

Proteggere il presente e il futuro

20 considerazioni sulla cybersecurity per il 2020



Include
contenuti
esclusivi
per l'Italia

**Vedere
pagina 23**

Sommario

Introduzione	3
20 considerazioni sulla cybersecurity per il 2020	4
1. Nella tua azienda chi si occupa di fornire supporto ai dirigenti e stabilire obiettivi chiari?	4
2. Come si può stabilire quali sono i parametri più importanti?	5
3. Quali sono le considerazioni principali di cui tenere conto con un budget limitato?	6
4. Qual è la corretta ripartizione della spesa tra verifica di affidabilità e rilevamento delle minacce?	8
5. Cosa può suggerire la misurazione dell'impatto delle violazioni della sicurezza sull'azienda?	9
6. Perché la divulgazione volontaria delle violazioni è sempre maggiore?	11
7. È possibile quantificare i vantaggi della collaborazione tra networking e sicurezza?	11
8. Oltre alla riduzione dei costi, quali sono secondo te i motivi alla base dell'outsourcing?	11
9. Secondo te la preparazione ha i suoi vantaggi?	13
10. Quanto è importante applicare le patch per la difesa dalle violazioni?	13
11. Cosa provoca l'interruzione dell'operatività?	14
12. Quanto è difficile proteggere la forza lavoro mobile?	14
13. Come si può estendere la sicurezza zero trust per proteggere le applicazioni?	14
14. La difesa dell'infrastruttura di rete rappresenta ancora una sfida?	16
15. È possibile misurare l'impatto del consolidamento dei fornitori?	17
16. A cosa sono dovuti cyber fatigue e stress informatico?	18
17. Quali vantaggi per la sicurezza sono associati all'infrastruttura di hosting nel cloud?	19
18. Secondo te quali sfide tiene in serbo il futuro?	20
19. Quanta attenzione si deve porre alla reazione agli incidenti?	21
20. Cosa puoi fare ora per migliorare la tua postura della sicurezza?	22
21. I danni di un attacco informatico in Italia	23
Proteggere il presente e il futuro	26
Cisco Cybersecurity Report Series	27

Introduzione

I responsabili della sicurezza, pur sostenendo la crescita del business e la trasformazione digitale, si trovano ad affrontare diverse sfide. Lo sappiamo perché ce lo racconti, sia durante le normali conversazioni che nell'ambito del nostro sondaggio comparativo annuale. Alcune sfide sono incentrate sulla sicurezza, come la necessità di migliorare la visibilità o l'automazione o la ricerca di una maggiore semplicità in termini di gestione e risposta. Alcune sono legate al successo della tua azienda, come il desiderio di promuovere la crescita e la trasformazione indipendentemente dall'applicazione cloud necessaria o dal dispositivo mobile utilizzato. Altre sfide riguardano la necessità di compiere adesso investimenti che saranno importanti in futuro quando la tua azienda cambierà.

E tutto questo va a sommarsi alle esigenze del lavoro quotidiano, come il rilevamento e il blocco delle minacce avanzate. È difficile gestire contemporaneamente criminali informatici sofisticati e la sempre maggiore vulnerabilità agli attacchi. Non si deve semplicemente riuscire a fare di più con un budget limitato, occorre anche mantenere la reputazione del marchio, la fiducia degli azionisti e degli amministratori, reclutare competenze per scoprire tattiche, tecniche e procedure di attacco informatico (TTP), per citare solo alcuni esempi.

Si deve fornire agli utenti l'accesso di cui hanno bisogno e affrontare nel contempo queste sfide in termini di sicurezza, complessità e budget. È inoltre necessario ridurre le spese per la tecnologia, evitare violazioni importanti, individuare le minacce prima che si infiltrino nella rete ed esfiltrare i dati, utilizzare il budget per la sicurezza in maniera più intelligente ed acquisire più clienti.

Secondo il Forum economico mondiale, gli attacchi informatici sono considerati il secondo rischio globale che causa preoccupazione tra i responsabili aziendali nelle economie avanzate, preceduto solo dalle crisi fiscali.¹

Con il nostro sesto sondaggio annuale su 2.800 responsabili delle decisioni IT provenienti da 13 paesi, abbiamo proseguito l'annuale tradizione di esaminare a fondo la situazione per redigere statistiche di confronto.² Abbiamo anche discusso a lungo con un gruppo di CISO per analizzare i risultati e creare un elenco di 20 considerazioni per il 2020. Questo report fornisce preziosi consigli e dati che potrai condividere con gli altri dirigenti o amministratori per formulare raccomandazioni concrete finalizzate al miglioramento della postura della sicurezza della tua azienda. Per l'Italia abbiamo intervistato un campione di 200 specialisti in ambito cybersecurity per un totale di 200 aziende.

Sappiamo bene che in questo settore nulla è certo tranne l'incertezza e pertanto abbiamo concepito le sezioni di questo report come domande che potresti porti mentre ti prepari per l'anno a venire. Se queste domande in qualche modo ti rappresentano o stimolano ulteriori approfondimenti, ci farebbe piacere ricevere la tua opinione all'indirizzo security-reports@cisco.external.com. Nel frattempo speriamo che il report ti aiuti a superare le sfide di sicurezza che incontrerai nel corso di quest'anno.

Per visualizzare tutti i report della nostra Cybersecurity Report Series, visita: cisco.com/go/securityreports.

¹ " [This is what CEOs around the world see as the biggest risks to business](#) ", Forum economico mondiale, 2019

² I paesi presi in esame sono Australia, Brasile, Canada, Cina, Francia, Germania, India, Italia, Giappone, Messico, Spagna, Regno Unito e USA.

20 considerazioni sulla cybersecurity per il 2020

1. Nella tua azienda chi si occupa di fornire supporto ai dirigenti e stabilire obiettivi chiari?

Nel corso degli anni, con il nostro sondaggio abbiamo analizzato quattro procedure critiche per promuovere un rapporto reciprocamente vantaggioso tra i dirigenti e l'organizzazione di sicurezza. Questo esercizio valuta le acquisizioni in termini di sicurezza dall'alto in basso, laddove abbiamo riscontrato una leggera tendenza verso il basso rispetto all'anno precedente. Analizzando questi risultati:

- L'89% degli intervistati ha affermato che i **dirigenti considerano ancora la sicurezza una priorità elevata**, ma questa percentuale si riduce leggermente (7%) nel corso dei quattro anni precedenti. In Italia la percentuale è del 86% con una diminuzione del 16% rispetto all'anno precedente.
- La percentuale di aziende che **hanno definito ruoli e responsabilità in materia di sicurezza del proprio management** è oscillata parecchio negli ultimi anni, arrivando quest'anno all'89%, 87% per l'Italia. Tenendo conto della sempre maggior rilevanza del tema della cybersecurity e dell'estrema necessità di responsabili della sicurezza in posizioni di alto profilo, la definizione di ruoli e responsabilità deve rimanere prioritaria.
- L'integrazione delle valutazioni dei rischi informatici nei processi generali di gestione del rischio è diminuita del 5% rispetto all'anno scorso, ma è ancora alta con il 91% degli intervistati che afferma di farne uso e il 90% per l'Italia.
- Anche se con una percentuale inferiore del 6% rispetto all'anno precedente, la definizione da parte del management di parametri chiari per stabilire l'efficacia dei programmi di sicurezza è ancora piuttosto elevata, con il 90% degli intervistati che afferma di praticarla a livello globale e 89% in Italia.

Negli ultimi quattro anni queste percentuali hanno registrato un leggero calo, il che può indicare: 1) che l'ambito di responsabilità in materia di sicurezza sta cambiando, 2) che la comunicazione con il management non è chiara come una volta, 3) che il management ha altre priorità, o 4) che CISO e dirigenti stanno ridiscutendo i parametri applicati.

E anche se in calo, si tratta di percentuali ancora molto elevate. Il motivo potrebbe essere il fatto che, pur essendo diventata operativa, la sicurezza ha bisogno di farsi sentire maggiormente nella "stanza dei bottoni". **La presenza di percentuali ancora molto elevate è indicativa di un rapporto solido e continuativo tra dirigenti e professionisti della sicurezza.**

sono molte le modalità di implementazione della leadership. Il ruolo di un CISO è quello di parlare con i responsabili per dimostrare che una sicurezza ben progettata darà valore all'azienda.

