colpiti In Base Al Settore

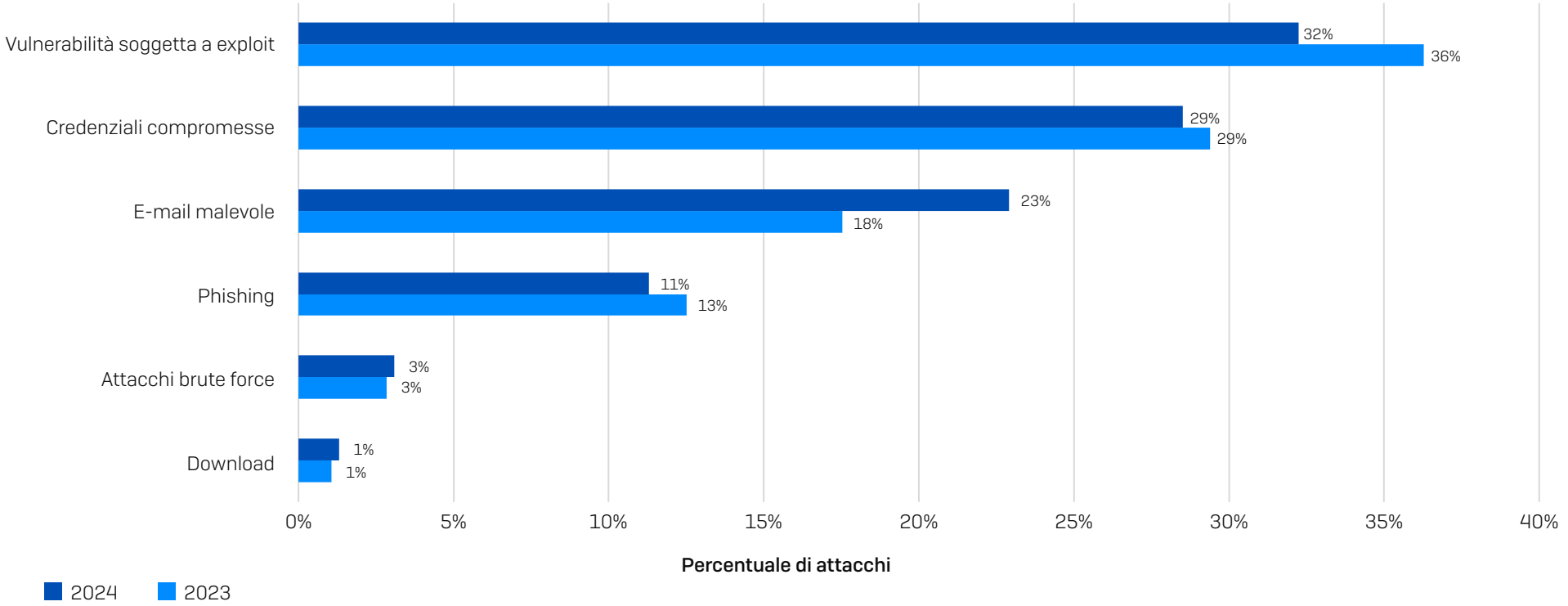
IT, tecnologie e telecomunicazioni è stato il settore che ha registrato la percentuale minore di dispositivi colpiti (33%), un dato che riflette il profilo di sicurezza informatica robusto che spesso caratterizza queste organizzazioni. Il settore *fonti di energia, petrolio/gas e utenze* è quello nel quale gli effetti di un attacco si sono fatti sentire maggiormente, con una media del 62% dei dispositivi colpiti, seguito dalla *sanità* (58%). A differenza di altri, entrambi questi settori devono affrontare la sfida di una maggiore presenza di tecnologie e controlli delle infrastrutture obsoleti, che sono fattori che complicano le attività di protezione dei dispositivi, limitazione dei movimenti laterali e blocco della diffusione degli attacchi.

Vedi l'appendice per un'analisi dettagliata della percentuale di computer colpiti in base al settore.

Cause All'Origine Degli Attacchi Ransomware

Nel 99% dei casi, le organizzazioni colpite dal ransomware sono state in grado di identificare la causa all'origine dell'attacco. Per il secondo anno consecutivo, le vulnerabilità soggette a exploit sono state il punto di inizio segnalato più frequentemente per gli attacchi. Nel complesso, la classifica è rimasta invariata rispetto al nostro studio del 2023.

Gli approcci basati su e-mail sono stati identificati come la causa all'origine dell'attacco dal 34% degli intervistati: gli attacchi causati da un'e-mail malevola (ovvero un messaggio con un link o un allegato dannoso che scarica malware) sono stati il doppio rispetto a quelli causati dal phishing (ovvero un messaggio realizzato per ingannare i destinatari e indurli a rivelare informazioni). È importante sottolineare che solitamente il phishing viene utilizzato per prelevare illecitamente credenziali di accesso e che pertanto può essere considerato come il primo passo in un attacco dovuto a credenziali compromesse.



Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? Sì. n= 2.974 organizzazioni colpite dal ransomware.

Attacchi Che Sfruttano Le Vulnerabilità Soggette A Exploit

Anche se tutti gli attacchi ransomware hanno esiti negativi, alcuni sono particolarmente devastanti. Le organizzazioni colpite da attacchi che hanno avuto inizio con l'exploit di una vulnerabilità a cui non erano state applicate patch hanno registrato esiti di gran lunga più gravi, rispetto alle aziende attaccate per via di credenziali compromesse. Questi esiti includono una maggiore propensione a:

- Subire una compromissione dei backup (tasso di successo delle attività criminali del 75%, rispetto al 54% per gli attacchi dovuti a credenziali compromesse)
- Essere soggette alla crittografia non autorizzata dei dati (tasso di crittografia del 67%, rispetto al 43% per gli attacchi dovuti a credenziali compromesse)
- Pagare il riscatto (tasso di pagamento del riscatto pari al 71%, rispetto al 45% per gli attacchi dovuti a credenziali compromesse)
- Dover pagare di tasca propria l'intero importo del riscatto (il 31% ha dovuto pagare l'intero importo del riscatto senza alcun aiuto, rispetto al 2% per gli attacchi dovuti a credenziali compromesse)

Hanno anche registrato:

- Costi necessari per rimediare ai danni degli attacchi ransomware 4 volte più alti (3 milioni di $, rispetto a 750.000 $ per gli attacchi dovuti a credenziali compromesse)
- Tempi di ripresa delle normali attività operative più lunghi (il 45% ha avuto bisogno di più di un mese, rispetto al 37% per gli attacchi dovuti a credenziali compromesse)

Per un'analisi ancora più approfondita, leggi Vulnerabilità Senza Patch: Il Vettore Di Attacco Che Non Perdona.

Cause All'Origine Degli Attacchi In Base Al Settore

Alcune vulnerabilità nelle difese informatiche sono più prevalenti in alcuni settori rispetto ad altri, e i cybercriminali non esitano a sfruttarle. Di conseguenza, la causa all'origine degli attacchi ransomware varia notevolmente in base al settore:

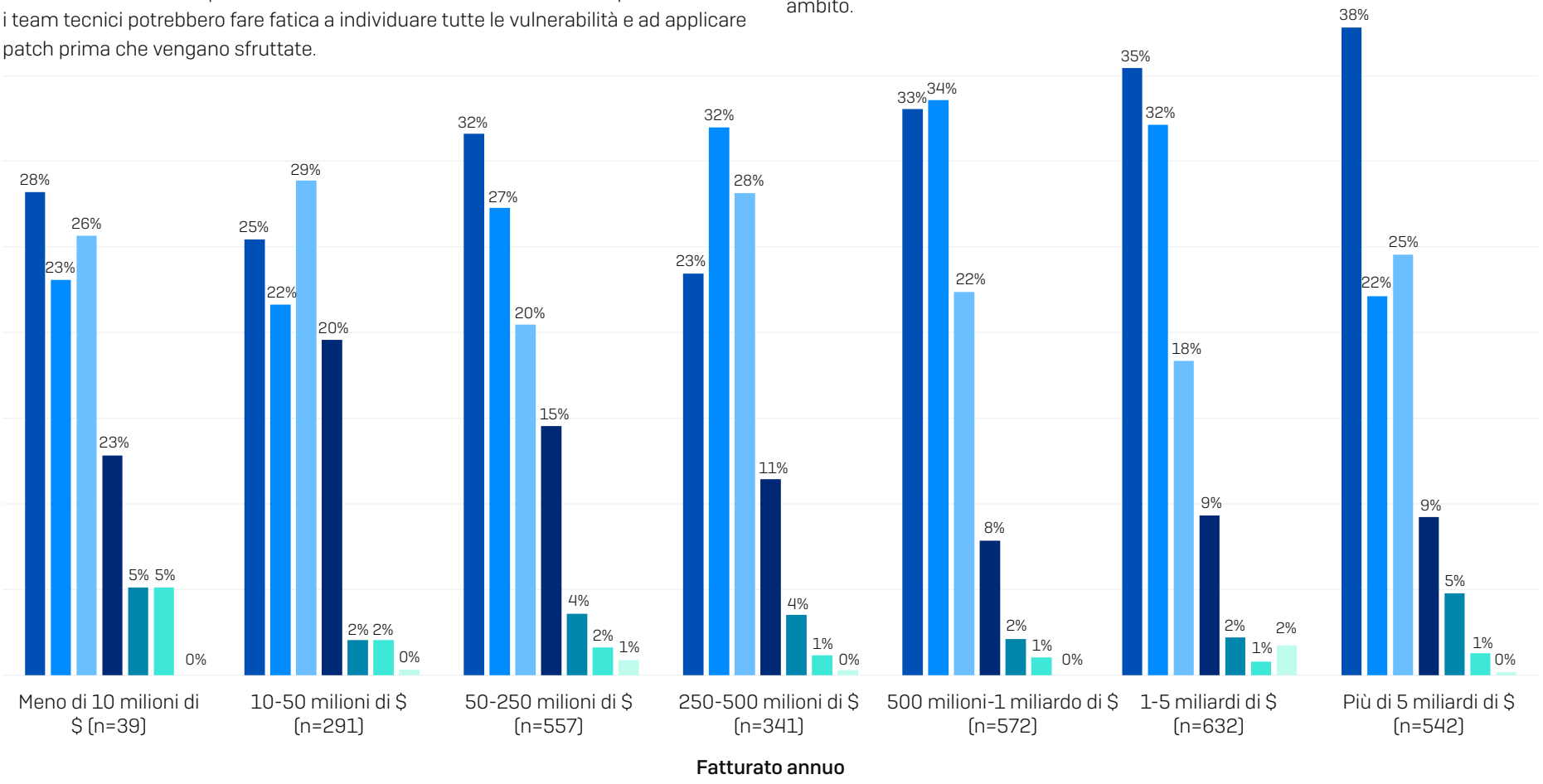
- *Fonti di energia, petrolio/gas e utenze* è il settore con la maggiore propensione a cadere vittima dell'exploit di vulnerabilità a cui non sono state applicate patch, con quasi la metà degli attacchi (49%) che iniziano in questo modo. Normalmente, questo settore utilizza una proporzione più alta di tecnologie meno recenti e pertanto più propense a presentare lacune di sicurezza. Inoltre, le patch per soluzioni obsolete e al termine del ciclo di vita potrebbero non essere più disponibili
- Gli enti governativi presentano una particolare suscettibilità agli attacchi che iniziano con l'uso improprio di credenziali compromesse: il 49% (*amministrazione locale/pubblica*) e il 47% (*governo centrale/federale*) degli attacchi sono stati causati da dati di accesso rubati
- *IT, tecnologie e telecomunicazioni* e *retail* hanno entrambi registrato incidenti di ransomware che hanno avuto inizio da un attacco di tipo brute force nel 7% dei casi. Ciò potrebbe essere dovuto al fatto che la minore esposizione di questi settori alla presenza di vulnerabilità senza patch e credenziali compromesse costringe i cybercriminali a concentrarsi, in parte, su approcci alternativi

Vedi l'appendice per un'analisi dettagliata della causa all'origine degli attacchi in base al settore.

Cause All'Origine Degli Attacchi In Base Al Fatturato

Generalmente, le organizzazioni più grandi sono caratterizzate da una maggiore probabilità di subire un attacco causato da una vulnerabilità a cui non sono state applicate patch, con la fascia di fatturato di più di 5 miliardi di $ che registra la percentuale più alta di attacchi che hanno avuto inizio in questo modo (38%). Con molta probabilità, alla crescita di un'azienda corrisponde un incremento delle dimensioni e della complessità delle infrastrutture informatiche. Per questo motivo i team tecnici potrebbero fare fatica a individuare tutte le vulnerabilità e ad applicare patch prima che vengano sfruttate.

L'uso di credenziali compromesse come vettore d'attacco mostra un picco nelle fasce medio-alte di fatturato, e costituisce la principale causa di attacco sia nella fascia 250-500 milioni di $ che nella fascia 500 milioni-1 miliardo di $. Sebbene le vulnerabilità e le credenziali compromesse ricevano (giustamente) molta attenzione, la principale causa all'origine degli attacchi segnalata dalle organizzazioni con 10-50 milioni di $ di fatturato sono le e-mail malevole. Nel complesso, le minacce basate sulle e-mail costituiscono poco meno della metà (49%) degli attacchi in questo ambito.



Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? n= 2.974 organizzazioni colpite dal ransomware.

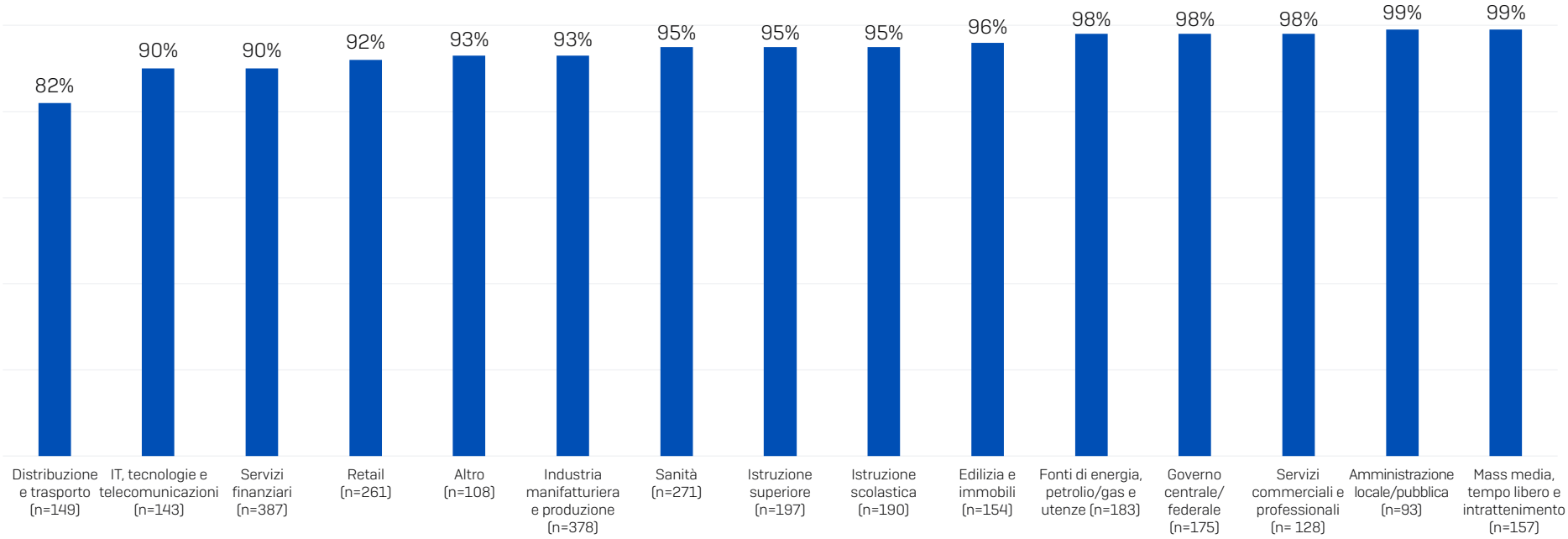
Compromissione Dei Backup

Per recuperare i dati crittografati durante un attacco ransomware, esistono due metodi principali: eseguire il ripristino dai backup e pagare il riscatto. Quando gli autori degli attacchi ransomware riescono a compromettere i backup di un'organizzazione, limitano la capacità di recupero dei dati crittografati della vittima e aumentano le pressioni per indurla a pagare il riscatto.

