FORTINET

REPORT

Il COO e la sicurezza informatica delle tecnologie operative

Report sulle priorità e le sfide attuali

Sommario

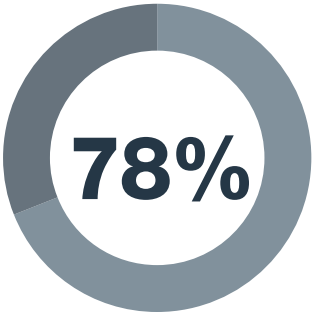
Sintesi preliminare

Il report "Il COO e la sicurezza informatica delle tecnologie operative" di Fortinet esamina le sfide che i COO si trovano ad affrontare quando devono mettere in sicurezza l'infrastruttura della tecnologia operativa (OT) e analizza il modo in cui stanno rispondendo a questi problemi. Anche se la responsabilità per la sicurezza OT è solitamente condivisa dal CISO o da altri dirigenti, i COO sono rilevanti per la sicurezza OT perché i loro team sono spesso responsabili della gestione e dell'acquisto delle attrezzature utilizzate sulla linea di produzione, compresi gli strumenti di sicurezza.

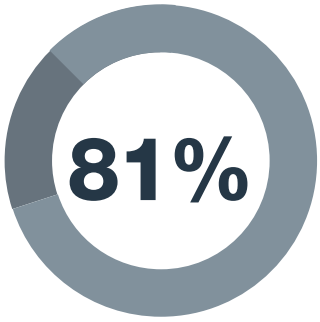
Un recente sondaggio di Fortinet ha raccolto una serie di informazioni sul ruolo del COO nella sicurezza OT. Questi i risultati principali:

1. Il COO deve affrontare un **livello di cambiamento senza precedenti** derivante dalla convergenza tra OT e IT, dalle maggiori aspettative dei dirigenti aziendali e da un crescente livello di coinvolgimento del CISO nella sicurezza informatica dei sistemi OT**.**
2. Il COO è preoccupato e in difficoltà di fronte alle **sfide connesse alla gestione del rischio** in misura molto maggiore rispetto a qualsiasi altro aspetto del proprio lavoro.
3. I dirigenti sono disposti ad approvare **aumenti dei budget per la sicurezza informatica OT**, ma si aspettano che il COO sfrutti questi investimenti per ottenere risultati tangibili.
4. Il COO ha inoltre difficoltà a **tenere il passo con i cambiamenti** a causa del panorama delle minacce avanzate.

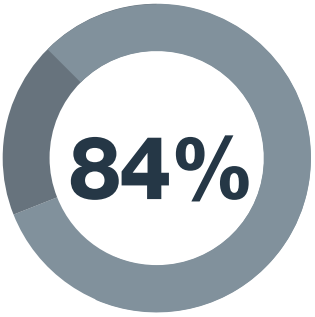
Date queste tendenze e sfide, abbiamo analizzato i dati in modo più approfondito e abbiamo identificato due sottoinsiemi di intervistati in base al numero di intrusioni subite nell'anno precedente. Abbiamo analizzato i tratti rappresentativi dei COO di livello superiore rispetto a quelli dei loro omologhi di livello inferiore per indagare sui motivi delle differenze di successo della strategia di sicurezza. Queste best practice dimostrano che i COO di maggior successo riescono a bilanciare intelligentemente la sicurezza informatica e le responsabilità operative, tracciando e registrando le metriche chiave della sicurezza informatica, eseguendo test regolari della sicurezza e della conformità e implementando misure di sicurezza collaudate, come l'autenticazione a più fattori.



Percentuale di intervistati direttamente responsabili dell'integrazione della sicurezza nei processi operativi

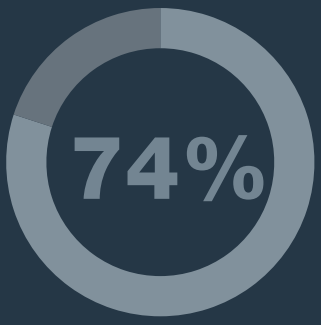


Percentuale di intervistati regolarmente coinvolti nella strategia di sicurezza informatica dell'organizzazione

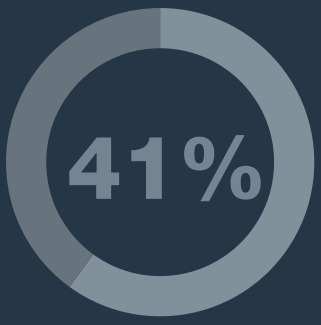


Percentuale di intervistati coinvolti regolarmente nelle decisioni di acquisto relative alla sicurezza informatica

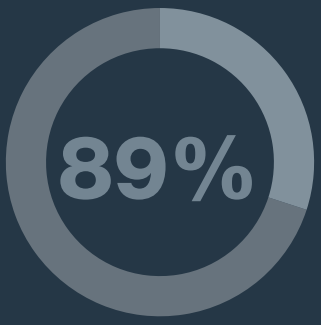
Infografica: risultati in evidenza



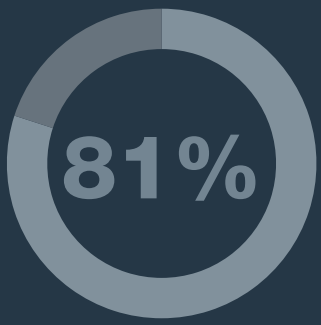
Percentuale di intervistati che gestiscono almeno 100 dispositivi



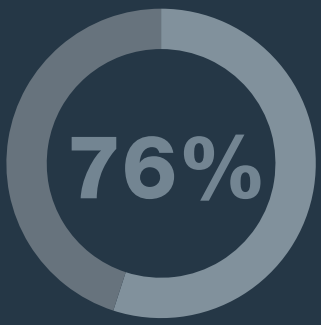
Percentuale di intervistati che hanno più di 250 dispositivi installati



Percentuale di intervistati che hanno subito intrusioni negli ultimi 12 mesi



Percentuale di intervistati che hanno subito interruzioni durante le intrusioni



Percentuale di intervistati che prevedono un aumento del loro budget per la sicurezza nel 2019, con 1 su 10 che prevede un aumento ***sostanziale***

Dati relativi ai COO di livello superiore:

168% Maggiore probabilità di citare i cambiamenti normativi come una delle sfide principali

124% Maggiore probabilità di lavorare in organizzazioni in cui un dirigente di livello C è responsabile della sicurezza informatica

79% Maggiore probabilità di classificare l'efficienza dell'area di produzione come una delle principali metriche per valutare il successo

45% Maggiore probabilità di programmare revisioni della conformità

Introduzione

Il termine OT si riferisce all'infrastruttura che monitora e controlla i processi e le attività di produzione negli stabilimenti di produzione, nelle reti elettriche, nei servizi idrici, nell'estrazione di petrolio e gas, nei trasporti e altro ancora. Tradizionalmente, tale infrastruttura si è basata su hardware e software sviluppati appositamente per esigenze industriali. Di conseguenza, le infrastrutture OT e IT sono state storicamente entità separate, sia fisicamente che dal punto di vista gestionale.