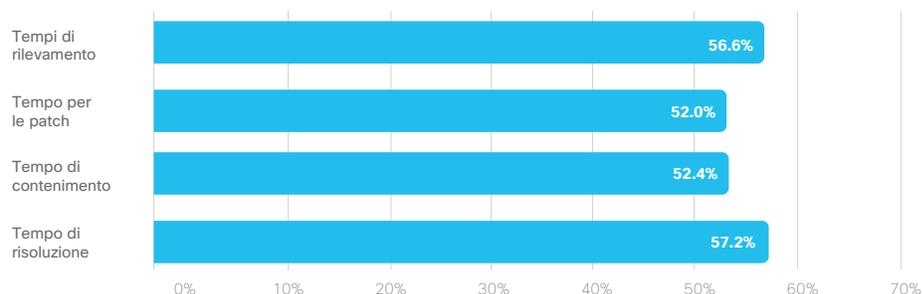
Mick Jenkins MBE, CISO per la Brunel University di Londra

2. Come si può stabilire quali sono i parametri più importanti?

Come abbiamo appena puntualizzato, il 90% a livello globale e 89% in Italia degli intervistati afferma che i dirigenti della propria azienda hanno definito parametri chiari per valutare l'efficacia del programma di sicurezza. Definire parametri chiari è un'attività essenziale per un modello di sicurezza e non è facile mettere d'accordo dirigenti e team di sicurezza su come misurare i miglioramenti operativi e gli esiti a livello di sicurezza.

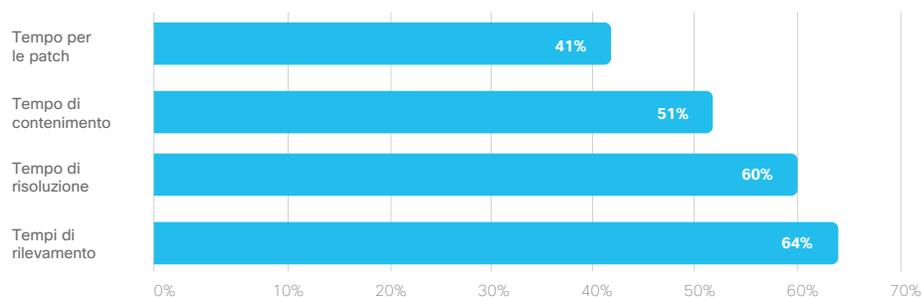
Secondo i responsabili delle decisioni IT che hanno risposto al nostro sondaggio, **i tempi di rilevamento sono al primo posto come indicatore di prestazioni chiave (KPI). Tuttavia, se parliamo di dirigenti o del Consiglio di amministrazione, il tempo di risoluzione si piazza in posizione analoga** poiché rappresenta l'impatto totale che può includere: interruzione dell'operatività del sistema, record interessati, costo dell'indagine, perdite di fatturato, clienti persi, opportunità svanite e costi imprevisti (Figura 1). In Italia è invece l'opposto il time to remediate per il 67% delle aziende viene usato per misurare le performance mentre nel reporting verso il board è il time to detect per 64% delle aziende. Può anche essere una variabile proxy dell'efficacia complessiva dell'organizzazione IT, poiché le misure correttive possono richiedere parecchia collaborazione tra i vari reparti.

Figura 1: Variabili utilizzate per segnalare internamente una violazione di forte impatto ai dirigenti o al Consiglio di amministrazione (N=2800). Le percentuali sono arrotondate.



Fonte: Sondaggio comparativo sui CISO 2020 di Cisco

Figura A: Metriche usate dalle aziende italiane per mostrare l'efficacia di un piano di sicurezza verso il consiglio di direzione.

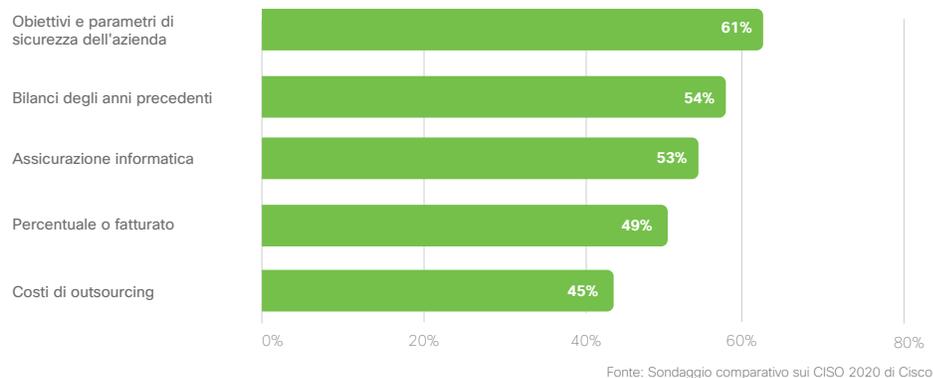


Dati: 200 aziende italiane intervistate

3. Quali sono le considerazioni principali di cui tenere conto con un budget limitato?

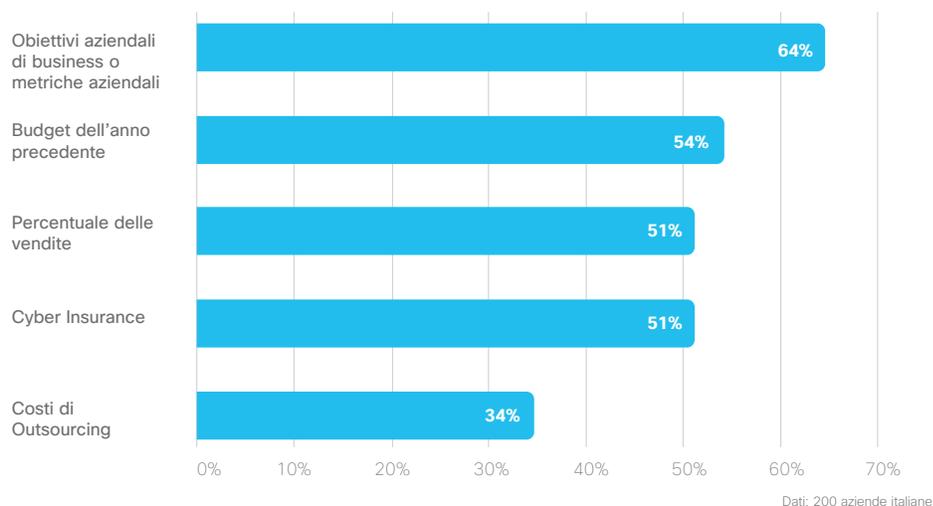
A livello globale e in Italia, ci è stato detto che il modo migliore per assegnare la spesa per la sicurezza è attraverso obiettivi e parametri basati sui risultati. Il 61% utilizza questo metodo di pianificazione e 64% in Italia, con un aumento del 10% a livello globale rispetto all'anno precedente e una tendenza incoraggiante (Figura 2).

Figura 2: Cosa utilizzano le aziende per stabilire e/o controllare la spesa per la sicurezza (N=2799). Le percentuali sono arrotondate.