Tentativi Di Compromissione Dei Backup

Il 94% delle organizzazioni colpite dal ransomware l'anno scorso sostiene che, durante l'attacco, i cybercriminali hanno cercato di compromettere i loro backup. Questa statistica sale al 99% sia nell'*amministrazione locale/pubblica*, sia nel settore *mass media, tempo libero e intrattenimento*. Il tasso più basso per i tentativi di compromissione è stato registrato da *distribuzione e trasporto*, tuttavia anche in questo settore più di otto organizzazioni su dieci (82%) che sono state colpite dal ransomware affermano che gli hacker hanno cercato di accedere ai loro backup.

Percentuale di attacchi nei quali i cybercriminali hanno cercato di compromettere i backup



I cybercriminali hanno cercato di compromettere i backup della tua organizzazione? Sì. Base di partecipanti indicata nel grafico.

Tasso Di Successo Dei Tentativi Di Compromissione Dei Backup

In tutti i settori, il 57% dei tentativi di compromissione dei backup è andato a segno, il che significa che i cybercriminali sono stati in grado di sabotare le attività di riparazione dei danni di oltre la metà delle loro vittime. Le analisi hanno rivelato una variazione significativa nel tasso di successo dei cybercriminali, a seconda del settore:

- La percentuale di hacker che sono riusciti a compromettere i backup delle loro vittime è risultata più alta nei settori *fonti di energia, petrolio/gas e utenze* (tasso di successo del 79%) e *istruzione* (tasso di successo del 71%)
- All'estremo opposto, *IT, tecnologie e telecomunicazioni* (tasso di successo del 30%) e *retail* (tasso di successo del 47%) hanno registrato i tassi più bassi di avvenuta compromissione dei backup

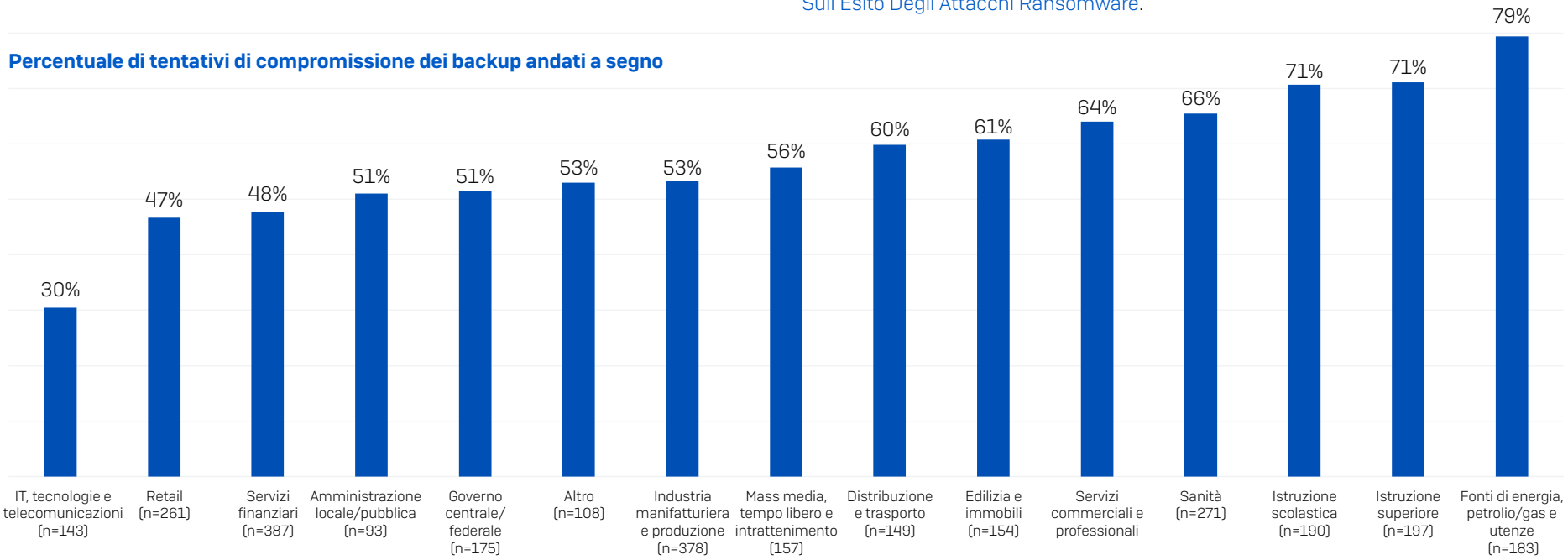
Esistono vari motivi che possono giustificare questa variazione nel tasso di successo dei cybercriminali. Le aziende che operano nell'ambito di *IT, tecnologie e telecomunicazioni* potrebbero aver adottato una protezione più efficace per i backup, che le ha rese più resilienti agli attacchi rispetto ad altri settori. È anche possibile che queste organizzazioni siano state più abili nel rilevare e bloccare i tentativi di compromissione prima che i cybercriminali potessero raggiungere il loro intento.

Qualsiasi sia la causa, le organizzazioni che hanno subito la compromissione dei backup hanno registrato esiti molto più negativi rispetto alle organizzazioni che sono riuscite a tutelare l'integrità dei loro backup:

- Le richieste di riscatto sono state in media pari al doppio, rispetto a quelle inviate alle organizzazioni i cui backup erano rimasti integri (somma mediana di richiesta di riscatto pari a 2,3 milioni di $ vs 1 milione di $)
- Le organizzazioni i cui backup erano stati compromessi presentavano una probabilità doppia di pagare il riscatto per recuperare i dati (67% vs 36%)
- I costi complessivi mediani per la riparazione dei danni del ransomware sono stati otto volte superiori (3 milioni di $ vs 375.000 $) per le organizzazioni con backup compromessi

Per maggiori approfondimenti, leggi L'Impatto Della Compromissione Dei Backup Sull'Esito Degli Attacchi Ransomware.

Percentuale di tentativi di compromissione dei backup andati a segno



I cybercriminali hanno cercato di compromettere i backup della tua organizzazione? Sì, base di partecipanti indicata nel grafico.

Tasso Di Crittografia Dei Dati

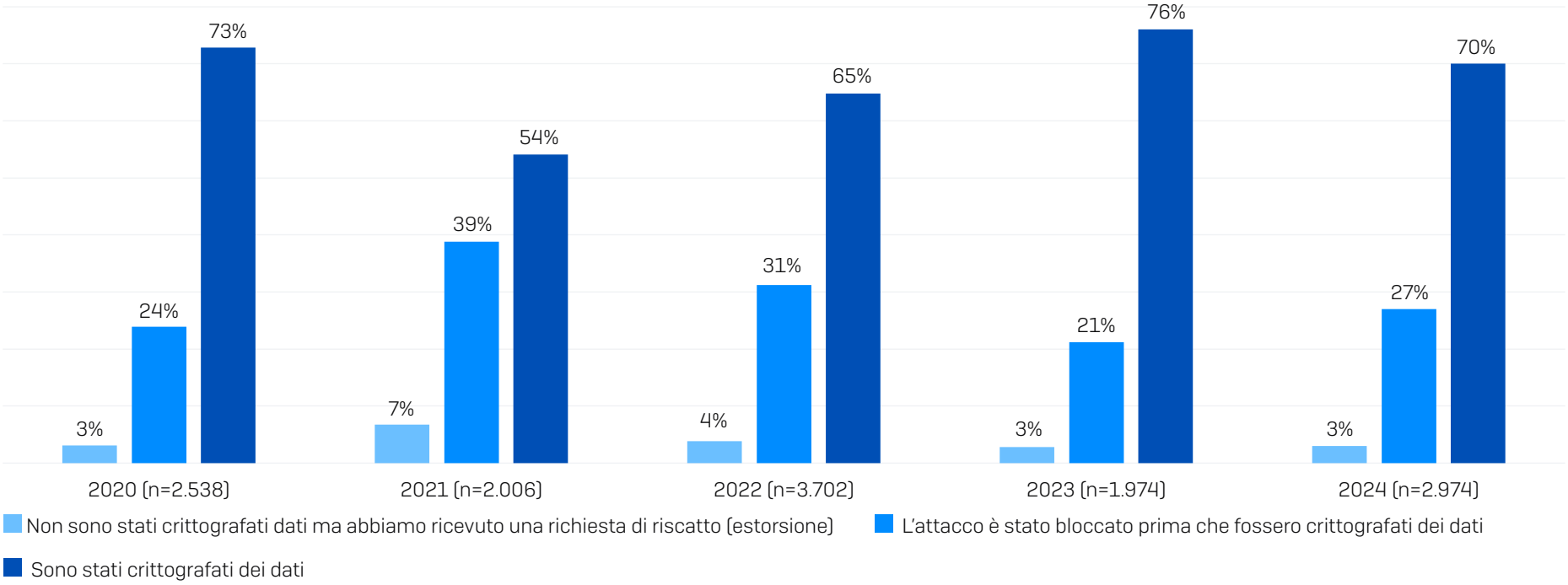
Sette attacchi ransomware su dieci (70%) nel corso dell'ultimo anno hanno portato alla crittografia non autorizzata dei dati. Sebbene sia alto, questo tasso è in leggera diminuzione rispetto al 2023, quando si era registrata la crittografia dei dati nel 76% degli attacchi.

Tasso Di Crittografia Dei Dati Per Settore

Il sondaggio del 2024 indica una variazione notevole nel tasso di crittografia in tutti i settori.

- Mentre l'*amministrazione locale/pubblica* ha registrato la minora frequenza di attacco quest'anno (34% delle organizzazioni colpite dal ransomware), ha anche segnalato il **più alto tasso di crittografia dei dati**, con il 98% degli attacchi nei quali i dati sono stati crittografati
- I *servizi finanziari* (49%), seguiti dal retail (56%), hanno riscontrato **i tassi più bassi di crittografia dei dati**
- *Distribuzione e trasporto* è il settore con maggiore propensione a subire un **attacco di estorsione**, con il 17% degli intervistati che dichiara che i dati non sono stati crittografati, ma che ha comunque ricevuto una ricetta di riscatto. Questa percentuale è quasi tre volte superiore a quella di qualsiasi altro settore

Vedi l'appendice per un'analisi dettagliata dei tassi di crittografia dei dati in base al settore.



Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? Base di partecipanti indicata nel grafico.

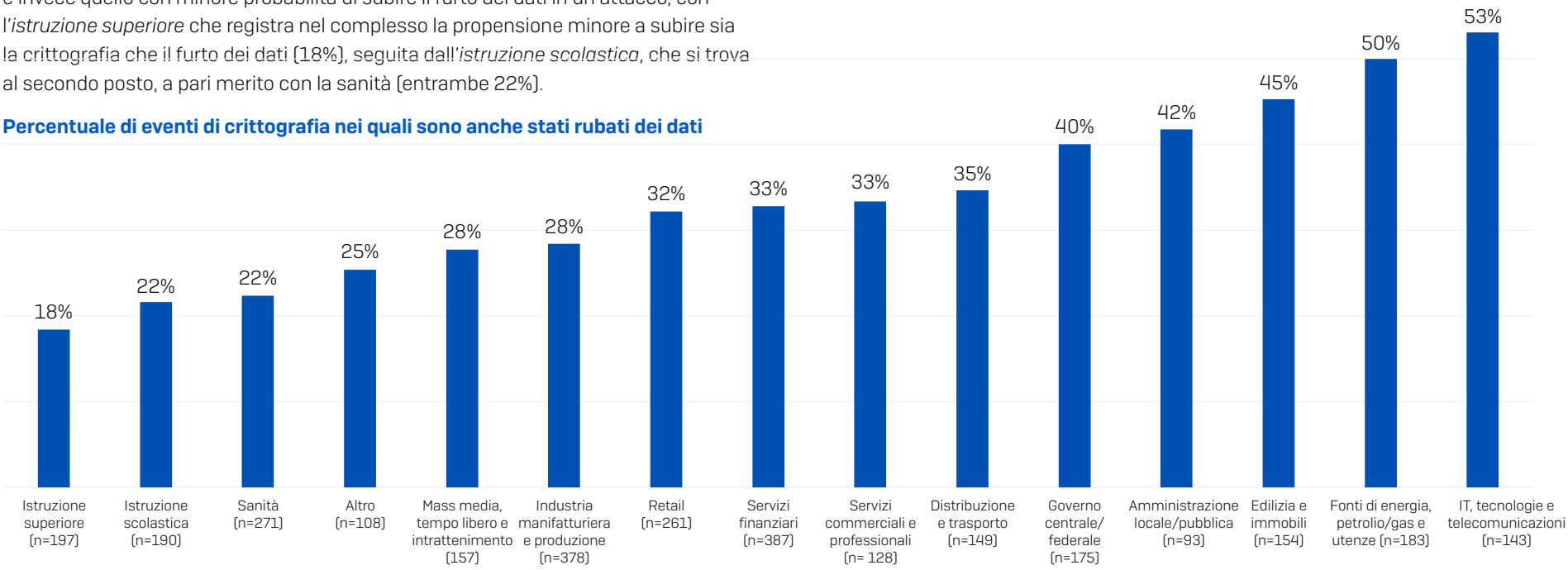
Furto Di Dati

I cybercriminali non si limitano solo a crittografare i dati, ma se ne appropriano anche illecitamente. Nel 32% degli incidenti nei quali sono stati crittografati dei dati, sono state rubate anche informazioni: leggermente al di sopra del tasso del 30% dello scorso anno. Il furto dei dati incrementa la capacità degli autori degli attacchi di estorcere denaro alle proprie vittime, e allo stesso tempo gli consente di monetizzare ulteriormente l'attacco, vendendo i dati rubati sul dark web.