Molte reti OT non sono segmentate e utilizzano un mix di protocolli di produzione, risorse non identificate e dispositivi legacy. Alcune hanno canali di comunicazione non sicuri con le reti aziendali/IT, mentre altre mancano completamente di connessioni a Internet e ad altre reti esterne. In generale, l'OT si sta aprendo al mondo esterno. Ad esempio, un sondaggio recente ha rilevato che il 34,5% delle reti di controllo è connesso a Internet e il 66,4% è connesso a un'infrastruttura privata di terzi o alla propria rete aziendale.[1]

Nel settore si registra la tendenza a far convergere le infrastrutture OT e IT, che porta all'organizzazione diversi vantaggi. Quando le infrastrutture OT e IT sono isolate, la condivisione dei dati è un processo oneroso che viene eseguito solo ogni mese o trimestre. Creando una piattaforma comune per i dati OT e IT, le organizzazioni possono generare indicatori di prestazioni chiave (KPI) in tempo reale sulla base di informazioni aggiornate da entrambi i gruppi. I KPI in tempo reale facilitano risposte più rapide ai cambiamenti del mercato, ad esempio, informando i responsabili della produzione di un improvviso aumento del costo delle materie prime che influisce sui margini di profitto. I manager di entrambi i gruppi traggono vantaggio dalla visibilità a livello aziendale e dalla capacità di lavorare in modo collaborativo superando la divisione tra IT e OT.

Tuttavia, la convergenza fra IT e OT ha implicazioni importanti per la sicurezza:

- **Espansione della superficie di attacco.** La connessione tra le infrastrutture OT e IT espone ciascuna di esse agli attacchi dagli endpoint dell'altra. I dispositivi OT relativamente poco sicuri, come valvole, pompe, sensori, serrature elettroniche, termostati e robot sono ora potenziali punti di ingresso nell'infrastruttura IT. Nell'altra direzione, gli attacchi informatici possono prendere di mira servizi pubblici critici, come la rete elettrica e i sistemi di trasporto, utilizzando la rete mobile come punto di ingresso.
- **Aumento della complessità.** Gli ambienti di rete OT sono complessi, con un numero di dispositivi da monitorare e proteggere compreso tra 50 e 500, di solito di fornitori diversi. Questa complessità acuisce le sfide relative alla visibilità e al personale, in quanto ogni dispositivo memorizza i propri dati e ha esigenze e requisiti di configurazione di sicurezza specifici.
- **Panorama delle minacce avanzate.** La connessione a Internet espone l'infrastruttura OT a una serie di minacce malware legacy, facilmente intercettate dalle soluzioni di sicurezza IT basate sulle signature, ma potenzialmente dannose per i dispositivi industriali non protetti. I cybercriminali spesso testano il vecchio malware attaccando un numero ristretto di macchine e poi utilizzano gli exploit riusciti per organizzare attacchi su larga scala. Questo "riciclaggio delle minacce" consente agli aggressori di sfruttare al massimo il malware esistente prima di investire in attacchi più sofisticati orientati al mondo OT.[2]

"L'espansione della superficie di attacco ci spinge a prendere maggiori precauzioni per proteggere i nostri sistemi database."

– Intervistato del sondaggio nel settore dell'energia

"L'aumento della complessità ci costringe a dedicare più tempo alla sicurezza informatica a scapito delle operazioni produttive."

– Intervistato del sondaggio nel settore manifatturiero

"Il panorama delle minacce avanzate porta il team a dedicare molte più ore alla settimana al rafforzamento della sicurezza."

– Intervistato del sondaggio nel settore sanitario

Metodologia di questo studio

Il report sui COO e la sicurezza informatica dei sistemi OT si basa su un sondaggio svolto presso i COO. I nostri intervistati provengono da aziende con più di 2.500 dipendenti di diversi settori, con più della metà (59%) del settore manifatturiero e più di un quarto (27%) del settore dell'energia e dei servizi pubblici.

L'analisi dei dati segue questi passaggi: in primo luogo, lo studio utilizza i dati del sondaggio per identificare diverse tendenze attuali sul ruolo del COO nella messa in sicurezza dell'infrastruttura OT dell'organizzazione. Successivamente, analizziamo le risposte in forma libera che gli intervistati hanno dato a diverse domande aperte sulle loro sfide chiave e costruiamo un quadro di ciò che influisce sul loro lavoro quotidiano. Infine esaminiamo i dati in modo più approfondito per individuare un sottoinsieme di organizzazioni che hanno avuto tre o meno intrusioni negli ultimi 12 mesi e un altro sottoinsieme che ha avuto più di quattro intrusioni nell'ultimo anno. Confrontiamo i due gruppi e identifichiamo le best practice che vengono adottate con maggiore probabilità dai COO di livello superiore per quanto riguarda la sicurezza informatica dei sistemi OT.

Tendenze della sicurezza informatica dei sistemi OT per il COO

Tendenza: il COO è responsabile della sicurezza informatica dei sistemi OT e influenza la strategia di sicurezza dell'organizzazione.

Più di tre quarti degli intervistati collocano la sicurezza informatica dei sistemi OT all'interno dell'organizzazione del COO, con 7 su 10 che indicano che è sottoposta alla supervisione del direttore OT o del responsabile della sicurezza informatica e un altro 8% che indica come responsabile il VP/direttore delle tecnologie e delle operazioni di rete (Figura 1). La stragrande maggioranza (81%) dei COO è coinvolta regolarmente nella formulazione della strategia di sicurezza informatica, mentre i restanti sono coinvolti occasionalmente (Figura 2).

Dato che i sistemi OT e IT sono ancora separati in molte organizzazioni, è ragionevole che il COO sia responsabile dell'intera infrastruttura OT, compresa la sicurezza. Come mostra questo report, il ruolo del COO nella sicurezza informatica è in una fase di transizione. Infatti, mentre si potrebbe supporre che le responsabilità in materia di sicurezza informatica si stiano riducendo per il COO, in realtà è vero il contrario.

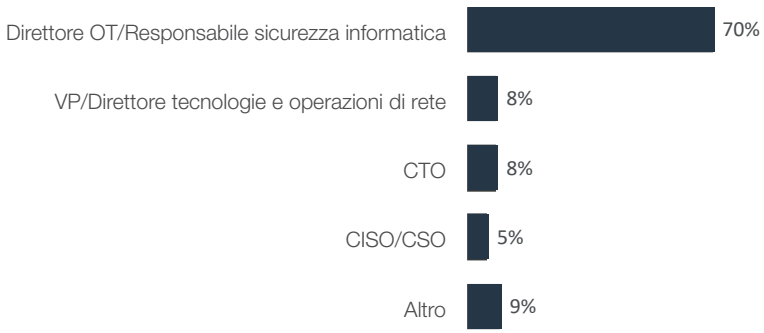


Figura 1: Responsabilità della sicurezza informatica OT all'interno dell'organizzazione.

