The Innovation Group
Innovating business and organizations through ICT

Cyber Risk Management 2023

Un'indagine su 200 aziende italiane di TIG e CSA – Cyber Security Angels

TIGSURVEY

Il Valore della Sicurezza per il Business

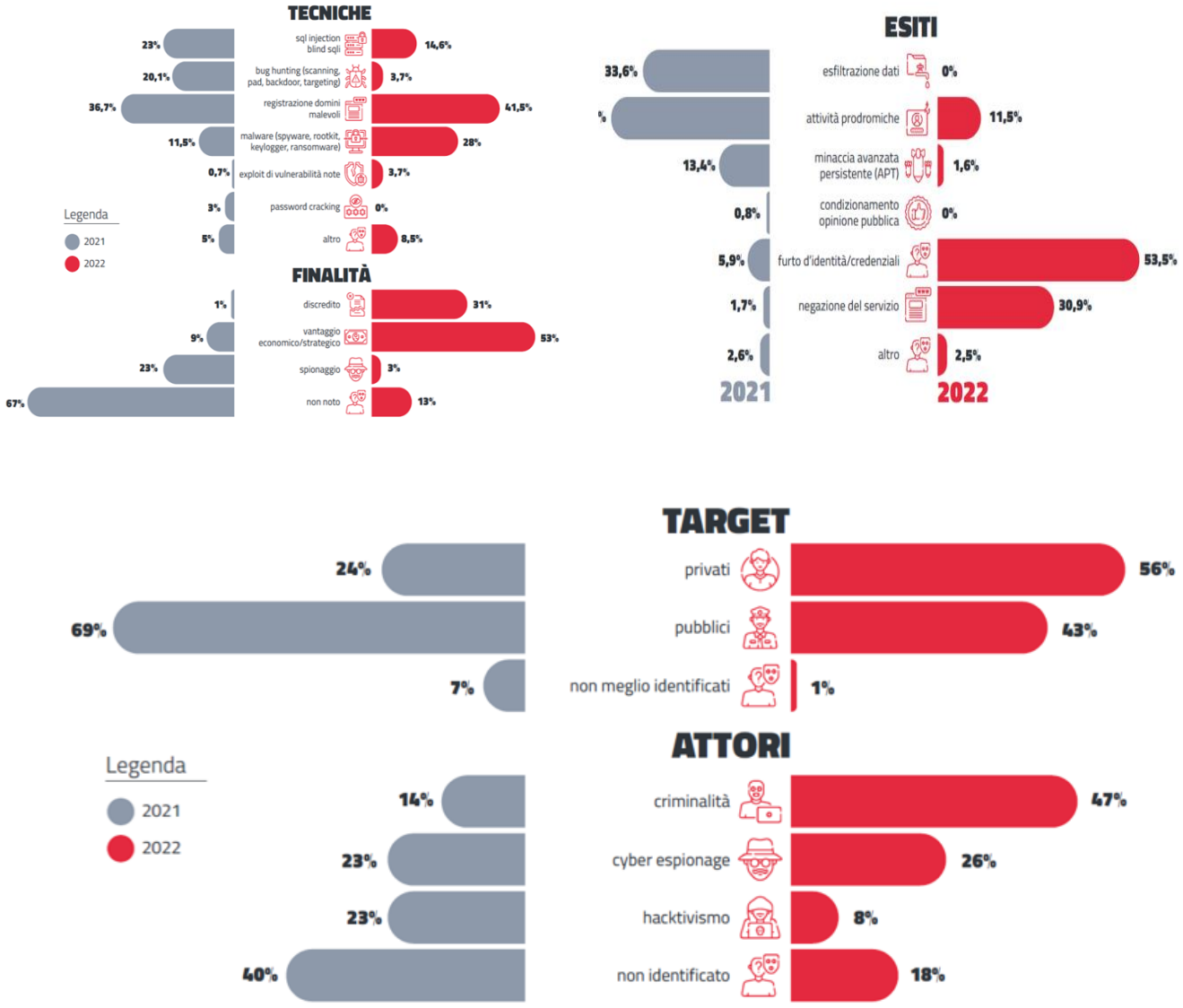
CYBERSECURITY SUMMIT 2023, Roma , 10 – 11 Maggio 2023

Attacchi informatici: scenario preoccupante, caratterizzato da tassi di crescita elevati e un collegamento costante con eventi geopolitici più ampi

Attacchi informatici ad infrastrutture critiche italiane, 2021 vs 2022*

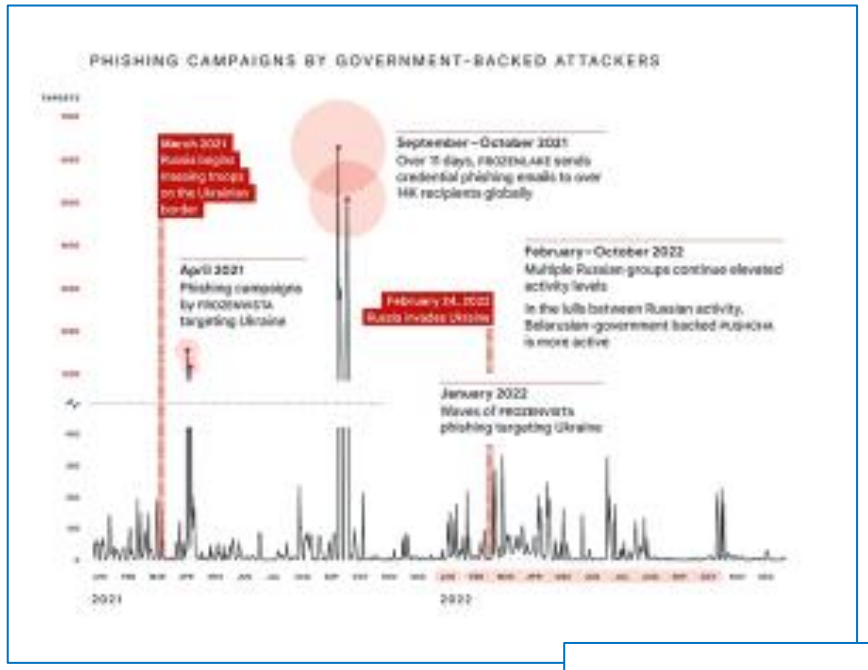
- **Attacchi rilevati**: da 5.434 nel 2021 a 12.947 nel 2022 (**+138**%)
- **Persone indagate**: da 187 nel 2021 a 332 nel 2022 (**+78**%)
- **Alert diramati**: da 110.524 nel 2021 a 113.226 nel 2022 (**+2**%)

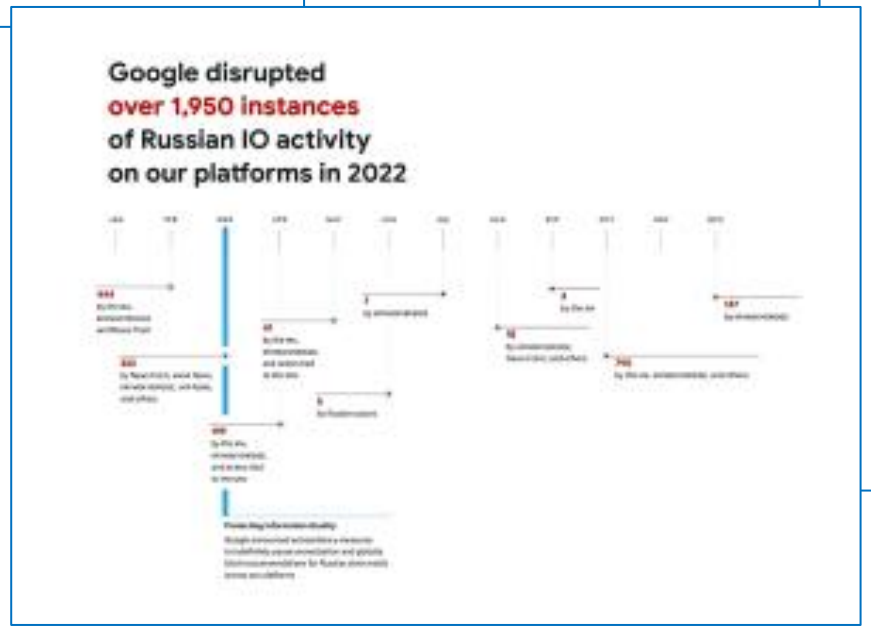
(* Resoconto attività 2022 di Polizia Postale e delle Comunicazioni)

