SOPHOS
Cybersecurity delivered.

La Vera Storia Del Ransomware 2022

I risultati di un sondaggio indipendente e agnostico rispetto ai vendor, condotto tra 5.600 IT Manager che lavorano in organizzazioni di medie dimensioni distribuite in 31 paesi.

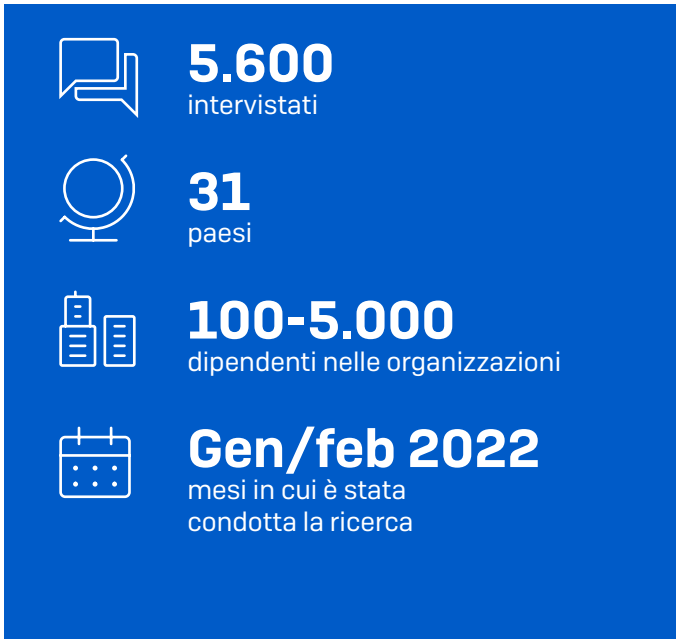
Whitepaper Sophos. Aprile 2022

Introduzione

Come ogni anno, Sophos ha condotto una ricerca sulle esperienze relative agli attacchi ransomware nel mondo reale, coinvolgendo vari professionisti dell'IT che ogni giorno affrontano queste minacce. Dallo studio è emerso che, ora più che mai, l'ambiente informatico è caratterizzato da attacchi sempre più problematici e che comportano un maggiore onere finanziario e operativo sulle loro vittime. I risultati mettono anche in luce nuovi aspetti sulla relazione tra ransomware e cyberassicurazioni, evidenziando il ruolo svolto dalle compagnie assicurative nell'evoluzione delle difese informatiche.

Informazioni sul sondaggio

Sophos ha affidato all'azienda di ricerca Vanson Bourne l'incarico di condurre una ricerca indipendente e agnostica rispetto ai vendor che ha coinvolto 5.600 IT Manager che lavorano in organizzazioni di medie dimensioni (100-5.000 dipendenti) in 31 paesi. Il sondaggio è stato svolto nei mesi di gennaio e febbraio 2022 e ai partecipanti è stato chiesto di rispondere tenendo in considerazione le proprie esperienze nell'anno precedente.

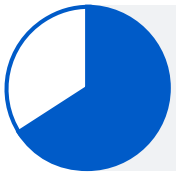


Attacchi più frequenti, con un aumento della complessità e dell'impatto

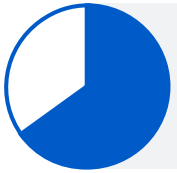
Il 66% delle organizzazioni è stato colpito dal ransomware negli ultimi 12 mesi, una percentuale molto più alta rispetto al 37% del 2020. Si tratta di un aumento del 78% in un anno, il che dimostra che i cybercriminali sono diventati molto più abili a sferrare attacchi di impatto significativo, adattandosi alle situazioni. Con molta probabilità, questa è anche una conseguenza del successo del modello del "Ransomware-as-a-Service", che estende notevolmente l'ambito di azione del ransomware, in quanto richiede meno competenze tecniche per sferrare un attacco (nota: con il termine "colpito dal ransomware" si intende uno scenario in cui l'attacco ha avuto un impatto su uno o più dispositivi, senza includere necessariamente attività di cifratura).

Gli hacker sono diventati anche più esperti a cifrare i dati durante i loro attacchi. Nel 2021 i cybercriminali sono riusciti a cifrare i dati nel 65% degli attacchi, con un aumento rispetto al 54% registrato nel 2020. Si è tuttavia osservato un calo dal 7% al 4% del numero di vittime che hanno subito un attacco di sola estorsione, nel quale i dati non sono stati cifrati, ma è stata inviata all'organizzazione una richiesta di riscatto con la minaccia di pubblicare le informazioni prelevate illecitamente.

L'aumento del numero di attacchi di ransomware andati a segno è solo uno dei molteplici fattori di un ambiente delle minacce sempre più problematico: l'anno scorso, il 57% dei partecipanti al sondaggio ha notato un incremento nel volume complessivo di attacchi informatici, il 59% ha osservato una maggiore complessità negli attacchi e il 53% sostiene di avere subito attacchi di maggiore impatto. Il 72% degli intervistati afferma di aver riscontrato un incremento in almeno uno di questi ambiti.



66%
Percentuale di organizzazioni colpite dal ransomware l'anno scorso



65%
Percentuale di attacchi nei quali sono stati cifrati i dati

72%
Percentuale di intervistati che hanno notato un aumento di volume/complessità/impatto degli attacchi informatici

Le organizzazioni migliorano la propria capacità di recuperare i dati dopo un attacco

Per contrastare la maggiore diffusione del ransomware, le organizzazioni hanno migliorato la propria capacità di gestire le conseguenze di un attacco. Quasi tutte le organizzazioni colpite dal ransomware l'anno scorso (99%) riescono ora a recuperare almeno parte dei loro dati, con un leggero aumento rispetto al 96% dell'anno precedente.

I backup sono il metodo preferito per ripristinare i dati, in quanto vengono utilizzati dal 73% delle organizzazioni che hanno subito una cifratura non autorizzata dei dati. Allo stesso tempo, il 46% degli intervistati dichiara di avere pagato il riscatto per recuperare i dati. Queste percentuali riflettono la realtà che molte organizzazioni si servono di più approcci per ripristinare i dati, al fine di ottimizzare la rapidità e l'efficacia con cui possono riprendere le operazioni. Complessivamente, quasi la metà (44%) degli intervistati la cui organizzazione aveva subito la cifratura non autorizzata dei dati ha dichiarato di avere utilizzato più di un unico metodo per recuperare i dati.

Sebbene pagare il riscatto garantisca quasi sempre il recupero di almeno parte dei dati, la percentuale di dati ripristinati dopo il pagamento è diminuita. In media, le organizzazioni che hanno pagato il riscatto sono riuscite a riavere solo il 61% dei dati, con un calo di qualche punto percentuale rispetto al 65% del 2020. Analogamente, solo il 4% delle organizzazioni che hanno pagato il riscatto è riuscito a recuperare TUTTI i dati nel 2021, con una diminuzione rispetto all'8% del 2020.

Le somme di riscatto sono aumentate

Tra i partecipanti appartenenti a organizzazioni che avevano pagato il riscatto, 965 intervistati hanno condiviso la cifra esatta, e i dati mostrano un aumento significativo rispetto all'anno precedente.

Negli ultimi 12 mesi le vittime che hanno pagato più di 1 milione di USD sono triplicate: erano infatti il 4% nel 2020, ma l'11% nel 2021. Parallelamente, la quantità di organizzazioni che hanno pagato meno di 10.000 USD è calata, passando da una su tre (34%) nel 2020 a una su cinque (21%) nel 2021.

