

IL RUOLO DEL CISO 2025

A CURA DI ELENA VACIAGO,
RESEARCH MANAGER, THE INNOVATION GROUP

Un'indagine di AssoCISO e TIG

CYBERSECURITY SUMMIT 2025,
19 Novembre 2025



1. **Il CISO evolve verso un ruolo di leadership strategica.** Dalla survey emerge una figura sempre più matura, chiamata non solo a proteggere, ma anche a guidare il cambiamento e a tradurre la sicurezza in valore per l'impresa. Il percorso professionale del CISO si apre a ruoli di vertice.
2. **Il ruolo del CISO si consolida ma con differenze di maturità e riconoscimento: è presente solo nel 61% delle aziende intervistate** (che già dispongono di una strategia formale di cybersecurity) mentre negli altri casi la responsabilità sulla cybersecurity ricade su altre funzioni (CIO, CTO, CSO). Con riferimento alla **collocazione aziendale** del Responsabile cybersecurity, si osserva una situazione molto disomogenea: il Responsabile cybersecurity nel 30% dei casi riporta al CIO e nel 29% al vertice.
3. Solo la metà delle aziende prevede un **flusso strutturato di comunicazione verso il CdA**, mentre altrove il dialogo resta sporadico o intermediato. Questo limita la capacità del CISO di influenzare le decisioni strategiche.
4. **Manca ancora una piena integrazione della sicurezza nei processi aziendali:** solo il 65% dichiara che la strategia di cybersecurity è pienamente attuata. La comprensione della strategia di cybersecurity da parte del business è buona solo nel 46% delle aziende, la disponibilità di risorse adeguate nel 36%.
5. **La carenza di personale di cybersecurity è la principale criticità.** Il team ideale di cybersecurity dovrebbe essere del 54% più ampio (in media).
6. L'evoluzione tecnologica, così come la situazione geopolitica, impongono un **ripensamento della sicurezza**.

STEERING COMMITTEE DELLA RICERCA:



Yuri Rassega

CISO, Enel Group e
Presidente AssoCISO



Massimo Cottafavi

Director Cyber Security & Resilience, Snam
Socio AssoCISO



Nicla Diomede

Direttore del Dipartimento Cybersecurity e
Sicurezza, Roma Capitale
Co-founder AssoCISO



Simonetta Sabatino

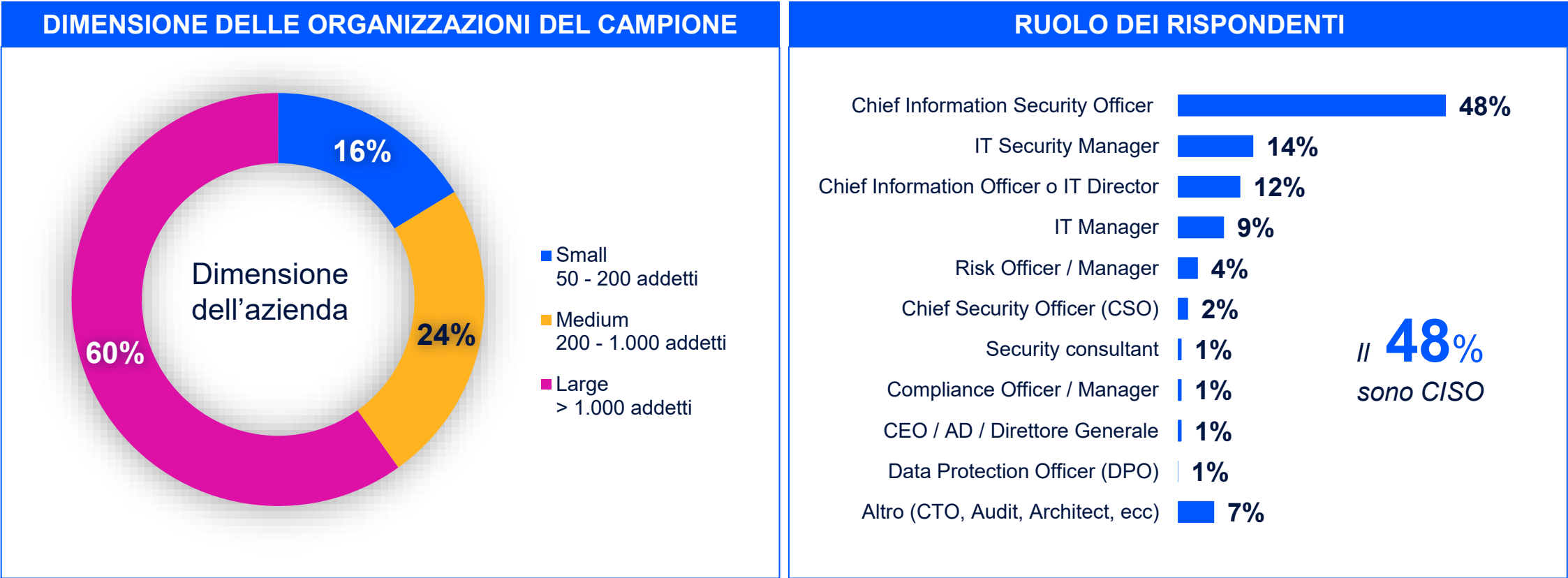
Head of Cyber Security, Saras
Co-founder AssoCISO