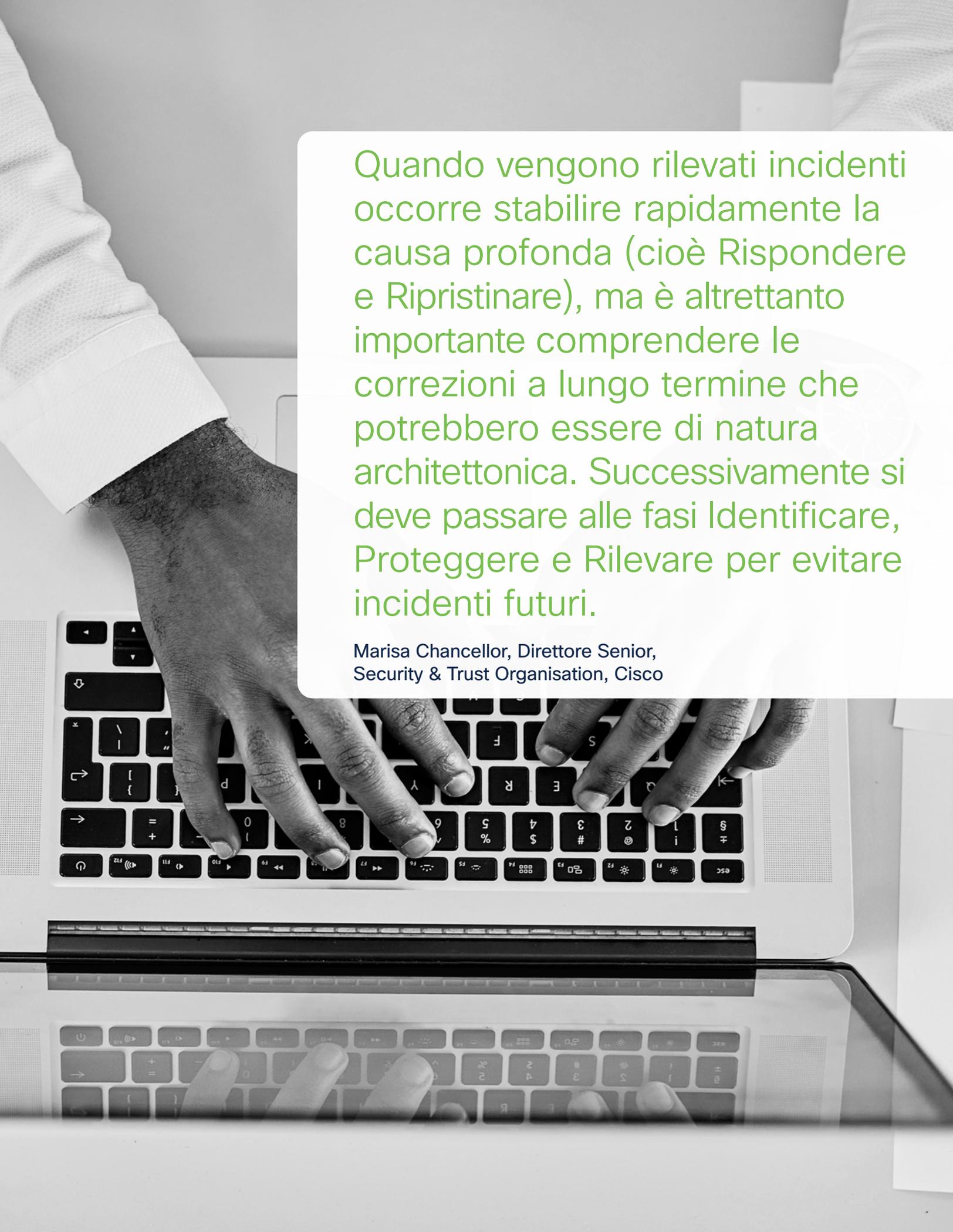


"Percentuale del fatturato" e "costi di outsourcing" sono stati indicati come i fattori meno utilizzati per stabilire i budget di sicurezza. Il 54% calcola la spesa in base al budget degli anni precedenti. Anche se potrebbe non sembrare un modo preciso per quantificare i costi di sicurezza, soprattutto quando si tiene raramente conto del costo medio di una violazione dei dati (3,92 milioni di dollari), se il budget è costantemente basso o se si hanno abbonamenti SaaS programmati, il budget previsto probabilmente cambierà pochissimo.³

Figura B: Criteri usati dalle aziende italiane per determinare e controllare il budget di cybersecurity.



³ [2019 Cost of a Breach Report](#), Ponemon Institute



Quando vengono rilevati incidenti occorre stabilire rapidamente la causa profonda (cioè Rispondere e Ripristinare), ma è altrettanto importante comprendere le correzioni a lungo termine che potrebbero essere di natura architettonica. Successivamente si deve passare alle fasi Identificare, Proteggere e Rilevare per evitare incidenti futuri.

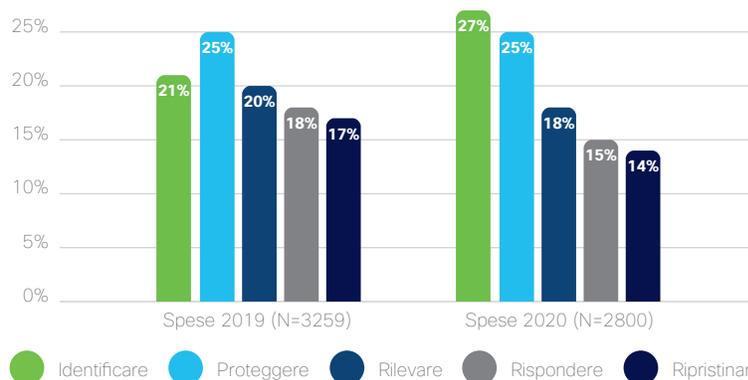
Marisa Chancellor, Direttore Senior,
Security & Trust Organisation, Cisco

4. Qual è la corretta ripartizione della spesa tra verifica di affidabilità e rilevamento delle minacce?

A livello globale esplorando il modo in cui vengono spesi i budget di sicurezza, abbiamo posto domande ai nostri intervistati su cinque categorie (Identificare, Proteggere, Rilevare, Rispondere e Ripristinare) che descrivono il ciclo di vita della difesa di cybersecurity e della gestione delle violazioni:

- **La categoria Identificare** ha registrato un aumento della spesa dal 21% al 27% dal 2019 al 2020
- **Proteggere e Rilevare** sono rimaste sostanzialmente uguali, rispettivamente al 25% e al 18%
- **La spesa nelle categorie Rispondere e Ripristinare** è diminuita di poco nello stesso lasso di tempo, passando rispettivamente al 15% e al 14%

Figura 3: Spesa per la sicurezza per categoria del ciclo di vita. Le percentuali sono arrotondate.



Fonte: Sondaggio comparativo sui CISO 2020 di Cisco

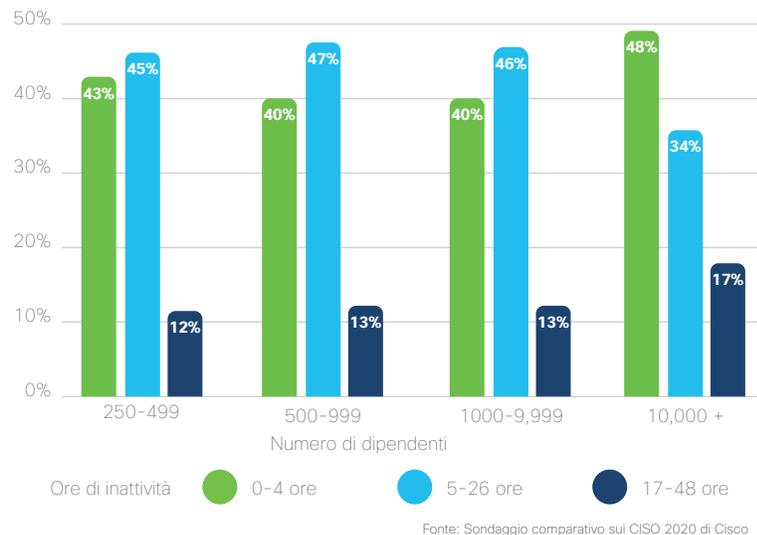
Questa tendenza mostra che le **aziende spendono di più nella prevenzione rispetto alla risposta** per quanto riguarda la loro postura della cybersecurity. Le imprese sono alla costante ricerca del giusto equilibrio tra proattività e reattività e resilienza, e l'ago della bilancia oscilla avanti e indietro ogni anno. Lo scorso anno le aziende potrebbero aver concentrato i propri sforzi sugli aspetti basilari (inventario delle risorse, ricerca, ecc.). In teoria, se si spende il giusto per identificare, proteggere e rilevare in anticipo, non si dovrebbe spendere altrettanto per rispondere e ripristinare perché risultano meno necessari.

5. Cosa può suggerire la misurazione dell'impatto delle violazioni della sicurezza sull'azienda?

Nel nostro sondaggio abbiamo posto domande su diverse conseguenze delle violazioni, tra cui interruzione dell'operatività, record e finanze.

In che misura le aziende subiscono tempi di inattività derivanti da violazioni gravi? Abbiamo confrontato aziende di dimensioni diverse e i risultati sono stati globalmente molto simili. Le grandi aziende (10.000 o più dipendenti) hanno maggiori probabilità di subire tempi di inattività più brevi (0-4 ore) poiché avranno a disposizione più risorse per rispondere all'evento e ripristinare l'operatività. Le aziende medio-piccole prevalgono nell'intervallo di ripristino di 5-16 ore, mentre interruzioni disastrose di 17-48 ore caratterizzano analogamente in misura ridotta imprese di ogni dimensione (Figura 4).

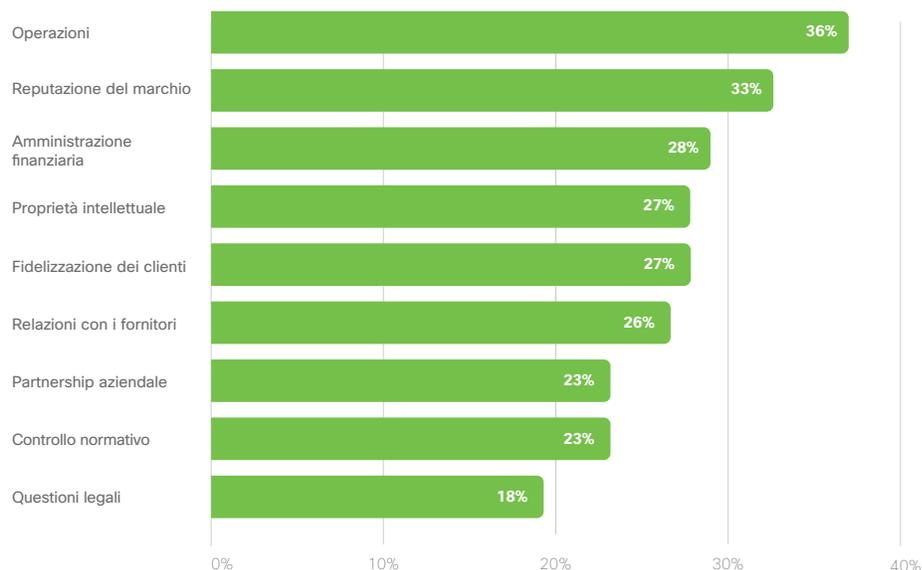
Figura 4: Per la violazione di sicurezza più grave gestita nell'ultimo anno, numero di ore in cui i sistemi sono stati inattivi correlato alle dimensioni dell'azienda (N=2265). Le percentuali sono arrotondate.