Complessivamente, la somma media di riscatto ammonta a 812.360 USD, ovvero 4,8 volte tanto la media di 170.000 USD del 2020 (statistiche basate su 282 partecipanti). Anche se su questa cifra esorbitante hanno influito 15 pagamenti a otto cifre, dai dati emerge chiaramente che la tendenza delle somme di riscatto è in aumento a livello globale. Ci sono variazioni notevoli a seconda del settore, in quanto gli hacker esigono somme più elevate dalle aziende che ritengono più in grado di versarle:

- La media PIÙ ALTA dei pagamenti di riscatto è stata 2,04 milioni di USD nel settore dell'industria manifatturiera e della produzione (n=38) e 2,03 milioni di USD nel settore di energia, petrolio/gas e utenze (n=91)
- La media PIÙ BASSA dei pagamenti di riscatto è stata 197mila USD nella sanità (n=83) e 214mila USD nell'amministrazione locale/pubblica (n=20)

In Italia, dove i pagamenti in caso di estorsione sono vietati per legge, e dove quindi le organizzazioni non sono legalmente autorizzate a pagare il riscatto, il 43% delle organizzazioni i cui dati erano stati cifrati ammette di avere versato la somma richiesta (n=76). I risultati di questo studio dimostrano che, da sole, le barriere legislative non sono efficaci nell'impedire il pagamento dei riscatti.

3x
Incremento della quantità di organizzazioni che hanno pagato riscatti di più di 1 milione di USD

21%
Organizzazioni che hanno pagato riscatti inferiori a $ 10.000

$ 812.360
Media dei pagamenti di riscatto (escludendo le eccezioni)

INDUSTRIA MANIFATTURIERA, UTENZE
Media più alta dei pagamenti di riscatto ($ 2 milioni)

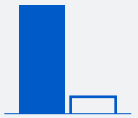
SANITÀ
Media più bassa dei pagamenti di riscatto ($ 197mila)

L'enorme impatto commerciale e operativo del ransomware

Le somme dei riscatti sono solo parte della storia e l'impatto del ransomware va ben oltre la cifratura di database e dispositivi. Il 90% dei partecipanti al sondaggio che sono stati colpiti dal ransomware l'anno scorso ha dichiarato che l'attacco più grave ha avuto ripercussioni sullo svolgimento delle loro attività. Inoltre, l'86% delle organizzazioni che operano nel settore privato ha ammesso di avere subito perdite commerciali e di fatturato a causa del ransomware.
La somma media complessiva che le organizzazioni hanno dovuto versare nel 2021 per fronteggiare l'impatto dell'attacco di ransomware più recente è stata 1,4 milioni di USD. Sebbene sia ben accetto, questo calo rispetto agli 1,85 milioni di USD del 2020 riflette probabilmente il fatto che, data la maggiore diffusione del ransomware, i danni alla reputazione causati da un attacco sono diminuiti. Allo stesso tempo, le compagnie di assicurazione sono ora in grado di fornire più velocemente migliori indicazioni alle vittime durante il processo di risposta agli incidenti, diminuendo così i costi di riparazione dei danni.
È bene notare che in molti casi nei quali viene pagato il riscatto è la compagnia di assicurazione, non la vittima, a fronteggiare le spese. Affronteremo questo argomento più avanti.

In media, le organizzazioni che hanno subito un attacco l'anno scorso hanno avuto bisogno di un mese per riprendere le attività in seguito all'attacco più grave: un periodo molto lungo per la maggior parte delle aziende. I tempi di recupero più lenti sono stati riscontrati nel settore dell'istruzione e in quello del governo centrale/federale, dove per due organizzazioni su cinque ci è voluto più di un mese. I settori con maggiore rapidità di recupero sono stati quello dell'industria manifatturiera e della produzione (il 10% ha avuto bisogno di più di un mese) e dei servizi finanziari (il 12% ha avuto bisogno di più di un mese); con molta probabilità, questo è dovuto agli elevati livelli di preparazione e pianificazione per un ripristino di emergenza.
Un altro risultato interessante è il fatto che alcune organizzazioni continuano ad affidarsi a metodi di difesa inefficaci. Tra le organizzazioni intervistate che non sono state colpite dal ransomware l'anno scorso e che prevedono che non ne cadranno vittima in futuro, il 72% giustifica questa affermazione con approcci che non prevengono gli attacchi: il 57% ha indicato i backup e il 37% le cyberassicurazioni come motivi per cui ritengono che non verranno colpite in futuro, con organizzazioni che hanno selezionato entrambe le opzioni. Anche se questi due fattori possono aiutare a riprendere le operazioni dopo un attacco, non hanno alcun impatto sulla prevenzione.

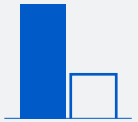
90%
Organizzazioni in cui l'attacco di ransomware ha avuto ripercussioni sullo svolgimento delle attività



86%
Organizzazioni in cui l'attacco di ransomware ha causato perdite commerciali e di fatturato

$ 1,4 M
Costo medio per la riparazione dei danni di un attacco

UN MESE
Tempo medio prima di riprendere le operazioni dopo un attacco



72%
Organizzazioni che si affidano ad approcci che non prevengono gli attacchi

Le organizzazioni non sono in grado di utilizzare budget e risorse in maniera efficace per bloccare il ransomware

Dal sondaggio è emerso che la soluzione non è semplicemente aumentare l'investimento finanziario e il personale. Occorre invece puntare su tecnologie adeguate e su persone dotate delle giuste competenze e conoscenze per usarle. Senza questi elementi, il ritorno sull'investimento sarà limitato.

Il 64% delle organizzazioni colpite dal ransomware l'anno scorso dichiara di avere a disposizione un budget di cybersecurity più alto del necessario, mentre un ulteriore 24% sostiene di avere un budget adeguato. Analogamente, il 65% delle vittime di ransomware sostiene di avere più personale di cybersecurity di quello richiesto e il 23% pensa che il numero dei propri addetti alla sicurezza sia adeguato. Questi risultati dimostrano che molte organizzazioni fanno fatica a utilizzare le proprie risorse in maniera efficiente per contrastare il rapido aumento del volume e della complessità degli attacchi.

Allo stesso tempo, i risultati sembrano anche suggerire che le organizzazioni potrebbero non rendersi conto di non avere le competenze necessarie per bloccare le nuove tecniche di attacco: il 58% degli intervistati che sono stati colpiti dal ransomware descrive la propria organizzazione come ampiamente o completamente in controllo della situazione in termini di lettura dei log per identificare segni sospetti o attività dannose, mentre il 56% si dichiara ampiamente o completamente in controllo della situazione quando si tratta di riconoscere i nuovi strumenti e metodologie di attacco.

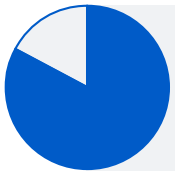
Tra le organizzazioni che non erano state colpite dal ransomware l'anno scorso e che prevedono di non caderne vittima in futuro, il motivo principale di questa certezza è la disponibilità di personale IT qualificato o di un Security Operations Center (SOC) interno in grado di bloccare gli attacchi.

L'impatto del ransomware sulle cyberassicurazioni

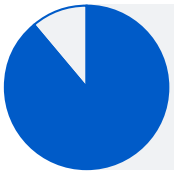
Più di quattro organizzazioni di medie dimensioni su cinque hanno sottoscritto una cyberassicurazione contro il ransomware. Tuttavia, mentre l'83% dei partecipanti al sondaggio dichiara che la propria organizzazione dispone di una cyberassicurazione che offre copertura in caso di attacco di ransomware, il 34% ammette che la polizza prevede esclusioni/eccezioni. Quello delle fonti di energia, petrolio/gas e utenze è il settore con la maggiore probabilità di stipulare una polizza (89%), seguito a distanza ravvicinata da quello della vendita al dettaglio (88%). La percentuale di intervistati con una cyberassicurazione cresce in base alle dimensioni dell'organizzazione: l'88% delle organizzazioni con 3.001-5.000 dipendenti ha stipulato una polizza, mentre solo il 73% di quelle con 100-250 dipendenti ne ha sottoscritta una.