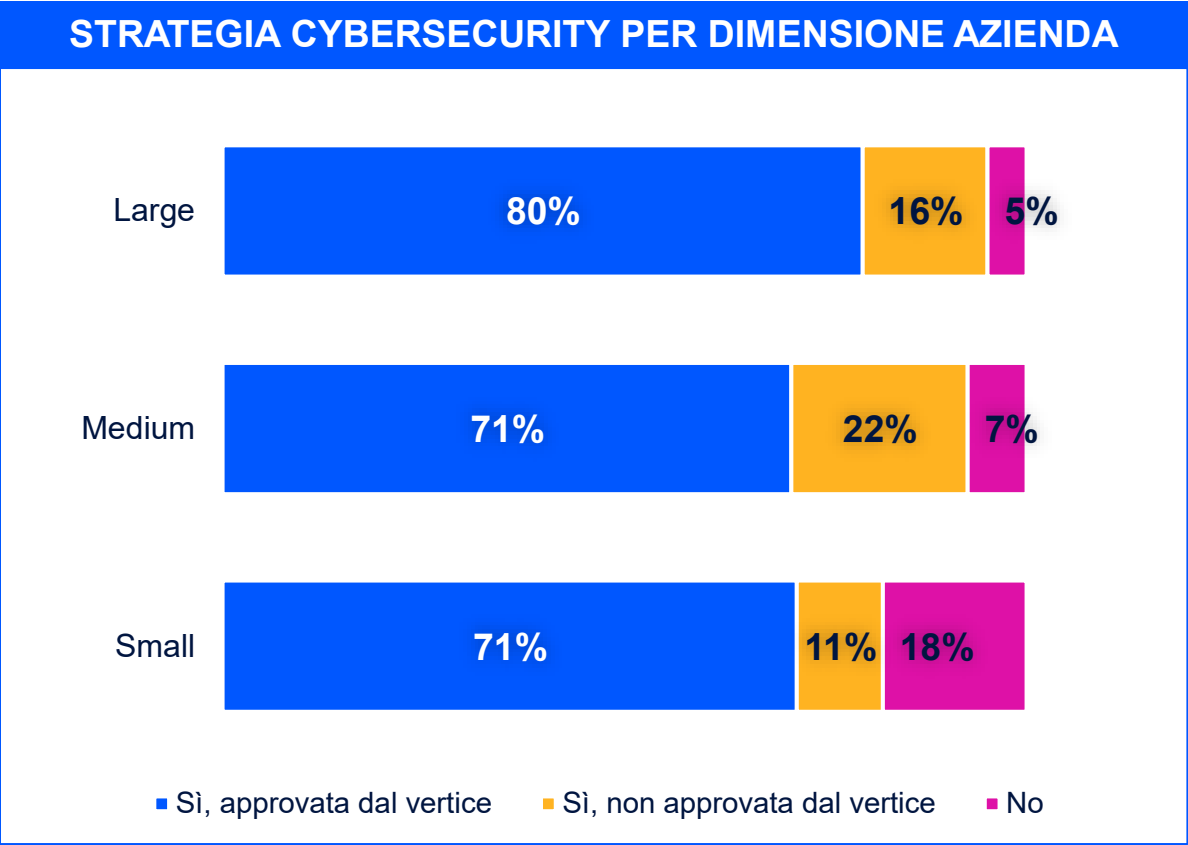
Nicola Sotira

Responsabile CERT, Poste Italiane
Co-founder AssoCISO

L'indagine è stata svolta tra luglio e settembre 2025 da The Innovation Group e AssoCISO in modalità CAWI. Hanno preso parte al questionario, in modo completo o parziale, **172 rispondenti**, soprattutto Chief Information Security Officer (CISO) e Manager della Cybersecurity. Nel 60% dei casi, le organizzazioni del campione appartengono ad organizzazioni di grande dimensione (oltre 1.000 addetti) e nel 24% di media dimensione (tra 1.000 e 200 addetti). I settori più rappresentati sono l'Industria e la Finanza.



PRESENZA DI UNA STRATEGIA FORMALE DI CYBERSECURITY

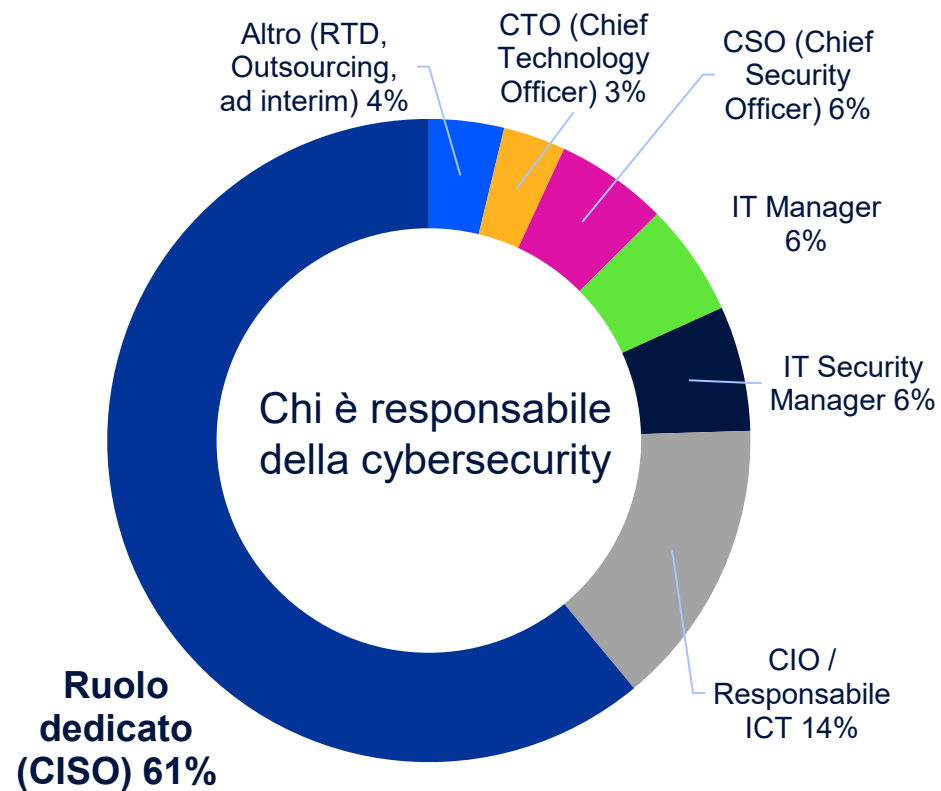


D. La Sua organizzazione ha una strategia formale di cybersecurity?
Base: tutti i rispondenti (172) con risposte per dimensione aziendale: Large (> 1.000 addetti); Medium (da 200 a 1.000 addetti) e Small (da 50 a 200 addetti)

COME SI CONFIGURA OGGI IL RUOLO DEL CISO, COME DOVREBBE EVOLVERE?