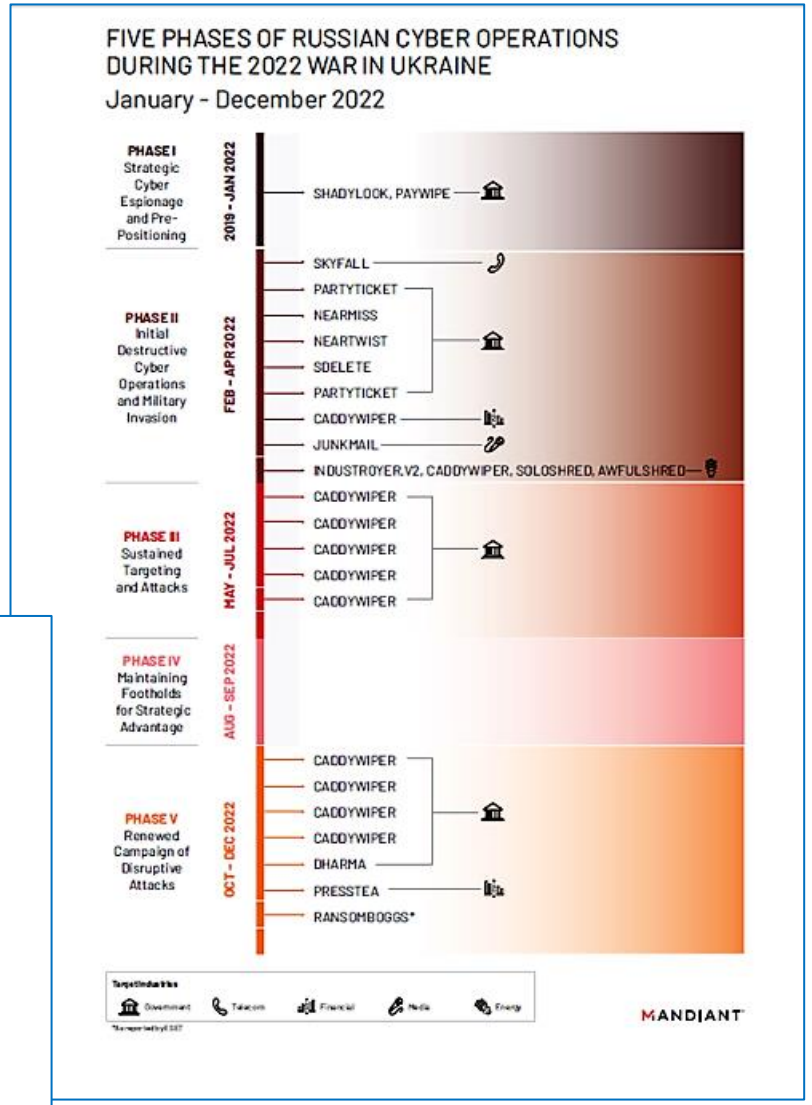


Da: Relazione sulla politica dell'informazione per la sicurezza relativa al 2022

Le operazioni informatiche hanno svolto un ruolo di primo piano nel conflitto russo ucraino







Mosca ha sfruttato l'intero spettro delle IO (Information Operations) per manipolare l'opinione pubblica sulla guerra

22 febbraio 2023: dopo la visita del Presidente Meloni a Kiev, attacchi a ripetizione da parte degli hacktivisti e delle gang ransomware

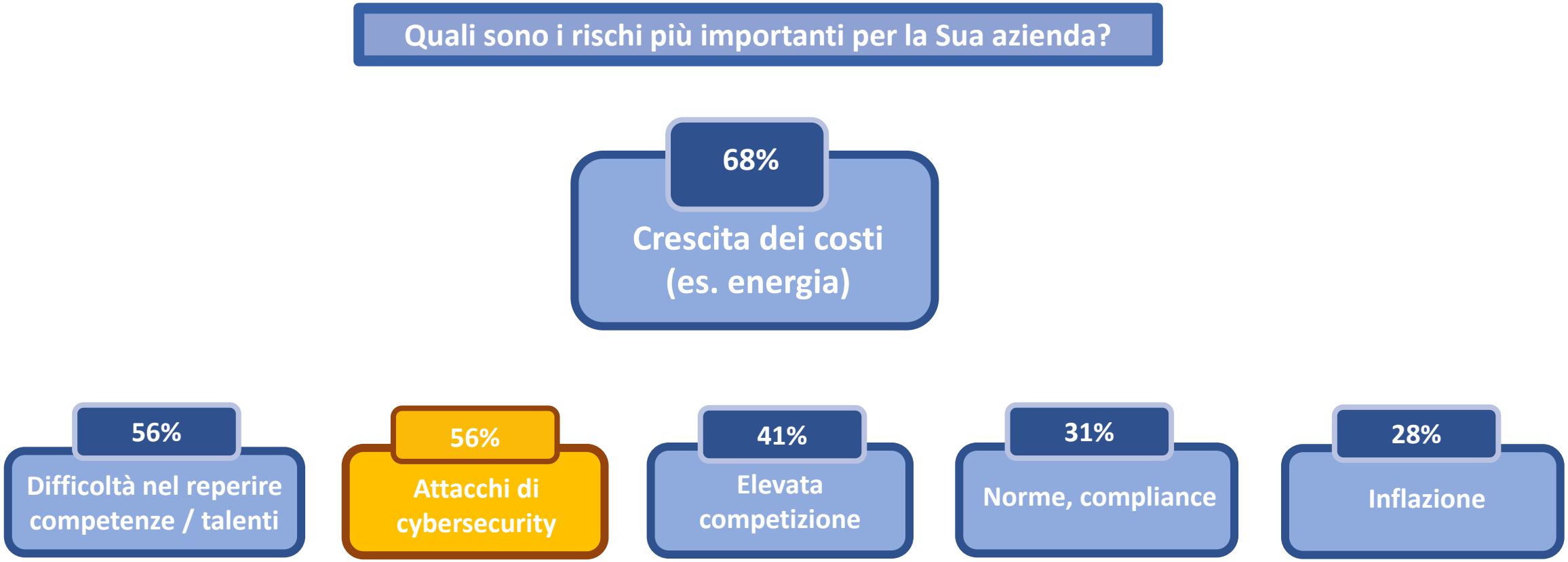
Attacco ransomware di Lockbit all'Italiana Cassa Ragionieri

Ministero degli Esteri, attacco Distributed Denial of Service da parte del gruppo filorusso NoName057

Dopo la messa in vendita degli account degli ufficiali dei carabinieri per 80 dollari, il sito dei carabinieri subisce un attacco DDoS, sempre da parte degli hacktivisti filorussi di NoName057

Gli hacktivisti di NoName, dopo aver colpito il Ministero della Difesa e il sito dei Carabinieri, mettono offline anche il sito di Banca Carige ora BPER Banca

Gli attacchi di cybersecurity sono visti come un rischio importante per la propria azienda, subito dopo la crescita dei costi, insieme alla difficoltà nel reperire i talenti