Le organizzazioni colpite dal ransomware l'anno scorso sono caratterizzate una maggiore probabilità di sottoscrivere una cyberassicurazione rispetto a quelle che sono rimaste illese: l'89% delle prime ha infatti una polizza, mentre solo il 70% delle seconde ne ha stipulata una. Il rapporto tra causa ed effetto non è molto chiaro. Una teoria è che l'esperienza diretta di un incidente di ransomware potrebbe avere indotto molte organizzazioni a sottoscrivere una polizza assicurativa per mitigare l'impatto degli attacchi futuri. Può anche darsi che gli hacker preferiscano prendere di mira le organizzazioni coperte da una polizza assicurativa, per aumentare le proprie possibilità di ricevere un pagamento. Un'altra ipotesi potrebbe essere che alcune organizzazioni hanno stipulato una polizza per bilanciare le lacune note delle proprie difese. La risposta è probabilmente una combinazione di queste tre possibilità.

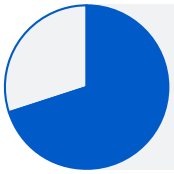
La copertura cyberassicurativa scende al 61% tra i partecipanti al sondaggio che non sono stati colpiti dal ransomware e prevedono di non caderne vittima in futuro. Poiché molti tra gli intervistati in quest'ultimo gruppo si affidano ad approcci che non sono in grado di bloccare il ransomware, la mancanza di copertura li lascia completamente esposti ai costi di un incidente.



83%
Organizzazioni con una cyberassicurazione contro il ransomware



89%
Organizzazioni colpite dal ransomware con una cyberassicurazione



70%
Organizzazioni non colpite dal ransomware con una cyberassicurazione

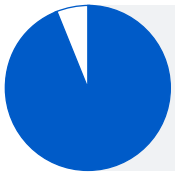
Le cyberassicurazioni influiscono sull'evoluzione delle difese informatiche

Il 94% delle organizzazioni con una cyberassicurazione dichiara che la procedura per ottenere una copertura assicurativa è cambiata negli ultimi 12 mesi.

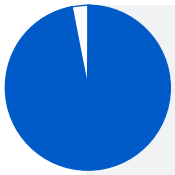
- Il 54% sostiene che il livello di cybersecurity necessario per soddisfare i requisiti di idoneità è ora più elevato
- Il 47% indica che le polizze sono ora più complesse
- Il 40% ha notato che ci sono meno compagnie di assicurazione che offrono cyberassicurazioni
- Il 37% ha osservato che il processo di approvazione richiede più tempo
- Il 34% sostiene che i costi sono aumentati

Poiché gli aumenti più significativi nei costi delle cyberassicurazioni hanno cominciato a verificarsi nel secondo e nel terzo trimestre del 2021, è probabile che molti degli intervistati non ne avessero ancora sperimentato l'impatto al momento del sondaggio.

Con l'irrigidimento del mercato delle cyberassicurazioni, e con la maggiore difficoltà nell'ottenere una copertura assicurativa, il 97% delle organizzazioni con una cyberassicurazione ha cambiato la strategia di difesa informatica per migliorare la propria posizione assicurativa. Il 64% ha implementato nuove tecnologie o servizi, il 56% ha incrementato le attività di formazione/sensibilizzazione del personale e il 52% ha cambiato procedure/comportamenti.



94%
Organizzazioni che hanno avuto più difficoltà a ottenere una copertura assicurativa l'anno scorso



97%
Organizzazioni dotate di una cyberassicurazione che hanno cambiato la strategia di difesa informatica per migliorare la propria posizione assicurativa

Indennizzi cyberassicurativi per quasi tutte le richieste causate dal ransomware

Una statistica rassicurante per chi ha sottoscritto una polizza assicurativa è il fatto che il 98% delle organizzazioni colpite dal ransomware che avevano una cyberassicurazione con copertura in caso di ransomware ha dichiarato di avere ricevuto un indennizzo per l'attacco più grave: una percentuale in aumento rispetto al 95% del 2019. In alcuni paesi, il tasso di pagamento degli indennizzi è stato del 100%: Svizzera (n=52), Messico (n=131), Svezia (n=68), Belgio (n=66), Polonia (n=75), Turchia (n=51), EAU (n=49), India (n=218) e Singapore (n=91).

Esaminando i dettagli di questi indennizzi, il sondaggio rivela un aumento delle somme elargite per i costi di rimozione del ransomware e una diminuzione dei pagamenti di riscatto da parte delle compagnie di assicurazione. Il 77% delle persone intervistate afferma che la compagnia di assicurazione ha pagato i costi di rimozione del ransomware, ovvero i costi necessari per far sì che l'organizzazione potesse riprendere le operazioni, con un incremento rispetto al 67% del 2019. C'è invece stato un calo nel numero di partecipanti al sondaggio che indicano che la compagnia di assicurazione ha pagato il riscatto: il 40%, a differenza del 44% nel 2019.

Il tasso di pagamento del riscatto, tuttavia, varia notevolmente a seconda del settore. Le percentuali più alte sono state riscontrate nell'istruzione secondaria (asili, scuole primarie e secondarie) (53%), nell'amministrazione pubblica/locale (49%) e nella sanità (47%); quelle più basse si sono osservate nel settore dell'industria manifatturiera e della produzione (30%) e in quello dei servizi finanziari (32%). È interessante osservare che i settori con le percentuali più basse in termini di pagamento del riscatto sono anche quelli in grado di rimediare più velocemente ai danni di un incidente, il che enfatizza l'importanza della preparazione e della pianificazione di un ripristino di emergenza.

Bisogna anche ricordare che, sebbene possano essere di aiuto per il ripristino dei sistemi allo stato originario, le cyberassicurazioni non offrono possibilità di "miglioramento", ovvero non coprono gli investimenti in tecnologie superiori e servizi per rimediare alle vulnerabilità che hanno causato l'attacco.

98%
Tasso di pagamento per le richieste di indennizzo dovute al ransomware

△ Pagamento dei costi di rimozione del ransomware △

67% 2019

77% 2021

▽ Pagamento del riscatto ▽

44% 2019

40% 2021

Conclusione

Il ransomware rappresenta una sfida sempre più ardua per le organizzazioni. Il numero di organizzazioni colpite direttamente da un attacco è quasi raddoppiato negli ultimi 12 mesi, passando da poco più di un terzo nel 2020 a due terzi nel 2021.

Per far fronte alla quasi completa normalizzazione di questo fenomeno, le organizzazioni hanno migliorato la propria capacità di gestire le conseguenze di un attacco: ora infatti riescono praticamente in ogni caso a recuperare almeno parte dei dati cifrati e in quasi tre quarti degli incidenti sono in grado di utilizzare i backup per ripristinare i dati.

Tuttavia, allo stesso tempo la percentuale dei dati recuperati dopo il pagamento di un riscatto è in calo, con una media del 61%. Nonostante questo, la quantità di vittime che hanno pagato riscatti che superano $ 1 milione è quasi triplicata.

Dal sondaggio è emerso che la soluzione non è semplicemente aumentare l'investimento finanziario e il personale. Occorre invece puntare su tecnologie adeguate e su persone dotate delle giuste competenze e conoscenze per usarle. Il nostro consiglio per le organizzazioni è collaborare con esperti in grado di aiutarle a potenziare il ritorno sul loro investimento nella cybersecurity, incrementandone l'efficacia dei sistemi di difesa.