Le aziende con oltre 100.000 record interessate dalla violazione dei dati più grave sono aumentate dal 15% dell'anno scorso a oltre il 19% quest'anno.

Inoltre, come mostrato nella Figura 5, una violazione grave può influire su nove aree critiche di un'azienda. **Le aree di business più colpite sono state le operazioni e la reputazione del marchio**, seguite da finanze, proprietà intellettuale e fidelizzazione dei clienti.

Figura 5: Percentuali di intervistati che riferiscono di aree di business colpite negativamente da una violazione (N=2121). Le percentuali sono arrotondate.



Fonte: Sondaggio comparativo sui CISO 2020 di Cisco

Osservando gli anni precedenti, il numero di intervistati che hanno subito un contraccolpo alla **reputazione del marchio da violazioni gravi è salito dal 26% al 33% in tre anni**. Il numero di chi riferisce un impatto sulle operazioni è rimasto stabile tra il 36 e il 38% degli intervistati. Inoltre, il numero di chi riferisce un impatto sulle finanze è diminuito di un solo punto percentuale all'arco negli ultimi tre anni, rimanendo quindi relativamente stabile. Con l'aumento dell'impatto sul marchio globale, è **fondamentale includere la pianificazione delle comunicazioni anticrisi nel piano generale di reazione agli incidenti**.

Nel capitolo I danni di un attacco informatico in Italia vi è un approfondimento dedicato all'Italia su questo capitolo.

6. Perché la divulgazione volontaria delle violazioni è sempre maggiore?

Con il 61%, la percentuale di intervistati che ha riferito di aver volontariamente divulgato una violazione l'anno scorso è al massimo nei quattro anni precedenti⁴. Ciò dimostra che, in generale, le aziende stanno segnalando in modo proattivo le violazioni, forse a causa di una nuova legislazione o forse per una maggior consapevolezza sociale e per un desiderio di mantenere la fiducia dei clienti.

Il vantaggio è che più del doppio del numero di aziende che hanno subito una violazione della durata di oltre 17 ore ha divulgato la violazione volontariamente rispetto a quelle che hanno divulgato la violazione involontariamente o a causa di richieste di segnalazione.

Oltre metà delle violazioni (51%) ha messo le aziende sulla difensiva, dovendo gestire il giudizio del pubblico che arriva dopo un evento di questo genere. Tuttavia, mentre le richieste di segnalazione da parte dei governi sono aumentate, la divulgazione involontaria rimane ampiamente identica per poco più di un quarto (27%) delle violazioni. **Inoltre, il 61% degli intervistati sta scoprendo ora che la loro credibilità aumenta quando rivelano volontariamente una violazione grave: in questo modo viene preservata la reputazione del marchio.**

7. È possibile quantificare i vantaggi della collaborazione tra networking e sicurezza?

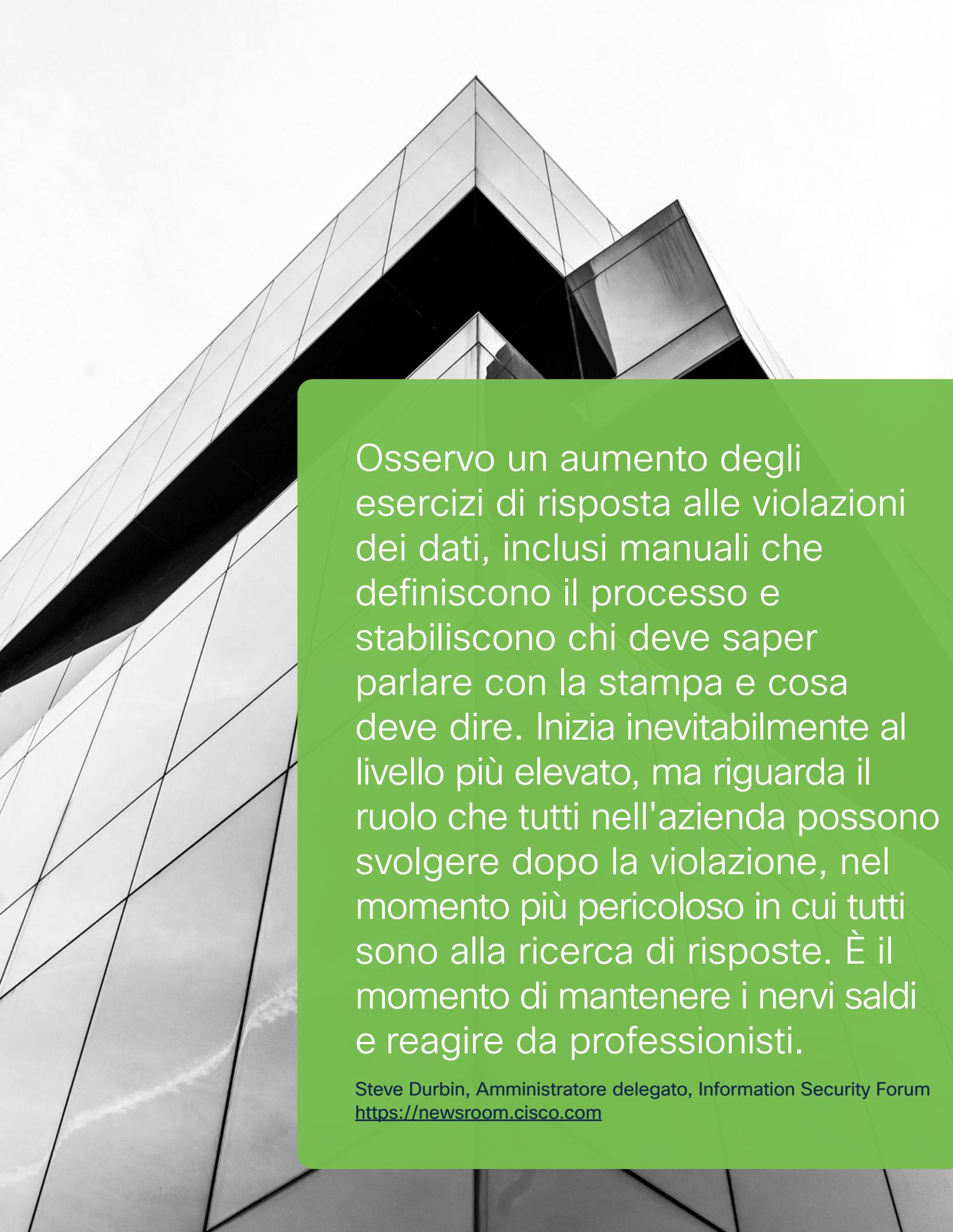
La collaborazione tra la **rete e i team di sicurezza rimane elevata** con oltre il 91% degli intervistati, 95% in Italia, che riferiscono di essere molto o estremamente collaborativi nel sondaggio di quest'anno. Anche la collaborazione tra gli **endpoint e i team di sicurezza rimane elevata con una percentuale dell'87%**. Nonostante la diminuzione di un paio di punti percentuali in queste aree, la tendenza generale è verso una maggiore collaborazione.

8. Oltre alla riduzione dei costi, quali sono secondo te i motivi alla base dell'outsourcing?

Rispetto al report dello scorso anno, l'outsourcing è aumentato notevolmente, il che potrebbe indicare un andamento storico poiché la gestione interna del parco fornitori diventa sempre più complessa. È interessante notare che le aziende hanno riferito di aspettarsi una diminuzione dell'outsourcing in futuro. In Italia invece l'outsourcing è rimasto stabile al 34%.

I nostri intervistati sfruttano l'outsourcing per svariati motivi importanti, non solo per ragioni di costo. L'efficienza dei costi è di poco avanti come primo motivo con il 55%. Subito dopo vi sono però i team di sicurezza che desiderano risposte più tempestive agli incidenti (53%).

⁴ Nel capitolo 21 i dati italiani



Osservo un aumento degli esercizi di risposta alle violazioni dei dati, inclusi manuali che definiscono il processo e stabiliscono chi deve saper parlare con la stampa e cosa deve dire. Inizia inevitabilmente al livello più elevato, ma riguarda il ruolo che tutti nell'azienda possono svolgere dopo la violazione, nel momento più pericoloso in cui tutti sono alla ricerca di risposte. È il momento di mantenere i nervi saldi e reagire da professionisti.