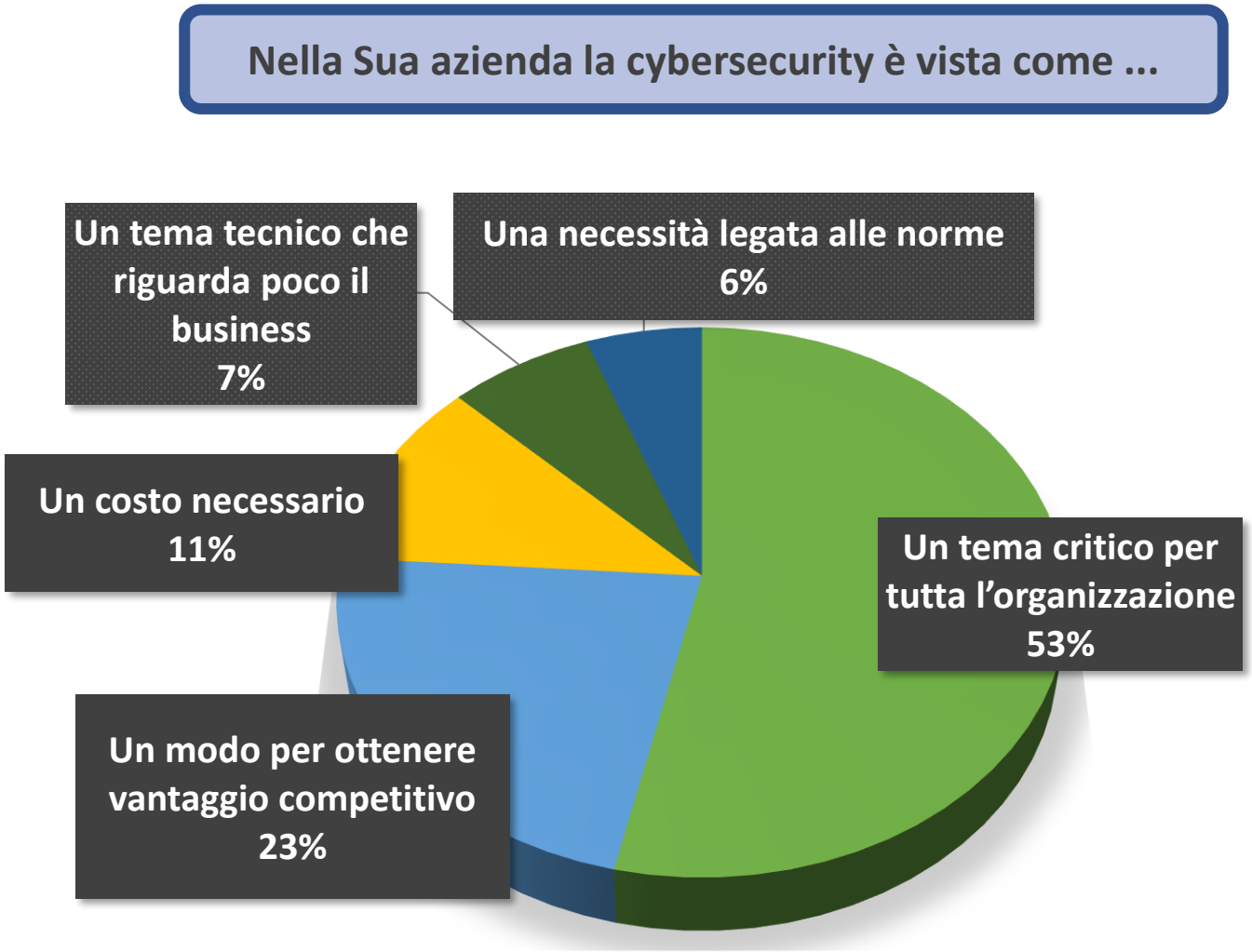


Altro: Tensioni geopolitiche, 26%; Ritorno eventuale della pandemia, 13%; Questioni ambientali / cambiamento climatico, 9%; Disastri naturali, 6%.

Fonte: Il Valore della Cybersecurity nelle Aziende 2023, The Innovation Group, gennaio 2023

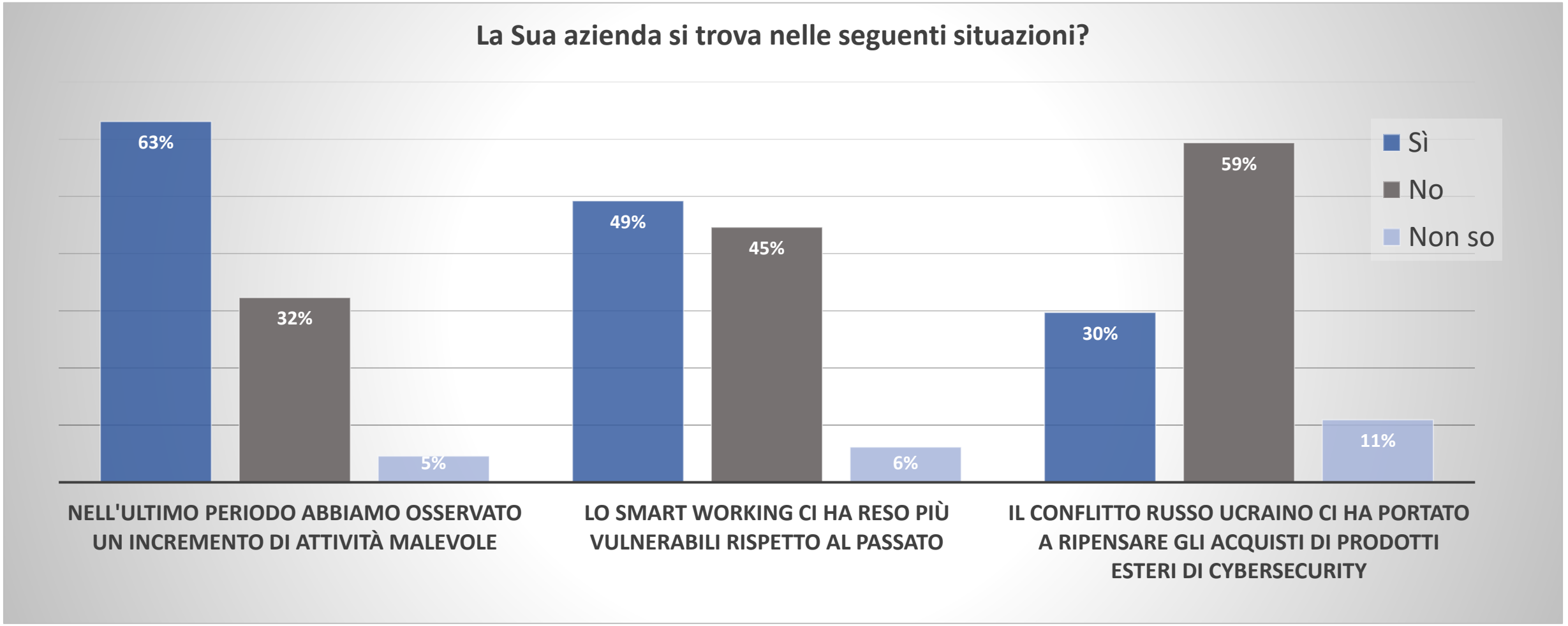
The Innovation Group
Innovating business and organizations through ICT

Una buona gestione della sicurezza informatica è una componente fondamentale per costruire il Trust dell'azienda. Oggi, la situazione è diversa rispetto al passato: per circa la metà delle aziende la cybersecurity è un tema critico che riguarda tutta l'organizzazione, per un 23% un modo per risultare più competitivi



Fonte: Il Valore della Cybersecurity nelle Aziende 2023, The Innovation Group, gennaio 2023

Nell’ultimo anno il tema dei rischi di cybersecurity è cresciuto a causa di una diffusa digitalizzazione e come conseguenza del conflitto in Ucraina, che ha costretto anche alcune aziende (il 30% dei rispondenti) a riconsiderare i propri fornitori di soluzioni di cybersecurity

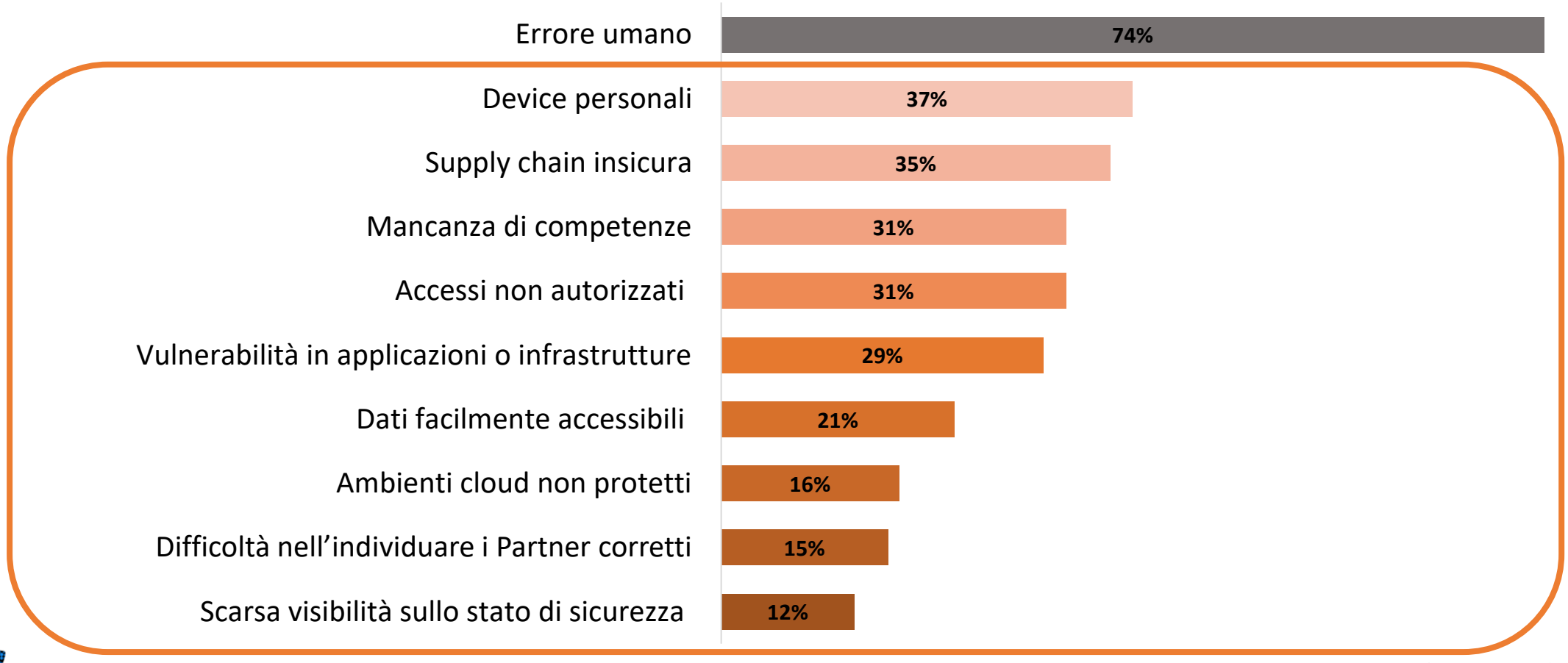


Fonte: Il Valore della Cybersecurity nelle Aziende 2023, The Innovation Group, gennaio 2023