Nella maggior parte dei casi, le organizzazioni scelgono di mitigare il rischio finanziario legato agli attacchi sottoscrivendo una polizza cyberassicurativa.

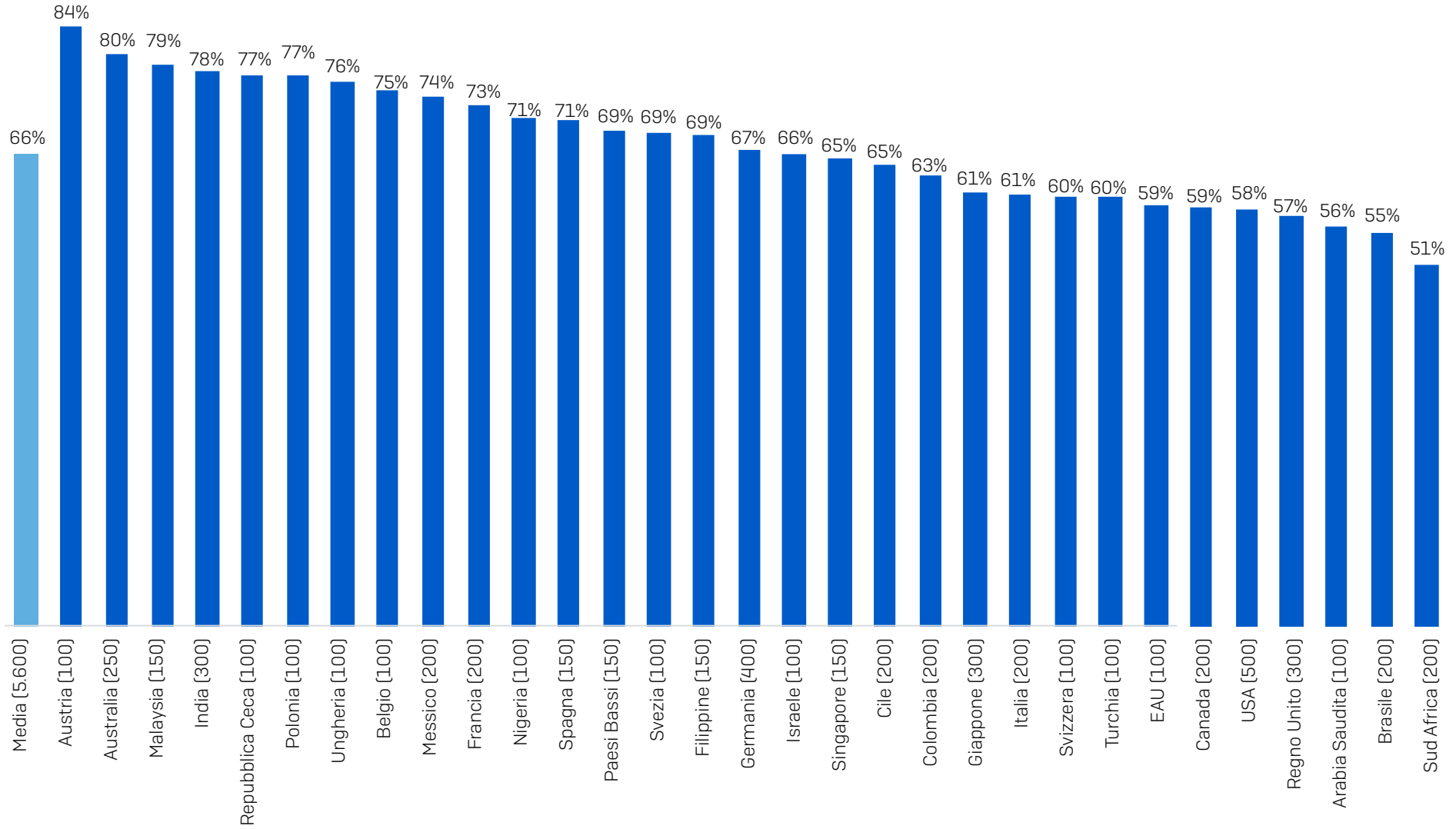
Per chi adotta questo approccio, è rassicurante osservare che le compagnie di assicurazione tendono a coprire almeno parte dei costi per quasi tutte le richieste di indennizzo. Tuttavia, ottenere una copertura assicurativa sta diventando sempre più difficile, e questo ha indotto la quasi totalità delle organizzazioni a cambiare la strategia di difesa informatica per migliorare la propria posizione assicurativa.

Sia che si desideri stipulare una polizza assicurativa o meno, potenziare la propria cybersecurity è ormai un must per tutte le organizzazioni. I nostri cinque consigli principali sono:

- Implementare difese di elevata qualità in ogni parte del proprio ambiente informatico. Verificare i controlli di sicurezza, per assicurarsi che continuino a soddisfare le proprie esigenze.
- Svolgere attività di individuazione proattiva delle minacce, per bloccare i cybercriminali prima che possano sferrare un attacco. In caso di mancanza di tempo o personale esperto, ci si può rivolgere a specialisti di Managed Detection and Response (MDR) esterni.
- Potenziare la sicurezza dell'ambiente, individuando e risolvendo le vulnerabilità di sicurezza, ovvero: i dispositivi a cui mancano patch, i computer non protetti, le porte RDP aperte ecc. Le soluzioni di Extended Detection and Response (XDR) sono ideali per svolgere questi tipi di attività.
- Prepararsi al peggio. Bisogna sapere esattamente cosa fare e chi contattare in caso di incidente informatico.
- Effettuare backup e svolgere esercitazioni di ripristino da questi backup. L'obiettivo è cercare di riprendere rapidamente le operazioni, con tempi di inattività minimi.