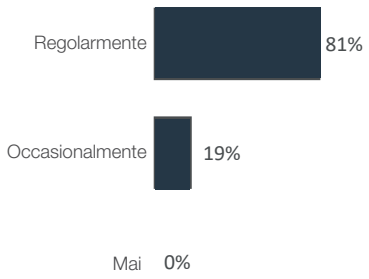


Figura 2: Coinvolgimento del COO nelle decisioni relative alla strategia di sicurezza informatica.

Tendenza: Il compito del COO relativo alla sicurezza è molto visibile all'interno dell'organizzazione.

Non sorprende che le organizzazioni prestino sempre maggiore attenzione alla sicurezza OT. Più della metà (54%) dei COO riferisce che la strategia di sicurezza OT è un fattore significativo nel punteggio di rischio complessivo dell'organizzazione, mentre gioca un ruolo moderato per più di un terzo (35%) (Figura 3). E la gestione del rischio domina le sfide che i COO devono affrontare, un argomento discusso di seguito nella sezione "Sfide principali per il COO".

Inoltre, riflettendo la crescente enfasi posta sulla sicurezza, il COO riferisce un'ampia gamma di metriche relative alla sicurezza e alla conformità, tra cui i risultati dei test di intrusione (70%), le compromissioni della sicurezza (65%), le valutazioni di sicurezza programmate (62%) e la conformità agli standard di sicurezza e alle normative di settore (59% e 57%, rispettivamente) (Figura 4).

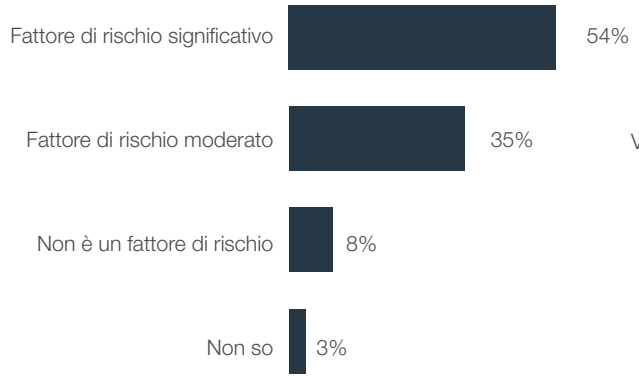


Figura 3: Impatto della strategia di sicurezza OT sul punteggio di rischio complessivo.

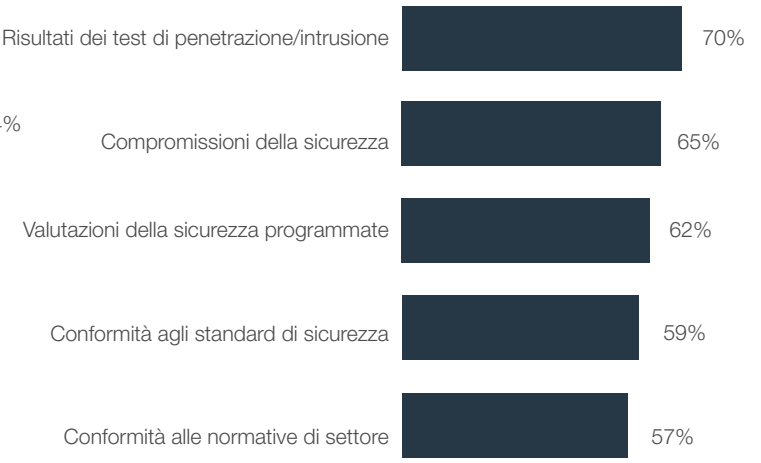


Figura 4: Metriche di sicurezza informatica OT riferite.

Tendenza: I COO hanno responsabilità importanti in materia di sicurezza oltre alla loro tradizionale attenzione ai fattori operativi.

Il compito principale del COO è quello di garantire che le operazioni dell'organizzazione si svolgano senza problemi e di tenere sotto controllo i costi operativi. Più di 8 su 10 hanno la responsabilità diretta della gestione dell'efficienza produttiva (86%), della supervisione dei team operativi (86%), della selezione e della gestione degli strumenti operativi (86%), della gestione del controllo di qualità (81%) e della supervisione di tecnici e ingegneri (81%). Tutte queste aree rientrano nel ruolo tradizionale del COO, che è quello di assicurare che le operazioni dell'organizzazione si svolgano senza problemi e di tenere sotto controllo i costi operativi.

Oltre a questi compiti, le organizzazioni si aspettano che i COO collaborino con il CISO e con altri responsabili della sicurezza per aiutare a proteggere l'infrastruttura produttiva. Più di tre quarti (78%) degli intervistati riferiscono di essere responsabili della sicurezza dei processi operativi, un compito per il quale spesso hanno poca formazione ed esperienza (Figura 5). Un tema ricorrente in questo report è la necessità per i COO di trovare un equilibrio tra le crescenti responsabilità in materia di sicurezza e i compiti operativi tradizionali. `

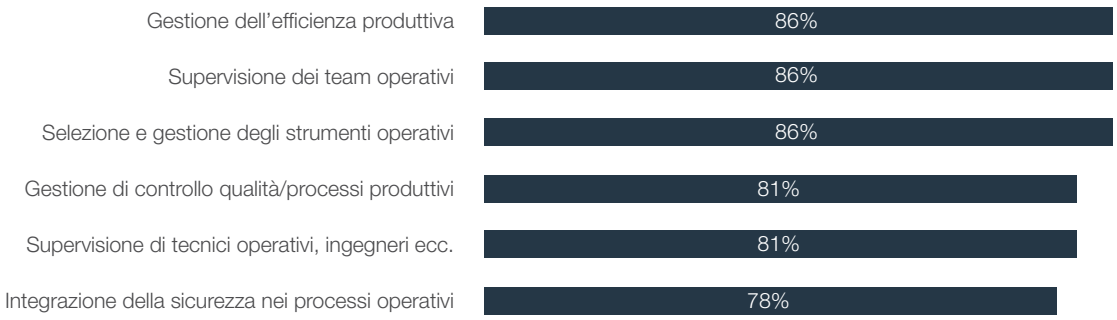


Figura 5: Responsabilità dirette dei COO.

Tendenza: La maggior parte dei COO ha subito più intrusioni nell'ultimo anno, con danni aziendali significativi.

Per i COO di questo sondaggio, il ripetersi delle intrusioni è la regola, non l'eccezione. Solo l'11% dei COO non ha riferito alcuna intrusione nei 12 mesi precedenti. Tra quelli che hanno subito intrusioni, il 42% ha avuto una o due intrusioni, mentre l'altro 47% ha avuto tre o più intrusioni (Figura 6). I tipi di attacchi hanno mostrato ampie variazioni: il 69% ha riscontrato malware e oltre il 41% ha segnalato attacchi di spyware e phishing (Figura 7).

Tra gli intervistati che hanno riferito intrusioni, l'81% ha riferito interruzioni nell'infrastruttura OT che hanno influito sulla produttività (53%), hanno messo a rischio la sicurezza fisica (31%), o hanno avuto un impatto sui ricavi (28%). D'altra parte, l'incidenza dei danni associati alle intrusioni nell'infrastruttura IT è piuttosto bassa: poco più di un quarto (28%) ha perso dati business-critical e solo il 22% ha subito un danno d'immagine (Figura 8).