Steve Durbin, Amministratore delegato, Information Security Forum
<https://newsroom.cisco.com>

9. Secondo te la preparazione ha i suoi vantaggi?

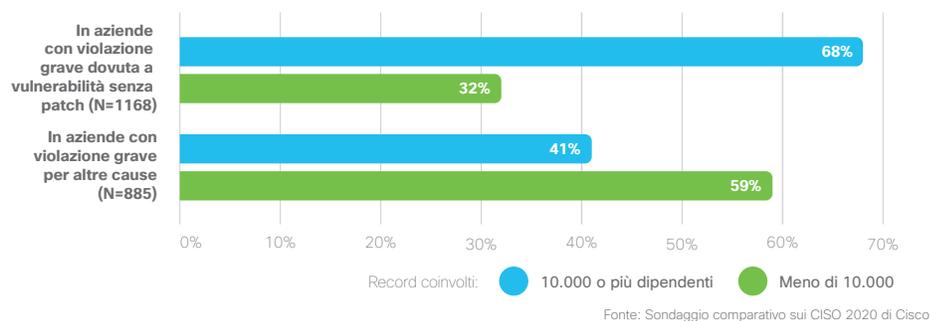
Quando è stato chiesto quali pratiche o policy di sicurezza si applicano alle loro aziende, abbiamo rilevato che gli **intervistati che hanno messo in pratica più di frequente i punti elencati di seguito hanno dovuto affrontare costi minori per violazioni gravi**. In altre parole, se le seguenti sei procedure si allineano con il programma di sicurezza, le violazioni tendono maggiormente a rimanere al di sotto di \$100.000.

- Le procedure di sicurezza vengono riviste e migliorate nel tempo in modo regolare, formale e strategico
- Analizziamo regolarmente l'attività di connessione in rete per assicurarci che le misure di sicurezza funzionino come previsto
- La sicurezza è ben integrata negli obiettivi e nelle capacità aziendali della nostra organizzazione
- Le violazioni della sicurezza vengono esaminate in modo regolare e sistematico
- Le nostre tecnologie di sicurezza sono ben integrate per interagire efficacemente
- Le nostre funzioni di rilevamento e blocco delle minacce vengono mantenute aggiornate

10. Quanto è importante applicare le patch per la difesa dalle violazioni?

Una preoccupazione primaria per il 2020 è rappresentata dal fatto che il 46% delle aziende (rispetto al 30% del report dello scorso anno), 30% delle organizzazioni in Italia, ha subito un incidente causato da una vulnerabilità senza patch. Inoltre, **coloro che hanno subito una violazione grave a causa di una vulnerabilità senza patch lo scorso anno, hanno registrato livelli più elevati di perdita di dati** (Figura 6). Ad esempio, il 68% delle aziende violate lo scorso anno da una vulnerabilità senza patch ha subito perdite per 10.000 o più record di dati. Per coloro che hanno dichiarato di aver subito una violazione per altre cause, solo il 41% ha perso 10.000 o più record nello stesso lasso di tempo.

Figura 6: È stato chiesto agli intervistati se hanno subito un incidente di sicurezza derivante da una vulnerabilità senza patch nell'ultimo anno, o da altre cause, correlato al numero di record di dati persi (N=2053). Le percentuali sono arrotondate.



Si sa che l'applicazione di patch può essere difficile e causare disagi. Tuttavia, questi risultati mostrano che l'implementazione di una policy minima per le patch più recenti garantisce un ritorno sicuro dell'investimento. **Le aziende devono mantenere un inventario aggiornato di tutti i dispositivi nel loro ambiente ed eseguire un'analisi del rischio per eventuali patch mancanti. Devono poi creare un processo di gestione delle modifiche per applicare il controllo della versione e la documentazione.**

11. Cosa provoca l'interruzione dell'operatività?

Come mostrato in precedenza, gli intervistati hanno segnalato un intervallo espresso in ore di interruzione dell'operatività. Quando è stata chiesta la causa più comune di tale interruzione, il primo e il secondo posto sono andati rispettivamente a malware e spam dannoso. È interessante notare che la terza causa varia in base alla durata dell'interruzione. Per le violazioni con interruzioni tra 0 e 4 ore, il phishing è la terza causa più comune. Per tempi di inattività tra 4 e 24 ore, è lo spyware. Oltre 24 ore, è il [ransomware](#).

È significativo notare che il ransomware non ha preferenze: è stata la minaccia più distruttiva per tutte le aziende, piccole e grandi, in termini di interruzione dell'operatività. I tempi di inattività prolungati che ne risultano possono essere dovuti alla profondità di indagine necessaria per valutare il danno, tentare di ripristinare i backup e correggere i vettori di attacco.

Per ulteriori informazioni su come gestire i vari tipi di attacchi, iscriviti al nostro [blog di intelligence sulle minacce Talos](#).

12. Quanto è difficile proteggere la forza lavoro mobile?

Abbiamo chiesto ai partecipanti al sondaggio di dirci quanto sia difficile proteggere i vari aspetti della loro infrastruttura. **Più della metà (52%) a livello globale e 32% in Italia ci ha detto che oggi è molto o estremamente difficile difendere i dispositivi mobili.** Si sono impadroniti del comportamento degli utenti, la sfida maggiore emersa dal report dell'anno scorso.

Con un'[architettura zero trust](#) è possibile identificare e verificare ogni persona e dispositivo che tenta di accedere all'infrastruttura. Zero trust è un modello pragmatico e a prova di futuro che può contribuire a garantire una sicurezza efficace in tutta l'architettura, dal personale al carico di lavoro all'ambiente di lavoro.

Un'architettura zero trust consegue tra gli altri questi tre parametri di successo:

- L'utente è noto e autenticato
- Il dispositivo viene controllato e risulta adeguato
- L'utente è soggetto a limiti su dove può andare all'interno dell'ambiente

Con zero trust non ci si deve affidare al caso per proteggere la propria infrastruttura da tutte le potenziali minacce, inclusi i dispositivi mobili.

13. Come si può estendere la sicurezza zero trust per proteggere le applicazioni?

La sicurezza del carico di lavoro riguarda la protezione di tutte le connessioni di utenti e dispositivi nella rete. Un'architettura zero trust può identificare le dipendenze all'interno e intorno a database e applicazioni per applicare la micro-segmentazione e contenere movimenti laterali.

Il 41% delle aziende intervistate, il 23% in Italia, trova i data center molto o estremamente difficili da difendere e il 39% afferma di dover lottare strenuamente per proteggere le applicazioni. L'aspetto più problematico sono i dati memorizzati nel cloud pubblico, con il 52% contro il 30% in Italia che ritiene siano molto o estremamente difficili da proteggere.

Un'architettura zero trust offre visibilità su quanto è in esecuzione e lo fa, punto fondamentale, identificando e applicando policy in tutta la rete. Avvisa anche in caso di violazione di una policy attraverso il monitoraggio continuo e la risposta agli indicatori di compromissione.



L'intelligence sulle minacce ti aiuta a comprendere le possibili conseguenze sulla tua azienda attraverso la comprensione delle minacce reali effettivamente presenti. L'assegnazione della priorità a questi rischi reali sulla base di un'intelligence concreta consente ai titolari di aziende di utilizzare i propri capitali limitati per i problemi effettivamente presenti.

Matt Watchinski, VP Progettazione, Talos

14. La difesa dell'infrastruttura di rete rappresenta ancora una sfida?

L'infrastruttura cloud privata è una delle principali sfide di sicurezza per le aziende (il 50% ritiene che difendersi sia molto o estremamente difficile contro 36% in Italia). Per quanto riguarda l'infrastruttura di rete, il 41% delle aziende ritiene che sia molto o estremamente difficile da difendere.

Ecco dove un'architettura zero trust offre valore. Zero trust prevede il mantenimento del controllo degli accessi definito da software su tutte le connessioni all'interno delle app e in un ambiente multi-cloud basato su utente, dispositivo e contesto delle applicazioni, non sulla posizione. Questo modello consente di mitigare, rilevare e reagire ai rischi all'interno dell'infrastruttura, indipendentemente dalla distribuzione o dalla posizione.

Di seguito sono illustrate le fasi di questo modello per sviluppare la maturità della sicurezza zero trust.

Sviluppare un modello di maturità della sicurezza zero trust

In Cisco impieghiamo cinque passaggi di trasformazione che i nostri clienti adotteranno come struttura per implementare **un'architettura zero trust** per la propria azienda:

Fase 1: Disponi di una strategia chiara per la gestione delle identità e degli accessi (IAM), allineata alle tue esigenze aziendali, che ha portato ad una piena implementazione e integrazione di una soluzione di autenticazione a più fattori (MFA) supportata da policy basate sui rischi?

Fase 2: Disponi di un inventario delle risorse aggiornato che distingue tra dispositivi gestiti e non gestiti, fornendo un controllo e una manutenzione degli stessi nell'ambito di una funzione di sicurezza e IT integrata?

Fase 3: Disponi di una policy per dispositivi sicuri che invita gli utenti ad aggiornare i propri dispositivi contro vulnerabilità misurate, all'interno di un processo gestito, e di report su dispositivi non contemplati dalla policy?