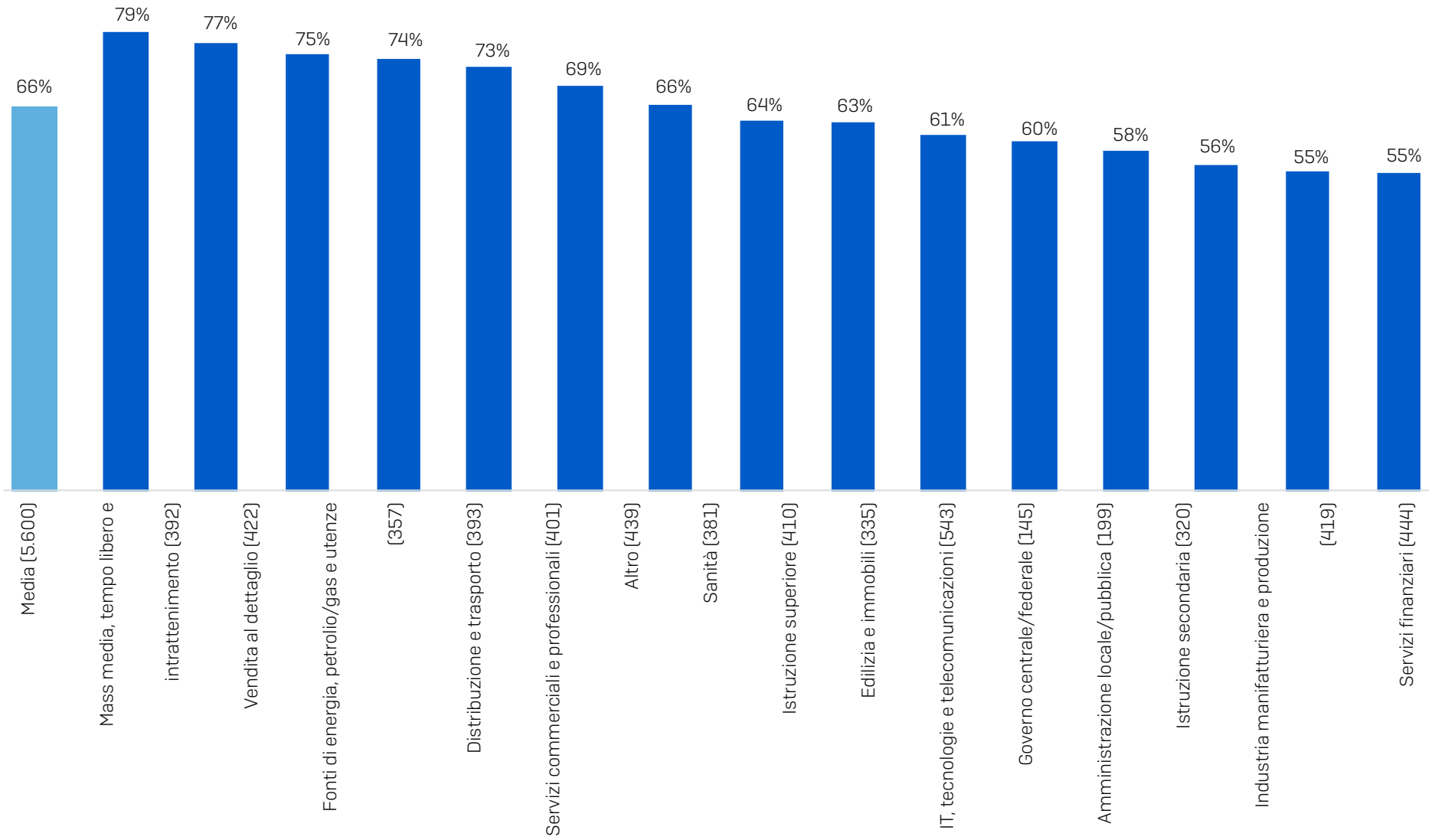
Per informazioni dettagliate sulle singole gang di ransomware, visita il Centro di intelligence Sophos sul ransomware.

Percentuale di organizzazioni colpite dal ransomware l'anno scorso



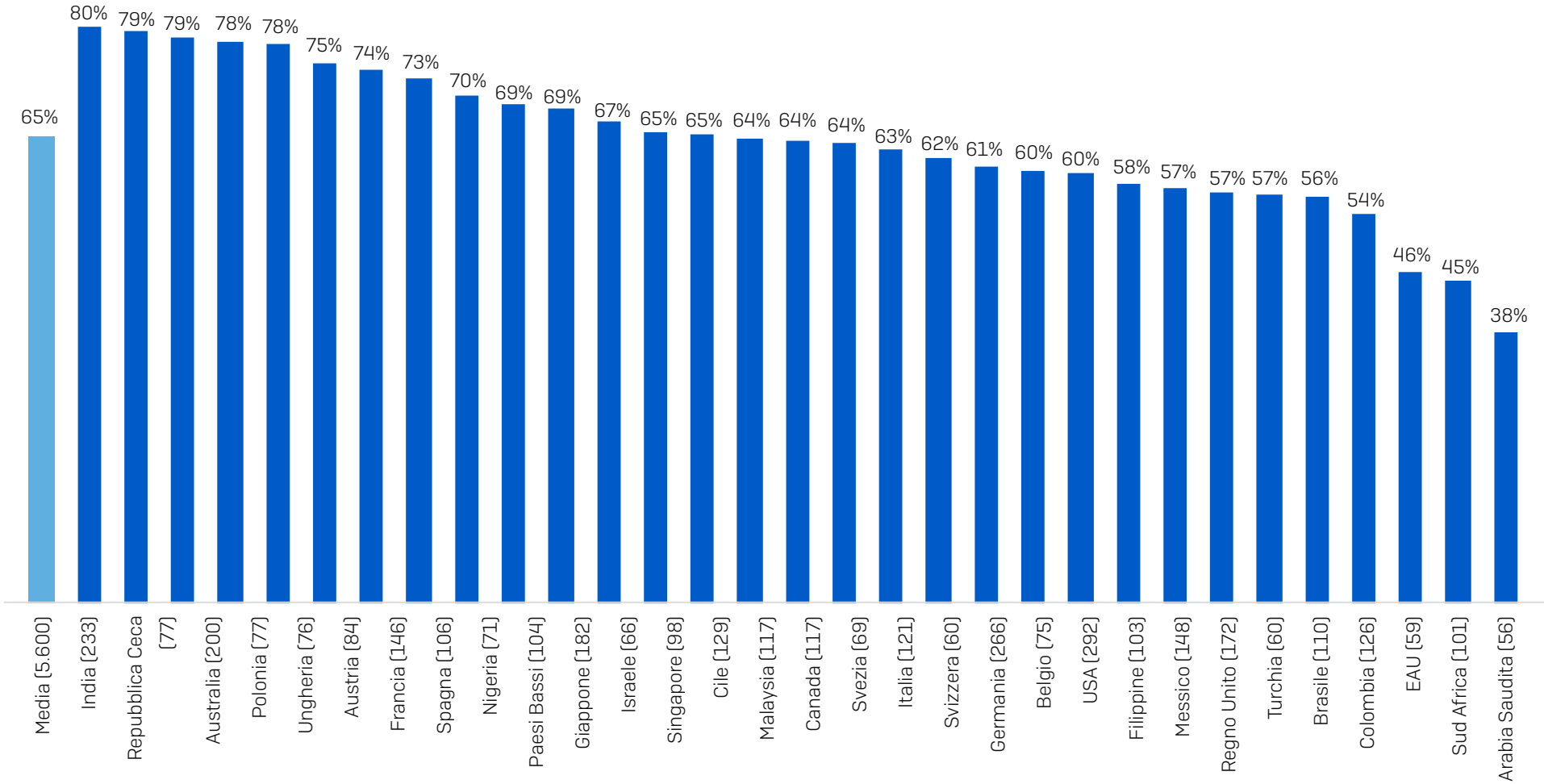
La tua organizzazione è stata colpita dal ransomware l'anno scorso? (n=5.600): Sì