Si confrontino questi dati con quelli di un recente studio di Fortinet, dove il 40% dei CISO ha riferito di interruzioni con un impatto sulla produttività, sul valore del marchio e sui ricavi.[3] Questo confronto sfavorevole per l'OT può aiutare a interpretare altri risultati di questo report, ad esempio la maggiore visibilità della sicurezza OT e l'inclusione della strategia di sicurezza OT nella valutazione del rischio complessivo.

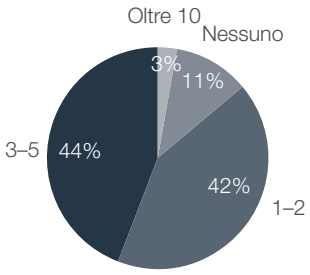


Figura 6. Numero di intrusioni nell'ultimo anno.

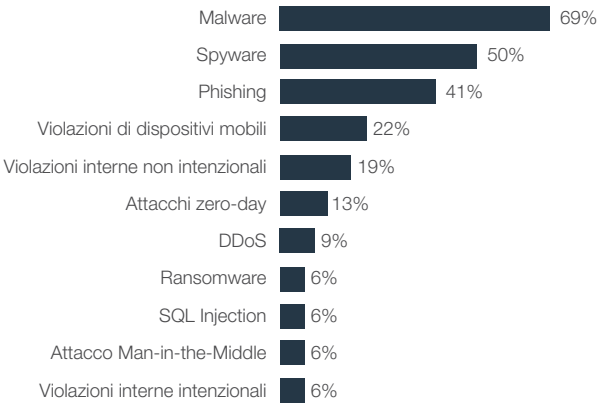


Figura 7. Tipi di intrusioni subite.

Figura 8: Impatto delle intrusioni sul business.

Tendenza: Le interruzioni possono influenzare negativamente il punteggio del COO relativamente alle metriche del successo.

Oltre a danneggiare l'azienda, le interruzioni possono anche avere un impatto diretto sulla carriera del COO, rendendo più difficile ottenere un buon punteggio relativamente alle metriche del successo. I cinque fattori di successo principali per i COO sono: l'efficienza dei costi (59%), l'aumento della produttività (54%), i livelli di sicurezza (54%), l'efficienza dell'area di produzione (51%) e i tempi di attività di sistemi/processi (30%), tutti fattori che possono essere influenzati negativamente da tempi di inattività non pianificati (Figura 9).

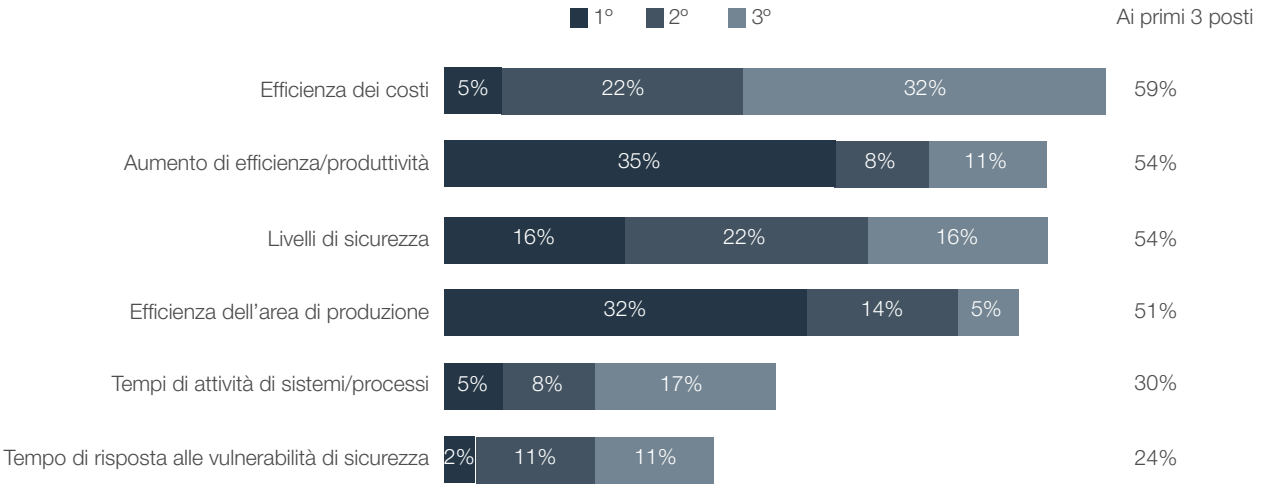


Figura 9: Fattori di successo per i COO.

Tendenza: I COO prevedono per il prossimo anno un aumento, in alcuni casi drastico, dei loro budget per la sicurezza.

Un'altra indicazione della crescente consapevolezza in azienda dei rischi delle violazioni dell'infrastruttura OT è la disponibilità dei dirigenti a investire nella sicurezza OT. Il 76% dei COO ha visto un aumento del proprio budget per la sicurezza nel 2019, con un aumento *drastico* in 1 caso su 10 (Figura 10). Un altro sondaggio ha rilevato che i budget OT sono aumentati in media del 17,9% nel 2019.[4]

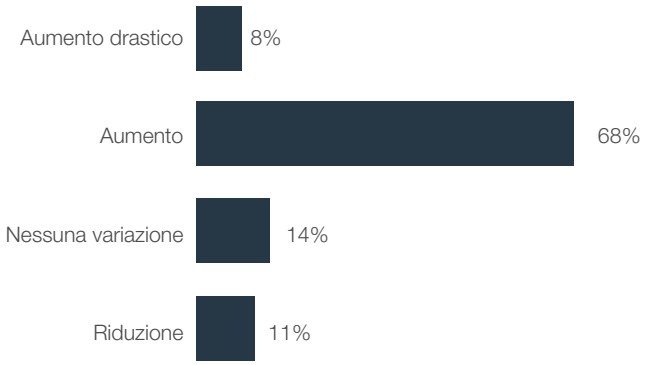


Figura 10: Tendenza dei budget di sicurezza dei COO per il 2019.

I top manager aziendali che autorizzano questi investimenti si aspettano che il COO fornisca risultati sotto forma di minori intrusioni, livelli di produttività più elevati e solide valutazioni di conformità. Per rispondere a queste aspettative, la maggior parte dei COO monitora e registra le metriche di sicurezza informatica per le intrusioni (68%), le implicazioni finanziarie (68%), le vulnerabilità individuate e bloccate (62%), la riduzione/eliminazione dei costi (57%) e i risultati tangibili della gestione del rischio (51%) (Figura 11). Per maggiori informazioni sulla risposta dei COO al rischio, vedere “Sfide principali per il COO” più avanti.