PRESENZA DI UN RUOLO DEDICATO (CISO) PER LA CYBERSECURITY

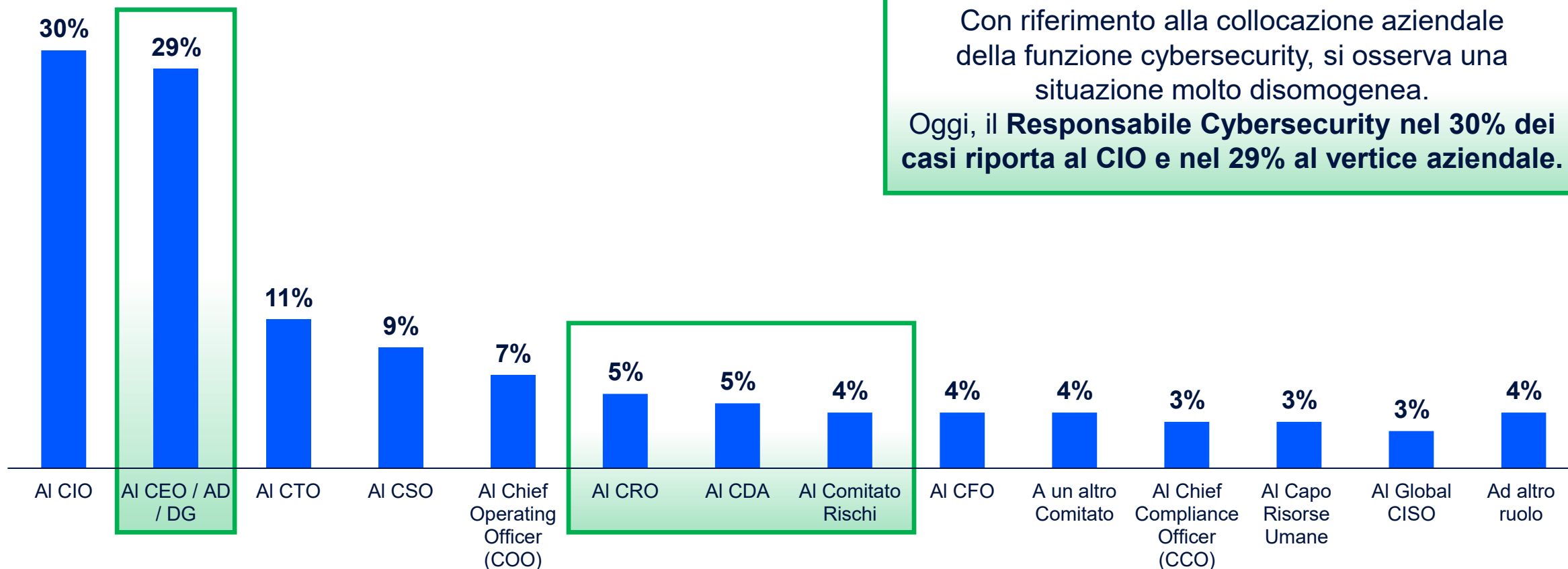
PRESENZA DEL CISO	
INDUSTRIA	52%
FINANZA	81%
PA	65%
UTILITIES	67%



PRESENZA DEL CISO	
TUTTE	61%
LARGE	66%
MEDIUM	56%
SMALL	45%

D. Chi è il Responsabile della Cybersecurity nella Sua organizzazione?
Base: tutti i rispondenti (159)

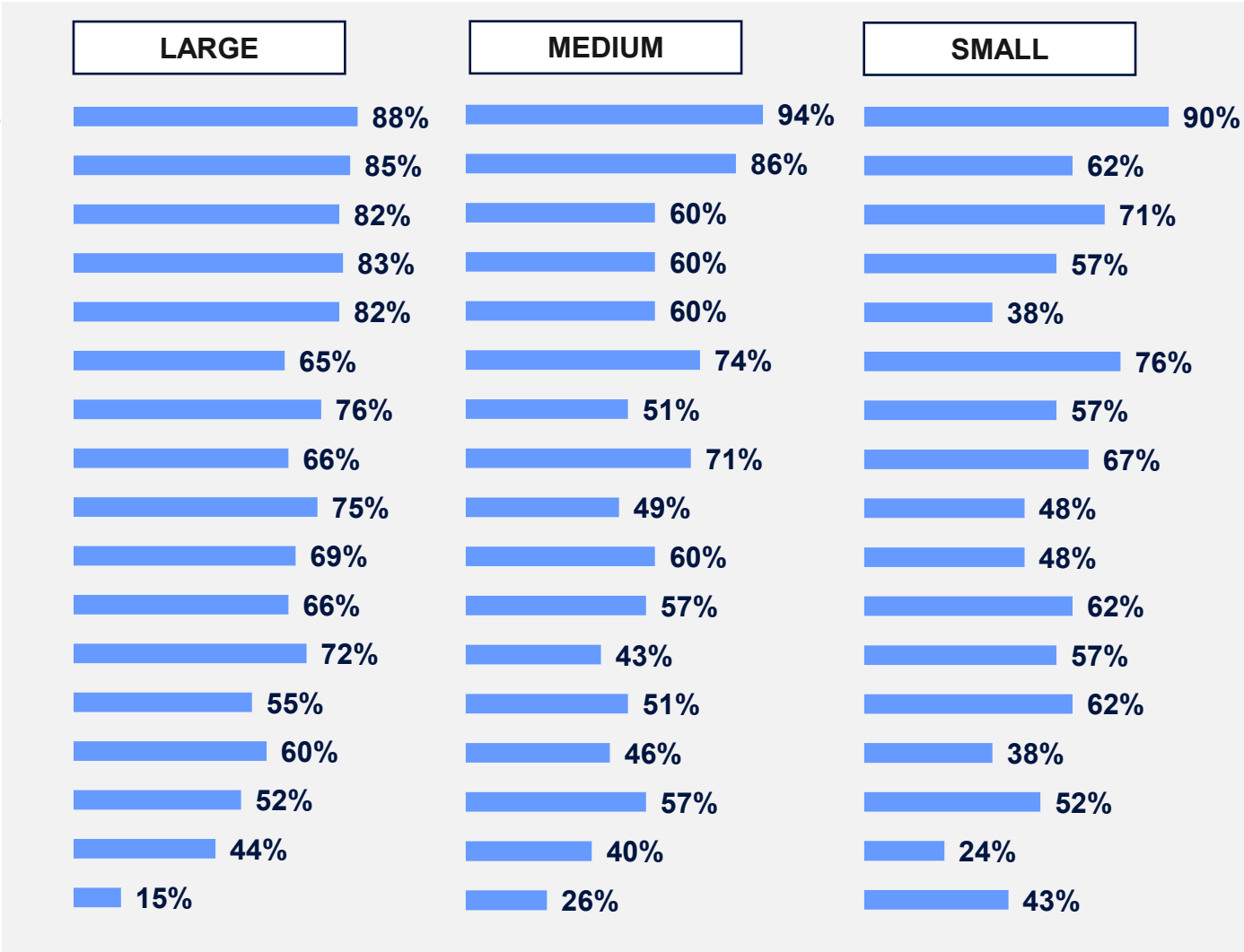
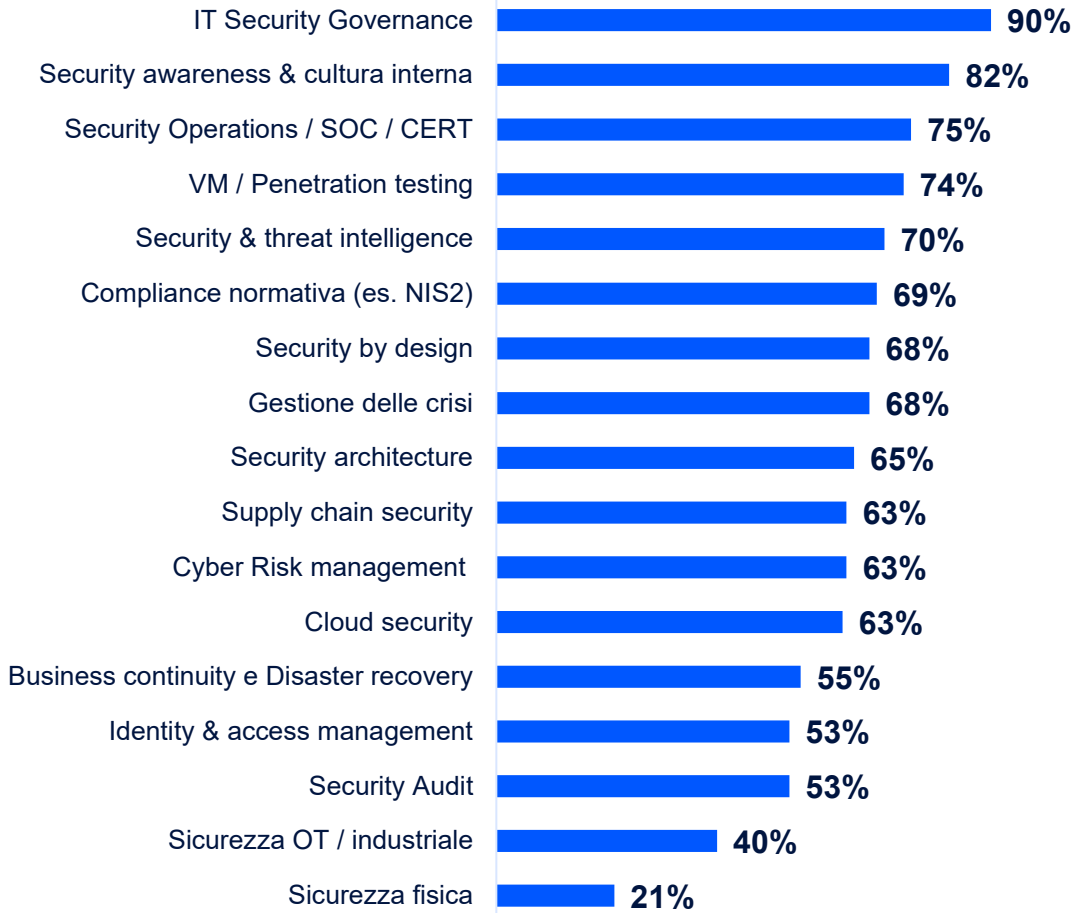
A CHI RIPORTA IL CISO O IL RESPONSABILE CYBERSECURITY NELLE ORGANIZZAZIONI