Percentuale di organizzazioni colpite dal ransomware l'anno scorso



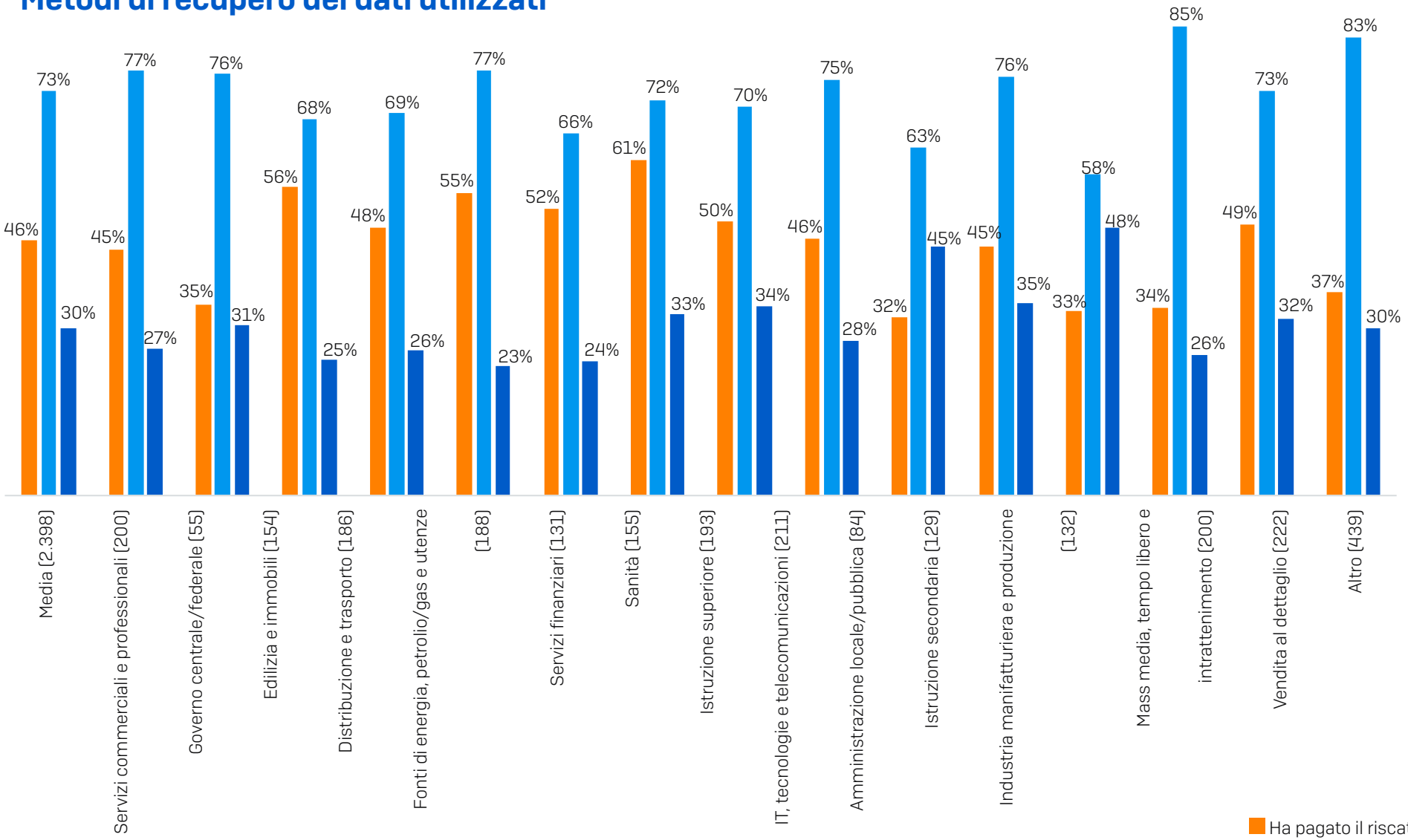
La tua organizzazione è stata colpita dal ransomware l'anno scorso? (n=5.600): Sì

Tasso di cifratura negli attacchi di ransomware



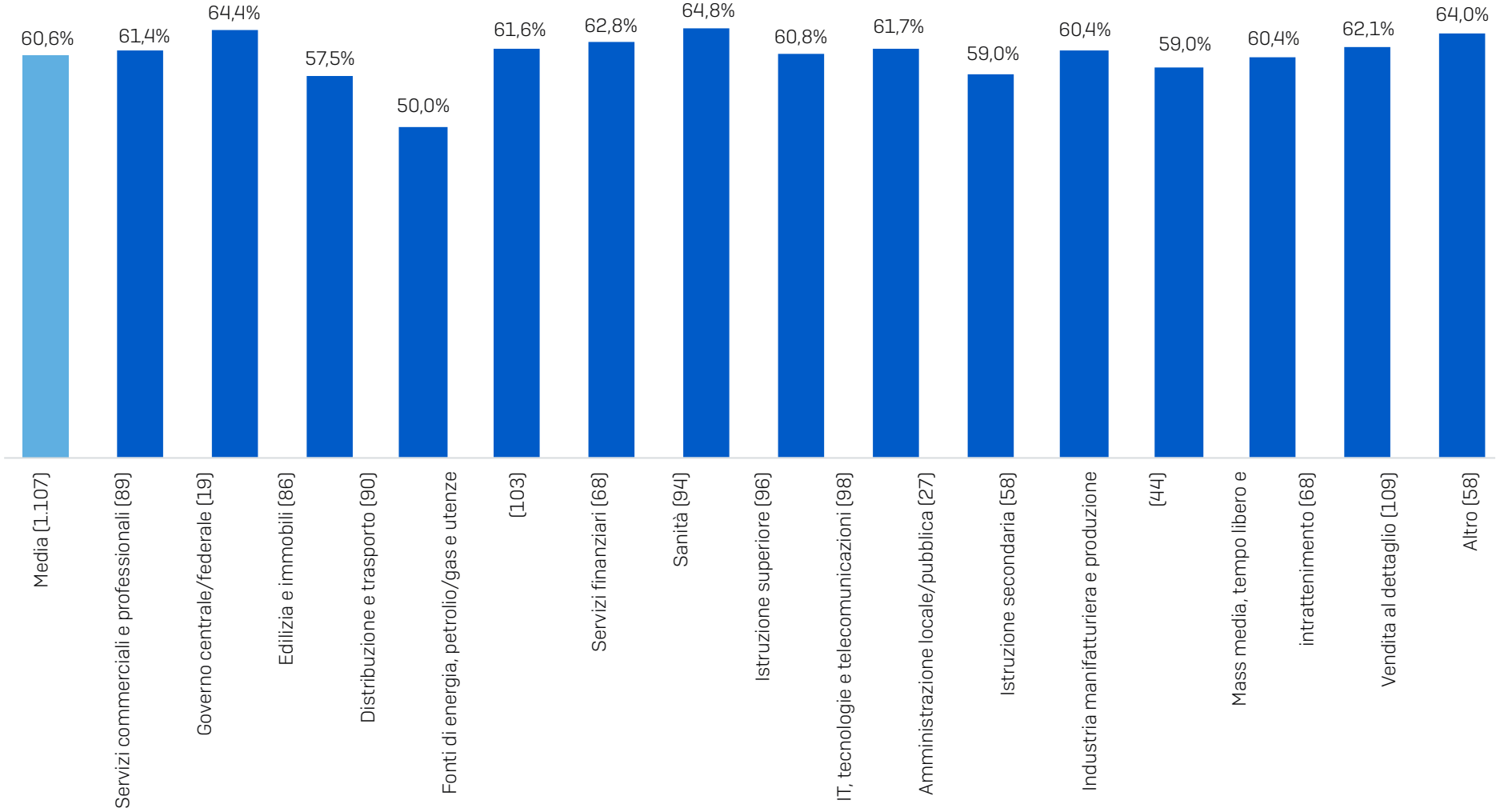
Nell'attacco di ransomware più grave, i cybercriminali sono riusciti a cifrare i dati dell'organizzazione? (n=3.702 organizzazioni colpite dal ransomware l'anno scorso): Sì