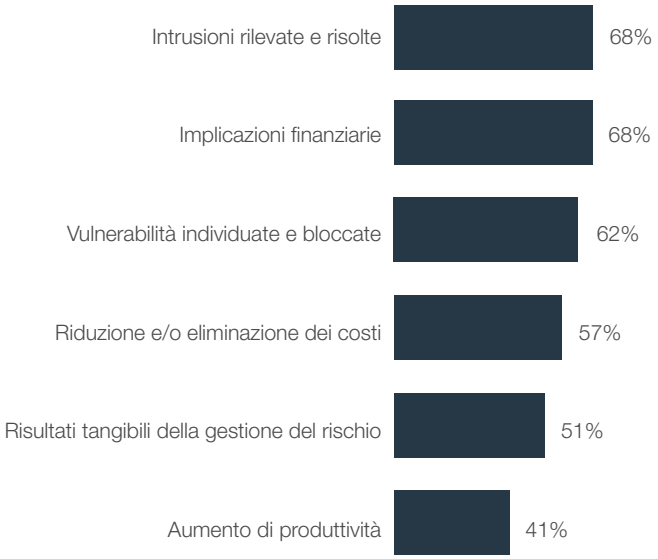


Figura 11: Metriche di sicurezza informatica monitorate e registrate.

Tendenza: Il ruolo del COO è in evoluzione, con il passaggio al CISO della responsabilità primaria della sicurezza OT.

Quasi 9 intervistati su 10 (89%) si aspettano che il CISO si assuma la responsabilità primaria della sicurezza OT nel prossimo anno (Figura 12). La convergenza fra OT e IT è la spiegazione più probabile, in un contesto in cui le organizzazioni unificano la sicurezza delle infrastrutture come modo per gestire la strategia complessiva di gestione del rischio. Pertanto questo passaggio non deve essere interpretato come una diminuzione delle responsabilità del COO in materia di sicurezza informatica, che anzi si possono prevedere in aumento con la distribuzione nella rete OT di difese informatiche sempre maggiori. Anche la crescita prevista nel numero di dispositivi industriali intelligenti aumenterà le pressioni sul COO in materia di sicurezza.

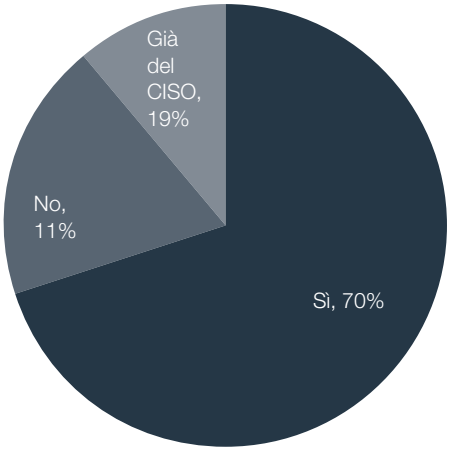


Figura 12: La sicurezza informatica dei sistemi OT passerà al CISO entro un anno.

Tendenza: Il COO monitora e registra le metriche chiave della sicurezza informatica con più probabilità rispetto al CISO.

Come discusso in precedenza, i CISO si assumeranno presto la responsabilità primaria della sicurezza OT nella maggior parte delle organizzazioni. Questa tendenza significa che i CISO e i COO dovranno lavorare insieme sulle questioni di sicurezza informatica dei sistemi OT, territorio inesplorato per entrambi. Il confronto delle tendenze nelle loro attività di misurazione e reporting delle metriche di sicurezza informatica rivela alcune interessanti somiglianze e differenze.

Innanzitutto, è più probabile che siano i COO piuttosto che i CISO a monitorare le quattro metriche di sicurezza informatica principali: intrusioni rilevate e risolte (il 68% contro il 59%), implicazioni finanziarie (il 68% contro il 46%), vulnerabilità individuate e bloccate (il 62% contro il 44%) e riduzione/eliminazione dei costi (il 57% contro il 51%) (Figura 13). Sebbene ciò sembri controintuitivo, ha più senso se si considera che una responsabilità primaria del COO implica la gestione dei processi produttivi, che sono una funzione di per sé basata sui dati. È pertanto opportuno che i CISO che si occupano di sistemi OT inizino ad adottare il linguaggio aziendale utilizzato dai propri COO per misurare l'efficacia complessiva delle iniziative di sicurezza. Questo approccio consentirà loro anche di comunicare in modo più efficace con gli altri dirigenti di livello C, come il CEO e il CFO, nonché con il consiglio di amministrazione.[5]

Le implicazioni finanziarie rappresentano la differenza maggiore, in quanto sono monitorate da oltre due terzi (68%) dei COO ma da meno della metà (46%) dei CISO. Questo dato riflette probabilmente l'importanza che le aziende attribuiscono ai margini di profitto, fortemente influenzati da fattori sotto il controllo del COO. Dato che i COO hanno spesso maggiore esperienza nel monitorare le implicazioni finanziarie, i CISO dovrebbero sfruttare l'opportunità per emulare le best practice delle loro controparti e dedicare maggiore attenzione agli aspetti finanziari.

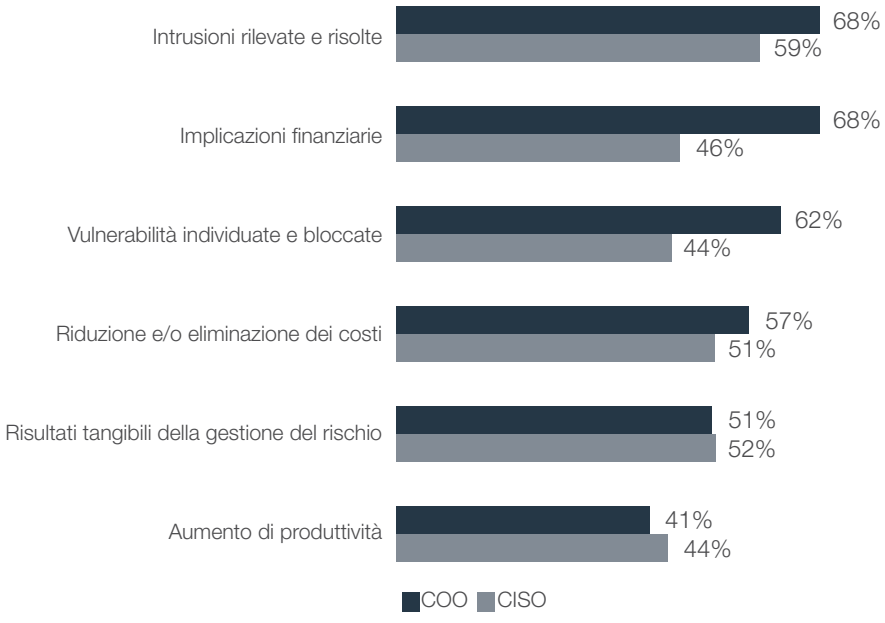


Figura 13: Confronto tra le metriche monitorate e registrate da COO e CISO.

Tendenza: I COO devono affrontare la sfida della gestione della complessità quando prendono decisioni sulle soluzioni di sicurezza informatica.

La stragrande maggioranza (84%) dei COO è coinvolta regolarmente nelle decisioni di acquisto per la sicurezza informatica dei sistemi OT, mentre i restanti (16%) sono coinvolti occasionalmente (Figura 14). I COO riferiscono che tali decisioni possono avere impatti negativi in termini di complessità (70%), adozione di standard di sicurezza (54%) ed efficienza operativa (49%) (Figura 15). Come in molte altre aree, il COO deve bilanciare la necessità di sicurezza con le esigenze di efficienza operativa nell'assunzione di decisioni di acquisto. Per una discussione sull'impatto della complessità sul rischio organizzativo, vedere "Sfide principali per il COO" qui di seguito.