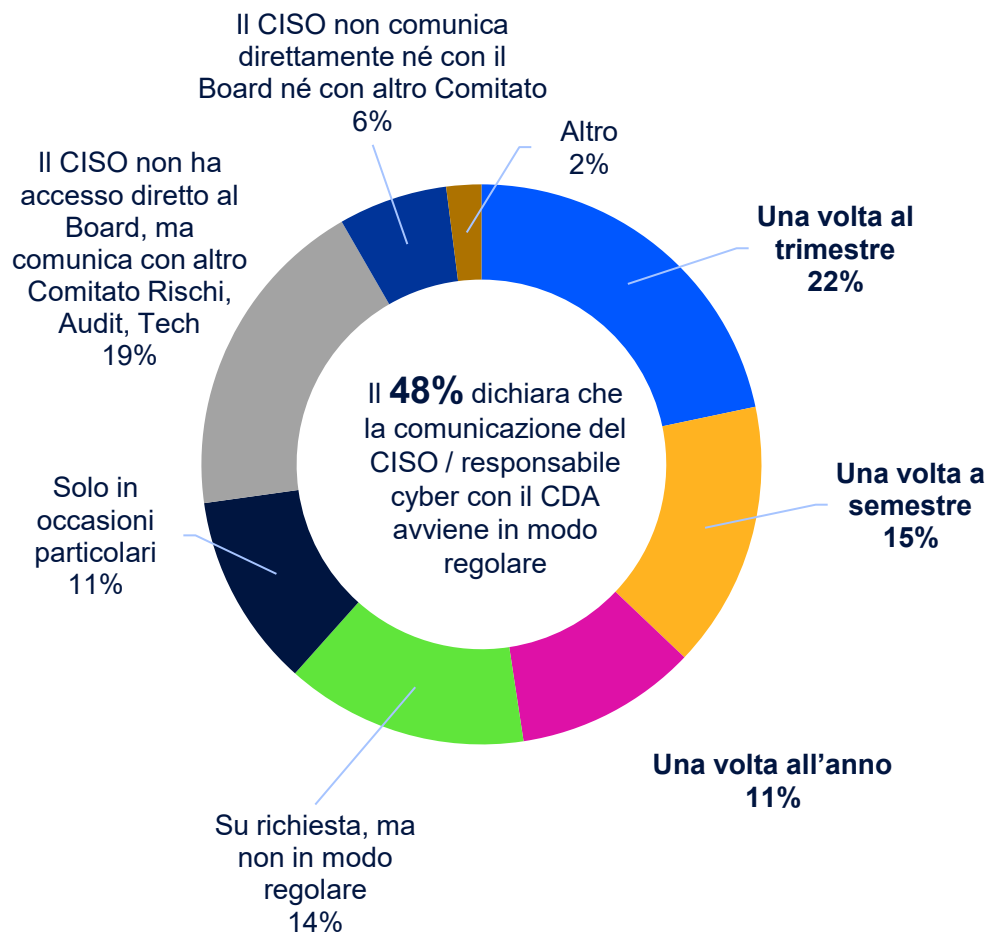
Con riferimento alla collocazione aziendale della funzione cybersecurity, si osserva una situazione molto disomogenea. Oggi, il **Responsabile Cybersecurity nel 30% dei casi riporta al CIO e nel 29% al vertice aziendale.**

D. A chi riporta il CISO / Responsabile della cybersecurity nella Sua organizzazione?
Base: tutti i rispondenti (148)

QUALI SONO LE RESPONSABILITA' DEL CISO

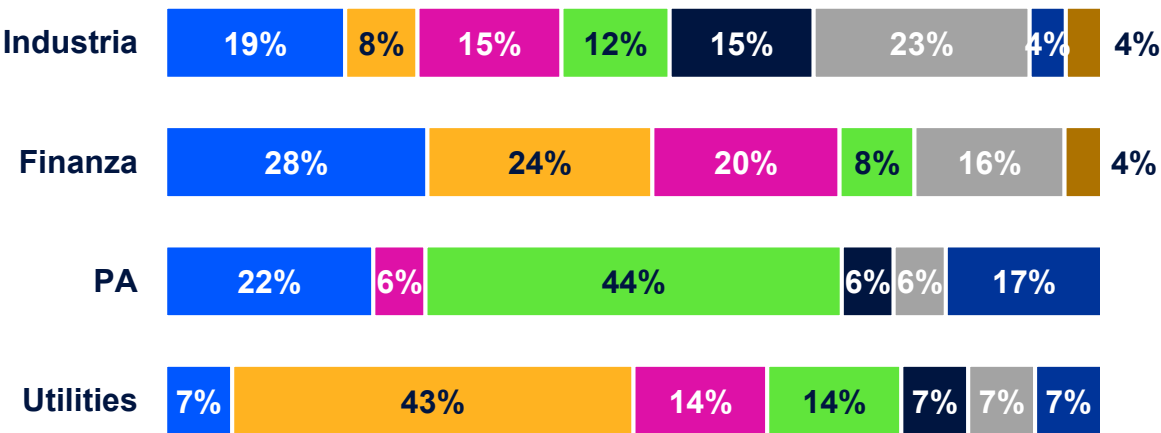


D. Quali responsabilità fanno oggi parte del perimetro del ruolo di CISO?
Base: tutti i rispondenti (145)



D. In che misura il CISO / responsabile cybersecurity della Sua organizzazione ha accesso diretto e regolare al Board per discutere di cybersecurity?
Base: tutti i rispondenti (144)

COMUNICAZIONE DEL CISO CON IL CDA PER SETTORE VERTICALE



- Una volta al trimestre
- Una volta a semestre
- Una volta all'anno
- Su richiesta, ma non in modo regolare
- Solo in occasioni particolari
- Il CISO non ha accesso diretto al Board, ma comunica con altro Comitato Rischi, Audit, Tech
- Il CISO non comunica direttamente né con il Board né con altro Comitato
- Altro

QUALI SONO LE PRINCIPALI SFIDE INCONTRATE DAL CISO?



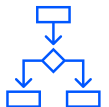
Carenza di **personale** o turnover nel team

57%



Difficoltà nel comunicare il **valore della cybersecurity**

39%



Ruolo non sufficientemente riconosciuto

38%



Mancanza di budget adeguato

36%



Scarso interesse / **accountability del business** sul tema cybersecurity

34%

Il problema maggiore avvertito dal CISO è legato alla **difficoltà di ottenere personale a sufficienza**, a seguire il problema di **far comprendere il reale valore della cybersecurity**