The Innovation Group
Innovating business and organizations through ICT

La conoscenza delle vulnerabilità aziendali è però bassa se l'interlocutore è una persona del Business.
Se la percezione del rischio legato alle persone è alta (74% delle risposte) per quanto riguarda invece ambiti di dominio IT (come device, accessi, applicazioni, dati, cloud), solo una minoranza ritiene di avere dei problemi

D. Parlando di vulnerabilità informatiche della Sua azienda, quali sono secondo Lei quelle più gravi?



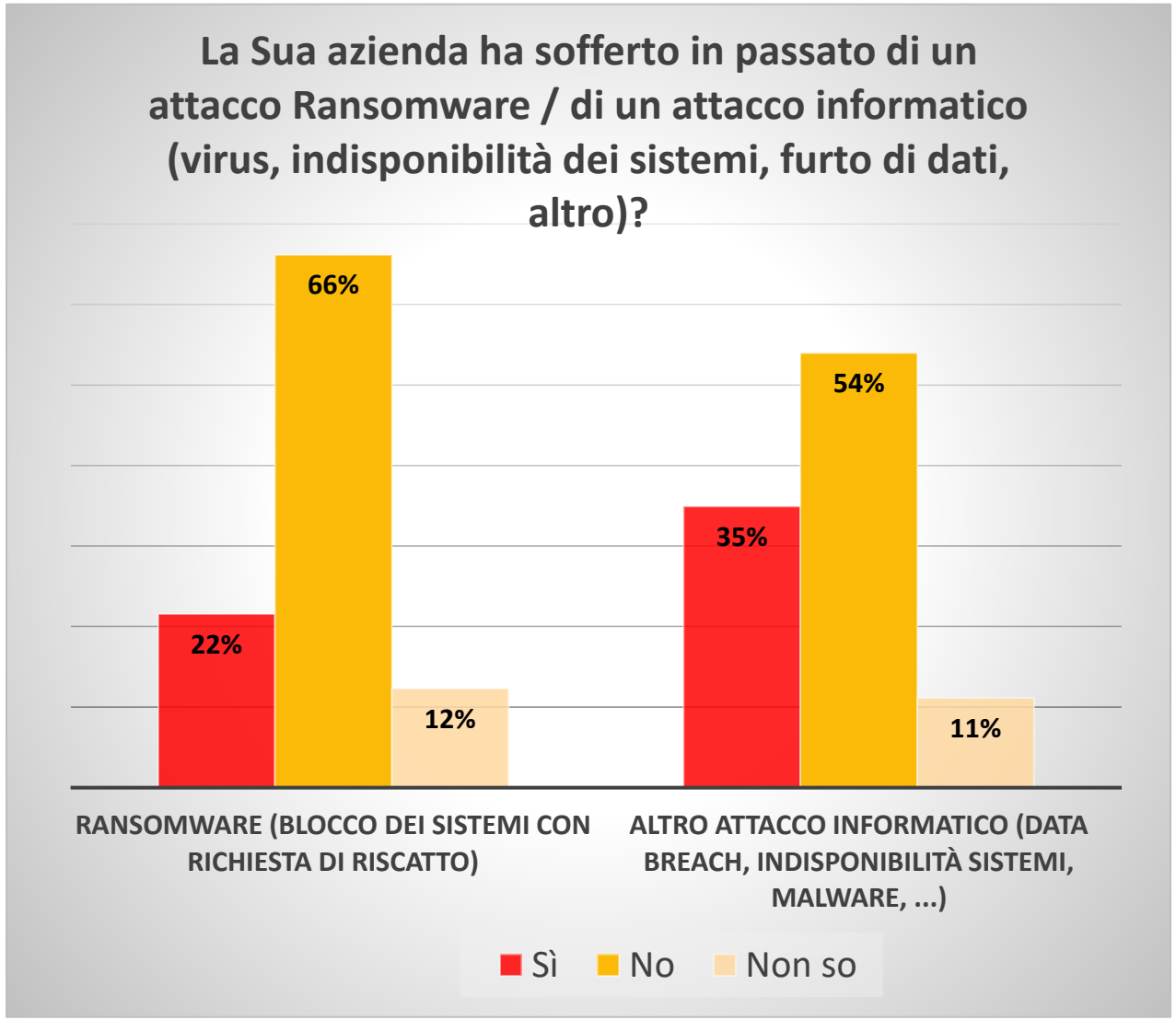
Fonte: Il Valore della Cybersecurity nelle Aziende 2023, The Innovation Group, gennaio 2023

The Innovation Group
Innovating business and organizations through ICT

- La conoscenza sugli incidenti informatici subiti dimostra che in molti, in azienda, sono poco consapevoli di quanto avviene. Solo un 22% pensa di aver subito in passato un attacco Ransomware (quando alla stessa domanda, il 40% dei CIO/CISO rispondono che è avvenuto)

- Questo risultato fa propendere per una bassa comunicazione interna con riferimento agli incidenti informatici. Come mostra la figura successiva infatti, il Board è nella maggior parte dei casi poco coinvolto sulla cybersecurity.

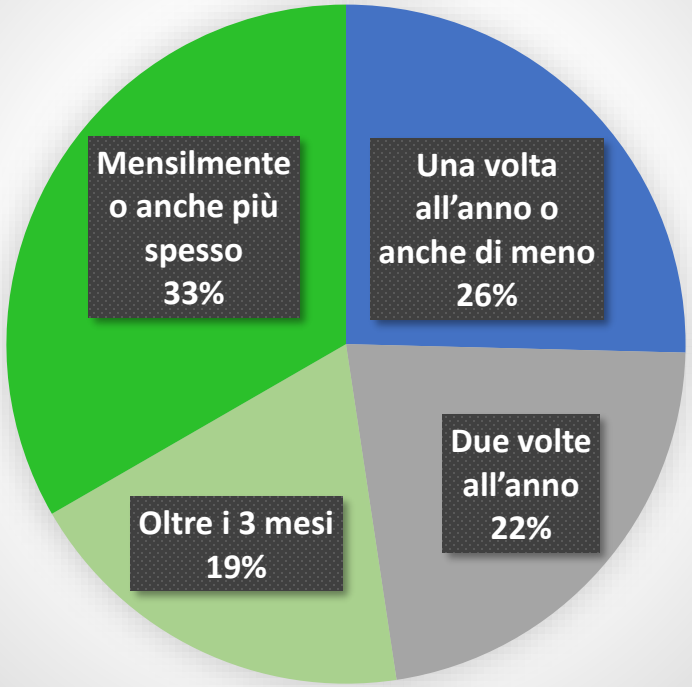
- Numerose barriere, dalla scarsa conoscenza del tema (molto tecnico) alle restrizioni sulla spesa in sicurezza impediscono un maggiore coinvolgimento del Management dell'azienda.



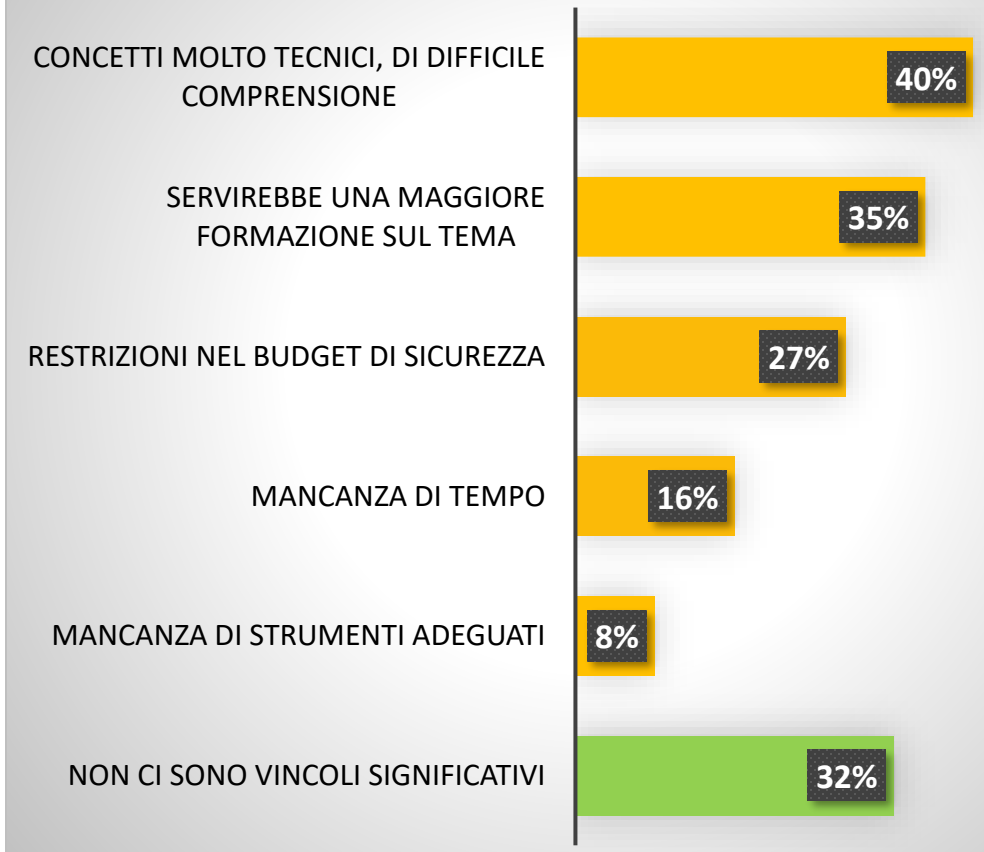
Fonte: Il Valore della Cybersecurity nelle Aziende 2023, The Innovation Group, gennaio 2023

Il coinvolgimento del management è ancora insufficiente sui temi della cybersecurity

Quanto spesso il tema della cybersecurity è affrontato negli incontri del Board / del Top management nella Sua azienda?