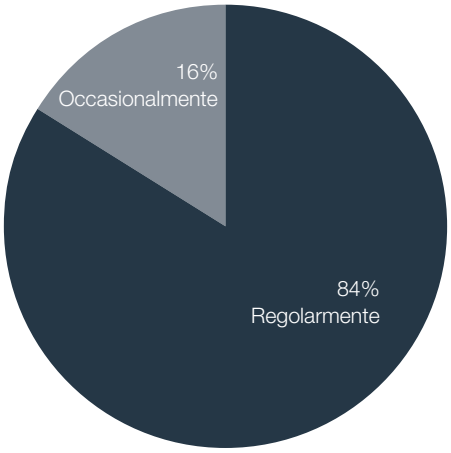


Figura 14: Coinvolgimento del COO nelle decisioni di acquisto OT.

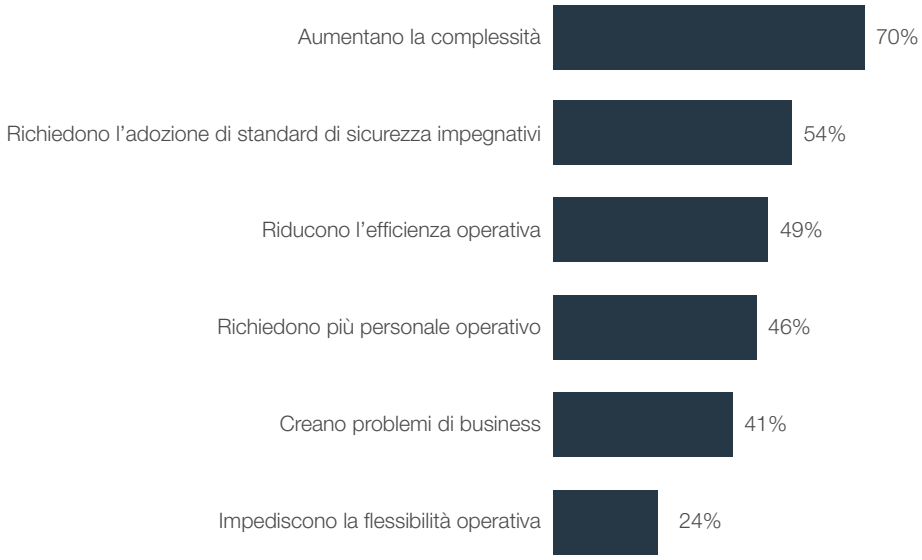


Figura 15: Impatto negativo delle soluzioni di sicurezza informatica sul successo professionale del COO.

Sfide principali per il COO

Nel nostro sondaggio abbiamo posto agli intervistati diverse domande a risposta aperta sulle sfide principali che devono affrontare nel loro lavoro. Anche se le risposte sono state molto diverse, le abbiamo categorizzate in modo da avere un'idea di ciò che è al primo posto per i COO in termini di OT. Le domande riguardavano le sfide derivanti da tre tendenze generali relative alla sicurezza: il panorama delle minacce avanzate, l'espansione della superficie di attacco e l'aumento della complessità.

Sfida: la maggior parte dei COO cita "tenere il passo con il cambiamento" come una delle sfide principali associate al panorama delle minacce avanzate.

In aggiunta alla gestione del rischio, il 61% dei COO riferisce che il panorama delle minacce avanzate rende difficile stare al passo con i cambiamenti (Figura 17). Questo dato può essere spiegato dal fatto che molte organizzazioni stanno collegando l'infrastruttura OT, un tempo isolata, con il mondo esterno. Di conseguenza, l'infrastruttura OT si trova improvvisamente bombardata da un gran numero di pacchetti malware legacy. Questi exploit legacy rappresentano una minaccia minima per l'infrastruttura IT, ma possono causare gravi danni in determinate aree di un sistema OT che non dispongono di una protezione basata sulle signature. Non sorprende quindi che i COO abbiano difficoltà a tenere il passo con questa nuova serie di sfide.

Sfida: l'espansione della superficie di attacco rende più difficile per i COO gestire i rischi, tenere il passo con i cambiamenti e prevenire le intrusioni.

I COO intervistati hanno riferito che l'espansione della superficie di attacco rende più difficile gestire il rischio (65%), tenere il passo con il cambiamento (48%) e implementare difese contro gli attacchi (26%) (Figura 18). Tenere il passo con il cambiamento è un tema ricorrente in questa parte dell'indagine e viene al secondo posto in tutte e tre le aree.

Sfida: la crescente complessità della gestione della sicurezza informatica contribuisce in modo significativo al carico di lavoro e allo stress lavorativo del COO.

Gli ambienti di rete OT stanno diventando sempre più complessi già solo in termini di numero di dispositivi in funzione. In questo sondaggio, l'87% degli intervistati gestisce almeno 100 dispositivi, mentre il 41% ne ha più di 250 da gestire (Figura 16). Questa crescita del numero di dispositivi contribuisce alla complessità, soprattutto in termini di aggiornamenti e manutenzione.

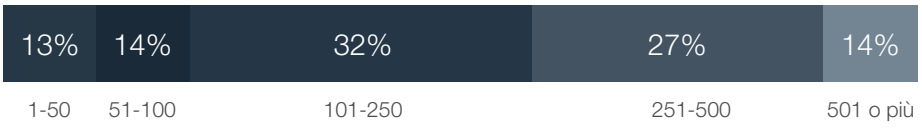


Figura 16. Numero di dispositivi in funzione.

Quasi un terzo (32%) degli intervistati afferma che la complessità della gestione dei propri sistemi di sicurezza informatica ha aumentato il carico di lavoro e, di conseguenza, il livello di stress. Quasi altrettanti (29%) riferiscono che la complessità rende anche più difficile colmare la carenza di competenze, il che pone maggiore pressione sul COO e contribuisce indubbiamente ad aumentare il carico di lavoro e lo stress lavorativo (32%) (Figura 19).

"La preoccupazione principale dei responsabili della sicurezza informatica e dei dirigenti aziendali è la superficie di attacco in continua espansione di cui devono quotidianamente assicurare la protezione."

– Relatore al summit della National Cyber Security Alliance [6]

L'implicazione di questi dati è che i COO devono affrontare sfide significative per bilanciare le responsabilità in materia di sicurezza informatica OT con il compito di assicurare disponibilità, efficienza e produttività. Questa tendenza è probabilmente destinata a crescere parallelamente al numero di dispositivi OT e alla complessità della loro gestione.