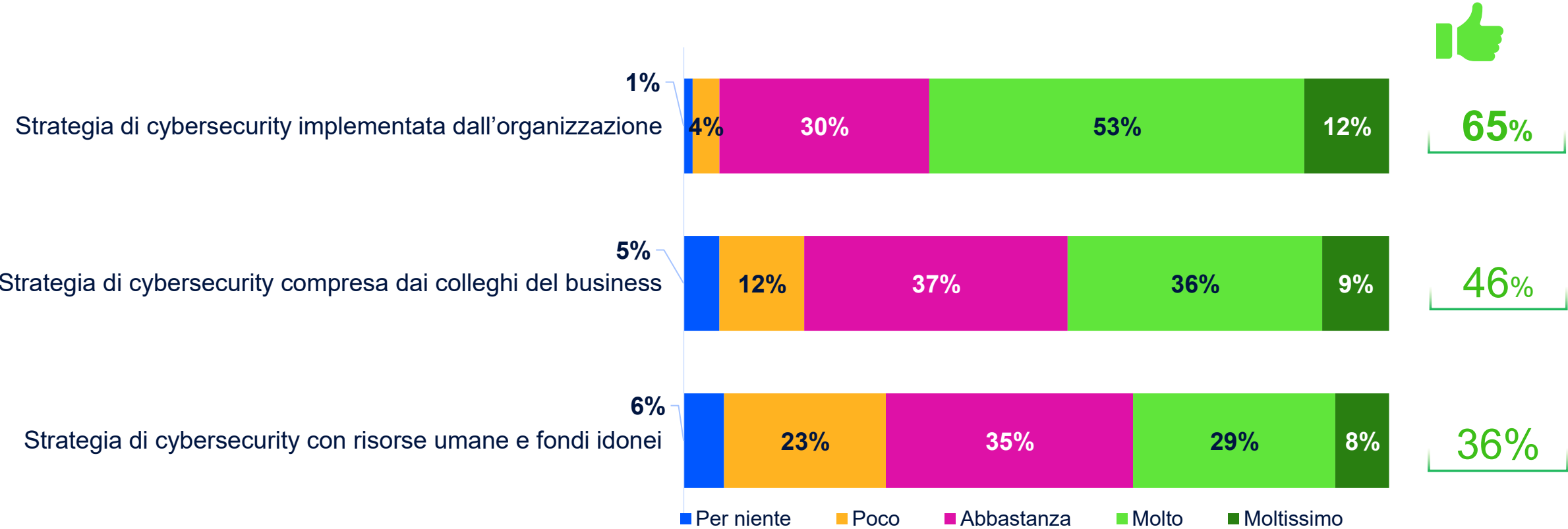
INDAGINE SUL RUOLO DEL CISO – SURVEY 2025 DI ASSOCISO E TIG, SETTEMBRE 2025

ALTRO: ECCESSIVA FRAMMENTAZIONE NORMATIVA; DIFFICOLTÀ NEL COORDINAMENTO TRA IT, OT E BUSINESS; AGGIORNAMENTO PROFESSIONALE CONTINUO; PESO ECCESSIVO DELLO STRESS PER IL CISO
PRESSIONI DA PARTE DI CLIENTI O FORNITORI; PRESSIONI DA PARTE DEGLI ENTI REGOLATORI
INCIDENZA DEL SISTEMA DEI CONTROLLI; MODELLO DI GOVERNANCE COMPLESSO

QUANTO LA CYBERSECURITY E' INTEGRATA NEI PROCESSI DELL'ORGANIZZAZIONE?

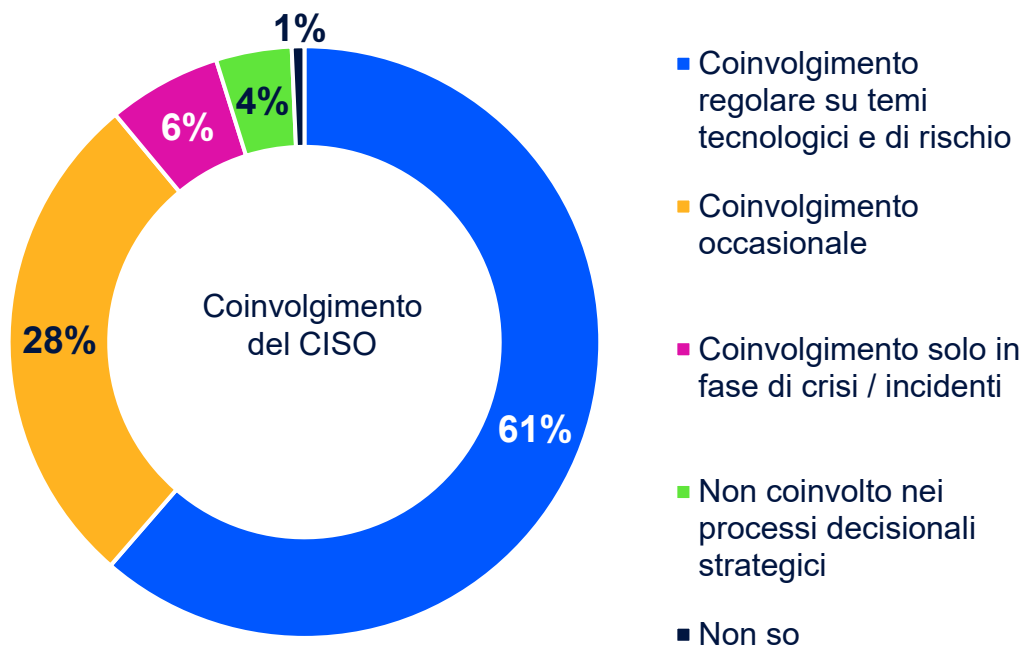
LA MATURITÀ MAGGIORE SI OSSERVA NELL'IMPLEMENTAZIONE, MINORE NEL SUPPORTO CON RISORSE E FONDI

LIVELLO RAGGIUNTO PER LA COMPrensIONE, IMPLEMENTAZIONE E FINANZIAMENTO DELLA STRATEGIA DI CYBERSECURITY



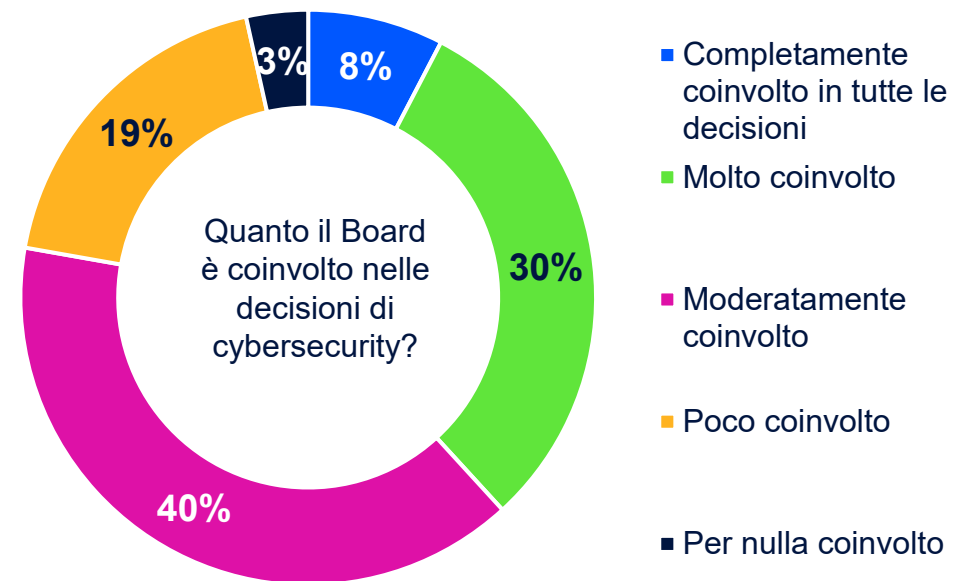
D. Se ne disponete, qual è la Sua valutazione sul livello raggiunto di comprensione, implementazione e finanziamento della strategia di cybersecurity? (In una scala da 1 a 5, dove 1= per niente e 5 = moltissimo)
Base: tutti i rispondenti (158)

COINVOLGIMENTO DEL CISO NEI PROCESSI DECISIONALI



D. In che misura il ruolo del CISO è integrato nei processi decisionali strategici dell'organizzazione?
Base: tutti i rispondenti (145)