Anche in questo caso si riscontra una variazione notevole in base al settore. All'apparenza, *IT, tecnologie e telecomunicazioni* risulta il settore con i peggiori risultati, visto che ha riportato un tasso del 53% di attacchi nei quali i dati sono stati sia crittografati che rubati. Le organizzazioni che operano nell'ambito di *fonti di energia, petrolio/gas e utenze* si trovano al secondo posto, visto che hanno subito il furto dei dati nel 50% degli eventi di crittografia. Il settore dell'istruzione è invece quello con minore probabilità di subire il furto dei dati in un attacco, con l'*istruzione superiore* che registra nel complesso la propensione minore a subire sia la crittografia che il furto dei dati (18%), seguita dall'*istruzione scolastica*, che si trova al secondo posto, a pari merito con la sanità (entrambe 22%).

I risultati potrebbero riflettere livelli diversi di capacità di indagine nei settori, nonché priorità differenti. Per poter stabilire se ci sia stata un'esfiltrazione dei dati, occorrono strumenti con funzionalità più avanzate di analisi approfondita e spesso queste analisi si basano sui log raccolti da software EDR/XDR. Una teoria potrebbe essere che il settore *IT, tecnologie e telecomunicazioni* sia semplicemente più abile nell'identificare il furto dei dati, rispetto ad altri settori. Anche la semplicità di molti ambienti informatici nel settore *fonti di energia, petrolio/gas e utenze* potrebbe rendere più facile il rilevamento di un furto in queste organizzazioni. Gli istituti scolastici, invece, sono spesso caratterizzati dalla mancanza di competenze e strumenti idonei per determinare se si sia verificato un furto dei dati. Allo stesso tempo, per alcune organizzazioni potrebbe essere preferibile non sapere se sono stati esfiltrati dei dati, in quanto una violazione dei dati implicherebbe attività di comunicazione dell'incidente molto dispendiose.

Percentuale di eventi di crittografia nei quali sono anche stati rubati dei dati



Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? Sì. Sì, e sono anche stati rubati dei dati. Base di partecipanti indicata nel grafico.

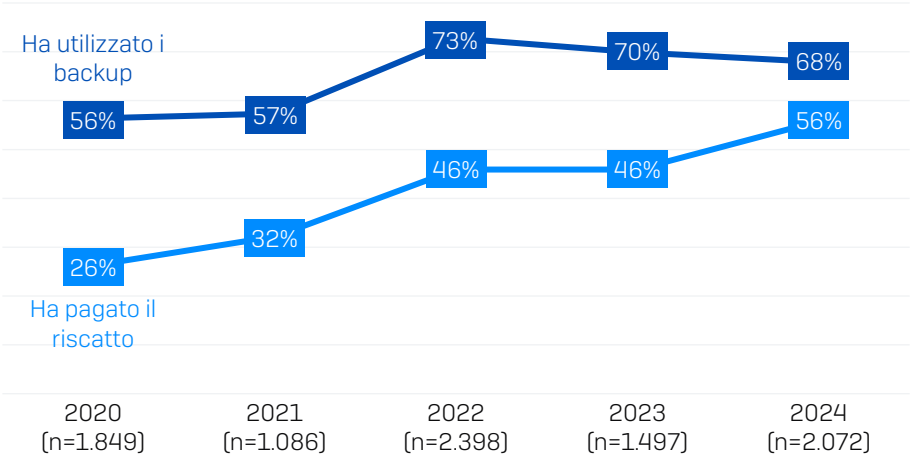
Recupero Dei Dati

Il 98% delle organizzazioni che sono cadute vittima della crittografia non autorizzata dei dati è riuscito a recuperare le proprie informazioni. I due metodi principali utilizzati per recuperare i dati sono stati il ripristino dai backup (68%) e il pagamento del riscatto per ottenere la chiave di decrittografia (56%). Il 26% delle organizzazioni che avevano subito la crittografia non autorizzata dei dati ha dichiarato di aver utilizzato "altri metodi" per recuperare le informazioni. Sebbene il sondaggio non abbia esplorato ulteriormente questo ambito, gli altri metodi potrebbero includere la collaborazione con le forze dell'ordine o l'uso di chiavi di decrittografia che erano già state rese pubbliche.

Ha utilizzato i backup per recuperare i dati	Ha pagato il riscatto e recuperato dei dati	Ha utilizzato altri metodi per recuperare i dati
68%	**56%**	**26%**

Un cambiamento significativo rispetto all'anno scorso è stato l'aumento nella propensione delle vittime ad adottare più approcci diversi per recuperare i dati crittografati (ad es. pagare il riscatto e utilizzare i backup). Questa volta, quasi la metà delle organizzazioni i cui dati erano stati crittografati ha dichiarato di aver utilizzato più di un metodo (47%), oltre il doppio rispetto alla percentuale registrata nel 2023 (21%).

Le statistiche nel corso di cinque anni rivelano che il divario tra l'uso dei backup e il pagamento del riscatto si sta riducendo sempre di più. L'uso dei backup è in calo (anche se leggermente) per il secondo anno consecutivo. Allo stesso tempo, per il pagamento del riscatto si è registrato un aumento del 10% rispetto allo studio del 2023. La propensione a pagare il riscatto dipende da vari fattori, inclusa la disponibilità di backup. Si tratta, tuttavia, di una tendenza preoccupante, visto che più della metà delle vittime sceglie di pagare per la chiave di decrittografia.



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 Fatturato

Generalmente, la propensione a pagare il riscatto per recuperare i dati cresce in maniera direttamente proporzionale al fatturato. Le organizzazioni con il fatturato minore (inferiore ai 10 milioni di $) hanno registrato il più basso tasso di pagamento del riscatto (25%), mentre quelle con il fatturato maggiore (oltre 5 miliardi di $) presentano il tasso di pagamento del riscatto più alto (61%). Fondamentalmente, la disponibilità di fondi per il pagamento del riscatto è probabilmente uno dei principali fattori che influenzano le statistiche: molte aziende di piccole dimensioni non hanno abbastanza soldi disponibili per pagare un riscatto.

Tuttavia, come abbiamo visto, per il recupero dei dati non si tratta solo di scegliere tra backup e pagamento del riscatto. Le sfumature che si celano dietro ai metodi di recupero delle informazioni diventano più evidenti quando analizziamo in maniera più approfondita i dati e mettiamo a confronto le statistiche del 2024 con i risultati dell'anno scorso.

Ad eccezione del gruppo con fatturato inferiore ai 10 milioni di $, tutte le fasce di fatturato hanno registrato un aumento nel tasso di pagamento del riscatto rispetto all'anno scorso. Inoltre, tre aziende hanno segnalato un incremento nell'uso dei backup per recuperare i dati. Anche se è stata la fascia di fatturato più bassa a registrare il più alto tasso di utilizzo dei backup (88%), la fascia con fatturato di 250-500 milioni di $ segue a distanza ravvicinata (85%).

Recupero Dei Dati In Base Al Settore

Probabilmente non sorprende il fatto che il settore del *governo centrale/federale* sia quello con la minore probabilità di pagare il riscatto per recuperare i dati (indubbiamente queste organizzazioni devono attenersi a normative molto severe in termini di pagamento del riscatto) e con i tassi più alti di uso dei backup per riappropriarsi delle informazioni sottratte (rispettivamente, 39% e 81%).

Nel complesso, non esiste una correlazione diretta tra uso dei backup e pagamento del riscatto:

- *Mass media, tempo libero e intrattenimento* hanno riportato il più alto tasso di pagamento del riscatto per recuperare i dati (69%) e uno dei più alti tassi di utilizzo dei backup (74%)
- *Fonti di energia, petrolio/gas e utenze* presentano il livello più basso di uso dei backup (51%) e un tasso di pagamento del riscatto pari al 61%, che è inferiore a quello di altri quattro settori

Vedi l'appendice per un'analisi dettagliata del metodo di recupero in base al settore.

	FATTURATO ANNUO													
	Meno di 10 milioni di $ (n=39)		10-50 milioni di $ (n=291)		50-250 milioni di $ (n=557)		250-500 milioni di $ (n=341)		500 milioni-1 miliardo di $ (n=572)		1-5 miliardi di $ (n=632)		Più di 5 miliardi di $ (n=542)	
Metodi di recupero dei dati utilizzati	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024
Ha utilizzato i backup per recuperare i dati	80%	88% ▲	72%	68% ▼	77%	60% ▼	75%	85% ▲	68%	70% ▲	66%	65% ▼	63%	66% ▲
Ha pagato il riscatto e recuperato dei dati	36%	25% ▼	41%	49% ▲	42%	57% ▲	33%	50% ▲	51%	59% ▲	52%	56% ▲	55%	61% ▲

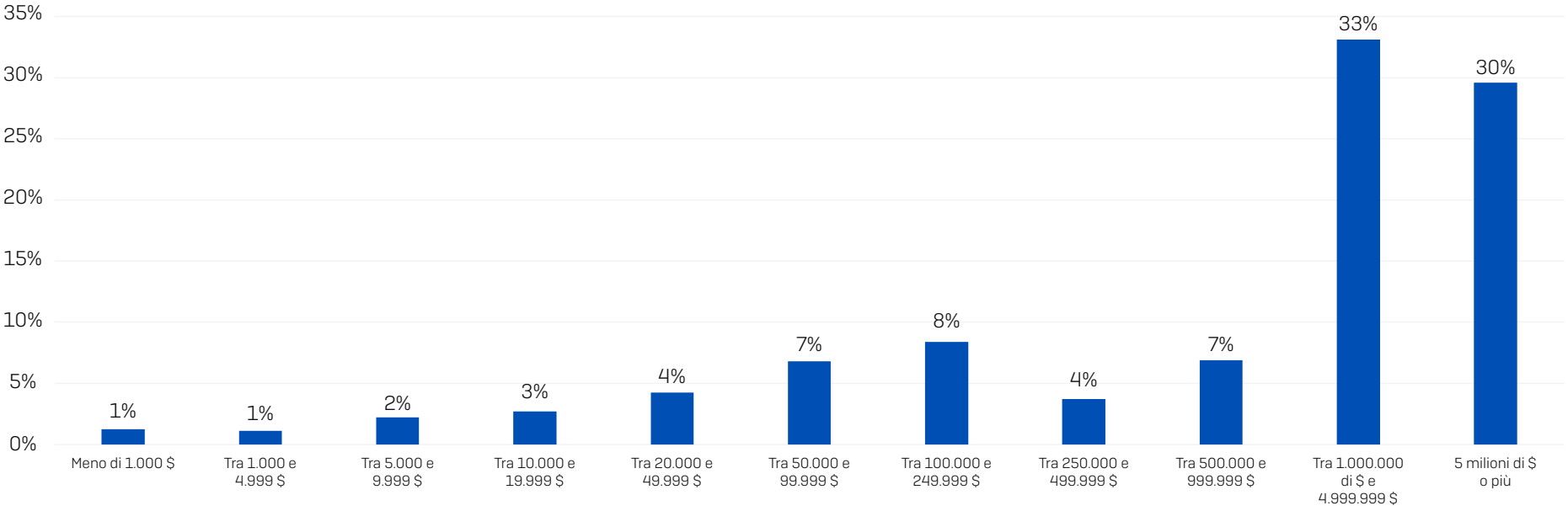
La tua organizzazione è riuscita a recuperare almeno parte dei dati? Sì, abbiamo pagato il riscatto e recuperato dei dati; Sì, abbiamo utilizzato i backup per recuperare i dati. Base di partecipanti per l'anno 2024 indicata nel grafico. Le frecce indicano l'aumento o la diminuzione rispetto al 2023.

Richieste Di Riscatto

Quest'anno, per la prima volta, abbiamo incluso nel report sia le richieste di riscatto che i pagamenti del riscatto. Tra le 1.701 organizzazioni che hanno subito la crittografia non autorizzata dei dati e sono state in grado di condividere la cifra richiesta inizialmente dai cybercriminali per il riscatto, la somma media è stata pari a 4.321.880 $ e quella mediana a 2 milioni di $.

Uno dei risultati più interessanti nello studio di quest'anno è stato che il 63% delle richieste di riscatto è stato di almeno 1 milione di $, con il 30% delle richieste che ha raggiunto o superato i 5 milioni di $. Sebbene parte degli intervistati abbia ricevuto richieste di riscatto a quattro cifre, si tratta pur sempre della minoranza.

Percentuale di richieste per la somma di riscatto



A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? n=1.701

Richieste Di Riscatto In Base Al Fatturato

Osservando sia i dati medi che mediani, la somma di riscatto richiesta tende ad aumentare a seconda del fatturato. Questo indica che i cybercriminali regolano le richieste di riscatto (almeno in parte) in base alla probabile capacità della vittima di poter pagare.

Le richieste di riscatto stratosferiche non sono più una prerogativa riservata alle organizzazioni con il fatturato più alto, e le somme di almeno 1 milione di $ sembrano ormai essere non più un'eccezione, bensì la regola: l'anno scorso, il 47% delle organizzazioni con un fatturato di 10-50 milioni di $ ha ricevuto richieste di riscatto a sette cifre.

Richieste Di Riscatto In Base Al Settore

Questa è una battaglia che non ha vincitori, visto che tutti i settori analizzati (ad eccezione di "Altro") hanno dichiarato di avere ricevuto richieste di riscatto pari ad almeno 1 milione di $.

- *Retail* e *IT, tecnologie e telecomunicazioni* hanno ricevuto le richieste con somme mediane più basse (1 milione di $), seguite dall'*edilizia* (1,1 milioni di $)
- *Governo centrale/federale* è il settore più colpito, visto che ha riportato le richieste di riscatto con somme mediane (7,7 milioni di $) e medie (9,9 milioni di $) più alte

Vedi l'appendice per un'analisi dettagliata delle richieste di riscatto in base al settore.

	FATTURATO ANNUO					
Richiesta di riscatto	**10-50 milioni di $ (n=207)**	**50-250 milioni di $ (n=288)**	**250-500 milioni di $ (n=158)**	**500 milioni-1 miliardo di $ (n=268)**	**1-5 miliardi di $ (n=366)**	**Più di 5 miliardi di $ (n=398)**
Cifra media	1.774.941 $	1.704.853 $	3.407.796 $	5.184.024 $	4.281.258 $	7.467.294 $
Cifra mediana	330.000 $	220.000 $	840.000 $	2.000.000 $	3.000.000 $	6.600.000 $

A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? Base di partecipanti indicata nel grafico. Nota: la coorte "Meno di 10 milioni di $" è stata esclusa da questa tabella, poiché presentava una base di partecipanti limitata.

Pagamenti del riscatto

1.097 intervistati la cui organizzazione ha pagato il riscatto hanno condiviso l'importo effettivo corrisposto ai cybercriminali. Analizzando sia le cifre medie che mediane, si osserva un incremento significativo nei pagamenti del riscatto nel corso dell'ultimo anno:

- Pagamento mediano: 2.000.000 di $ (una cifra 5 volte superiore ai 400.000 $ registrati nel 2023)
- Pagamento medio: 3.960.917 $ (una cifra 2,6 volte superiore a quella di 1.542.330 $ registrata nel 2023)

Il grafico riportato di seguito indica chiaramente come la percentuale di pagamenti del riscatto più bassi sia diminuita in maniera costante nel corso degli ultimi tre anni, mentre la proporzione di pagamenti molto alti ha subito un'impennata. Pagare riscatti a sette cifre è ormai la norma.