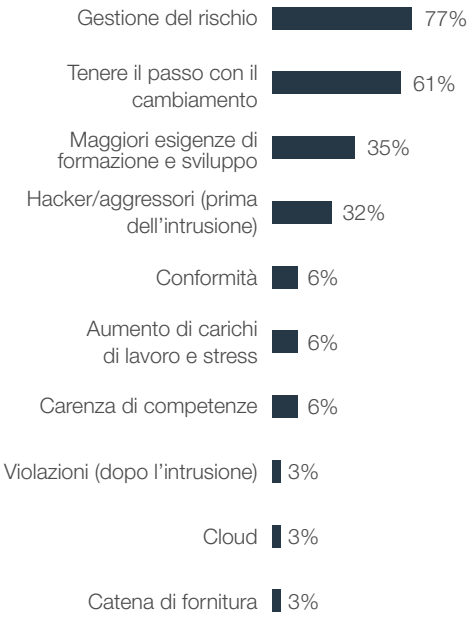


Figura 17: Sfide per i COO causate dal panorama delle minacce avanzate.

Figura 18: Sfide per i COO causate dall'espansione della superficie di attacco.

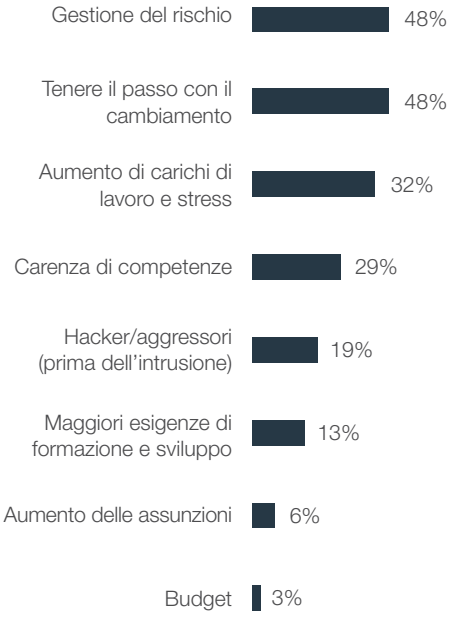


Figura 19: Sfide per i COO causate dall'aumento della complessità.

Sfida: Nel complesso, la gestione del rischio è la più grande sfida della sicurezza informatica che il COO di oggi deve affrontare.

Il rischio informatico è attualmente la preoccupazione principale delle imprese di ogni dimensione. Dei 1.200 leader aziendali che hanno partecipato a un recente sondaggio, il 55% ha dichiarato di preoccuparsi in parte o in gran parte dei rischi informatici.[7]

Considerando questa parte del sondaggio come un insieme, è stato maggiore il numero di COO che hanno citato la gestione del rischio rispetto a qualsiasi altro fattore: il 77% a causa del panorama delle minacce più avanzato (Figura 17), il 65% a causa dell'espansione della superficie di attacco (Figura 18) e il 48% a causa dell'aumento della complessità (Figura 19). Questi dati sono allineati alla precedente constatazione che la strategia di sicurezza OT influenza la valutazione complessiva dei rischi dell'organizzazione.

Per fornire ulteriore contesto, abbiamo confrontato i risultati relativi ai COO con quelli relativi alle figure del CIO,[8] del CISO[9] e del responsabile della gestione tecnica e operativa della rete[10] (Figura 20). Emergono diverse osservazioni:

"Il nostro istituto sta affrontando l'aumento della complessità insegnando ai nostri dipendenti a gestire le nuove tecnologie in modo proattivo."

– Intervistato del sondaggio nel settore dell'energia

- Predomina il numero dei COO che considera il panorama delle minacce in evoluzione come una sfida per la gestione del rischio rispetto alle altre tre figure. Un'interpretazione positiva di questa constatazione è che i COO sono ben consapevoli delle sfide poste dalla relativa scarsa protezione dell'infrastruttura OT e identificano correttamente questa realtà come un rischio per l'organizzazione.
- Un numero molto maggiore di COO e di responsabili della gestione tecnica e operativa della rete indica nella gestione del rischio la sfida principale in materia di sicurezza informatica rispetto ai CIO e ai CISO. Questo dato non significa che i CIO e i CISO non si preoccupino della gestione del rischio, ma riflette piuttosto le loro priorità. Ad esempio, sia i CIO che i CISO considerano le maggiori esigenze di formazione e sviluppo come una sfida più grande rispetto alla gestione del rischio.
- I CIO sono i meno propensi a citare la gestione del rischio come la sfida principale della sicurezza informatica. Questo dato potrebbe riflettere il fatto che i CIO tendono a concentrarsi più sulla disponibilità e sull'affidabilità che sulla sicurezza. Un'altra possibile spiegazione è che i CIO, semplicemente, hanno più esperienza nella gestione del rischio e quindi è meno probabile che considerino fattori come l'espansione della superficie di attacco un ostacolo significativo a una gestione appropriata del rischio.

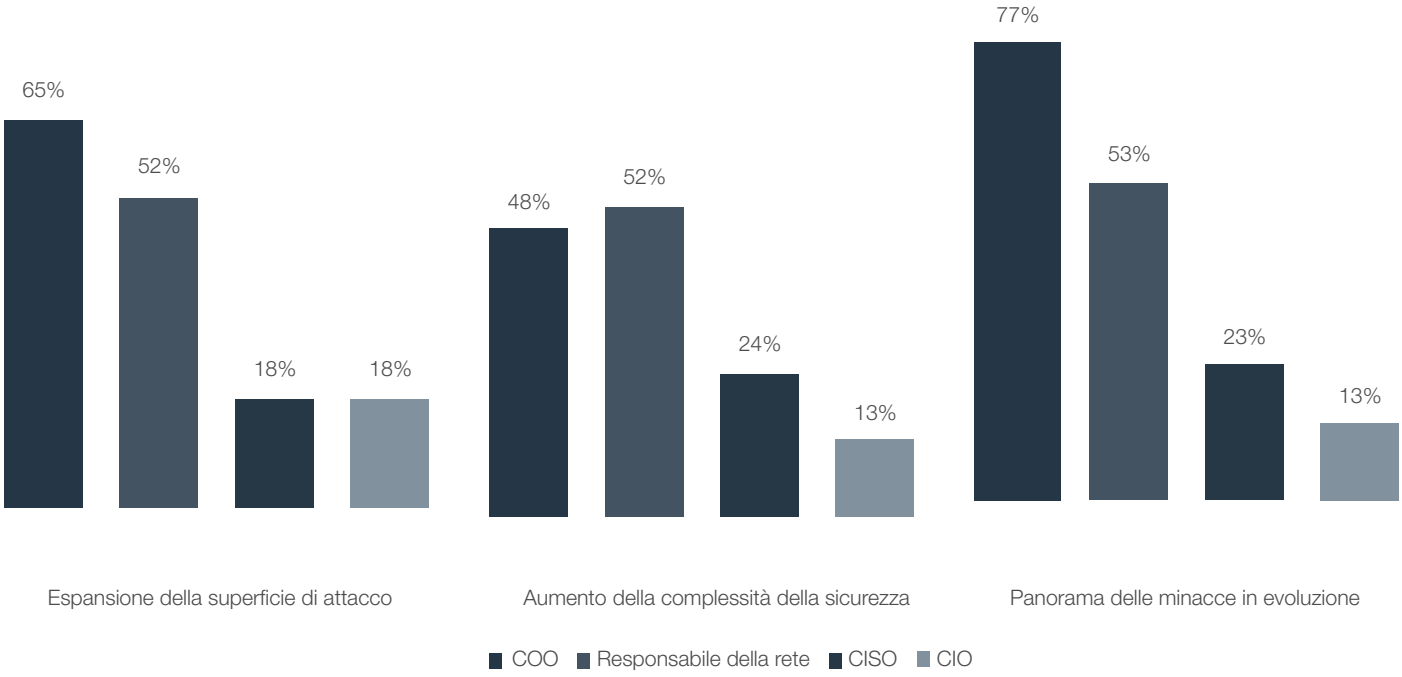


Figura 20: Percentuale di intervistati che citano le sfide della gestione del rischio: confronto tra COO, responsabili IT e CISO.