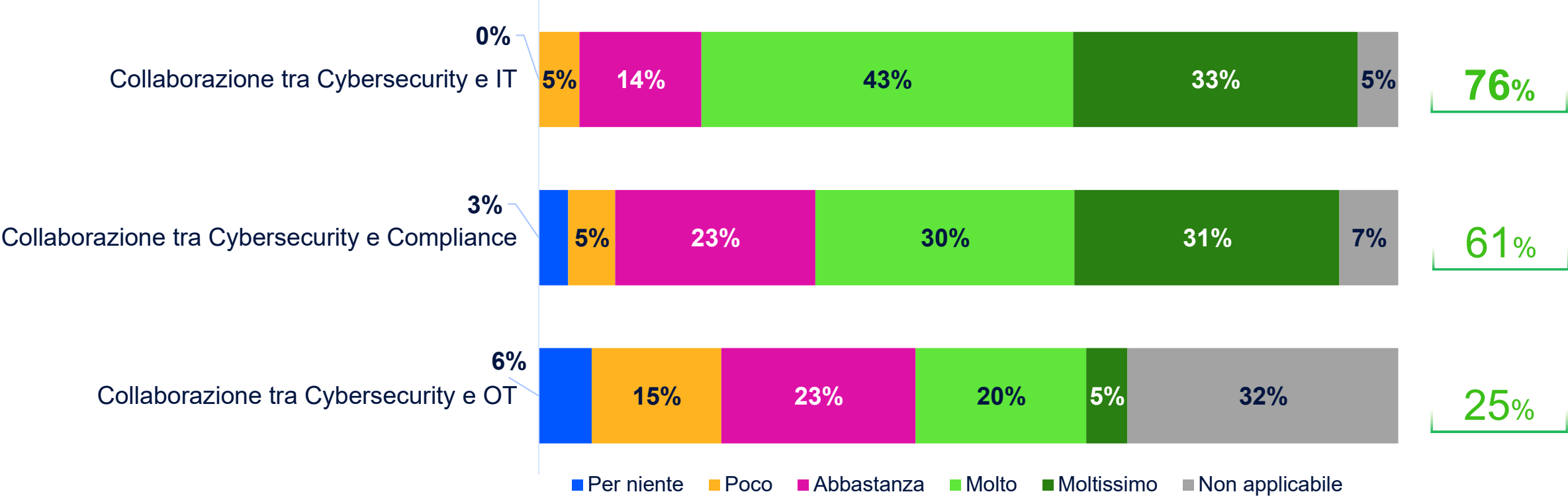
COINVOLGIMENTO DEL BOARD



D. Quanto ritiene che il Board della Sua organizzazione sia coinvolto nelle decisioni strategiche legate alla cybersecurity?
Base: tutti i rispondenti (144)

LA COLLABORAZIONE DELLA IT SECURITY È MOLTO BUONA CON IT E COMPLIANCE, POCO CON OT

LIVELLO DI MATURITA' DELLA COLLABORAZIONE TRA CYBERSECURITY E IT, COMPLIANCE, OT



D. Come valuta la collaborazione tra i Team Cybersecurity, IT, OT e Compliance nella Sua organizzazione? (In una scala da 1 a 5, dove 1= molto scarsa e 5 = eccellente. Scegliere l'opzione "Non applicabile" nel caso in cui manchino questi team)
Base: tutti i rispondenti (148)

QUALI SONO OGGI LE PRINCIPALI COMPETENZE (NON TECNICHE) RICHIESTE AL CISO?



Capacità di **comunicazione** con il board e il top management

96%



Leadership e gestione dei team

79%



Orientamento al business per comprenderne i processi critici

70%



Competenze in ambito **Risk Management**

67%



Pensiero critico e **problem solving**

65%

Le risposte evidenziano necessità di **NUOVE** competenze IN **AGGIUNTA** a quelle tecniche: dalla capacità di **comunicare in modo efficace**, alla leadership; orientamento al business, competenze di risk management e capacità problem solving

PRINCIPALI CRITICITÀ NELLA COMUNICAZIONE CON IL BOARD



Difficoltà del CISO a tradurre i rischi e i benefici della cybersecurity in **termini comprensibili per il business**

41%



Mancanza di comprensione tecnica degli interlocutori (Board / altro Comitato)

40%



La cybersecurity non è ancora percepita internamente come una **priorità strategica**

39%



Carenza di tempo e di spazio durante le riunioni per discutere a fondo di cybersecurity

39%



Insufficiente supporto o coinvolgimento da parte del top management

25%

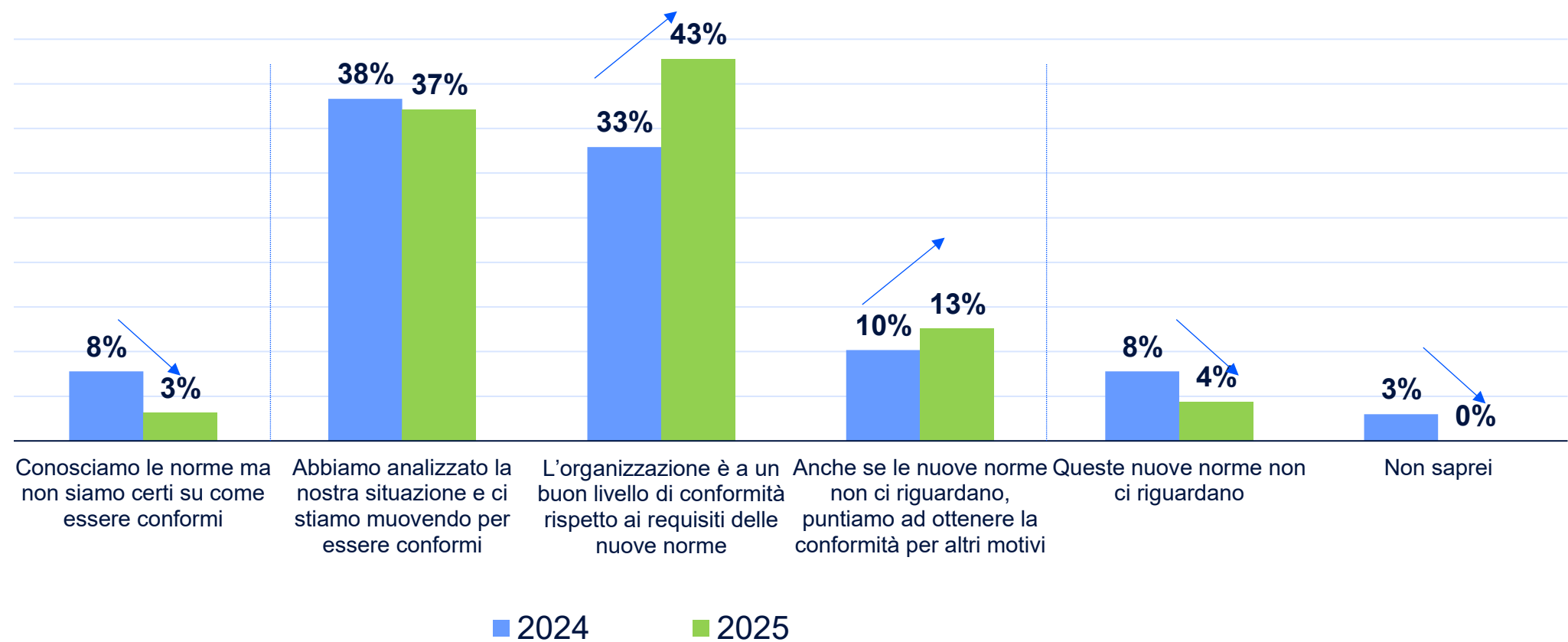
Per migliorare la comunicazione con il Board il CISO deve ripensare il proprio linguaggio, abbandonare i tecnicismi, coinvolgere gli interlocutori e individuare i momenti opportuni

D. Quali sono le principali difficoltà che il CISO incontra nel comunicare efficacemente con il Board / Altro Comitato sulla cybersecurity?
Base: tutti i rispondenti (144)

ALCUNE URGENZE: COMPLIANCE, TRASFORMAZIONE TECNOLOGICA, IMPATTI GEOPOLITICI E TEAM SECURITY

RISPETTO A FINE 2024 SI OSSERVA UN GRADUALE MIGLIORAMENTO

Qual è la situazione della Sua organizzazione con riferimento alla compliance alla direttiva NIS2?
(2024 vs 2025)



QUALI SONO I PRINCIPALI OSTACOLI INCONTRATI NEL PERCORSO NIS2?