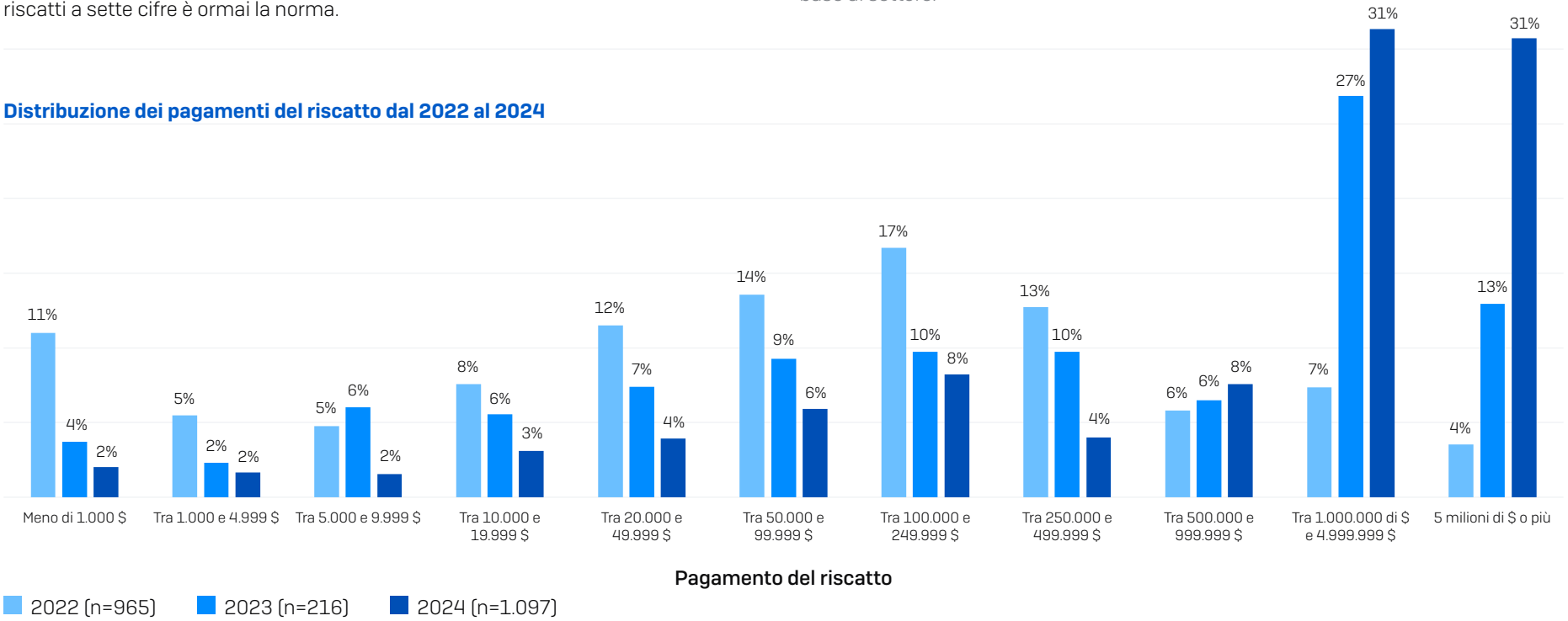
Pagamenti Del Riscatto In Base Al Settore

Proprio come le richieste medie di riscatto, anche i pagamenti del riscatto variano significativamente in base al settore. *IT, tecnologie e telecomunicazioni* è il settore che ha riportato il pagamento mediano più basso (300.000 $), seguito da *distribuzione e trasporto* (440.000 $). All'estremo opposto, sia *istruzione scolastica* che *governo centrale/federale* hanno pagato somme di riscatto mediane pari a 6,6 milioni di $.

Sebbene si osservi generalmente una correlazione diretta tra richieste basse e pagamenti bassi (e viceversa), ci sono delle eccezioni: quella più significativa è il settore *distribuzione e trasporto*, la cui richiesta di riscatto mediana è stata superiore ai 2,8 milioni di $, ma il cui pagamento è stato, in media, pari a 440.000 $.

Vedi l'appendice per una ripartizione dettagliata dei pagamenti medi di riscatto in base al settore.

Distribuzione dei pagamenti del riscatto dal 2022 al 2024



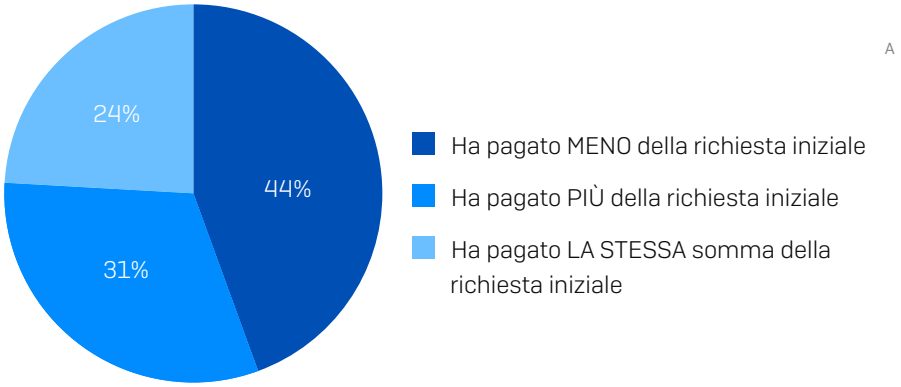
A quanto ammonta la somma di riscatto pagata ai cybercriminali? Base di partecipanti indicata nel grafico.

Richiesta Di Riscatto vs Pagamento Del Riscatto

Quando vengono crittografati i dati, aumentano le pressioni per tutte le persone coinvolte. E sia i cybercriminali che le vittime cercano di conseguire esiti ottimali. Le organizzazioni che hanno subito la crittografia dei dati cercano di ridurre l'impatto finanziario, mentre gli autori degli attacchi cercano di accaparrarsi quanti più soldi possibili nel più breve arco di tempo, spesso minacciando di aumentare la somma del riscatto se il pagamento non viene effettuato entro una certa data, a scopo di incrementare ulteriormente la pressione sulle vittime.

Propensione A Negoziare La Somma Del Riscatto

Lo studio ha rivelato che è raro che le vittime paghino la somma iniziale richiesta dai cybercriminali, con solo il 24% degli intervistati che dichiara di aver versato un pagamento pari alla cifra richiesta inizialmente. Il 44% delle vittime ha pagato meno della richiesta iniziale, mentre il 31% ha pagato di più.



quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? A quanto ammonta la somma di riscatto pagata ai cybercriminali? n=1.097.

Analizzando i dati in base al settore, si nota che i due settori dei servizi (*servizi commerciali e professionali* e *servizi finanziari*) sono quelli più propensi a negoziare e pagare una somma di riscatto più bassa, con il 67% degli intervistati che dichiara di aver pagato meno della richiesta iniziale. *Industria manifatturiera e produzione* seguono a distanza ravvicinata, con il 65% delle organizzazioni che ha pagato meno della prima richiesta ricevuta.

I settori che invece hanno mostrato una maggiore probabilità di pagare più della somma richiesta inizialmente sono quelli con un'alta percentuale di organizzazioni che operano nel settore pubblico:

- *Istruzione superiore* è il settore più propenso a pagare più della richiesta iniziale (il 67% degli intervistati ha pagato di più) e quello con meno probabilità di pagare meno rispetto alla richiesta iniziale (il 20% ha pagato di meno)
- La *sanità* si trova al secondo posto per quanto riguarda la propensione a pagare più della somma richiesta inizialmente (il 57% delle organizzazioni ha pagato di più), seguita dall'*istruzione scolastica* (il 55% ha pagato di più)

Potrebbe darsi che per questi settori sia meno fattibile ricorrere a negoziatori professionisti per il riscatto, che aiuterebbero a ridurre i costi. Inoltre, potrebbero essere caratterizzati da una maggiore necessità di recuperare i dati "a qualsiasi costo", poiché operano nell'ambito dei servizi pubblici. Qualsiasi sia il motivo, è evidente che nelle trattative c'è margine d'azione tra richiesta iniziale e pagamento effettivo.

Vedi l'appendice per una ripartizione dettagliata delle differenze tra richieste di riscatto e pagamento del riscatto in base al settore.

Percentuale Della Somma Di Riscatto Pagata

Anche se nella maggior parte dei casi sono presenti negoziazioni sulle somme di riscatto, l'impatto è relativamente poco significativo, in quanto gli intervistati in tutte le coorti indicano di aver pagato in media il 94% della somma di riscatto richiesta inizialmente.

Analizzando le statistiche in maniera più approfondita, osserviamo che tutte le fasce di fatturato tranne quella più alta sono riuscite a ridurre la somma di riscatto iniziale. La fascia con 50-250 milioni di $ di fatturato ha pagato la percentuale minore rispetto alla somma di riscatto richiesta inizialmente (84%). L'unica fascia a pagare più della somma iniziale è stata la fascia con fatturato superiore ai 5 miliardi di $, che ha dovuto versare, in media, il 115% della richiesta di riscatto iniziale.

	FATTURATO ANNUO					
Coorte	**10-50 milioni di $ (n=100)**	**50-250 milioni di $ (n=206)**	**250-500 milioni di $ (n=104)**	**500 milioni-1 miliardo di $ (n=175)**	**1-5 miliardi di $ (n=233)**	**Più di 5 miliardi di $ (n=275)**
Percentuale della somma di riscatto pagata	93%	84%	90%	88%	85%	115%

A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? A quanto ammonta la somma di riscatto pagata ai cybercriminali? n=1.097. Nota: la coorte "Meno di 10 milioni di $" è stata esclusa dalla ripartizione del fatturato annuo, poiché presentava una base di partecipanti molto limitata.

Percentuale Della Somma Di Riscatto Pagata In Base Al Settore

A livello di settore, si nota che le organizzazioni con la maggiore propensione a negoziare una somma di riscatto più bassa sono anche quelle che pagano la percentuale più bassa della somma iniziale, e viceversa.

MENO DEL 100%	PIÙ DEL 100%
Industria manifatturiera e produzione (70%)	Istruzione superiore (122%)
Servizi commerciali e professionali (74%)	Istruzione scolastica (115%)
Servizi finanziari (75%)	Sanità (111%)
Altro (79%)	Amministrazione locale/pubblica (104%)
IT, tecnologie e telecomunicazioni (82%)	Governo centrale/federale (103%)
Retail (84%)	Fonti di energia, petrolio/ gas e utenze (101%)
Edilizia e immobili (95%)	
Distribuzione e trasporto (95%)	
Mass media, tempo libero e intrattenimento (95%)	

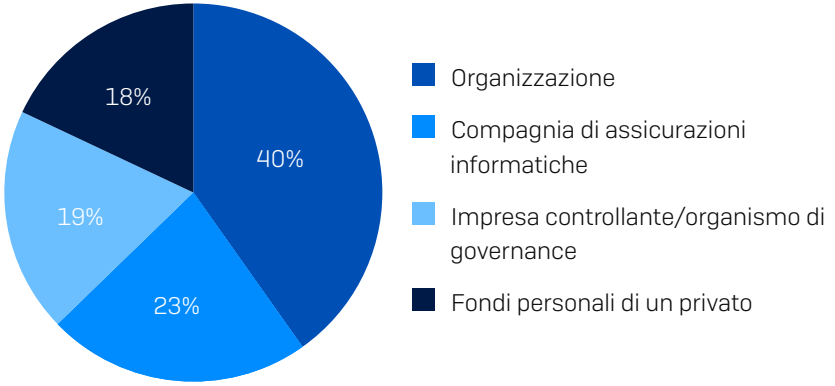
A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? A quanto ammonta la somma di riscatto pagata ai cybercriminali? n=1.097.

Origine Dei Fondi Utilizzati Per Il Pagamento Del Riscatto

La provenienza del denaro utilizzato per pagare il riscatto è un dato particolarmente interessante, e lo studio ci ha permesso di approfondire vari aspetti di questa dimensione:

- I fondi utilizzati per pagare il riscatto sono il risultato di uno sforzo congiunto, in quanto oltre quattro quinti (82%) degli intervistati dichiarano di avere ottenuto il denaro da più fonti
- La principale fonte dei fondi utilizzati per il pagamento del riscatto sono state le stesse organizzazioni, che in media hanno versato il 40% della somma; tipicamente, le imprese controllanti e/o gli organismi di governance delle organizzazioni hanno contribuito versando il 19% della cifra totale
- Le compagnie di assicurazioni svolgono un ruolo molto importante nei pagamenti del riscatto
  - Il 23% di tutti i fondi utilizzati per i pagamenti dei riscatti proviene da compagnie di assicurazioni
  - Le compagnie di assicurazioni contribuiscono a pagare il riscatto nell'83% degli attacchi
  - Tuttavia, è molto raro (l'1% dei casi) che le compagnie di assicurazioni paghino l'intera somma e nel 79% dei casi la compagnia di assicurazioni ha versato meno della metà della cifra totale

Origine dei fondi utilizzati per il pagamento del riscatto



Da quale o quali delle seguenti fonti provengono i fondi che sono stati utilizzati per pagare il riscatto? n=1.168.

La Transazione Del Pagamento Del Riscatto

Anche se più entità possono contribuire al pagamento del riscatto, di solito i fondi vengono trasferiti con un'unica transazione, effettuata da una sola parte.

A livello globale, le compagnie di assicurazioni hanno trasferito i fondi in quasi la metà dei pagamenti del riscatto, sia direttamente (26%), sia attraverso uno specialista di incident response incaricato (21%). La transazione è stata effettuata dall'organizzazione colpita dall'attacco nel 37% dei casi, e dall'ente giuridico che rappresenta la vittima nell'8% degli incidenti.

Complessivamente, il 28% (cifra arrotondata) delle transazioni è stato effettuato da specialisti di incident response, che possono essere stati incaricati dalla compagnia di assicurazioni (21%) o da un'altra parte, di solito la vittima (6%).

Esecutore della transazione del pagamento del riscatto

Chi ha eseguito la transazione del pagamento del riscatto? Ovvero, chi ha trasferito i fondi nel conto degli autori dell'attacco? n=1.168.

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 pagate, nel 2024 le organizzazioni hanno dovuto affrontare un costo medio di riparazione dei danni causati da un attacco ransomware pari a 2,73 milioni di $: un aumento di quasi 1 milione di $ rispetto agli 1,82 milioni di $ registrati nel 2023.