Best practice dei COO di livello superiore

Abbiamo confrontato le risposte al sondaggio di due sottoinsiemi in base al numero di intrusioni subite. Questo confronto tra gli intervistati "di livello superiore" e "di livello inferiore" ha identificato una serie di best practice che i COO di livello superiore adottano con maggiore probabilità:

1. I COO di livello superiore hanno il 168% di probabilità in più di citare i cambiamenti normativi come una delle principali sfide da superare per il successo e il 45% di probabilità in più di programmare controlli di conformità come risposta.

Mentre gli intervistati citano una serie di questioni che influiscono sul loro lavoro, quelli di livello superiore mostrano una propensione maggiore del 168% a citare i cambiamenti normativi come uno dei tre maggiori problemi che incidono sul successo professionale. Un aspetto correlato è quello che vede una propensione maggiore del 45% dei COO di livello superiore a condurre controlli regolari della conformità alle norme di sicurezza, il che indica probabilmente che questi COO rispondono alle sfide normative in modo proattivo.

2. I COO di livello superiore hanno il 124% di probabilità in più di lavorare in organizzazioni in cui un dirigente di livello C ha la responsabilità finale della sicurezza informatica.

Data la maggiore consapevolezza aziendale dell'importanza della sicurezza OT discussa in precedenza, non sorprende che una responsabilità di alto livello sia correlata a un numero minore di intrusioni. Come già detto, molte organizzazioni stanno trasferendo la responsabilità della sicurezza informatica dei sistemi OT al CISO ed è prevedibile che questa scelta sia ripagata da una riduzione delle intrusioni.

3. I COO di livello superiore hanno il 79% di probabilità in più di classificare l'efficienza dell'area di produzione come la metrica principale del loro successo.

I COO devono costantemente trovare un punto di incontro tra la loro tradizionale attenzione alle operazioni e le crescenti aspettative sulla sicurezza dell'infrastruttura OT. I COO di livello superiore trovano il modo di adempiere agli obblighi di sicurezza pur continuando a concentrarsi sull'efficienza operativa.

4. I COO di livello superiore hanno il 49% di probabilità in più di utilizzare l'autenticazione a più fattori.

L'autenticazione a più fattori è un modo comprovato per migliorare i livelli di sicurezza di un'organizzazione. Un recente sondaggio ha rilevato che i professionisti della sicurezza adottano la combinazione di password e autenticazione a più fattori per la loro sicurezza personale più di qualsiasi altra misura.[11] Quando si tratta di sicurezza informatica, i COO di maggior successo adottano questa best practice e, di conseguenza, migliorano le loro difese contro le minacce.

5. I COO di livello superiore hanno il 34% di probabilità in più di monitorare l'aumento della produttività come metrica della sicurezza informatica.

I COO sono valutati in base alla produttività ed è quindi logico che associno i programmi di sicurezza all'efficienza operativa, che si tratti di velocizzare le attività o semplicemente di evitare i flussi di lavoro manuali automatizzandoli. I COO di livello superiore hanno il 49% di probabilità in più di monitorare le implicazioni finanziarie come metrica della sicurezza informatica.

Le organizzazioni valutano regolarmente i loro COO in base ai risultati finanziari complessivi. Pertanto, non sorprende che i COO di livello superiore estendano il loro processo di monitoraggio del budget alle responsabilità in materia di sicurezza informatica.

6. I COO di livello superiore hanno il 34% di probabilità in più di riferire i risultati dei test di penetrazione e di intrusione al responsabile della sicurezza informatica.

Questo dato sottolinea l'importanza che i leader della sicurezza informatica attribuiscono ai test come modo per valutare accuratamente il rischio. I test individuano in modo proattivo le vulnerabilità e indicano le aree dove applicare azioni correttive. Il fatto che i COO di livello superiore abbiano tempo da dedicare ai test suggerisce che dispongono di personale aggiuntivo in grado di gestire le attività di gestione quotidiana della sicurezza.

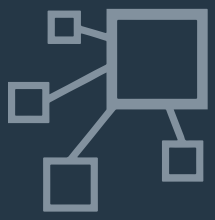
Conclusioni

La ricerca mostra che, quando si tratta di sicurezza informatica dei sistemi OT, i COO hanno una visibilità elevata in azienda e, allo stesso tempo, sono sottoposti a forti pressioni per gestire il rischio e assolvere alle loro responsabilità in merito alla sicurezza in aggiunta ai loro tradizionali compiti operativi. I COO che intendono migliorare i loro risultati in materia di sicurezza possono utilizzare queste best practice adottate dai loro colleghi di maggior successo:

Registrare e monitorare le principali metriche di sicurezza e operative

Effettuare regolarmente test della sicurezza e verifiche della conformità

Rivolgere l'attenzione alle implicazioni finanziarie delle misure di sicurezza informatica



Investire in contromisure collaudate come l'autenticazione a più fattori

Riferimenti

[1] Barbara Filkins and Doug Wylie, "SANS 2019 State of OT/ICS Cybersecurity Survey", SANS Institute, 11 giugno 2019.

[2] "Report Fortinet: Tendenze nella sicurezza delle tecnologie operative 2019. Un aggiornamento sul panorama delle minacce per i sistemi ICS e SCADA", Fortinet, 8 maggio 2019.

[3] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 26 aprile 2019.

[4] Barbara Filkins and Doug Wylie, "SANS 2019 State of OT/ICS Cybersecurity Survey", SANS Institute, 11 giugno 2019.

[5] "The CFO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 11 settembre 2019.

[6] Doug Olenick, "Expanding Attack Surfaces and Difficulties Obtaining The Right People Worry NCSA panelists", SC Magazine, 16 ottobre 2018.

[7] "Cyber Risk Is Top Concern for All, SMB Risks CISOs Need to Heed", The CISO Collective, 25 ottobre 2019.

[8] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 maggio 2019.

[9] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 26 aprile 2019.

[10] "Cybersecurity and the Network Engineering and Operations Leader: A Report on Current Priorities and Challenges", Fortinet, 4 settembre 2019.

[11] "The 2019 State of Password and Authentication Security Behaviors Report", Ponemon Institute, gennaio 2019.

www.fortinet.com

4 gennaio 2020 04:13

report-FA-COO-and-cybersecurity

323524-0-1-IT