Difficoltà nel gestire la sicurezza della **supply chain**

51%



Carenza di **risorse economiche** o umane dedicate

41%



Integrazione complessa con i processi aziendali esistenti

31%



Difficoltà nell'interpretazione dei **requisiti normativi**

19%



Coordinamento interno tra IT, OT, compliance e risk management

19%

La messa in sicurezza della supply chain è considerato l'ostacolo più importante, per almeno 1 organizzazione su 2, seguito da vicino dalla carenza di risorse da dedicare a questi sviluppi

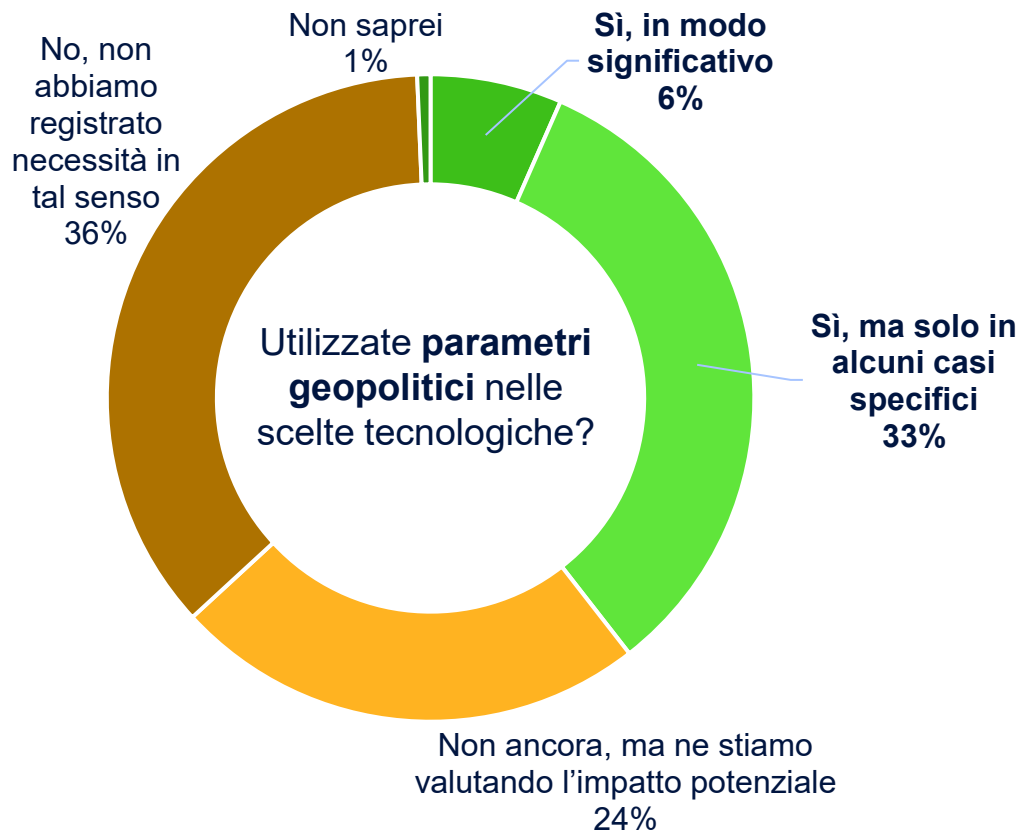
SITUAZIONE GEOPOLITICA, QUANTO IMPATTA SULLA CYBERSECURITY?

TREND GEOPOLITICI CHE INFLUENZANO SCELTE E INVESTIMENTI IN CYBERSECURITY

		INDUSTRIA	FINANZA	PA	UTILITIES
Politiche di cybersicurezza nazionale o UE (es. NIS2, EUCS)	61%	68%	42%	65%	71%
Rischi legati alla sovranità e localizzazione dei dati	53%	43%	58%	65%	50%
Tensioni o instabilità in aree chiave della supply chain	34%	39%	31%	35%	43%
Volontà di ridurre la dipendenza da tecnologie extra-UE	26%	25%	31%	35%	21%
Timori legati a backdoor o ingerenze statali nei software	20%	21%	35%	30%	21%
Restrizioni/ sanzioni internazionali verso vendor/ Paesi	20%	39%	27%	20%	7%

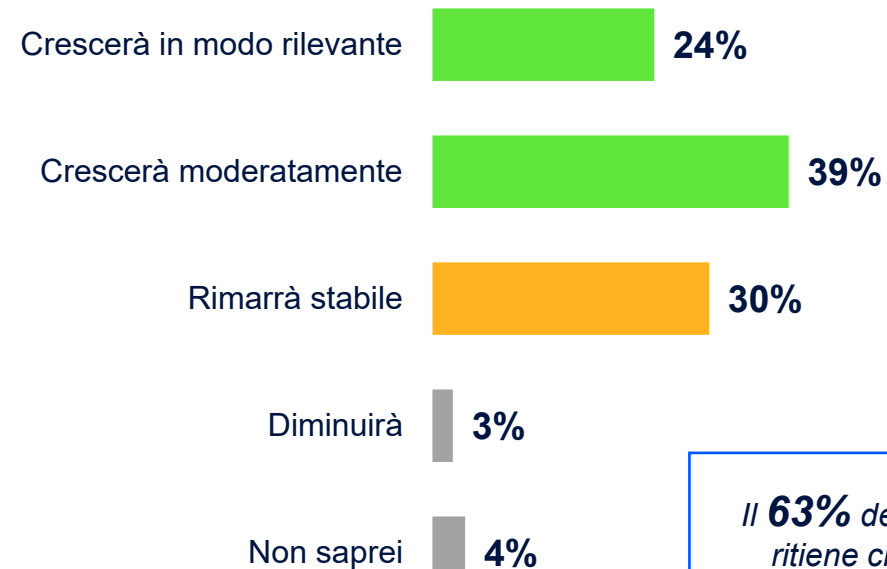
D. Quali aspetti geopolitici influenzano maggiormente le valutazioni su tecnologie e fornitori nella Sua organizzazione?