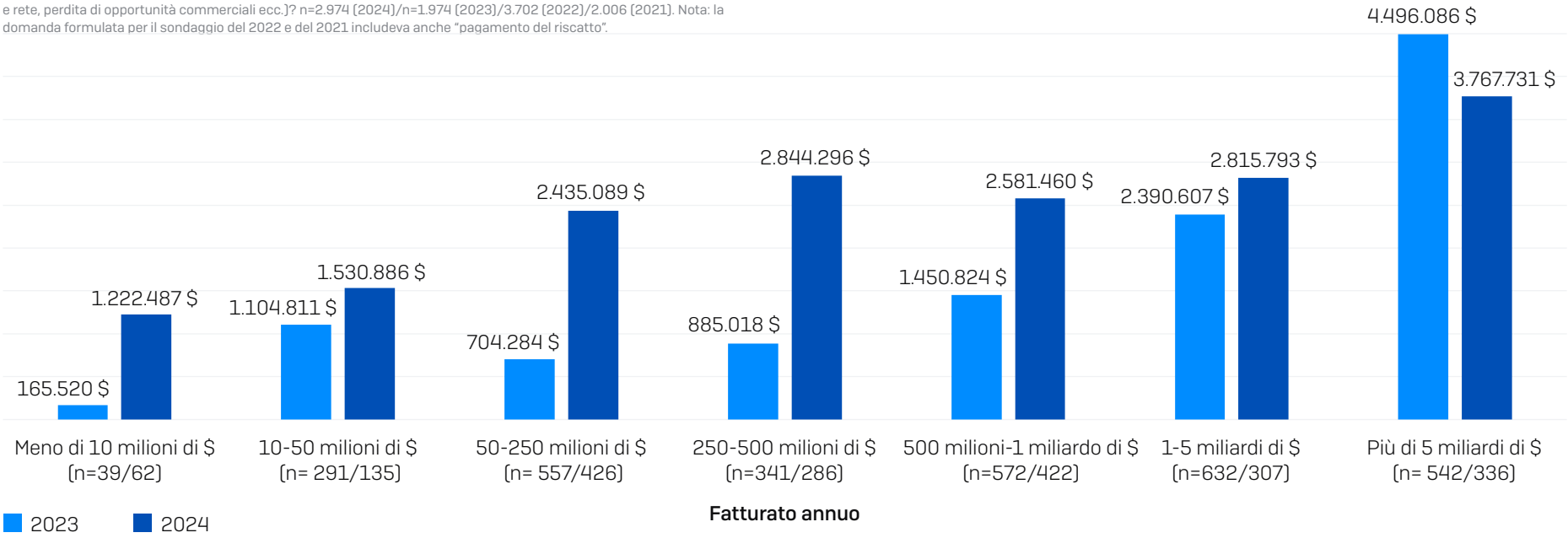
2021	2022	2023	2024
1,85 Mio di $	1,4 Mio di $	1,82 Mio di $	2,73 Mio di $

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=2.974 (2024)/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".

L'incremento più significativo nei costi complessivi di riparazione dei danni è stato registrato nelle fasce di fatturato medio-basse, con la coorte con 250-500 milioni di $ di fatturato che ha subito l'aumento maggiore in assoluto: 2 milioni di $ (da 885.018 $ a 2.885.296 $).

Le organizzazioni con un fatturato di 1-5 miliardi di $ hanno riscontrato un aumento (relativamente) basso di soli 400.000 $, mentre le organizzazioni più grandi (fatturato annuo superiore ai 5 miliardi di $) sono stata l'unica coorte in cui si è osservata una diminuzione nei costi di riparazione dei danni, scendendo da 4.496.096 $ a 3.767.731 $.

Un'analisi dei dati relativi al costo mediano di riparazione dei danni conferma questa tendenza. A livello globale, i costi mediani di riparazione dei danni sono raddoppiati, passando da 375.000 $ a 750.000 $ negli ultimi 12 mesi. Questi incrementi si concentrano principalmente nelle cinque fasce di fatturato più basse, che hanno tutte segnalato un aumento significativo dei costi. Per le due fasce di fatturato più alte, i costi sono rimasti quasi invariati.



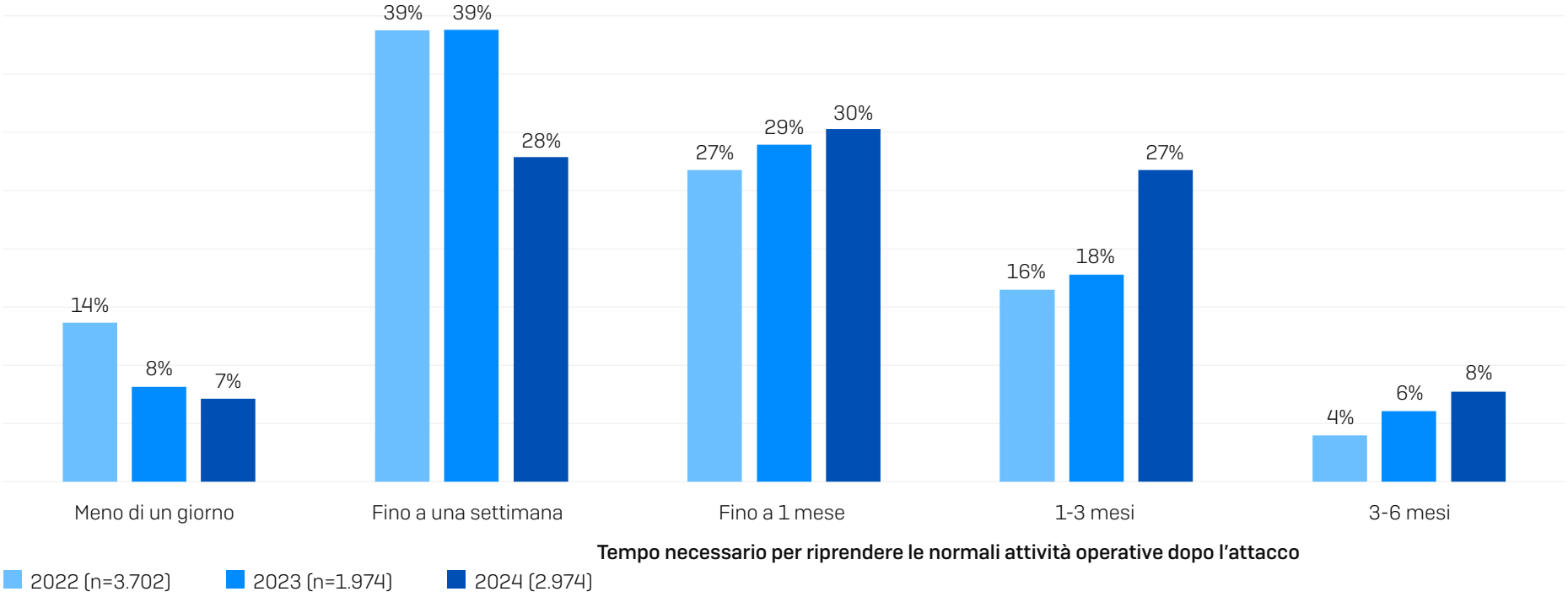
Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.)? n=2.974 (2024), 1.974 (2023). Base di partecipanti per gli anni 2024/2023 in base al fatturato indicata nel grafico

Tempo Necessario Per Riprendere Le Normali Attività

Il tempo necessario per riprendere le normali attività operative dopo un attacco ransomware sta aumentando in maniera costante. Il nostro studio del 2024 ha rivelato che:

- Il 35% delle vittime del ransomware ha avuto bisogno di una settimana o meno per riprendere completamente le attività, una statistica in calo rispetto al 47% del 2023 e al 52% del 2022
- Per un terzo (34%) delle organizzazioni è ora necessario più di un mese per riprendere le normali attività, un aumento rispetto al 24% del 2023 e al 20% del 2022

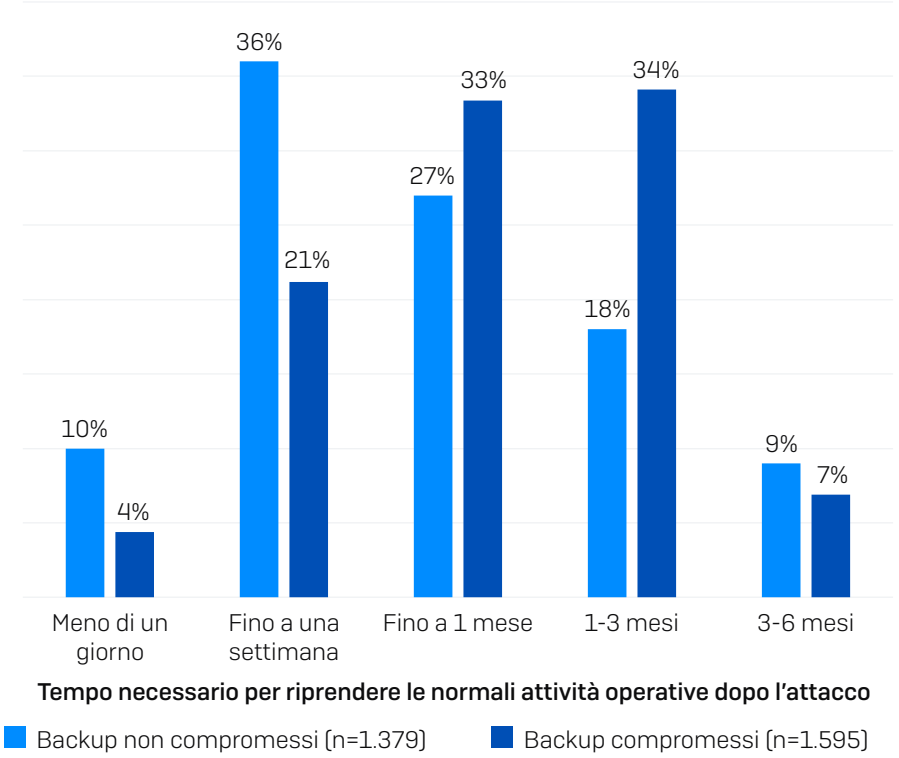
Questo rallentamento dei tempi potrebbe riflettere l'aumento della complessità e della gravità degli attacchi, che implicano ora un maggiore impegno per la ripresa delle attività. Potrebbe anche indicare una mancanza sempre più diffusa della preparazione necessaria per il ripristino dei sistemi.



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: L'Impatto Della Compromissione Dei Backup

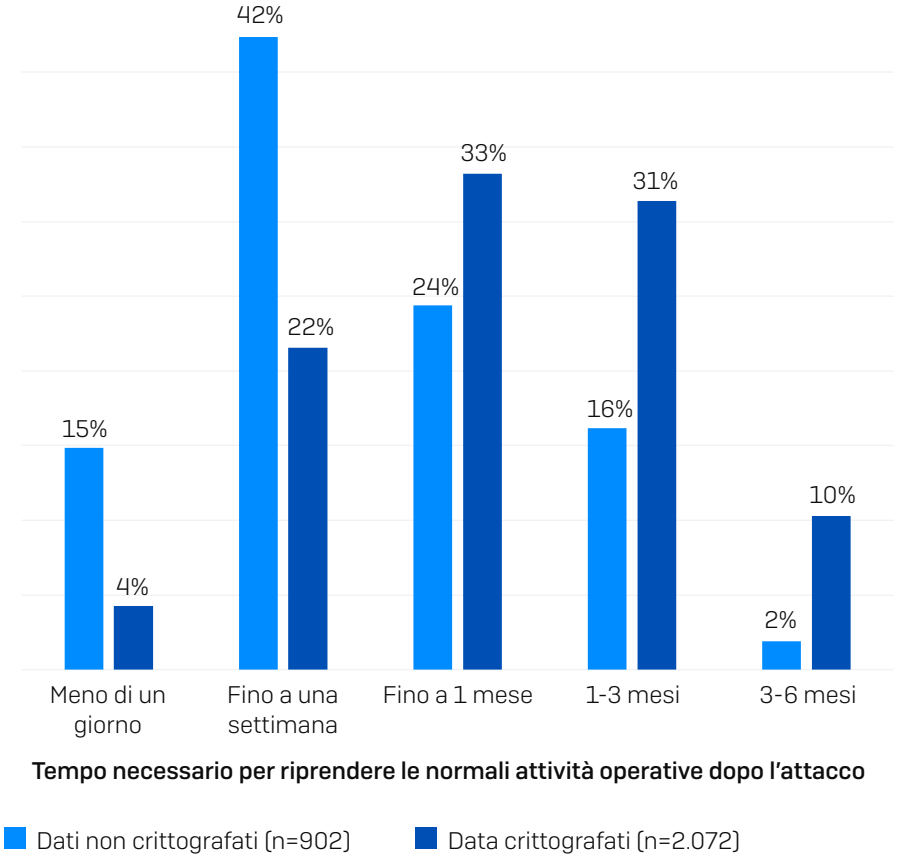
La compromissione dei backup ha un enorme impatto sui tempi complessivi di ripresa delle normali attività. Quasi la metà delle organizzazioni che riescono a preservare l'integrità dei loro backup riprendono le attività in una settimana o meno (46%), rispetto a un quarto (25%) delle aziende con backup compromessi. Quando vengono compromessi i backup, aumenta sia la complessità del processo di recupero dei dati crittografati, sia l'onere di dovere creare e proteggere nuovi backup integri.



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: L'Impatto Della Crittografia Dei Dati

Probabilmente non sorprende il fatto che, quando vengono crittografati i dati durante un attacco, i tempi di ripresa delle normali attività operative sono più lunghi. Il 57% degli intervistati che non avevano subito la crittografia non autorizzata dei dati è riuscito a riprendere le normali attività entro una settimana, a differenza del 25% di chi aveva subito la crittografia dei dati.

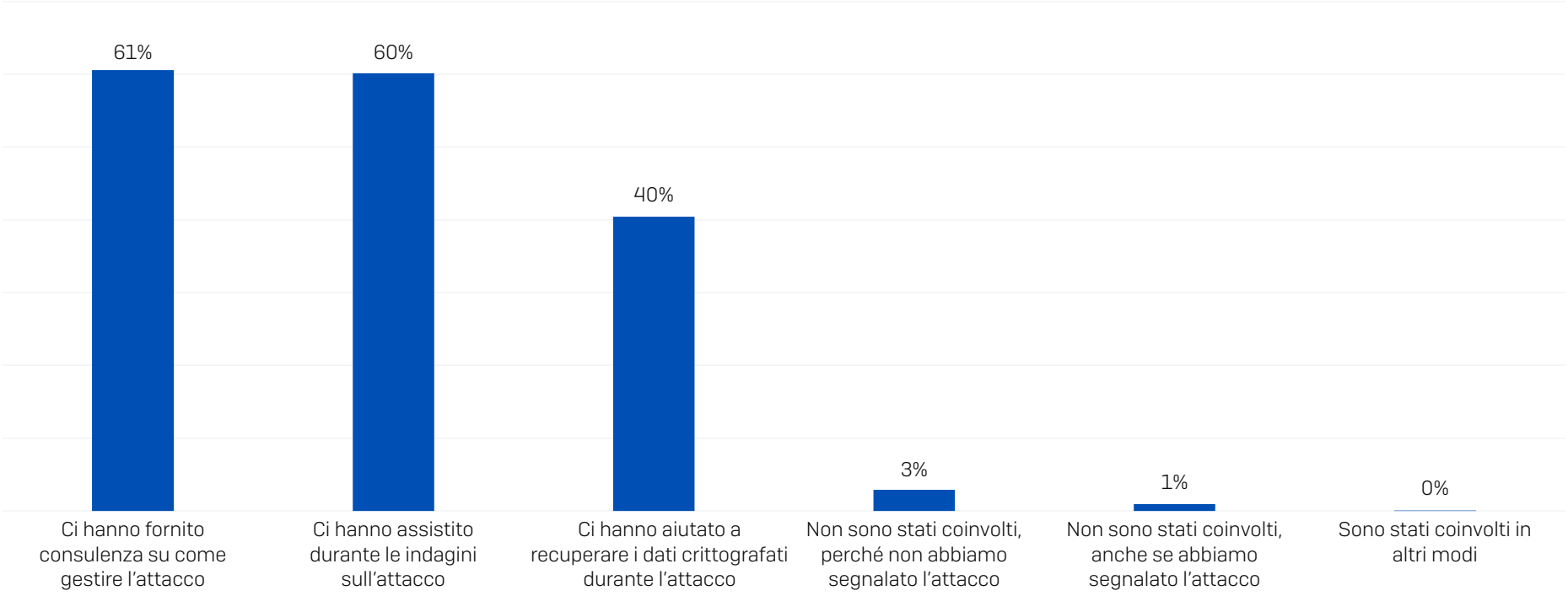


Di quanto tempo ha avuto bisogno la tua organizzazione per riprendere completamente le normali attività operative dopo l'attacco ransomware? Base di partecipanti indicata nel grafico.