Quali sono le barriere a una migliore comprensione dei temi della cybersecurity da parte del Board?

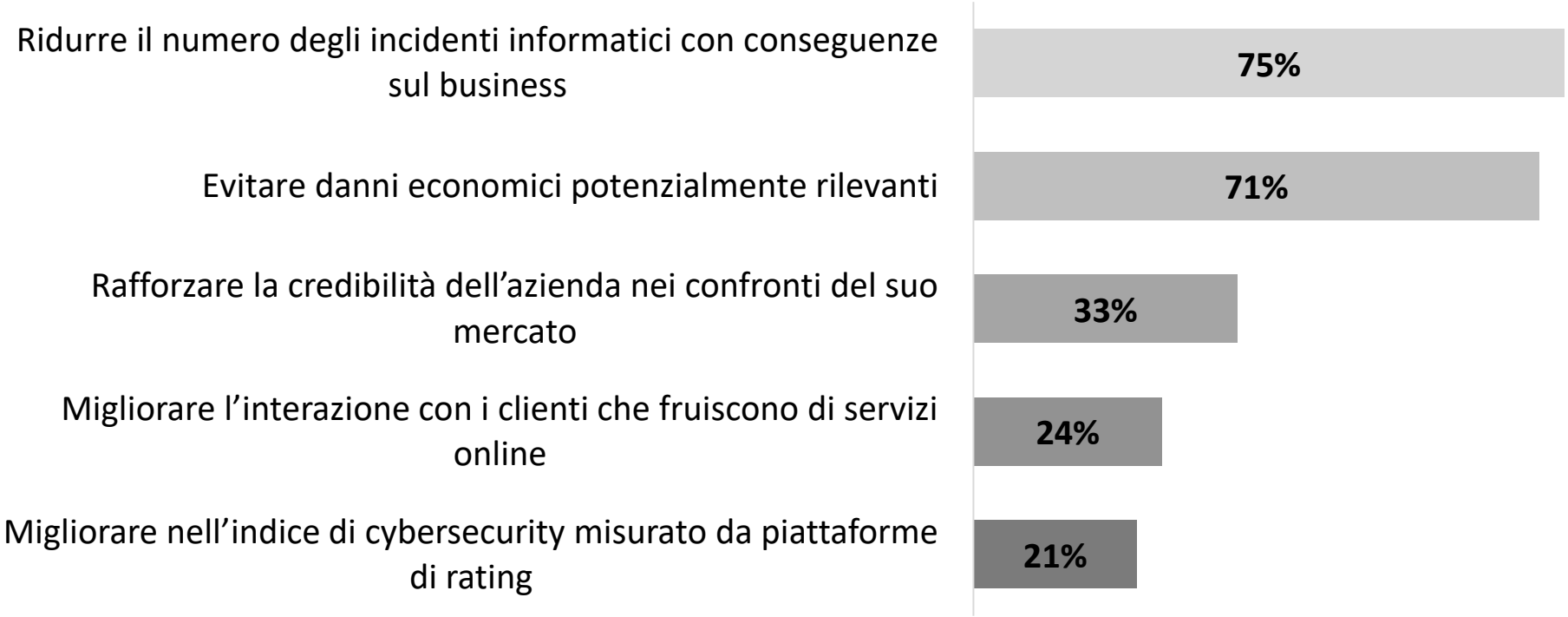


Fonte: Il Valore della Cybersecurity nelle Aziende 2023, The Innovation Group, gennaio 2023

The Innovation Group
Innovating business and organizations through ICT

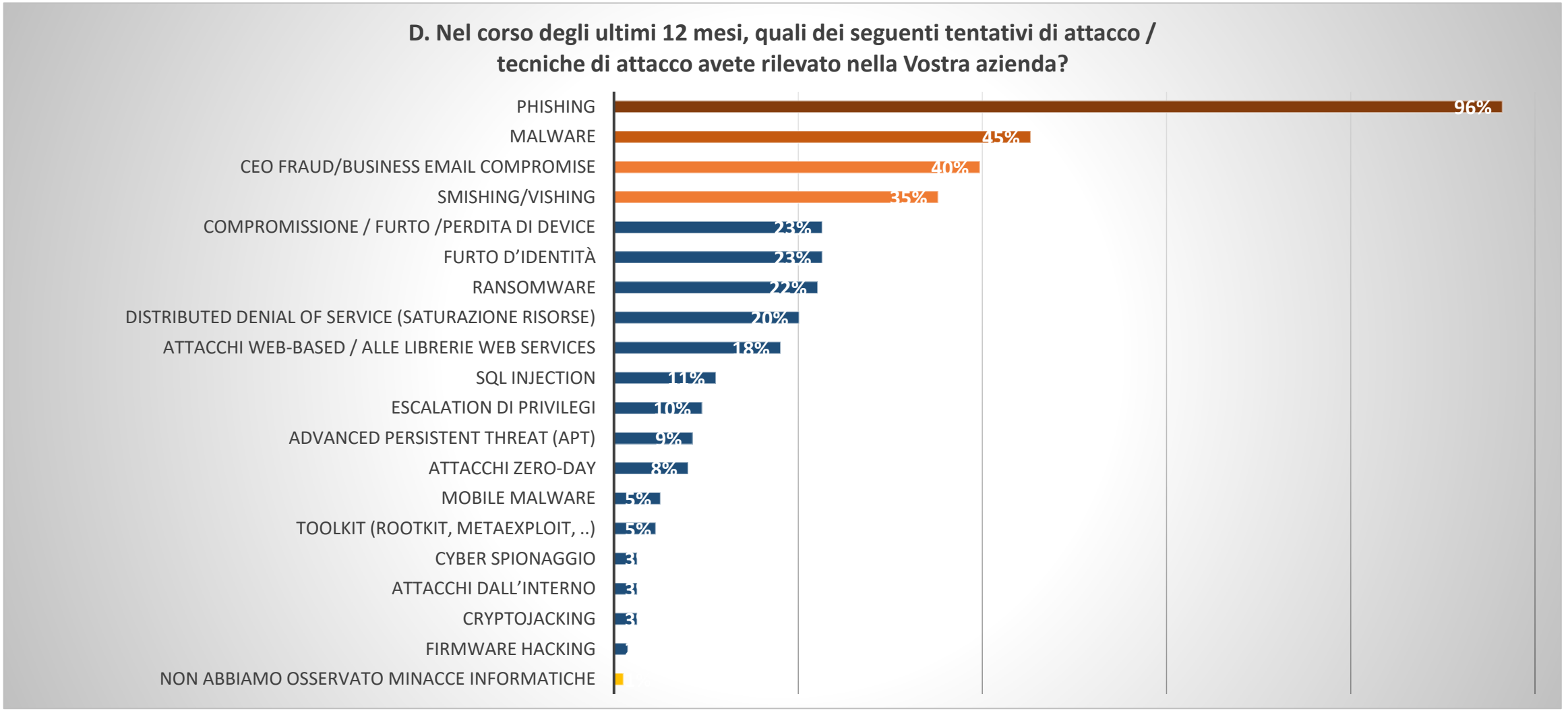
Il ROI della Cybersecurity è al momento strettamente collegato alla riduzione degli impatti negativi, mentre in futuro sarà sempre più elemento per costruire il Trust

Quale potrebbe essere il ritorno misurabile degli investimenti in cybersecurity nel lungo termine?