Base: tutti i rispondenti (152)



D. La Sua organizzazione ha recentemente rivalutato o modificato le scelte tecnologiche (vendor, servizi, cloud, etc.) a causa di dinamiche geopolitiche?
Base: tutti i rispondenti (152)

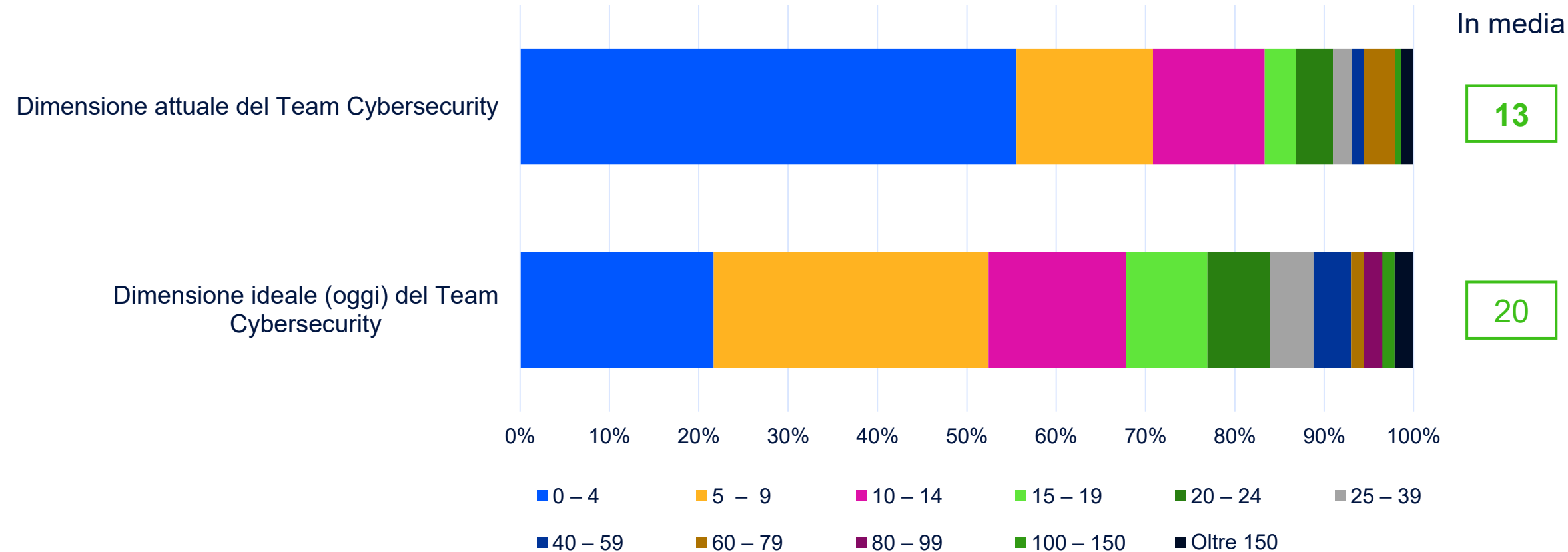
L'INFLUENZA DELLE TENSIONI GEOPOLITICHE SULLE SCELTE TECNOLOGICHE CRESCERÀ O DIMINUIRÀ?



*Il **63%** del campione ritiene che il peso geopolitico andrà ad aumentare in futuro*

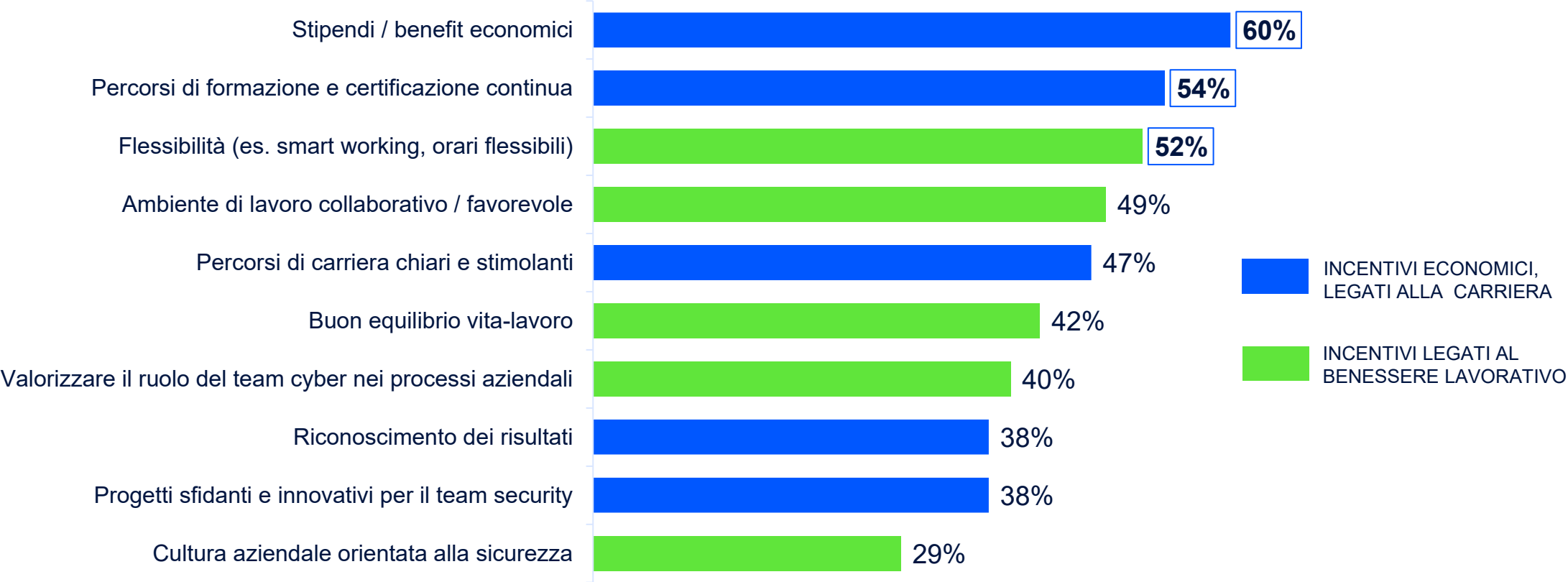
D. Ritiene che nei prossimi 12-24 mesi l'influenza delle tensioni geopolitiche sulle scelte tecnologiche crescerà o diminuirà?
Base: tutti i rispondenti (152)

IL TEAM IDEALE DI CYBERSECURITY DOVREBBE ESSERE DEL 54% PIÙ AMPIO (IN MEDIA)



D. Qual è la dimensione attuale del Team Security nella Sua organizzazione (FTE, sia interni sia consulenti esterni con ruolo da interno) e quale dovrebbe essere la dimensione ideale in questo momento?
Base: tutti i rispondenti (144)

PER TRATTENERE E INGAGGIARE IL TEAM SECURITY SERVE LA COMPRESENZA DI INCENTIVI ECONOMICI E LEGATI AL BENESSERE LAVORATIVO



D. In base alla Sua esperienza, quali dei seguenti aspetti sono più importanti per motivare, trattenere, ingaggiare i talenti della cybersecurity?
Base: tutti i rispondenti (144)



WE DRIVE **TRANSFORMATION**

TIG - THE INNOVATION GROUP

The Innovation Group (TIG) è una società di servizi di consulenza e di ricerca di mercato indipendente, specializzata nello studio delle evoluzioni del mercato digitale e nei processi d'innovazione abilitati dalle tecnologie e dalla conoscenza.

TIG si rivolge ad aziende e organizzazioni dell'economia digitale che desiderano sviluppare strategie di crescita attraverso programmi e iniziative di go-to-market.

Vengono pertanto sviluppate analisi, ricerche, approfondimenti sul digitale per il mercato italiano. Per fare questo, si mettono a disposizione piattaforme integrate di servizi e contenuti per facilitare scambi e relazioni con clienti, influencer, stakeholder ed ecosistemi.

www.tig.it
info@tig.it
+39 02.49988.1

Via Ettore Romagnoli, 6
20146, Milano



ASSOCISO

AssoCISO è l'Associazione Nazionale dei Chief Information Security Officer, nata per rappresentare e valorizzare la figura del CISO nel panorama italiano. Promuove la cultura della sicurezza informatica e della gestione del rischio, favorisce la condivisione di esperienze e conoscenze tra i professionisti del settore e sostiene la definizione di standard e buone pratiche operative. Collabora con istituzioni, imprese e organizzazioni per rafforzare la resilienza digitale del Paese e contribuire allo sviluppo di un ecosistema cyber maturo, competente e consapevole.

<https://associso.org/>
info@associso.org

Viale delle Milizie 124,
Roma