Il Coinvolgimento Delle Forze Dell'Ordine

La natura e la disponibilità del sostegno da parte di organi ufficiali durante un attacco ransomware variano in base al paese, e lo stesso si può dire degli strumenti disponibili per segnalare un cyberattacco. Negli Stati Uniti, le vittime possono rivolgersi alla Cybersecurity and Infrastructure Security Agency (CISA), nel Regno Unito possono ricevere consulenza dal National Cyber Security Centre (NCSC), mentre in Australia possono richiedere l'intervento dell'Australian Cyber Security Center (ACSC), per citare solo alcuni esempi.

In linea con la normalizzazione del ransomware, il 97% delle organizzazioni che erano state colpite dal ransomware a livello globale si è rivolto alle forze dell'ordine e/o a enti governativi ufficiali a causa dell'attacco. Il 61% degli intervistati sostiene di aver ricevuto consulenza su come gestire l'attacco, il 60% di essere stato assistito durante le indagini sull'attacco e il 40% dichiara di aver ricevuto aiuto per riprendere le normali attività operative dopo l'attacco.

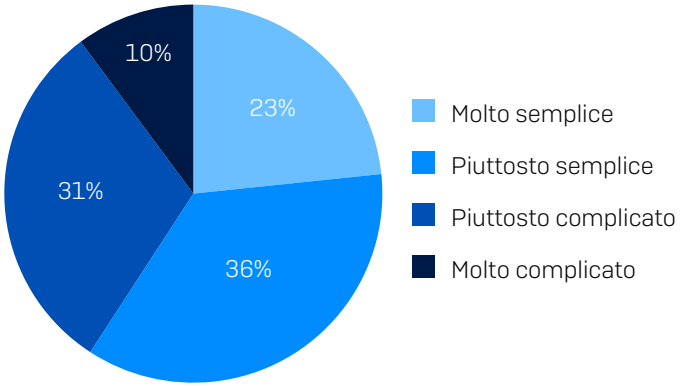


Come sono stati coinvolti forze dell'ordine e/o enti governativi?

Se la tua organizzazione ha segnalato l'attacco alle forze dell'ordine e/o a un ente governativo ufficiale, come sono stati coinvolti? n=2.974.

La Semplicità Del Coinvolgimento

Un dato incoraggiante è che oltre la metà (59%) delle organizzazioni che hanno coinvolto le forze dell'ordine e/o enti governativi ufficiali in merito all'attacco sostiene che il processo è stato semplice (23% lo ha definito "molto semplice", il 36% "piuttosto semplice"). Solo il 10% degli intervistati indica che il processo è stato "molto complicato", mentre il 31% l'ha descritto come "piuttosto complicato".



Quanto è stato semplice o complicato per la tua organizzazione coinvolgere le forze dell'ordine e/o enti governativi ufficiali in merito all'attacco? n=2.874 (le risposte "Non lo so" sono state omesse).

La Scelta Di Non Coinvolgere Enti Ufficiali

Il 3% degli intervistati (86 partecipanti) non ha segnalato l'attacco, e ci sono vari motivi alla base di questa scelta. I più comuni sono stati il timore che una segnalazione avrebbe avuto un impatto negativo sull'organizzazione, ad es. sanzioni, multe o lavoro in più da svolgere (27%), e l'idea che segnalare l'attacco non avrebbe portato alcun vantaggio per l'organizzazione (anche in questo caso, 27%). Diversi partecipanti hanno dichiarato testualmente di non essersi rivolti a enti ufficiali perché erano riusciti a risolvere il problema internamente.

Temevamo che una segnalazione avrebbe avuto un impatto negativo sull'organizzazione, ad es. sanzioni, multe o lavoro in più da svolgere	**27%**
Non pensavamo che segnalare l'attacco avrebbe portato alcun vantaggio per la nostra organizzazione	**27%**
Non pensavamo che si sarebbero interessati dell'attacco	**22%**
Eravamo talmente occupati a gestire l'attacco che non abbiamo pensato di coinvolgerli	**21%**
Gli autori dell'attacco non volevano che li coinvolgessimo	**19%**
Non sapevamo a quali forze dell'ordine o enti ufficiali rivolgerci	**10%**
Non eravamo tenuti per legge a segnalare l'attacco	**9%**
Altro (specifica)	**3%**
Non lo so	**1%**

Perché non hai segnalato l'attacco alle forze dell'ordine e/o a enti ufficiali? (n=86).

Conclusione

Il ransomware continua a essere una minaccia molto grave per le organizzazioni, indipendentemente dalle dimensioni e da dove si trovino nel mondo. Sebbene si sia riscontrata una diminuzione nel tasso complessivo degli attacchi rispetto agli ultimi due anni, l'impatto degli attacchi sulle vittime è invece aumentato. Con cybercriminali che continuano a replicare ed evolvere i loro attacchi, è fondamentale che i team di sicurezza e le difese informatiche delle organizzazioni non restino indietro.

Prevenzione. I migliori attacchi ransomware sono quelli che non si verificano, perché i cybercriminali non sono riusciti a infiltrarsi nei sistemi della tua organizzazione. Dato che un terzo degli attacchi inizia sfruttando vulnerabilità a cui non sono state applicate patch, è importante che tu assuma il controllo della tua superficie di attacco e applichi le patch seguendo un sistema di assegnazione di priorità stabilite in base al rischio. Anche adottare l'autenticazione a più fattori (MFA) per limitare l'uso improprio delle credenziali deve essere una priorità per qualsiasi organizzazione. La formazione continua degli utenti in merito a come rilevare i tentativi di phishing e le e-mail malevole continua a essere fondamentale.

Protezione. Avere una solida base di sicurezza è un must. Questa sicurezza deve includere tecnologie di protezione endpoint, e-mail e firewall. Gli endpoint (server inclusi) sono l'obiettivo iniziale primario per i cybercriminali del ransomware, per cui è importante assicurarsi che vengano difesi adeguatamente, con una protezione antiransomware dedicata, in grado di bloccare i tentativi di crittografia non autorizzata e ripristinare i file allo stato pre-attacco. Gli strumenti di sicurezza devono essere configurati e implementati correttamente, per garantire una protezione ottimale. Ti consigliamo quindi di cercare soluzioni che siano subito pronte per l'uso, con controlli trasparenti per il profilo di sicurezza. Una protezione complicata e difficile da distribuire può incrementare il livello di rischio, anziché ridurlo.

Rilevamento e risposta. Prima viene bloccato un attacco, meglio è. La capacità di rilevare e neutralizzare un cybercriminale all'interno del tuo ambiente prima che riesca a compromettere i backup o crittografare i dati migliorerà nettamente i tuoi risultati di cybersecurity.

Pianificazione e preparazione. Poter contare su un piano strategico di incident response con cui hai già acquisito familiarità migliorerà notevolmente i risultati, qualora succedesse il peggio e la tua organizzazione dovesse subire un attacco grave. Svolgi esercitazioni regolari di ripristino dei dati dai backup, per assicurarti che il processo possa avvenire in maniera rapida e fluida, se ne dovessi avere bisogno in futuro, in seguito a un attacco.

Per esplorare come Sophos può aiutarti a ottimizzare le tue difese antiransomware, parla con un consulente o visita www.sophos.it

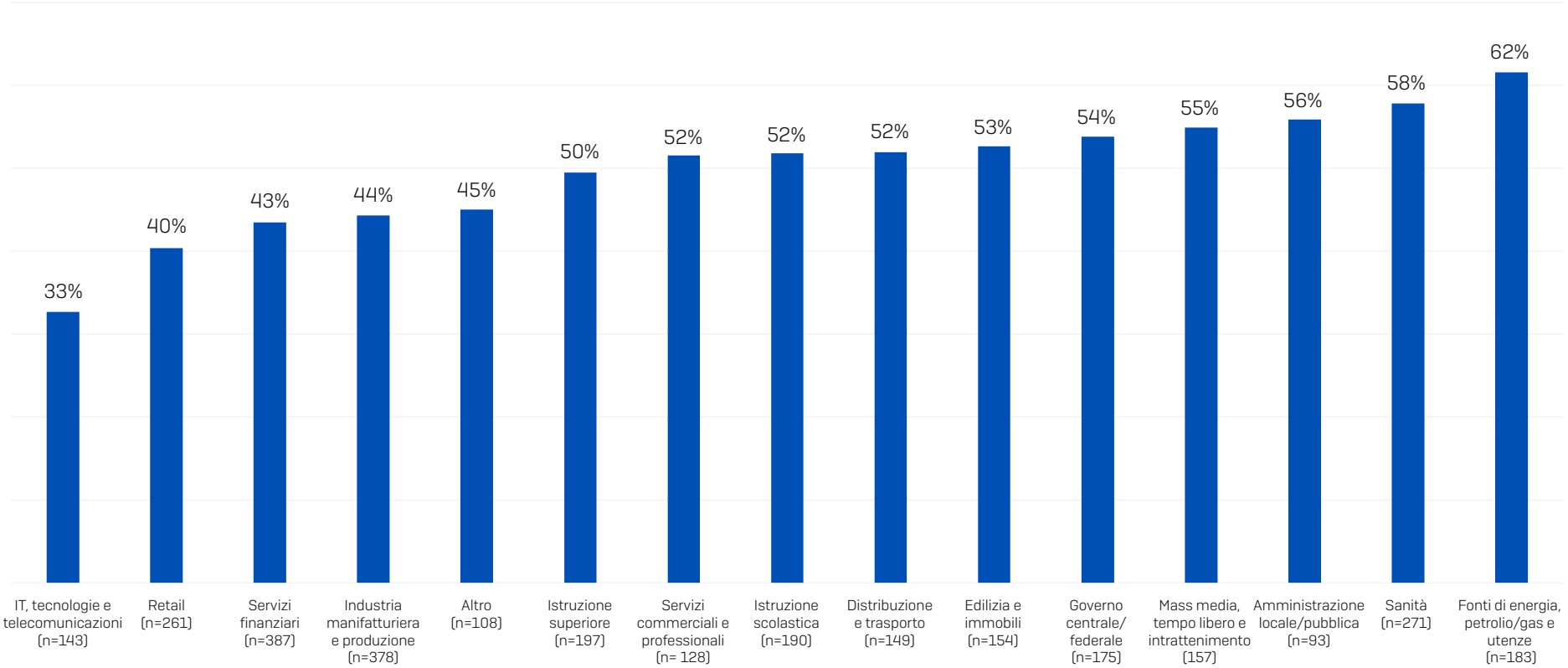
Informazioni su Vanson Bourne

Vanson Bourne è un'azienda indipendente, specializzata negli studi di mercato per il settore delle tecnologie. La sua reputazione, garanzia di analisi valide, attendibili e basate sulla ricerca, è fondata sui suoi rigorosissimi principi di ricerca e sulla sua abilità nell'ottenere i pareri dei principali decision maker in ruoli tecnici e commerciali, in tutti i settori ed in tutti i mercati più importanti. Per maggiori informazioni, visita www.vansonbourne.com

Appendice

Percentuale Di Computer Colpiti In Base Al Settore

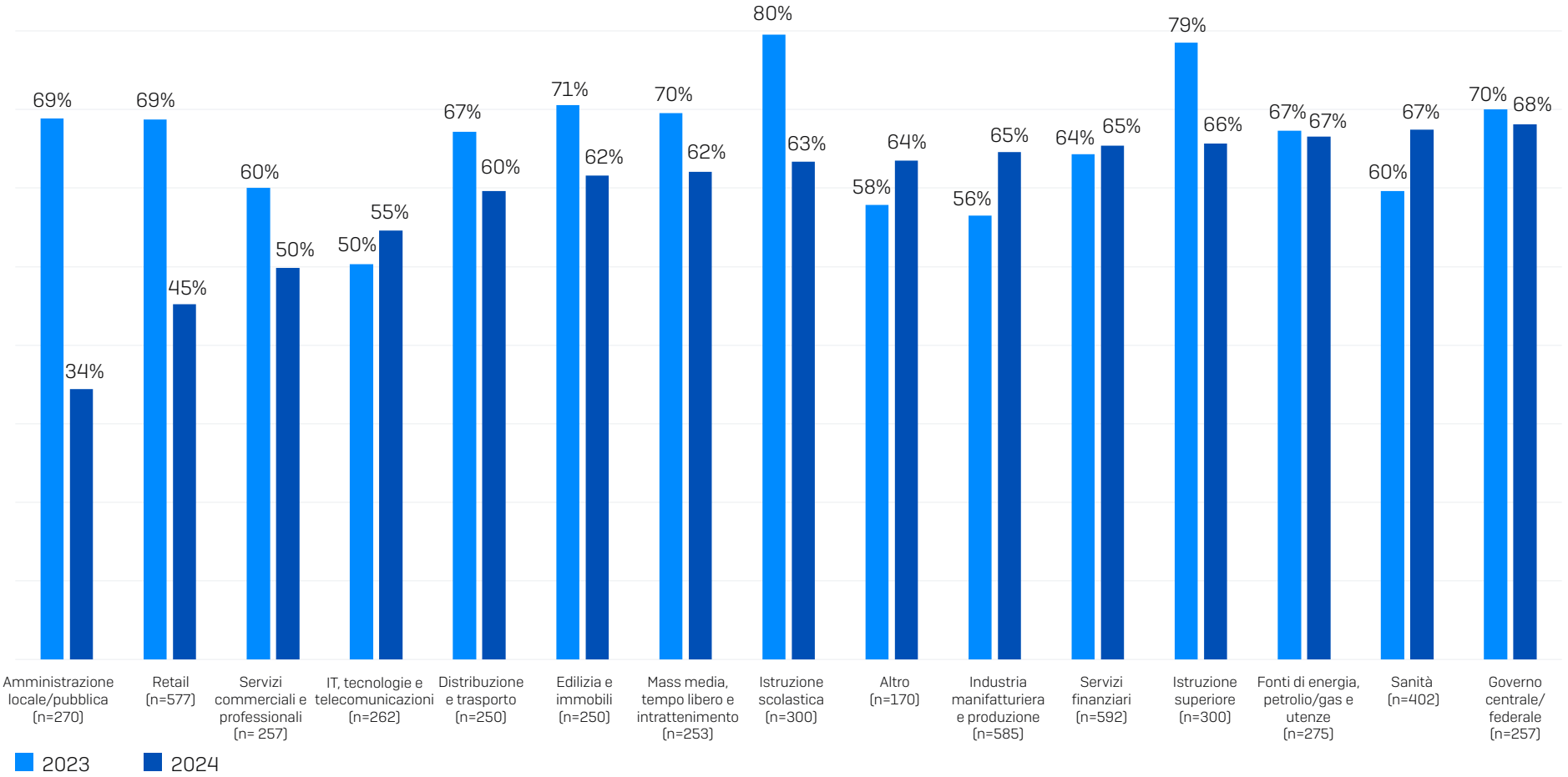
Percentuale Di Dispositivi Colpiti



Qual è la percentuale di computer della tua organizzazione che sono stati colpiti ransomware l'anno scorso? n=2.974 organizzazioni colpite dal ransomware. Base di partecipanti in base al settore indicata nel grafico.