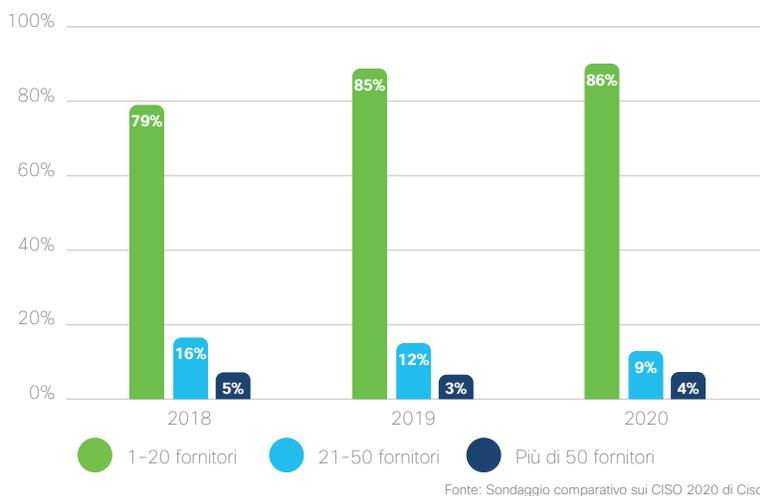
Fase 4: Controlli l'accesso degli utenti tramite una policy gestita centralmente che identifica e agisce sulle eccezioni?

Fase 5: Disponi di una strategia zero trust allineata all'attività economica e supportata da un'architettura e da un insieme di processi che consente agli utenti di accedere sempre ad applicazioni on-premise e cloud?

15. È possibile misurare l'impatto del consolidamento dei fornitori?

La tendenza a consolidare i fornitori per ridurre la complessità continua e si mantiene stabile, con l'**86% delle aziende che utilizza tra 1 e 20 fornitori, in Italia 91%, e solo il 13%, 8% per l'Italia, oltre 20** (Figura 7).

Figura 7: Numero di fornitori di sicurezza diversi (ossia marchi, produttori) utilizzati negli ambienti di sicurezza degli intervistati (N=2800). Le percentuali sono arrotondate.



Dal 2017 è cambiato il modo in cui le aziende ritengono di affrontare una strategia basata su più fornitori. **Oggi il 28% considera la gestione di un ambiente con più fornitori molto difficile, con un aumento dell'8% dal 2017. Il 53% ritiene che sia abbastanza difficile.** Meno aziende (con un calo dal 26% al 17%) trovano semplice gestire un ambiente con più fornitori. La maggior parte delle aziende appartiene alle categorie "lo trovo difficile" (81%). Questo potrebbe significare che ci sono meno fornitori da gestire o che si è iniziato ad utilizzare strumenti come i motori di analisi per migliorare i risultati ottenuti con più strumenti diversi.

Abbiamo esaminato anche le tendenze tra gli avvisi all'interno di un ambiente con più fornitori e l'impatto che hanno sulla cyber fatigue (di cui parleremo un po' più avanti nel prossimo argomento). **Il 42% degli intervistati soffre di cyber fatigue, che si può definire come la rinuncia virtuale a difendersi in modo proattivo contro gli hacker, 29% in Italia.**

I nostri dati hanno dimostrato che le aziende che soffrono di cyber fatigue sono molto più propense a ritenere impegnativo un ambiente con più fornitori. Oltre a dover reagire a troppi avvisi e a lottare con la complessità dei fornitori, abbiamo scoperto che la presenza di una violazione più gravosa (in termini di numero di ore di interruzione dell'operatività) aumenta anche la cyber fatigue. Tuttavia, con oltre il 96% di chi soffre di cyber fatigue che ritiene difficile la gestione di un ambiente con più fornitori, **la complessità sembra essere una delle principali cause di stress informatico.**

Non voglio passare il tempo a integrare prodotti di sicurezza. Voglio solamente agire in sicurezza. Dico al mio team che di un nuovo prodotto mi interessano tre cose:

- Assicurarsi che funzioni
- Assicurarsi che mi dia piena visibilità Niente buchi neri
- Assicurarsi che sia integrato con il resto del nostro ecosistema di sicurezza

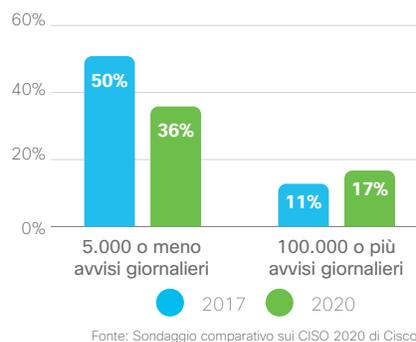
Steve Martino, SVP, Chief Information Security Officer, Cisco

16. A cosa sono dovuti cyber fatigue e stress informatico?

Nella sezione precedente abbiamo iniziato ad intravedere una correlazione tra ambienti con più fornitori e aumento della cyber fatigue. Ora diamo un'occhiata al volume medio di avvisi di sicurezza che un'azienda riceve ogni giorno.

Il numero complessivo di avvisi giornalieri da gestire è aumentato rispetto agli anni precedenti. Nel 2017, il 50% delle aziende riceveva 5.000 o meno avvisi giornalieri; ora solo il 36% rientra in questa categoria. E la quantità di aziende che ricevono 100.000 o più avvisi giornalieri è aumentata dall'11% del 2017 al 17% del 2020 (Figura 8).

Figura 8: Numero riferito di avvisi ricevuti (N=2800). Le percentuali sono arrotondate.



Forse a causa di questo aumento di volume e di risorse di elaborazione necessarie, le analisi di sicurezza hanno raggiunto in quattro anni il livello più basso, poco meno del 48% (nel 2017 la percentuale era del 56% ed è diminuita ogni anno). Il 26% di incidenti fondati rimane costante di anno in anno e suggerisce che molte indagini si stanno rivelando falsi positivi.

Un dato positivo è il miglioramento del numero di minacce fondate che vengono risolte rispetto al report dello scorso anno: con un valore del 50% siamo infatti tornati ai livelli del 2017. Tuttavia, ciò significa ancora che la metà di tutti gli incidenti effettivi viene trascurata.

In particolare, l'enorme numero di avvisi sta incrementando la cyber fatigue. **Di coloro che affermano di essere affetti da cyber fatigue, il 93% riceve più di 5.000 avvisi ogni giorno.**

Per affrontare l'aumento di rumore e volume degli avvisi proponiamo un approccio incentrato sull'automazione. L'automazione consente di applicare le policy in modo più coerente, rapido ed efficiente. Quando viene stabilito che un dispositivo è infetto o vulnerabile, viene automaticamente messo in quarantena o viene negato l'accesso ad esso senza richieste di azione da un amministratore.

17. Quali vantaggi per la sicurezza sono associati all'infrastruttura di hosting nel cloud?

Con la nostra ricerca abbiamo scoperto che una maggiore efficacia, efficienza e visibilità sono alcuni dei principali fattori che spingono le aziende a spostare sicurezza (88%) ed infrastruttura (89%) nel cloud. E non sorprende che **l'86% affermi che utilizzare la sicurezza del cloud ha aumentato la visibilità nelle loro reti.** Nel 2020 abbiamo continuato a vedere più dell'83% delle aziende che gestisce oltre il 20% dell'infrastruttura IT nel cloud (internamente o esternamente).

I clienti dipendono sempre più dai fornitori per approfondire gli incidenti, con analisi avanzate e report dettagliati di analisi forense. In questo senso i provider di reazioni agli incidenti devono fornire combinazioni di prodotti e processi altamente specializzati per ridurre il tempo medio di contenimento (MTTC) e il tempo medio di risoluzione (MTTR) di un incidente attivo.

Market Guide for Digital Forensics and Incident Response Services, Gartner, dicembre 2019⁴

⁴ Brian Reed, Toby Bussa, Market Guide for Digital Forensics and Incident Response Services, Gartner, 11 dic 2019

18. Secondo te quali sfide tiene in serbo il futuro?

Nonostante lo tsunami di cambiamenti a livello di infrastruttura che possono risultare difficili da implementare, la trasformazione digitale continua a presentarsi come un'opportunità per i responsabili IT e della sicurezza per innovare ed avvantaggiarsi sulla concorrenza.

I professionisti della sicurezza stanno adottando tecnologie ed approcci avanzati, dall'intelligenza artificiale e apprendimento automatico all'implementazione sicura di DevOps e micro-segmentazione. E come tutti sappiamo, gli ambienti multi-cloud continuano a prevalere.

Data la natura dinamica di questo ambiente, gli esperti della sicurezza non devono solo padroneggiare le basi, ma anche rimanere aggiornati con le tecnologie più recenti a loro disposizione. Presumibilmente, alcune di queste tecnologie più recenti diventeranno un elemento fondamentale nell'ecosistema di sicurezza, anche se al momento non lo sono.

Ad esempio, osserviamo che in questa epoca di ubiquità digitale **solo il 27% delle aziende sta attualmente utilizzando l'autenticazione a più fattori (MFA) mentre in Italia sono il 38%**. È una percentuale piuttosto bassa per una tecnologia zero trust tanto favorevole. Gli intervistati dei seguenti paesi hanno mostrato le percentuali più elevate di adozione dell'autenticazione MFA, in questo ordine: Stati Uniti, Cina, Italia, India, Germania e Regno Unito. I settori con le percentuali più elevate (in questo ordine) sono sviluppo di software, servizi finanziari, pubblica amministrazione, commercio al dettaglio, settore manifatturiero e telecomunicazioni.