Fonte: Il Valore della Cybersecurity nelle Aziende 2023, The Innovation Group, gennaio 2023

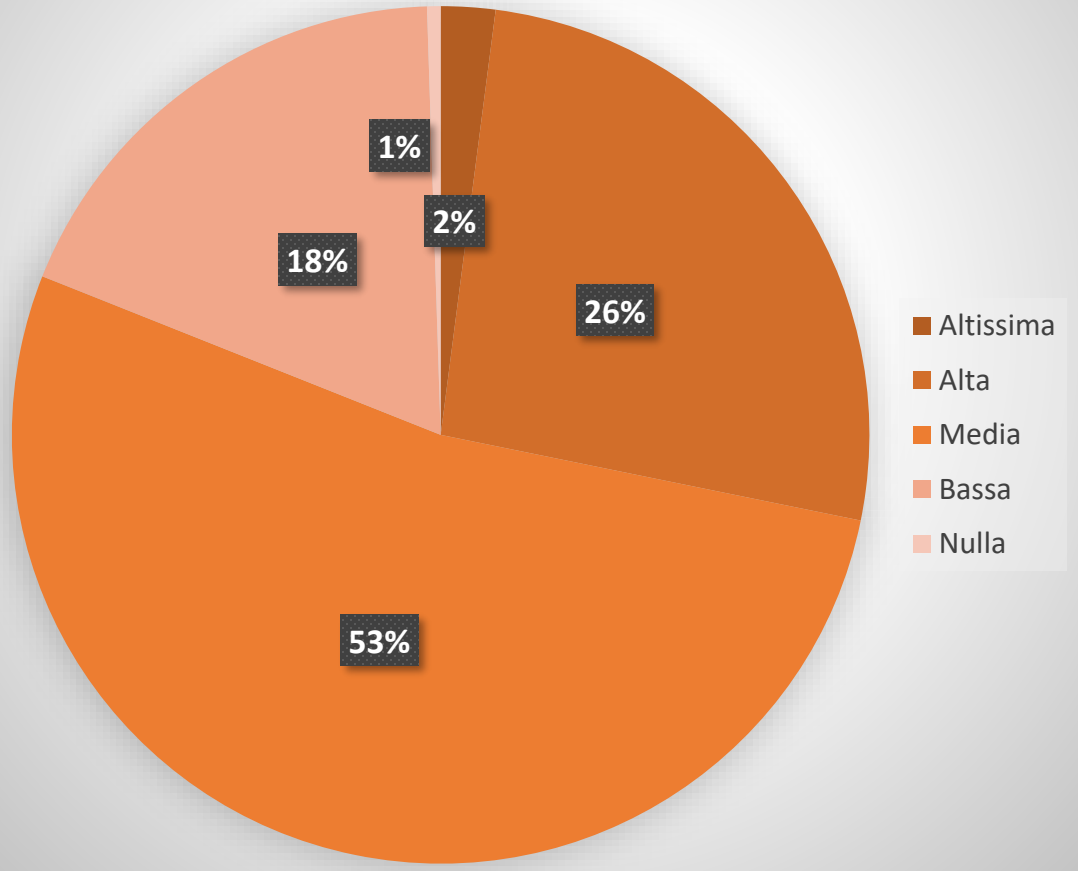
Lo scenario degli attacchi continua a mostrare una prevalenza di Phishing (osservato da quasi tutti), Malware, Ceo Fraud/BEC, Smishing/Vishing



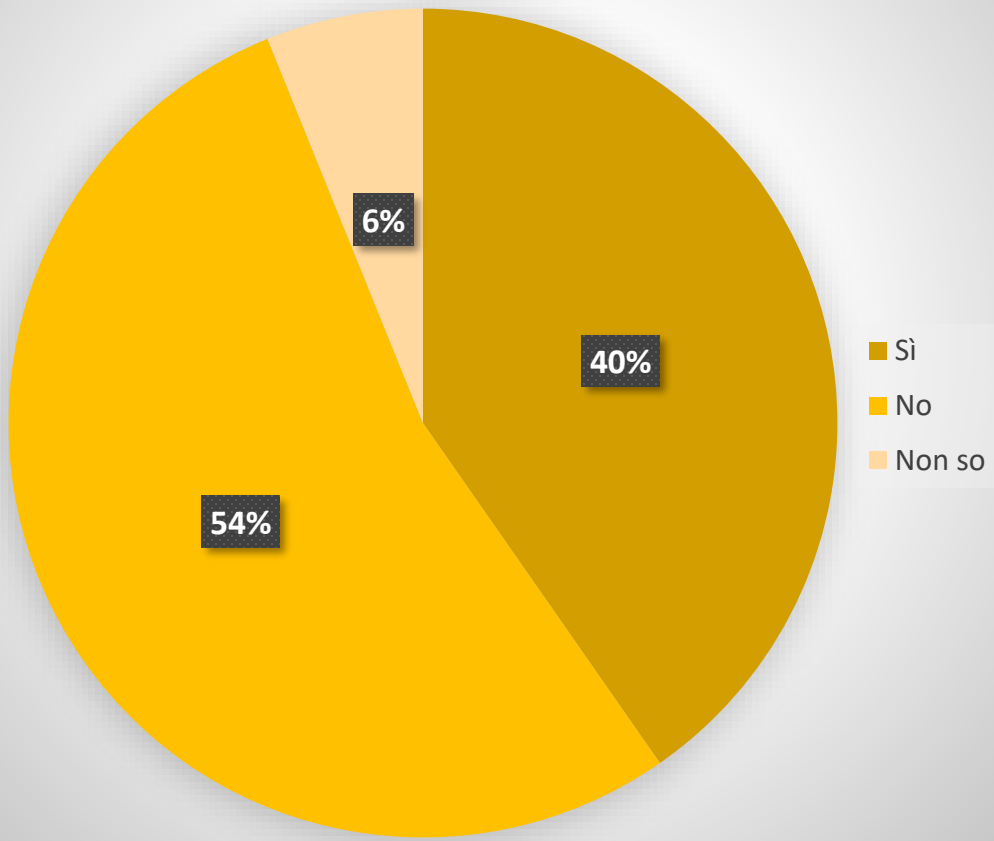
Fonte: Cyber Risk Management 2023 Survey, Gennaio 2023

Ransomware

D. Qual è secondo Lei la probabilità che la sua azienda sia vittima di un attacco Ransomware nei prossimi 12 mesi?



D. La Sua azienda ha sofferto in passato di un attacco ransomware?



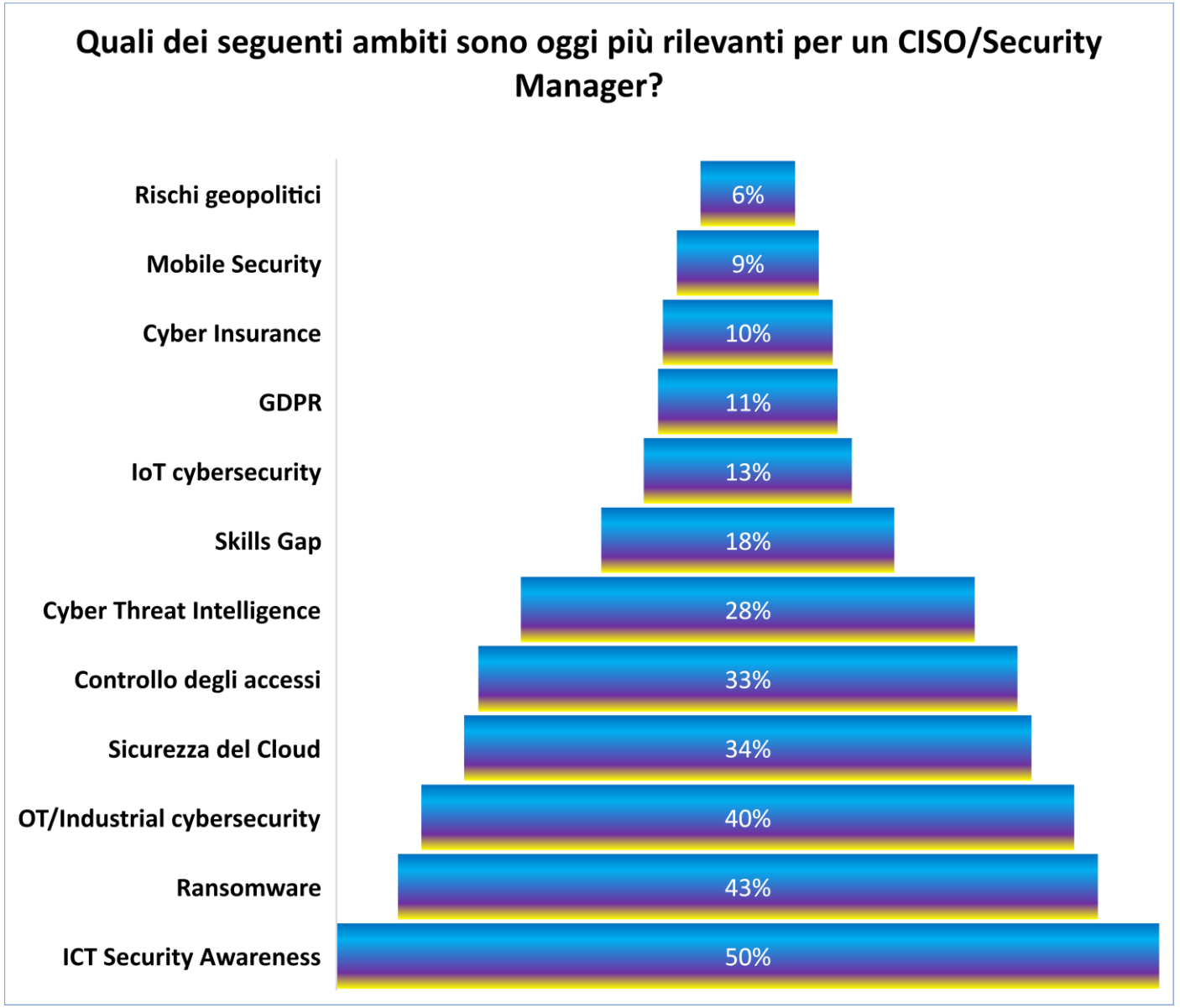
The Innovation Group
Innovating business and organizations through ICT