Metodi di recupero dei dati utilizzati



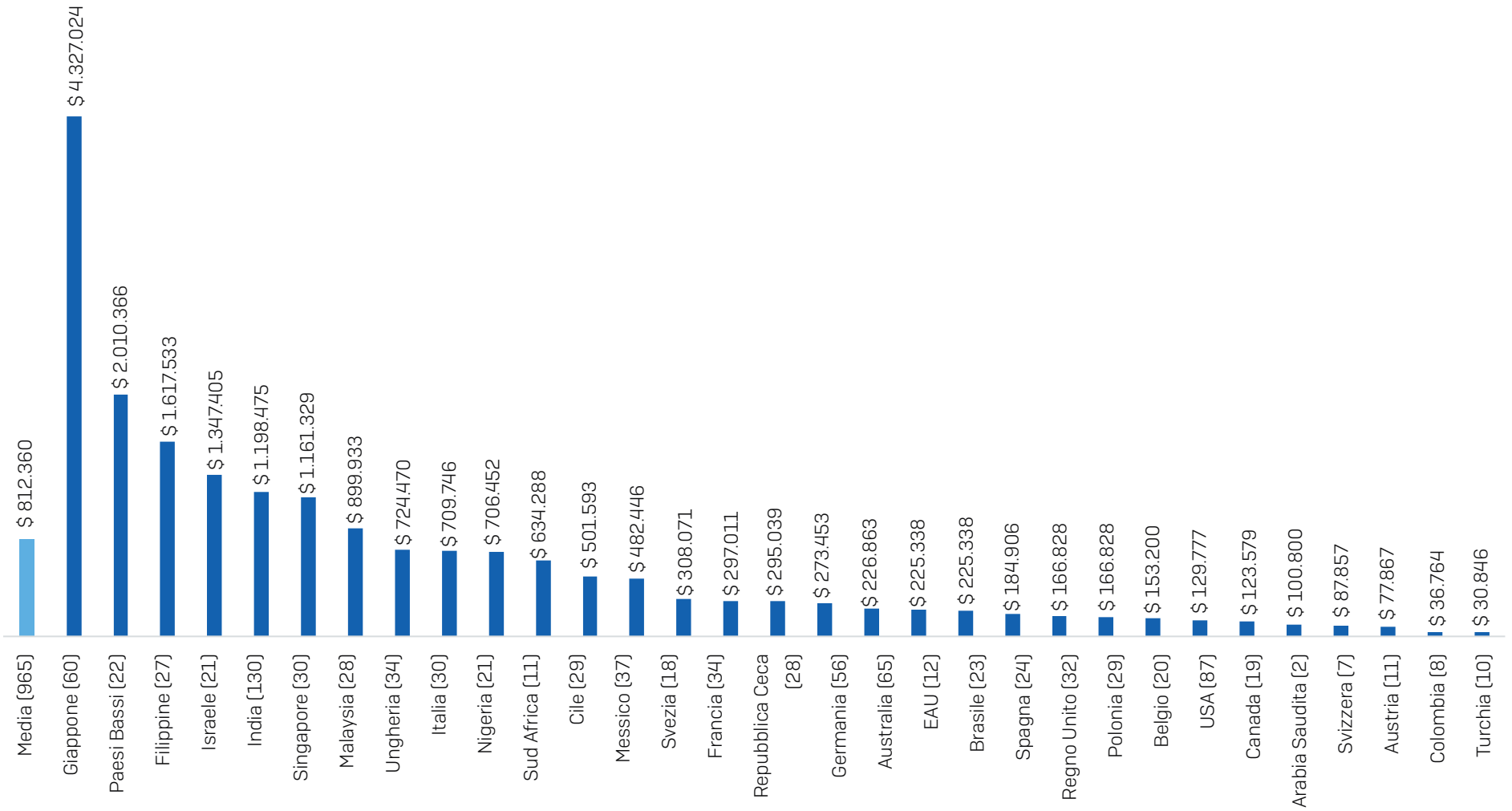
Nell'attacco di ransomware più grave, la tua organizzazione ha recuperato almeno parte dei dati? (n=2.398 organizzazioni che avevano subito la cifratura dei dati): Sì, abbiamo pagato il riscatto e recuperato i dati; Sì, abbiamo utilizzato i backup per ripristinare i dati; Sì, abbiamo usato altri metodi per recuperare i dati.

Percentuale di dati recuperati dopo aver pagato riscatto



Quanti dati della tua organizzazione è stato possibile recuperare in seguito all'attacco di ransomware più grave?
(n= 1.107 organizzazioni che hanno pagato il riscatto e hanno recuperato i propri dati)

Media dei pagamenti di riscatto in base al paese



A quanto ammonta la somma di riscatto pagata dalla tua organizzazione nell'attacco di ransomware più grave? USD. Base di partecipanti indicata nel grafico. Le risposte "Non lo so" e le eccezioni sono state omesse.

Nota: per i paesi con basi di partecipanti limitate, i risultati sono da considerarsi puramente indicativi.

Costo medio sostenuto dalle organizzazioni per la riparazione dei danni dell'attacco (milioni di USD)

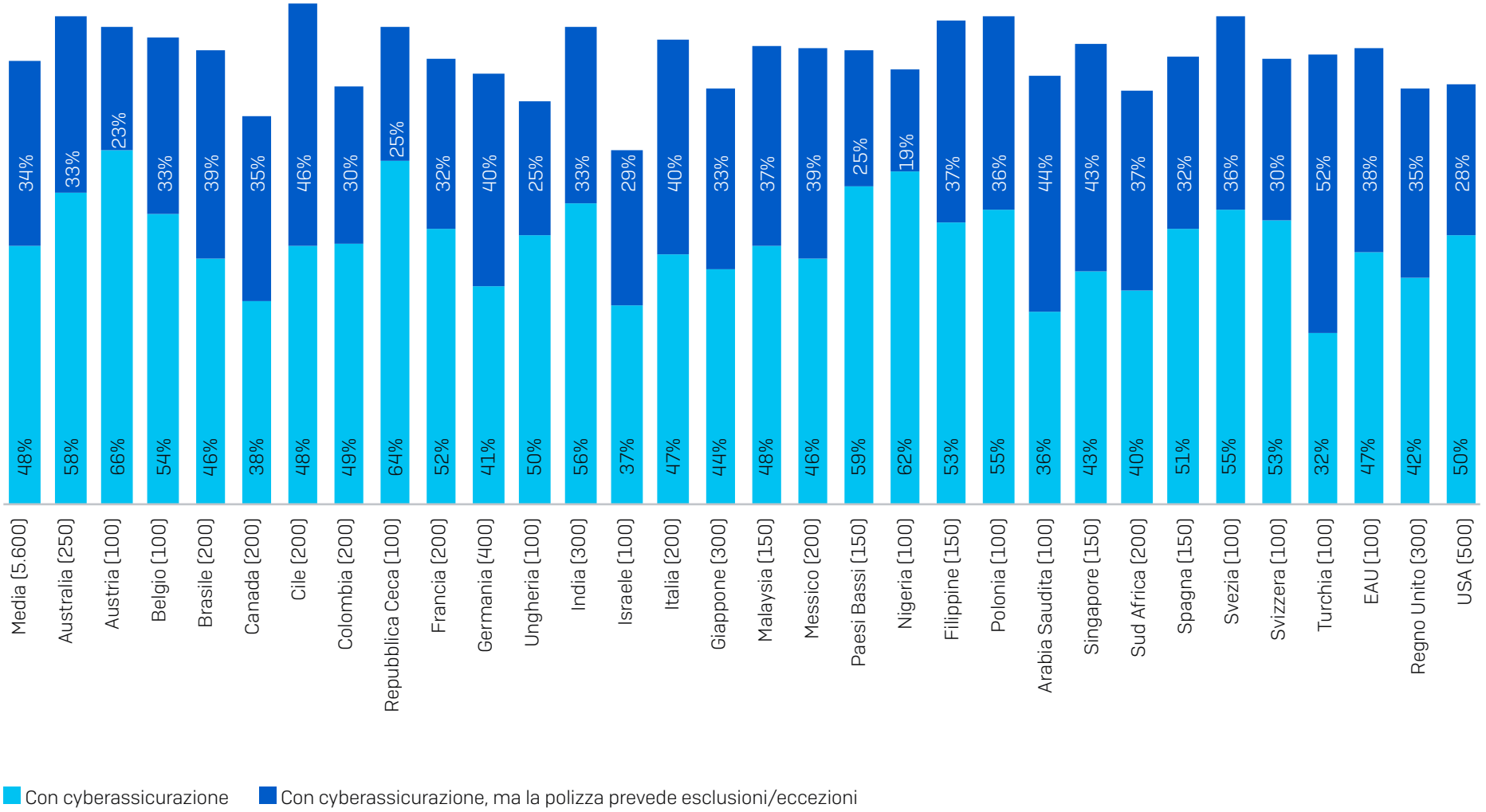
Paese	2021	2020	Cambiamento annuo
Media (3.702)	$ 1,40	$ 1,85	-24%
Australia (200)	$ 1,01	$ 1,84	-45%
Austria (84)	$ 0,81	$ 7,75	-90%
Belgio (75)	$ 3,71	$ 4,75	-22%
Brasile (110)	$ 0,69	$ 0,82	-16%
Canada (117)	$ 0,65	$ 1,92	-66%
Cile (129)	$ 1,58	$ 0,73	116%
Colombia (126)	$ 0,50	$ 1,26	-60%
Repubblica Ceca (77)	$ 2,58	$ 0,37	589%
Francia (146)	$ 2,03	$ 1,11	83%
Germania (266)	$ 1,73	$ 1,17	48%
Ungheria (76)	$ 1,51	n/a	n/a
India (233)	$ 2,81	$ 3,38	-17%
Israele (66)	$ 1,41	$ 0,57	148%
Italia (121)	$ 1,65	$ 0,68	141%