Tasso Di Attacchi Ransomware In Base Al Settore

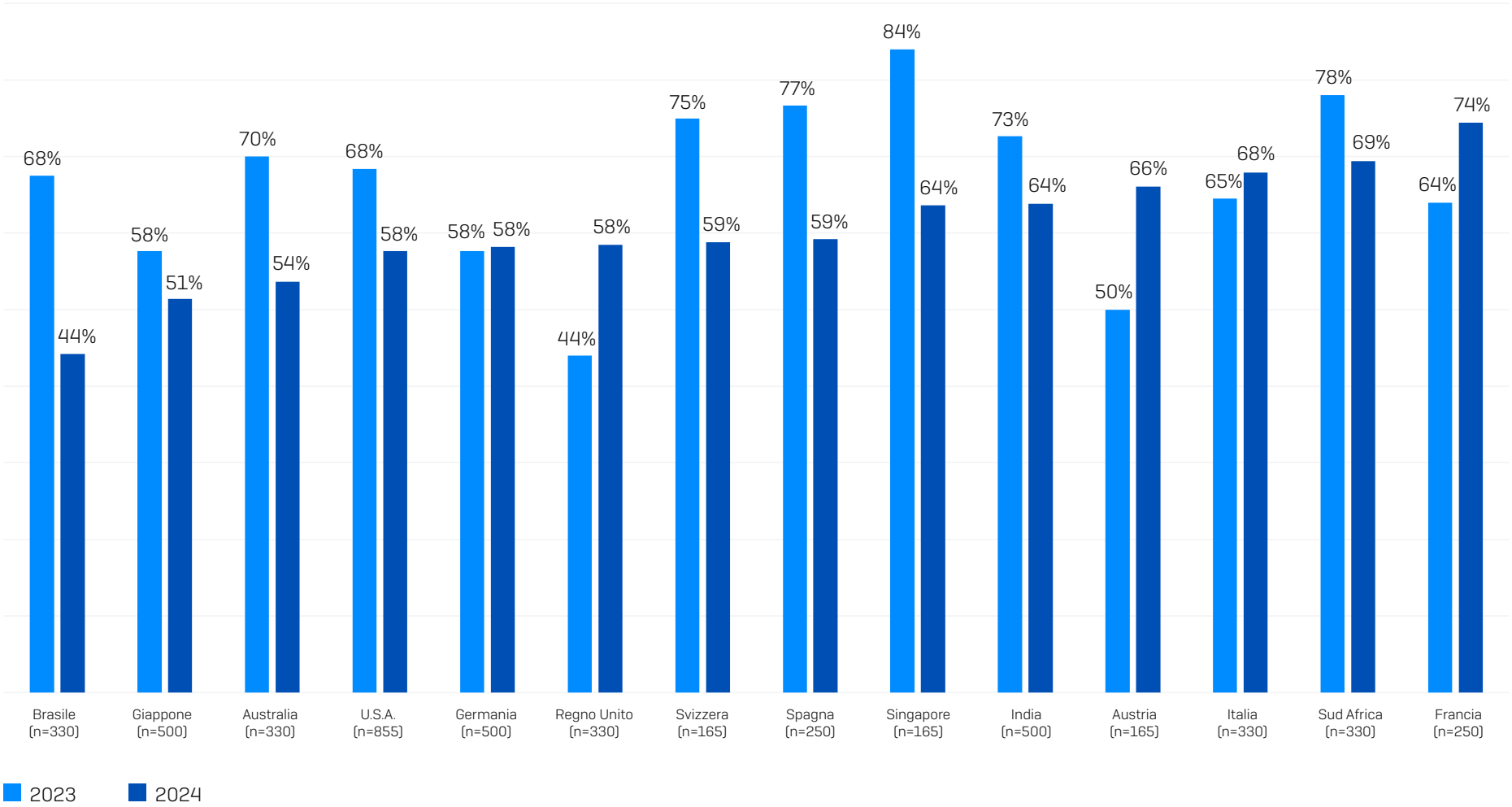
Percentuale delle organizzazioni colpite dal ransomware negli ultimi 12 mesi



La tua organizzazione è stata colpita dal ransomware l'anno scorso? Sì. n=5.000 (2004), n=3.000 (2023), n=5.600 (2022). Base di partecipanti in base al settore per l'anno 2024 indicata nel grafico.

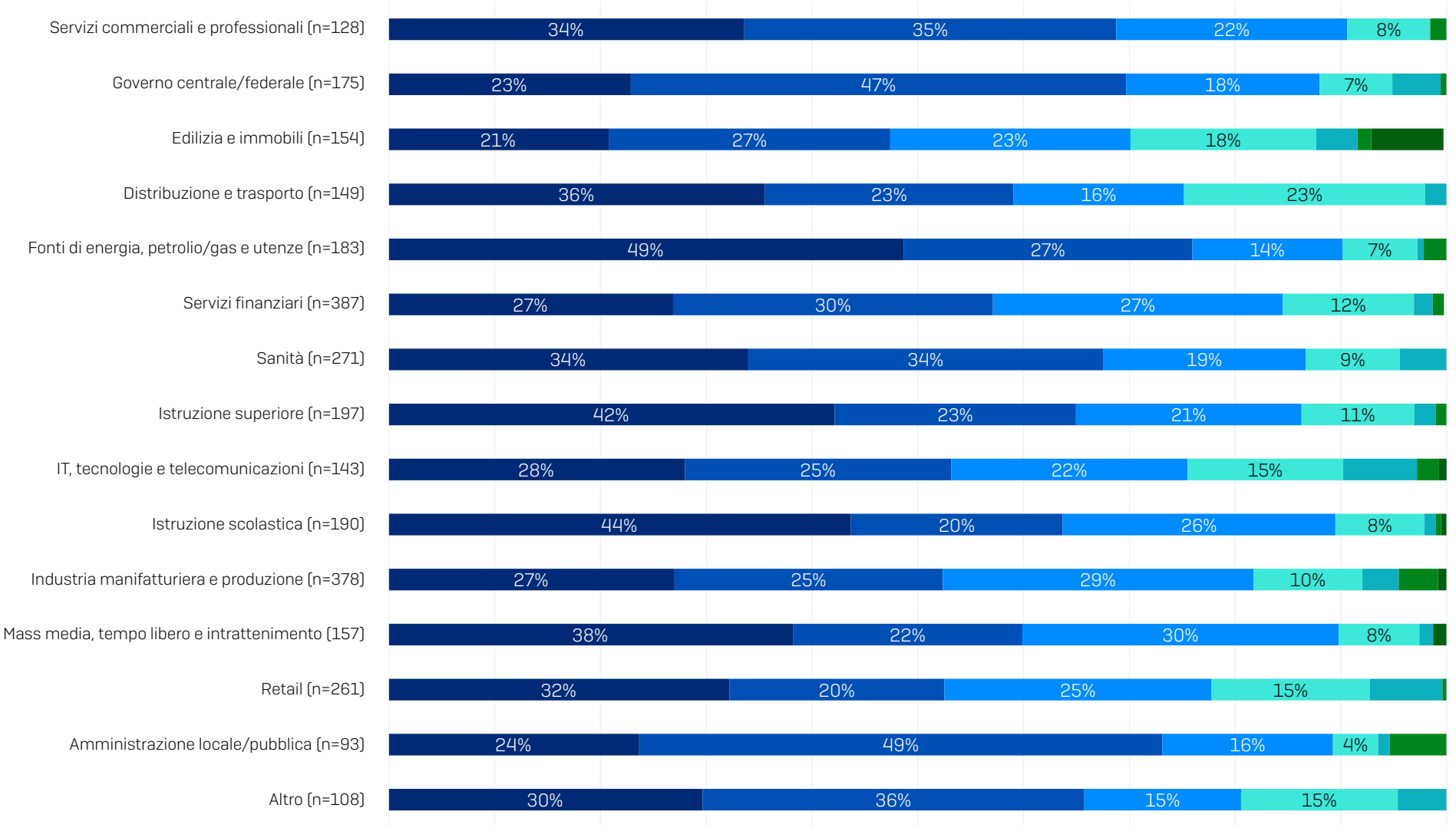
Tasso Di Attacchi Ransomware In Base Al Paese

Percentuale delle organizzazioni colpite dal ransomware negli ultimi 12 mesi



La tua organizzazione è stata colpita dal ransomware l'anno scorso? Sì. n=5.000 (2024) n=3.000 (2023). Base di partecipanti in base al paese per l'anno 2024 indicata nel grafico.

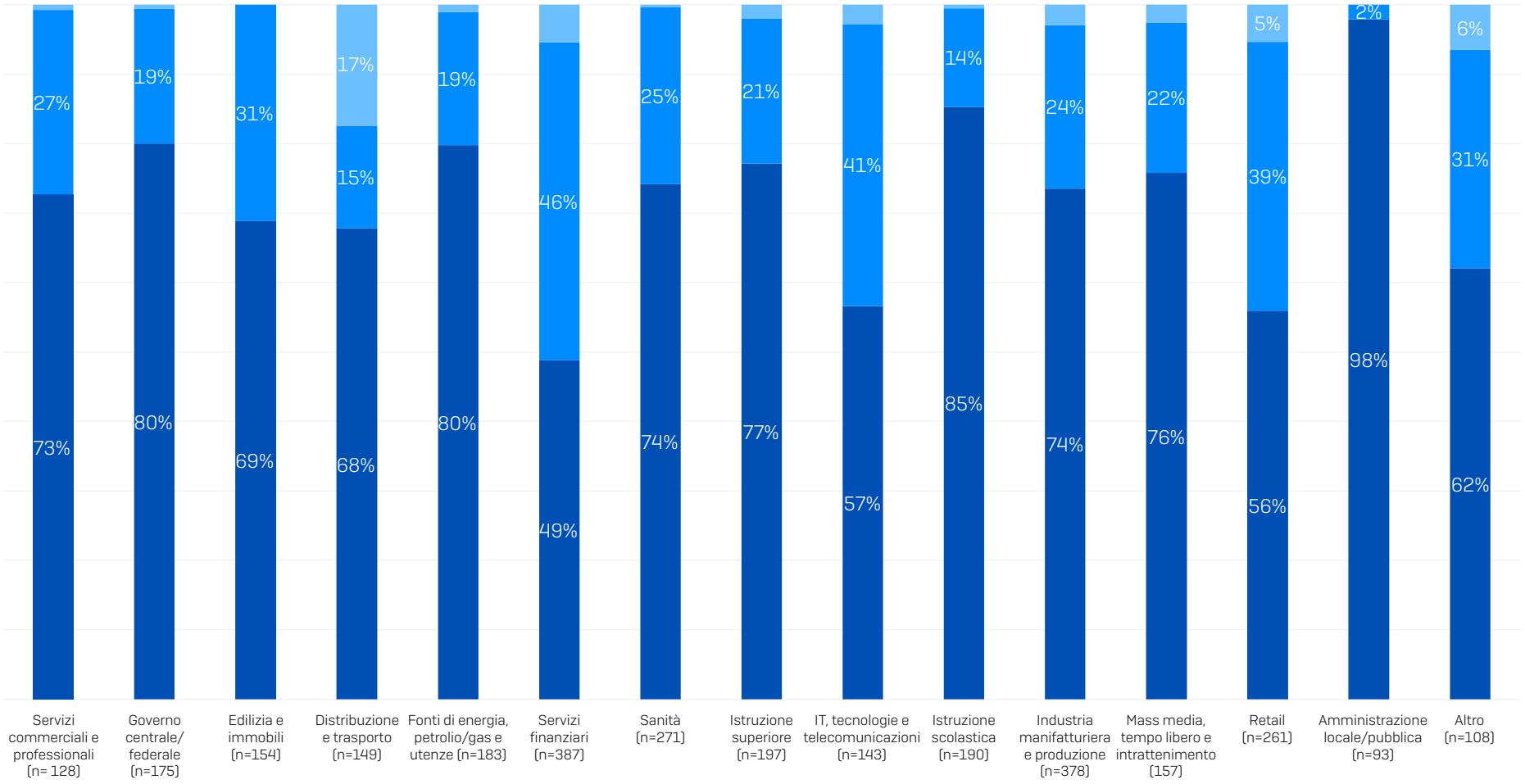
Cause All'Origine Degli Attacchi In Base Al Settore



Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? n= 2.974 organizzazioni colpite dal ransomware.