Fonte: Cyber Risk Management 2023 Survey, Gennaio 2023

CSA Cyber Security Angels

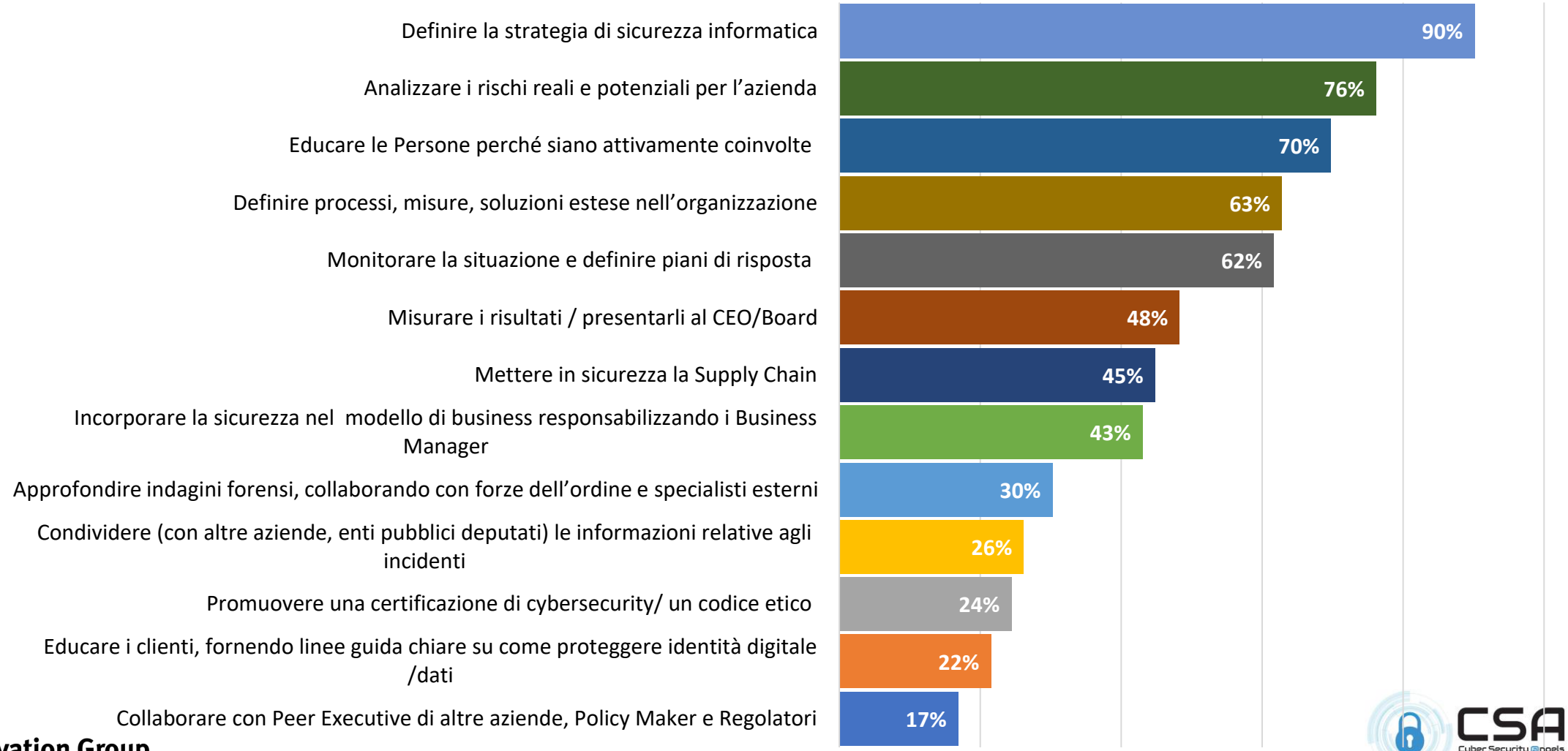
Le priorità 2023 del CISO

- Le attività di formazione dei dipendenti (ICT Security Awareness) e il contrasto al Ransomware saranno anche nel 2023 le priorità da affrontare nella maggior parte dei casi (come emerso già nel 2022)
- Si conferma alto anche il posizionamento della Cloud Security (al quarto posto) e del controllo degli accessi che è considerato fondamentale da 1 azienda su 3
- La Cyber Threat Intelligence è fondamentale per un 28% di aziende, segnale che – pur importante – non riesce a raggiungere ancora una diffusione elevata, per complessità del tema
- L'Industrial Cybersecurity è una priorità per la maggior parte dei rispondenti del settore manifatturiero (sono il 47% del campione)
- Il rischio geopolitico alla fine – in questa classifica – risulta il meno importante. In qualche modo, è sempre stato parte dello scenario della cybersecurity.



Fonte: Cyber Risk Management 2023 Survey, Gennaio 2023

Quali sono i compiti del CISO



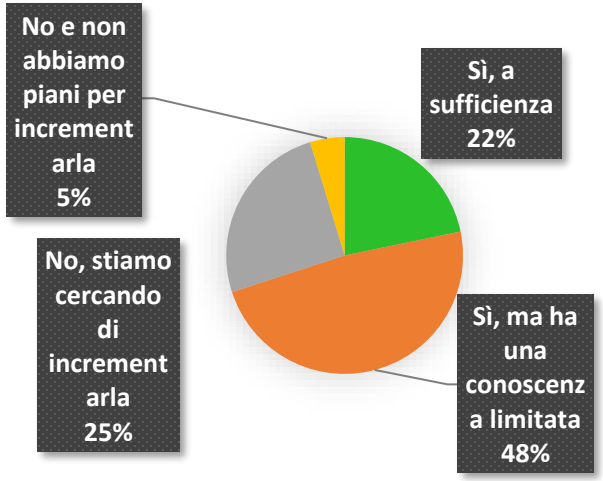
The Innovation Group
Innovating business and organizations through ICT

CSA Cyber Security Angels

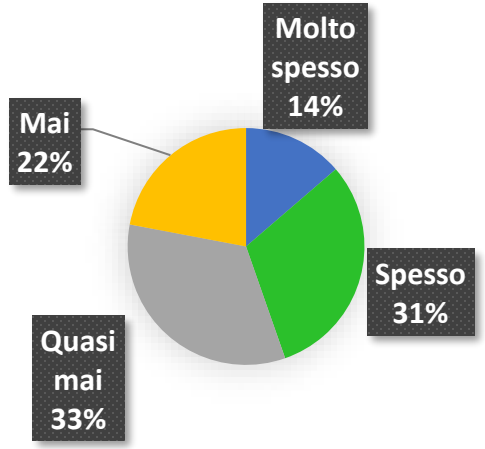
Fonte: Cyber Risk Management 2023 Survey, Gennaio 2023

Gli ambiti di miglioramento nel ruolo della cybersecurity per il business sono numerosi, fondamentale sarebbe una maggiore integrazione con le altre aree del business

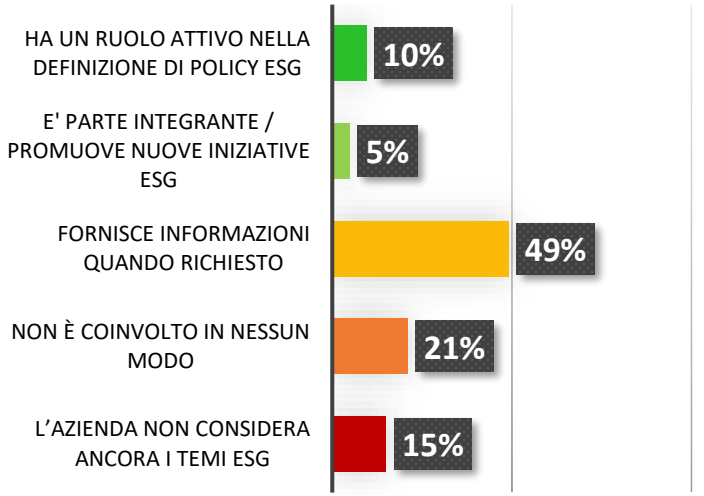
Il Board / il Top management della Sua azienda ha una conoscenza adeguata dell'ICT Security?