Per quanto riguarda la trasformazione digitale, oltre all'adozione del cloud, l'automazione sale sul podio al primo posto. Molti professionisti della sicurezza stanno comprendendo i vantaggi dell'automazione per risolvere il problema della carenza di competenze quando adottano soluzioni con maggiori [capacità di apprendimento automatico e intelligenza artificiale](#).

Come illustrato nella Figura 9, **la maggioranza (77%) degli intervistati prevede di incrementare l'automazione per semplificare e accelerare i tempi di risposta negli ecosistemi di sicurezza**. Quando si prevede di automatizzare, è necessario definire in modo strategico dove l'automazione sarà più efficace e fornirà il ROI più elevato all'interno della propria azienda.

Figura 9: Chi prevede di incrementare l'utilizzo dell'automazione nell'ecosistema di sicurezza delle aziende nel corso del prossimo anno (N=2800). Le percentuali sono arrotondate.



Fonte: Sondaggio comparativo sui CISO 2020 di Cisco

19. Quanta attenzione si deve porre alla reazione agli incidenti?

Il panorama delle minacce si è evoluto in un ambiente complesso ed impegnativo per le aziende in tutto il mondo. Una carenza di talenti, unita ad un aumento degli incidenti, ha portato a una postura della sicurezza generalmente debole nella maggior parte delle aziende. Sedersi e aspettare che arrivi un avviso può comportare multe severe, maggiori controlli, perdita di proprietà intellettuale, [problemi di privacy dei dati](#) e perdite a livello di business. Per proteggere l'infrastruttura diventa fondamentale la prevenzione attraverso l'acquisizione di visibilità, il threat hunting e la creazione di un'architettura zero trust.

Nel nostro sondaggio rivolto a responsabili delle decisioni IT, **il 76% degli intervistati si riteneva molto informato sulla reazione agli incidenti e il 23% affermava di essere abbastanza informato, che sommati danno il 99%**. Ecco la buona notizia. Tuttavia, come rilevato dal nostro sondaggio, la complessità della sicurezza sta creando cyber fatigue e questo potrebbe limitare le risorse difficili da ottenere. È qui che l'outsourcing può essere utile.

Figura 10: Percentuali di intervistati che sono molto e abbastanza informati sulla reazione agli incidenti per un totale del 99%. N=2800. Le percentuali sono arrotondate.



Abbiamo scoperto che il 34% degli intervistati sta esternalizzando i servizi di reazione agli incidenti e il 36% si affida a servizi esterni/di terze parti per analizzare i sistemi compromessi, percentuali in aumento rispetto all'anno scorso. Affidarsi ad un servizio di reazione agli incidenti è diventato un approccio efficiente per proteggere le risorse, ridurre i rischi e mantenere la conformità. In questo modo la tua azienda potrà proteggersi dalle minacce sconosciute con pianificazioni proattive e competenze utili per coordinare ed implementare una reazione.

[Vuoi sapere come promuovere le carriere nella cybersecurity per te o il tuo personale?](#)
[Visita: Certificazioni di sicurezza Cisco.](#)

20. Cosa puoi fare ora per migliorare la tua postura della sicurezza?

Sei alle prese con hacker attivi, che dispongono di risorse finanziarie e di una pazienza infinita. Stai anche affrontando sfide perenni che sembrano non avere fine, come mantenere un inventario accurato di utenti, applicazioni e dispositivi. Ti stai barcamenando tra rischi per l'azienda e rischi di sicurezza, mentre cerchi di promuovere l'avanzamento dei team. Tuttavia, le decisioni aziendali continuano ad essere prese senza tenere conto della sicurezza. E quando si aggiungono nuove normative, mandati del Consiglio di amministrazione, budget limitati, gestione dei rischi e turnover di esperti della sicurezza, il meccanismo non si ferma mai.

Le sfide da affrontare per difendere le aziende sono sempre più pressanti e non sembrano attenuarsi. È il momento di lavorare in modo più intelligente, ottimizzando la difesa e concentrandosi sulla prevenzione, oltre a rilevare e correggere le minacce. In questo report abbiamo indicato 20 aree di cui tenere conto per una gestione più sicura delle aziende. Inoltre abbiamo fornito consigli che si possono sintetizzare così:

- Applicare una difesa a più livelli, che deve includere MFA, segmentazione della rete e protezione degli endpoint
- Ottenere i massimi livelli di visibilità per rafforzare la governance dei dati, ridurre i rischi e aumentare la conformità
- Puntellare le difese, aggiornare e applicare le patch ai dispositivi e concentrarsi sull'igiene informatica attraverso esercitazioni e corsi di formazione
- Migliorare la propria maturità della sicurezza creando un'architettura zero trust (Figura 13).

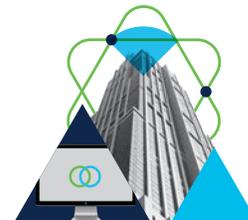
Figura 11: Una strategia zero trust può proteggere personale, carichi di lavoro e ambiente di lavoro.



Proteggi la tua forza lavoro
Proteggi l'accesso per utenti e dispositivi che si collegano ad applicazioni



Proteggi il tuo carico di lavoro
Proteggi le connessioni all'interno delle tue app in tutti gli ambienti



Proteggi il tuo ambiente di lavoro
Connettiti in modo sicuro nella tua rete

Noi di Cisco riteniamo che sia ora che il settore della sicurezza si evolva. Le soluzioni di sicurezza devono funzionare come un team. I team comunicano in tempo reale, imparano gli uni dagli altri e rispondono come un'unità coordinata. La sicurezza degli endpoint deve interagire con la sicurezza della rete e del cloud ed occorre un'autenticazione MFA che riguardi identità e accesso. **A nostro parere la protezione effettiva di un'azienda può essere realizzata al meglio attraverso un approccio basato su piattaforme per garantire la copertura di sicurezza globale.**

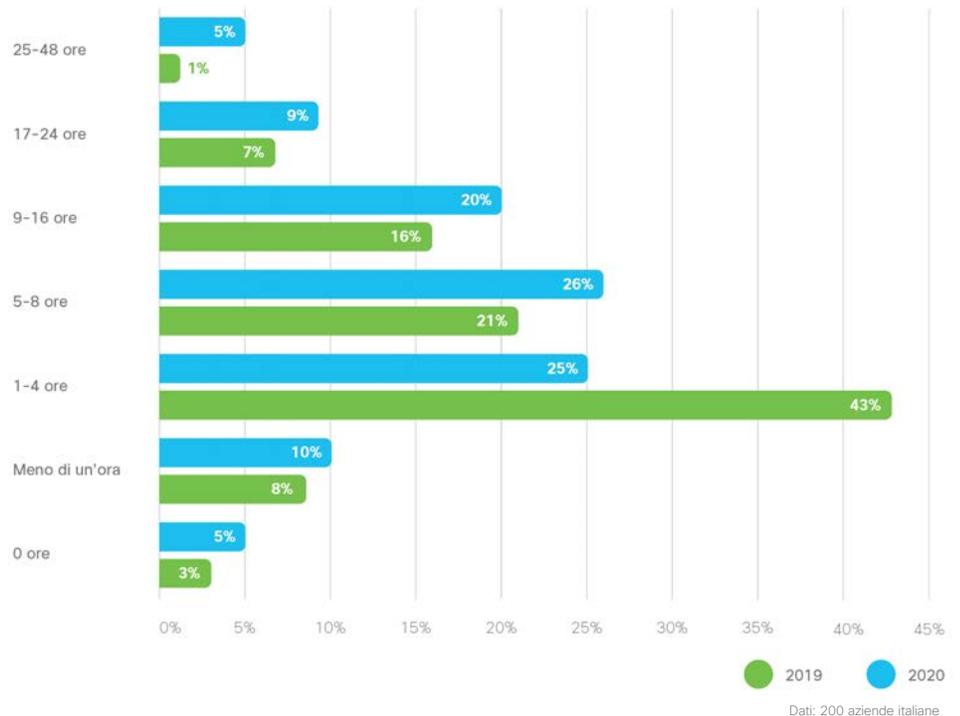
21. I danni di un attacco informatico in Italia

I danni di un attacco informatico possono essere valutati seguendo tre parametri: il tempo di inattività dei sistema aziendali a seguito di un attacco grave, il numero di dati persi e l'impatto sulle diverse aree di business.

Tempo di inattività dei sistemi a causa di un attacco grave

Il 26% delle aziende italiane intervistate necessita tra cinque e le otto ore per ripristinare il normale funzionamento dei propri sistema a seguito di un attacco grave. Come si vede dalla Figura C sotto inoltre il tempo medio di ripristino di 4 ore si è notevolmente ridotto rispetto all'anno precedente passando da un 43% di aziende al 25%.