Paese	2021	2020	Cambiamento annuo
Giappone (182)	$ 0,96	$ 1,61	-40%
Malaysia (118)	$ 1,22	$ 0,77	58%
Messico (148)	$ 0,88	$ 2,03	-57%
Paesi Bassi (104)	$ 0,98	$ 2,71	-64%
Nigeria (71)	$ 3,43	$ 0,46	644%
Filippine (103)	$ 1,34	$ 0,82	63%
Polonia (77)	$ 1,78	n/a	n/a
Arabia Saudita (56)	$ 0,65	$ 0,21	212%
Singapore (98)	$ 1,91	$ 3,46	-45%
Sud Africa (101)	$ 0,71	n/a	n/a
Spagna (106)	$ 0,75	$ 0,60	25%
Svezia (69)	$ 0,75	$ 1,40	-46%
Svizzera (60)	$ 1,64	$ 1,43	15%
Turchia (60)	$ 0,37	$ 0,58	-36%
EAU (59)	$ 1,26	$ 0,52	144%
Regno Unito (172)	$ 1,08	$ 1,96	-45%
USA (292)	$ 1,08	$ 2,09	-49%

Nota: le basi di partecipanti si riferiscono solo ai dati del 2021.
Nota: i valori sono espressi in milioni di USD.

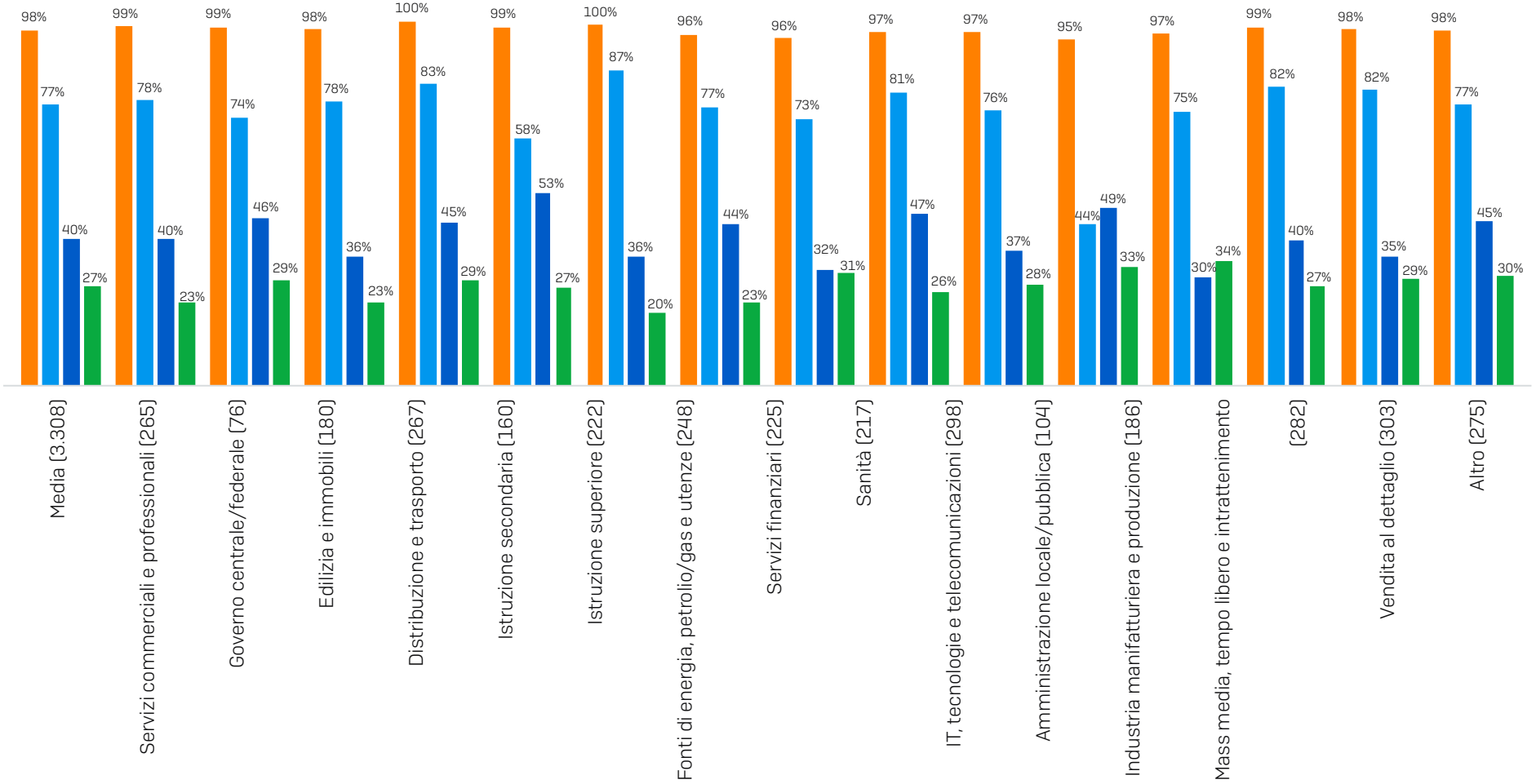
Qual è stato approssimativamente il costo sostenuto dall'organizzazione per rimediare ai danni provocati dall'attacco di ransomware più recente (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali, somma pagata per il riscatto ecc.)? (n=3.702 organizzazioni che erano state colpite dal ransomware l'anno precedente)

Percentuale di organizzazioni con una copertura cyberassicurativa



La tua organizzazione ha stipulato una polizza cyberassicurativa che la tutelerebbe se dovesse essere colpita dal ransomware? (n=5.600). Sì; Sì, ma la polizza prevede eccezioni/esclusioni

Tasso di pagamento di un indennizzo da parte delle cyberassicurazioni



La compagnia di assicurazione ha coperto i costi associati al più grave attacco di ransomware subito dalla tua organizzazione? (n=3.308 organizzazioni che erano state colpite dal ransomware l'anno precedente e che avevano una polizza assicurativa contro il ransomware). Sì, ha coperto i costi di rimozione del ransomware (ovvero i costi necessari per far sì che l'organizzazione potesse riprendere le operazioni); Sì, ha pagato il riscatto; Sì, ha coperto altri costi (ad es. i costi legati ai tempi di inattività, alla perdita di opportunità ecc.)

Scopri di più sul ransomware e su come Sophos può aiutarti a proteggere la tua organizzazione.

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.

04/04/2022 (WP-NP)

SOPHOS