Quanto spesso il CISO (o ruolo equivalente) partecipa ad incontri con il CEO/CDA?



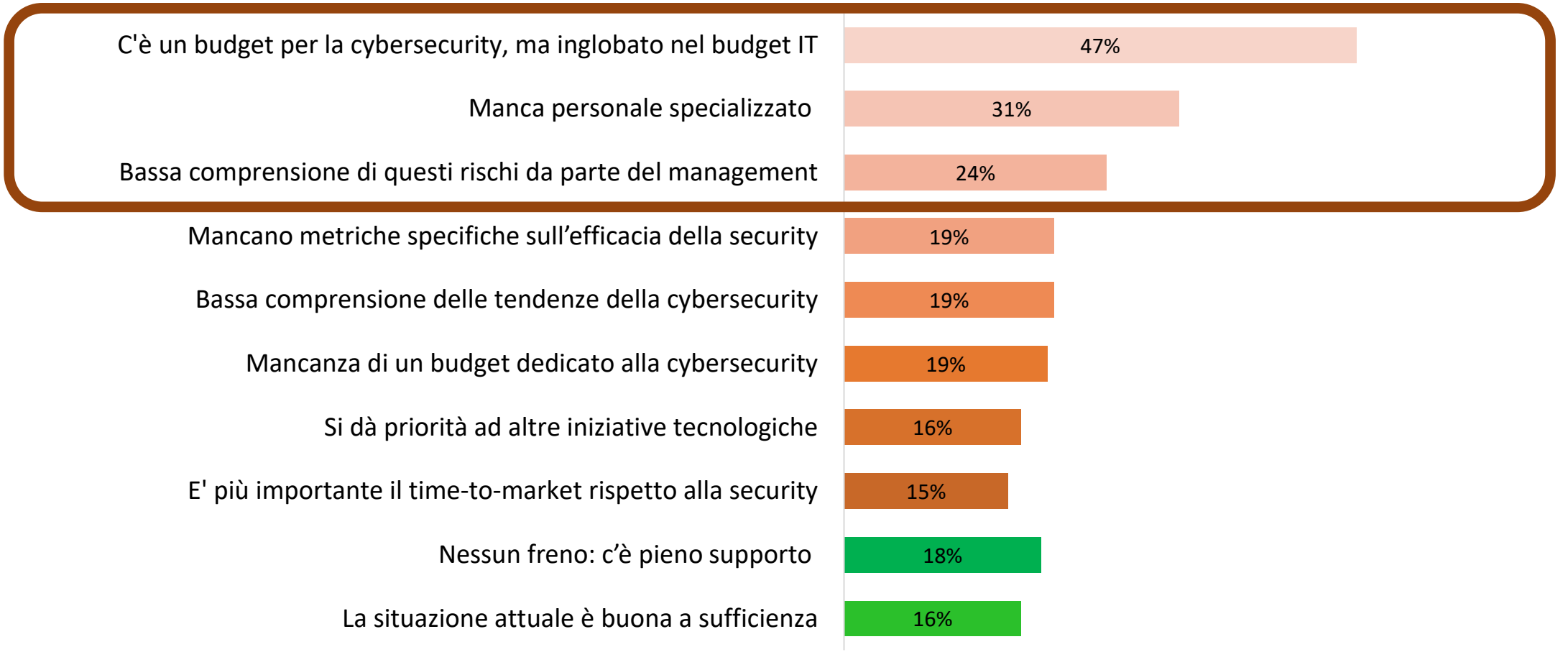
Qual è il coinvolgimento del CISO sulle politiche ESG?



Fonte: Cyber Risk Management 2023 Survey, Gennaio 2023

Molti elementi frenano ancora un migliore sviluppo delle attività per la cybersecurity, al primo posto, la mancanza di un budget separato, la scarsità di personale, la bassa comprensione da parte del management

D. Quali fattori frenano nella Sua azienda una più ampia gestione dei rischi cyber?



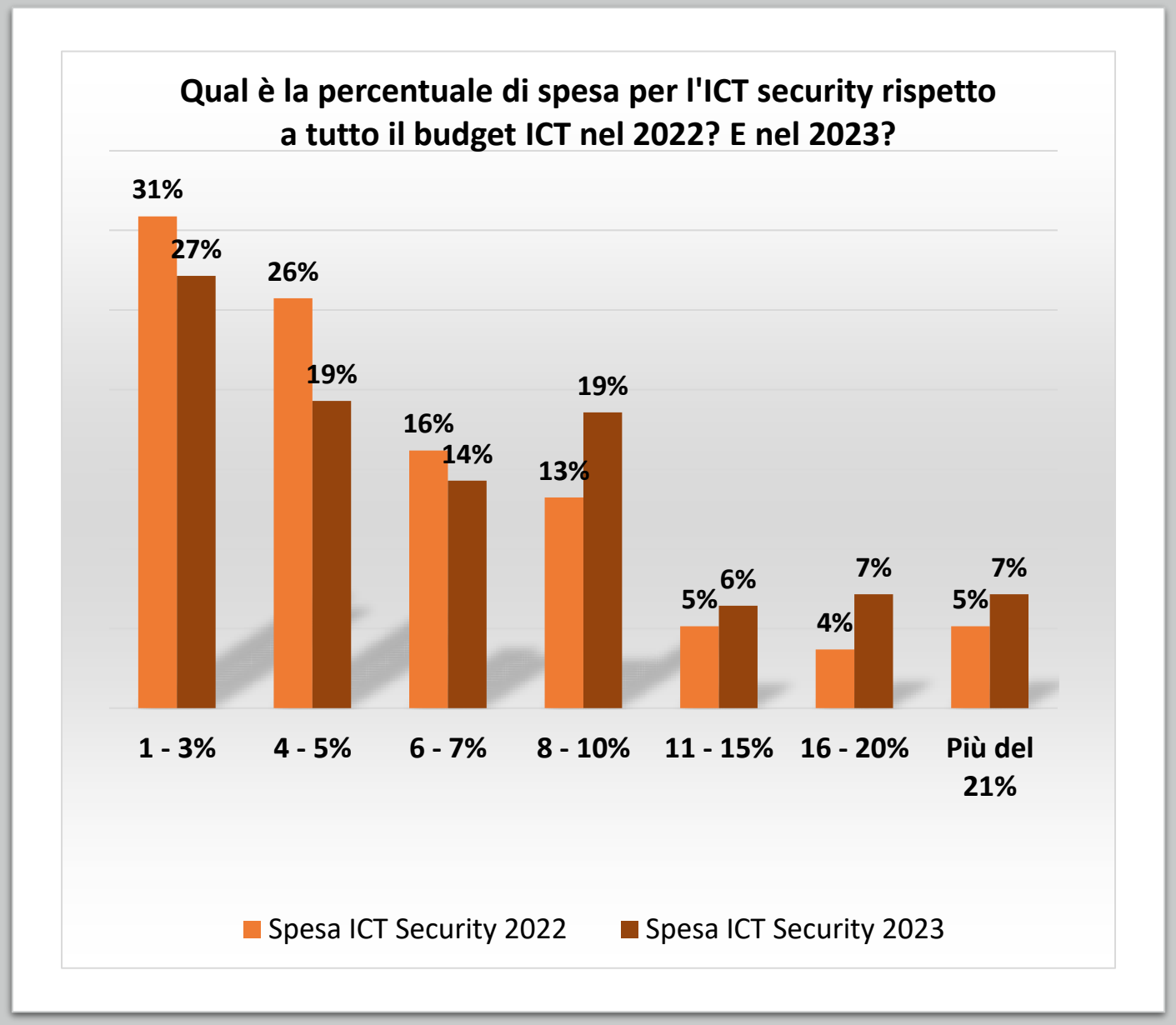
The Innovation Group
Innovating business and organizations through ICT

Fonte: Cyber Risk Management 2023 Survey, Gennaio 2023

CSA Cyber Security Angels

Il Budget di cybersecurity non cresce a sufficienza

- Rispetto agli investimenti ICT, la spesa in cybersecurity rimane (anche in una situazione di grande necessità), intorno a percentuali molto basse, **il 7% in media nel 2022, e in previsione un 9% in media nel 2023.** Rispetto ad analoghe indagini internazionali*, questi valori sono dai 3 ai 5 punti percentuali sotto la media registrata da altri Paesi europei
- (* 2022 Cyberthreat Defense Report, ISC2, marzo 2022)



Fonte: Cyber Risk Management 2023 Survey, Gennaio 2023

The Innovation Group
Innovating business and organizations through ICT

CSA Cyber Security Angels