Figura C: Tempo medio di inattività dei sistemi occorso in Italia a causa di un grave attacco.



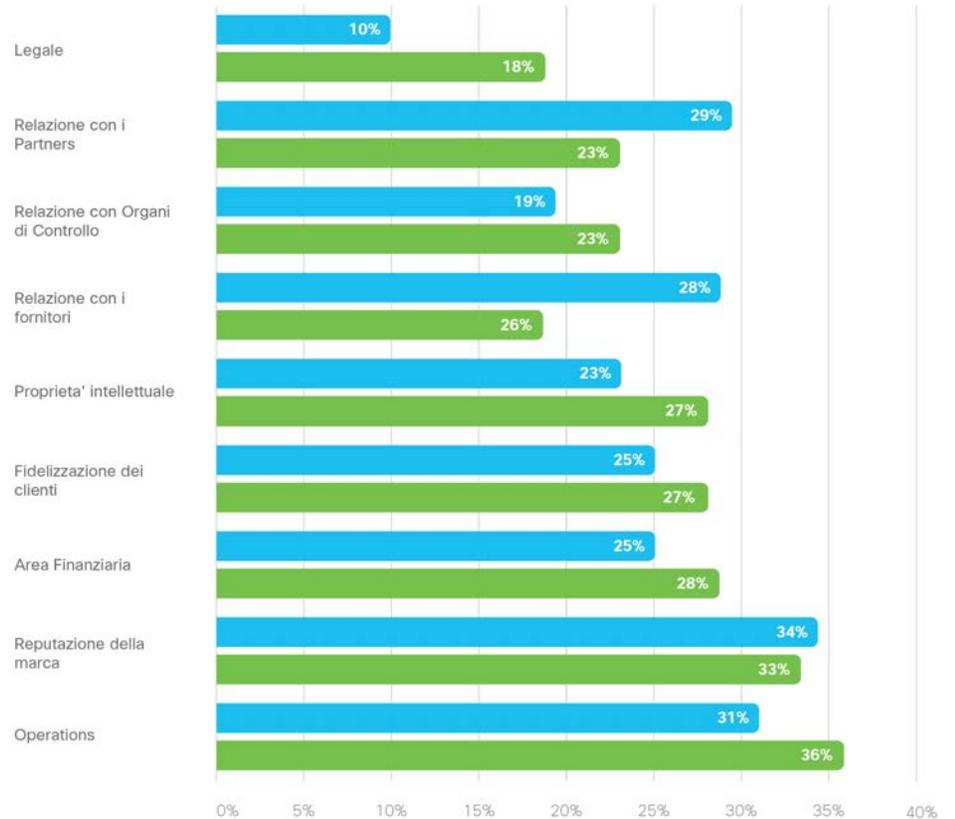
Dati persi

Il 33% delle aziende italiane ha dichiarato di aver perso tra dieci e centomila dati a seguito di un attacco informatico grave contro il 38% dell'anno scorso, mentre il 29% tra nove e diecimila dati contro il 33% dell'anno scorso.

Danni alle aree di business

È la Brand Reputation il maggior danno che le aziende italiane subiscono a seguito di un attacco informatico andato a buon fine, più che nel resto del mondo come si vede nel grafico sottostante che compara dati italiani con quelli global.

Figura D: Aree di business maggiormente colpite in Italia a seguito di attacchi informatici.



Dati: 200 aziende italiane

La necessità di avere sempre un piano in caso di incidente informatico è evidente dall'analisi di questi dati. L'organizzazione e la capacità di adottare processi e strumenti automatici, diventa fondamentale per riuscire a tenere basso il costo di un incidente.

L'informazione si conferma un'obiettivo strategico per i male-intenzionati. L'importanza crescente del valore dell'informazione aumenta il rischio di un'azienda di essere attaccata. Visibilità e controllo vanno di pari passo: non posso proteggere cosa non conosco.

In un paese come l'Italia, composto da aziende che fanno del "brand" un asset importante, è chiaro quanto siamo significativo proteggerlo. La valutazione del rischio, in tutti i suoi elementi, è pratica fondamentale per una buona postura di sicurezza.

Fabio Panada, Cisco Senior Security Consultant

Proteggere il presente e il futuro

Il nostro fine è proteggere i clienti dalle minacce di oggi e di domani, affinché possano concentrarsi sui loro obiettivi strategici affidando a noi la questione della sicurezza.

Presentazione della piattaforma di sicurezza Cisco, [SecureX](#), creata dal team di sicurezza più avanzato del pianeta, che offre la protezione necessaria per la modalità operativa della tua azienda.

- Iniziamo dalle **soluzioni migliori** per proteggere rete, endpoint, applicazioni e cloud
- Usiamo la **verifica di affidabilità** per consentire l'accesso alle sole persone autorizzate
- Supportiamo ogni prodotto con l'**intelligence sulle minacce** del centro di ricerca [Talos](#), leader nel settore, per bloccare più minacce e proteggere le aziende
- Le soluzioni che offriamo sono caratterizzate da **risposte automatizzate a minacce avanzate e processi operativi razionalizzati con gestione integrata di minacce e sicurezza**
- **Le nostre soluzioni sono concepite per interagire con le altre tecnologie installate in azienda** per fornire risposte di sicurezza integrate anche al di fuori degli ambienti Cisco

SecureX offre visibilità, azioni automatizzate e una postura della sicurezza migliorata. Nella **piattaforma SecureX** sono inoltre state integrate soluzioni personalizzate, fornite tramite cloud, per ridurre la complessità della sicurezza. Creiamo un'interfaccia coerente combinando le soluzioni di sicurezza integrata di Cisco e i prodotti di terze parti presenti nell'ambiente del cliente. L'innovazione a livello di piattaforma di Cisco offre inoltre l'analisi maggiormente integrata di tutto il pianeta. Si lavora insieme:

- [SecureX](#) unisce team operativi di sicurezza, rete e IT a flussi di lavoro collaborativi per migliorare la produttività
- [Cisco Threat Response](#) semplifica le indagini sulle minacce e le misure correttive per migliorare l'efficienza delle operazioni di sicurezza
- [L'analisi](#) semplifica il rilevamento delle minacce sconosciute per migliorare le scelte delle policy, i tempi di risposta e l'efficacia della risposta alle minacce

Grazie al nostro portafoglio integrato e all'intelligence sulle minacce leader del settore, Cisco ti fornisce la portata, le dimensioni e le funzionalità necessarie per tenere il passo con la complessità e il volume delle minacce. Mettere la sicurezza al primo posto ti aiuta a innovare garantendo la protezione delle risorse. Cisco privilegia la sicurezza in ogni sua attività. Solo Cisco ti offre una sicurezza di rete efficace per far fronte all'evoluzione futura delle minacce. Scopri di più sul nostro approccio basato sulla piattaforma su cisco.com/go/security.

Cisco Cybersecurity Report Series

Nell'ultimo decennio, Cisco ha pubblicato molte informazioni sulla sicurezza e l'intelligence sulle minacce per i professionisti del settore interessati allo stato della sicurezza informatica mondiale. Questi report esaustivi contenevano resoconti dettagliati degli scenari delle minacce, le implicazioni per le aziende e le procedure consigliate per difendersi dall'impatto nefasto della violazione dei dati.

Cisco Security pubblica ora una serie di testi basati su ricerche e dati concreti che usciranno con l'intestazione Cisco Cybersecurity Series. Il numero di titoli è stato ampliato per includere varie tematiche e rivolgersi ai professionisti della sicurezza con interessi diversi. Basandosi sulla vastità e profondità della nostra esperienza nella ricerca delle minacce e nell'innovazione della sicurezza, i report di ogni serie includono lo studio comparativo sulla privacy dei dati, il report sulle minacce e lo studio comparativo sui CISO (Chief Information Security Officer). Altri verranno pubblicati nel corso dell'anno.

Per ulteriori informazioni e per accedere a tutte le relazioni e le copie archiviate, visita www.cisco.com/go/securityreports.



Privacy dei dati 2019



Report sulle minacce 2019



Studio comparativo sui CISO 2019



E-mail: Anche un solo clic può costare caro



Soglia minima di sicurezza



Ricerca delle minacce



Sondaggio sulla privacy dei consumatori



Minacce dell'anno 2019



Privacy dei dati 2020



Studio comparativo sui CISO 2020

Sede centrale Americhe
Cisco Systems, Inc.
San Jose, CA

Sede centrale Asia Pacifico
Cisco Systems (USA), Pte. Ltd.
Singapore

Sede centrale Europa
Cisco Systems International BV
Amsterdam, Paesi Bassi

Le filiali Cisco nel mondo sono oltre 200. Gli indirizzi, i numeri di telefono e di fax sono disponibili sul sito web Cisco all'indirizzo www.cisco.com/go/offices.

Pubblicato nel febbraio 2020

CISO_02_0220

© 2020 Cisco e/o relativi affiliati. Tutti i diritti sono riservati.