Tasso Di Crittografia Dei Dati Per Settore

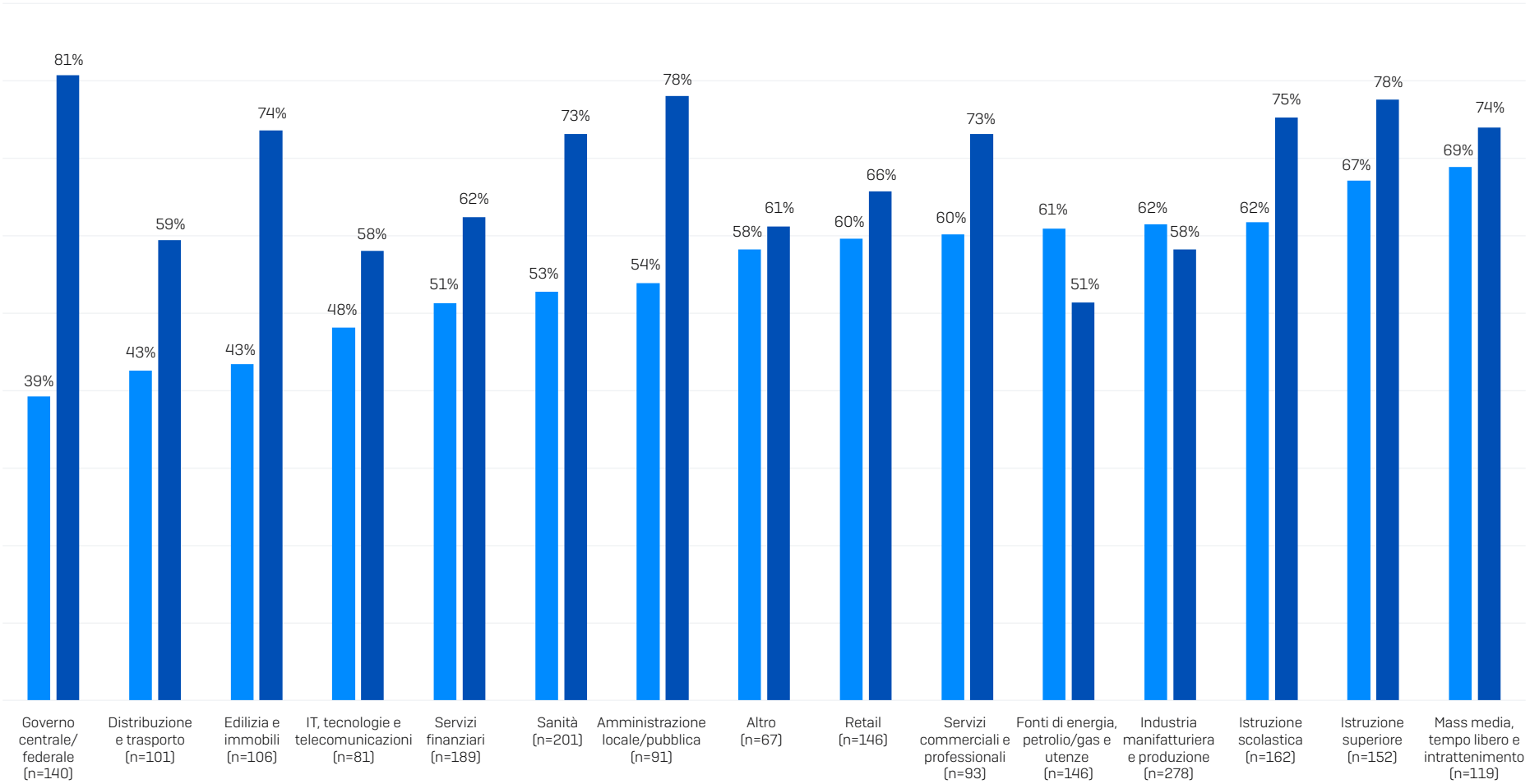
Propensione A Subire La Crittografia Non Autorizzata Dei Dati Durante Un Attacco



Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? Base di partecipanti indicata nel grafico.

Metodi Di Recupero Dei Dati Utilizzati In Base Al Settore

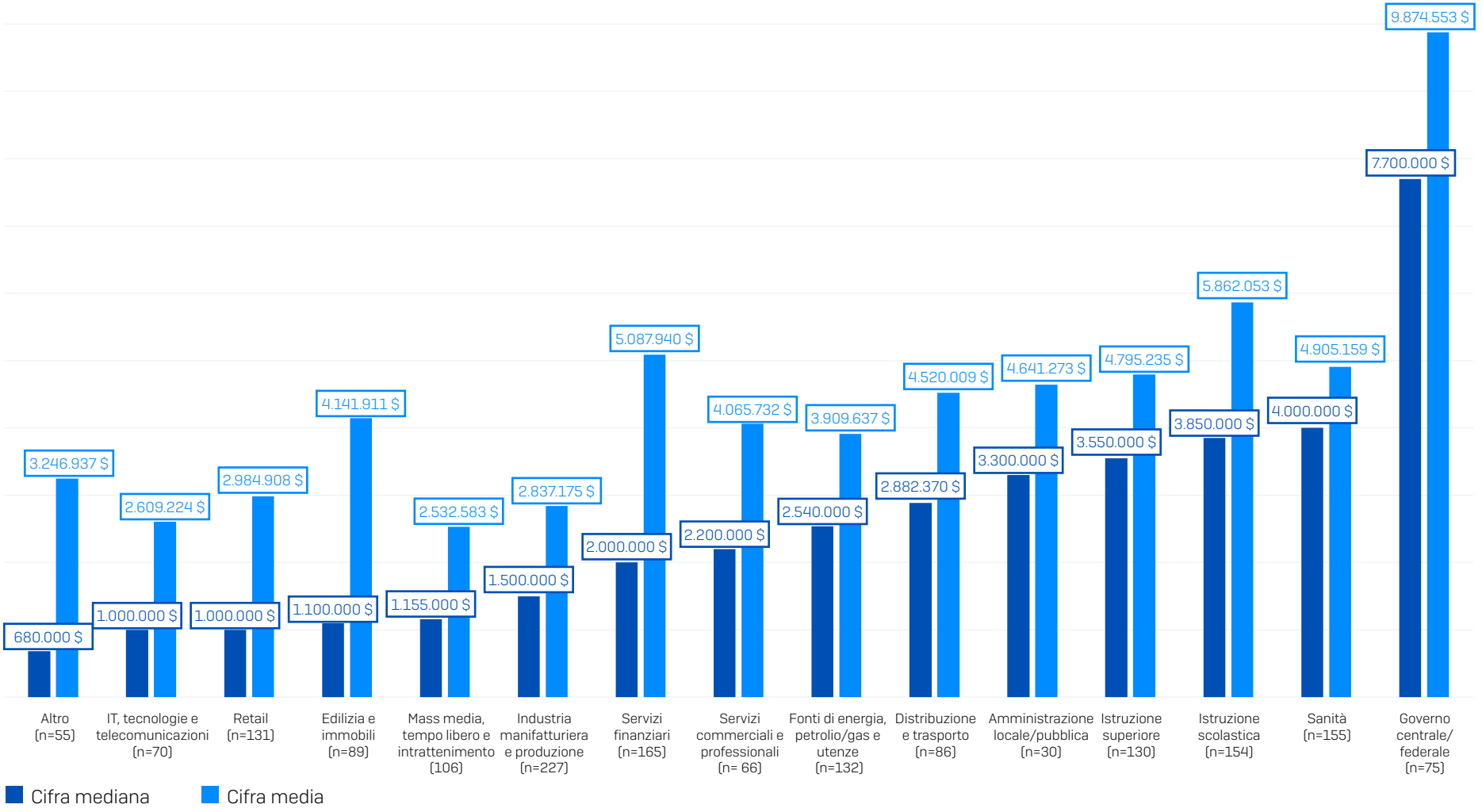
Frequenza Con Cui I Dati Sono Stati Recuperati Utilizzando I Backup E Pagando Il Riscatto



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. Risultati presentati in ordine di propensione a pagare il riscatto.

Richieste Di Riscatto In Base Al Settore

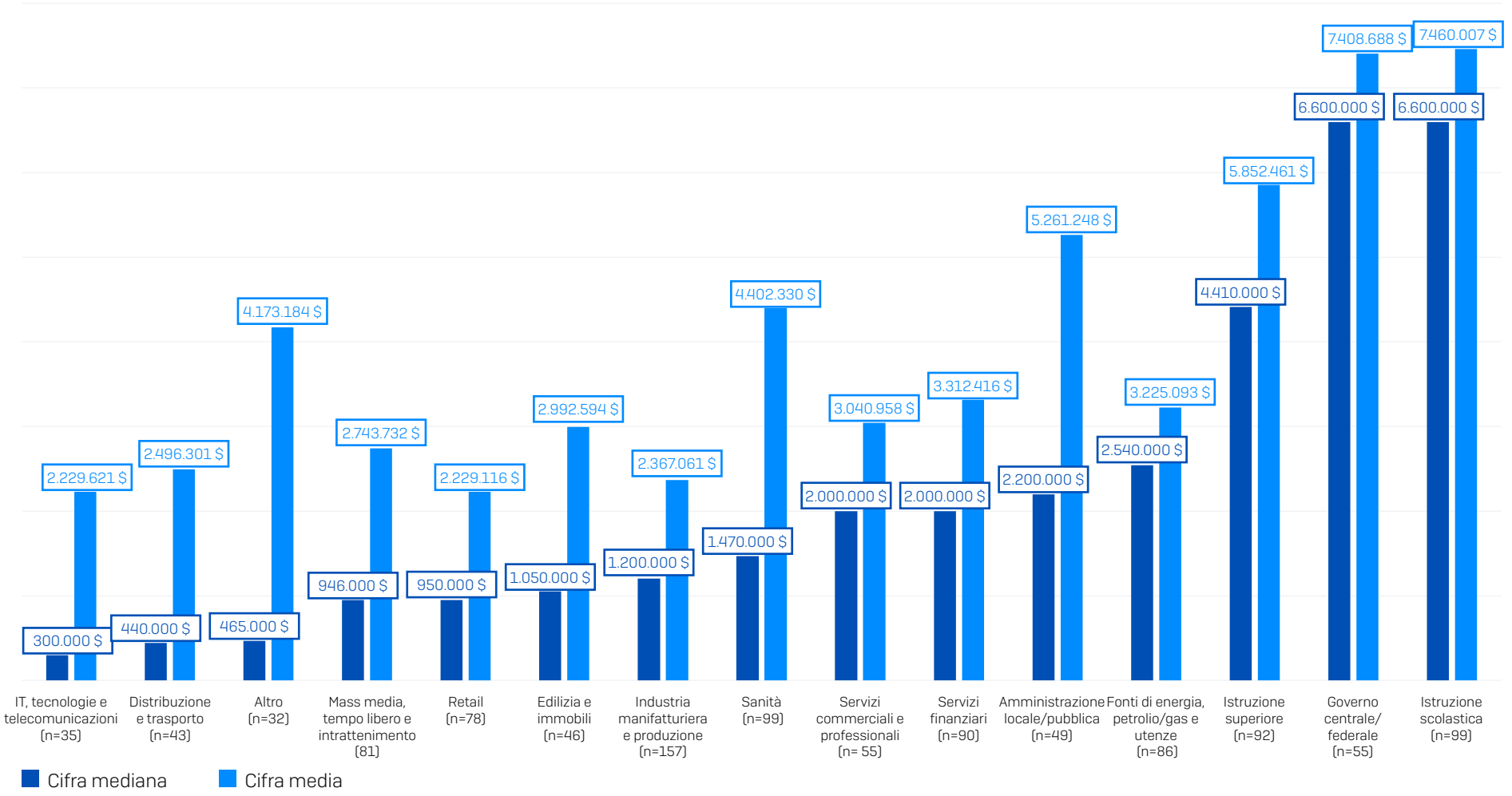
Richiesta di riscatto



A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? Base di partecipanti indicata nel grafico. Risultati presentati in ordine di richiesta mediana.

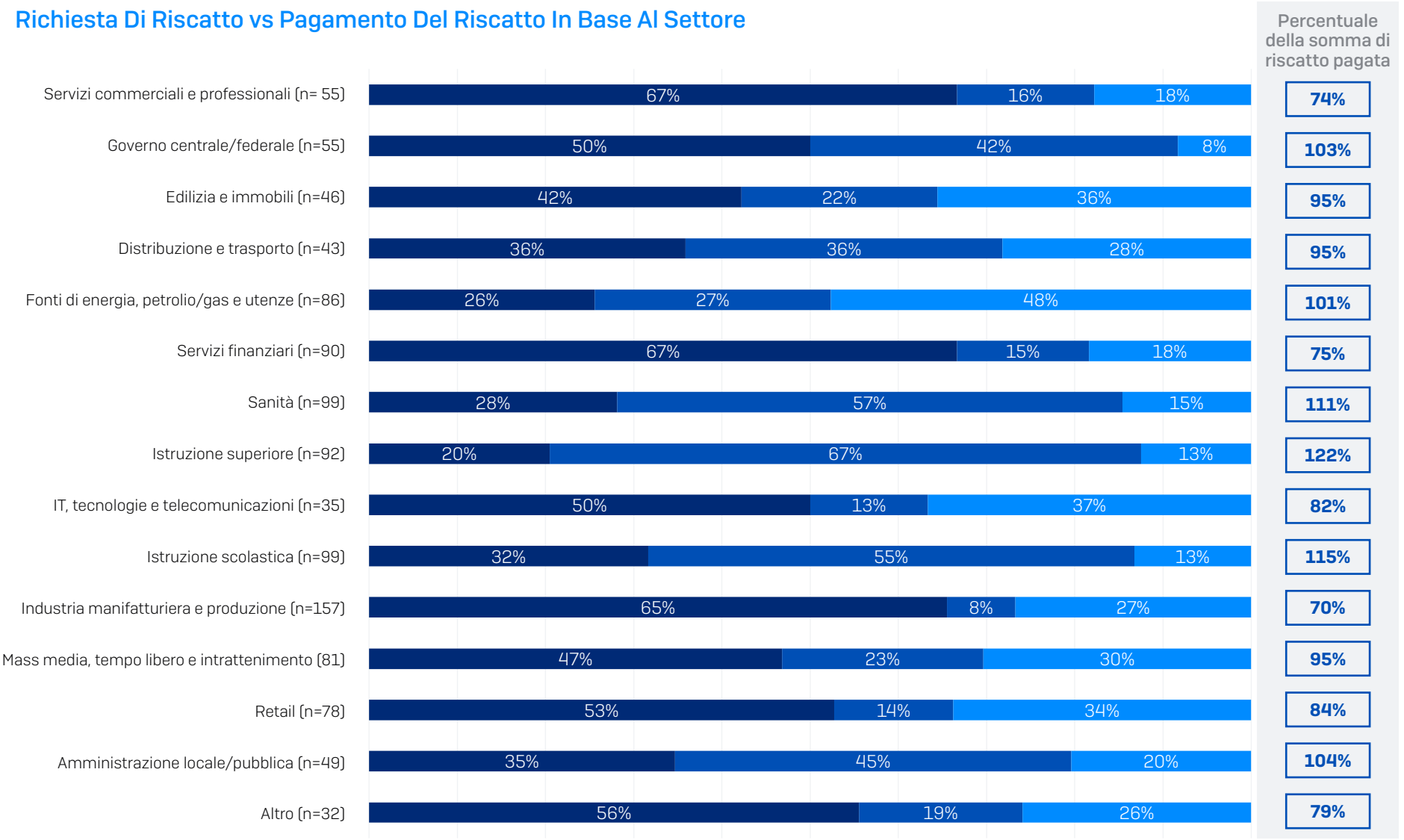
Pagamento Del Riscatto In Base Al Settore

Pagamento del riscatto



A quanto ammonta la somma di riscatto pagata ai cybercriminali? Base di partecipanti indicata nel grafico. Risultati presentati in ordine di pagamento mediano.

Richiesta Di Riscatto vs Pagamento Del Riscatto In Base Al Settore



A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? A quanto ammonta la somma di riscatto pagata ai cybercriminali? Base di partecipanti indicata nel grafico.

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.

2024-04-16 (WP-PC)

SOPHOS