TIG | THE INNOVATION GROUP

WE DRIVE **TRANSFORMATION**

CYBER RISK MANAGEMENT SURVEY 2025

PROFILI DI GESTIONE DEL RISCHIO E DELLA COMPLIANCE, MATURITÀ DELLA SECURITY POSTURE, SFIDE E OPPORTUNITA' LEGATE ALL'AI

EZIO VIOLA, CO-FOUNDER, TIG – THE INNOVATION GROUP

MILANO, 20 MARZO 2025

FACTORY EVENTS MEDIA

TIG | THE INNOVATION GROUP

WE DRIVE **TRANSFORMATION**

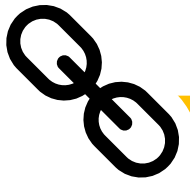
COME STA EVOLVENDO LO SCENARIO DELLE MINACCE DI CYBERSECURITY?

RISCHI FUTURI DI CYBERSECURITY: PHISHING AI-BASED E IT SUPPLY CHAIN

Con riferimento ai rischi futuri di cybersecurity, quali sono le minacce da monitorare già oggi?

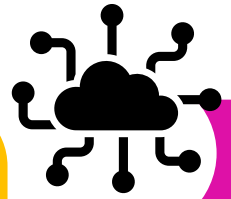
Phishing avanzato "AI-based" (es Deepfakes)

86%



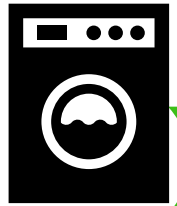
Compromissioni a catena lungo la IT Supply chain

64%



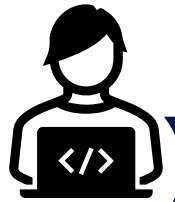
Aumento di vulnerabilità zero-day, exploit in mercati underground

52%



Ransomware su oggetti connessi (IoT)

36%



Minaccia Insider

30%

FONTE: **CYBER RISK MANAGEMENT 2025 SURVEY**, TIG – THE INNOVATION GROUP E CSA – CYBER SECURITY ANGELS. EFFETTUATA TRA DICEMBRE 2024 E GENNAIO 2025 SU UN CAMPIONE DI **191 ORGANIZZAZIONI PUBBLICHE E PRIVATE** (CON UNA PREVALENZA DI BEST PRACTICE, ESSENDO COMPOSTO PER IL 74% DA AZIENDE CON OLTRE 100 MILIONI DI EURO DI FATTURATO)

TIG THE INNOVATION GROUP

WE DRIVE **TRANSFORMATION**

COME BILANCIARE AI E CYBERSECURITY?

COME GLI ATTACCANTI UTILIZZANO L'AI

Quali saranno le principali evoluzioni degli attacchi legate alle nuove capacità AI degli attaccanti?

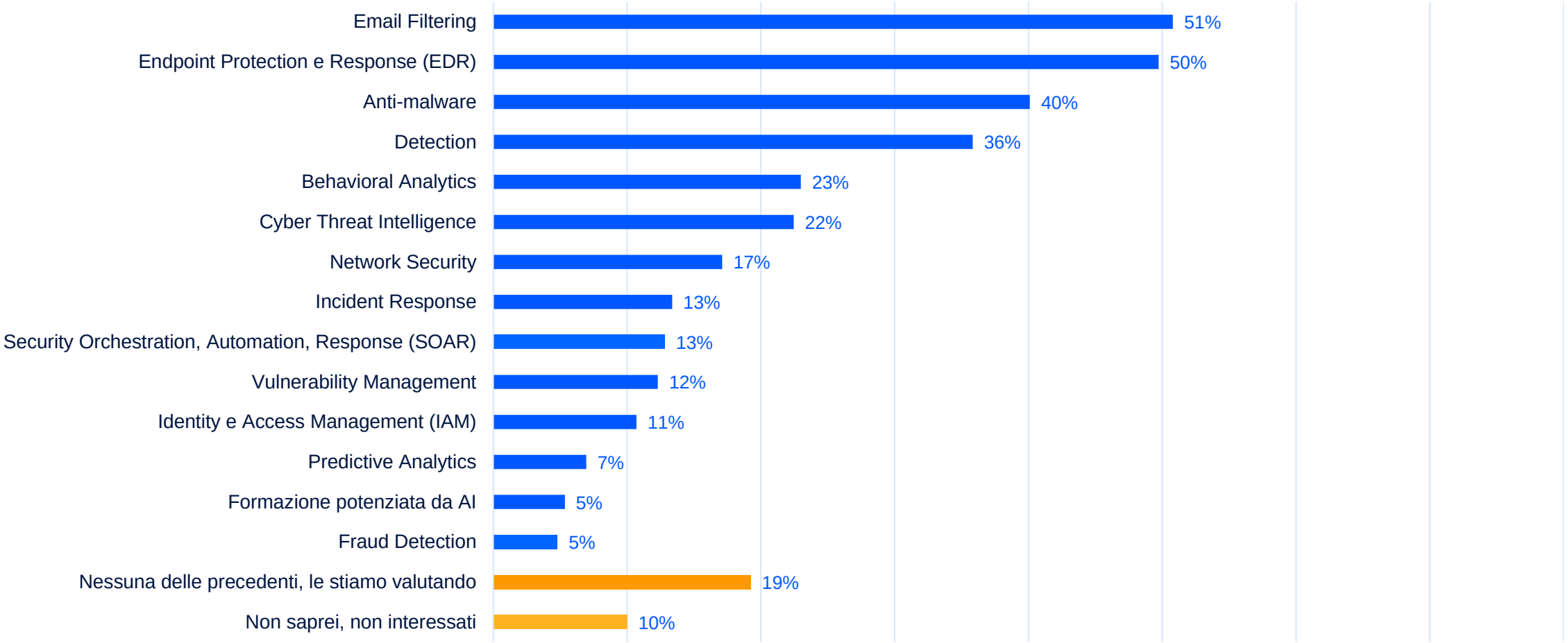
84%	53%	45%	43%	43%	42%
Mail di phishing scritte meglio / più efficaci	Audio e video deepfake per impersonare dirigenti aziendali o altri	Attacchi potenziati da ricognizione sofisticata basata su AI	Capacità più avanzate nella scoperta di vulnerabilità della difesa / zero days	Incremento del volume degli attacchi	Malware autonomi che apprendono e si adattano in tempo reale per eludere la sicurezza

FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

ALTRO: RANSOMWARE POTENZIATO DALL'AI (39%): AUTOMAZIONE DEGLI ATTACCHI DI BRUTE FORCE, PER VELOCIZZARE L'INDIVIDUAZIONE DI PASSWORD O CHIAVI CRITTOGRAFICHE (37%); ATTACCHI MULTI-VECTOR COORDINATI, SIMULTANEI E ADATTATIVI SU PIÙ FRONTI (RETE, ENDPOINT, CLOUD) (33%); EVASIONE DEI SISTEMI DI RILEVAMENTO: ALGORITMI DI AI PER TESTARE I PROPRI MALWARE CONTRO SANDBOX O SISTEMI DI RILEVAMENTO (32%); GENERAZIONE DI CONTENUTI DANNOSI SU LARGA SCALA (ES. DISINFORMAZIONE, SPAM) (31%)

ADOZIONE DELL'AI IN CYBERSECURITY

Quali sono gli ambiti della Cybersecurity in cui fate utilizzo di tecnologie di intelligenza artificiale?



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025
ALTRO: DATA PROTECTION; SAST/DAST; NON SO, SONO ATTIVITÀ ESTERNALIZZATE

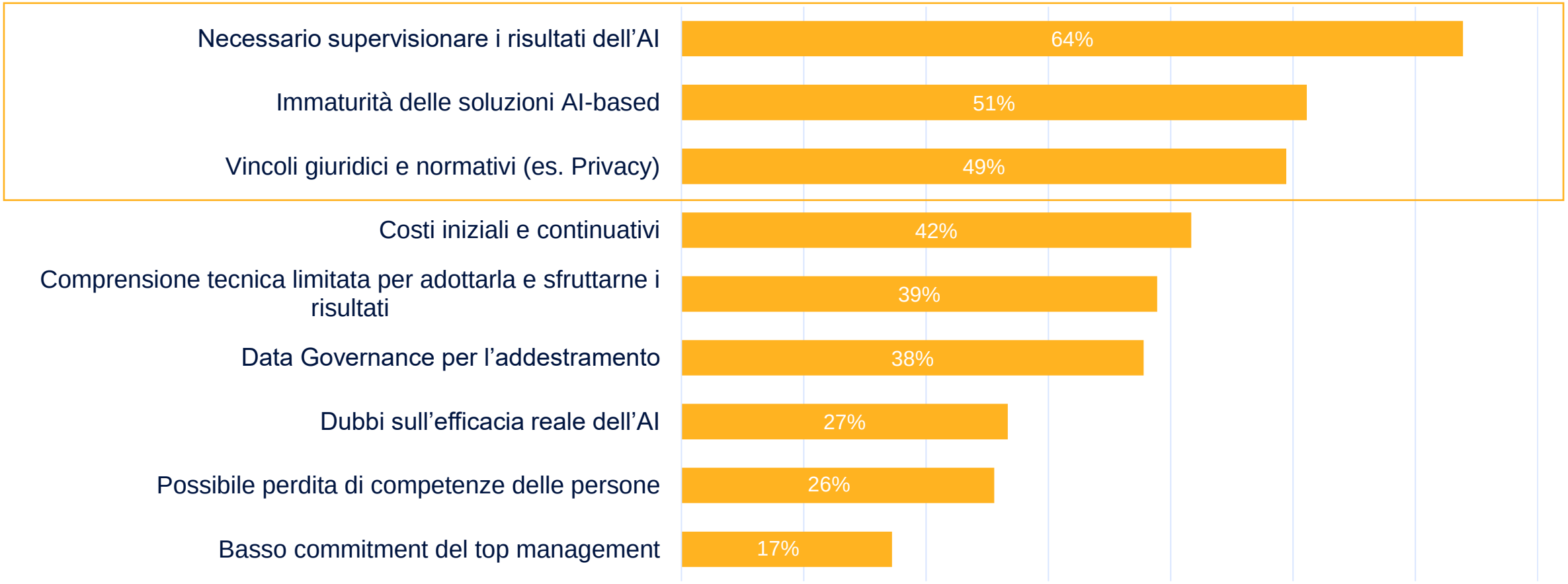
VANTAGGI DELL'AI IN CYBERSECURITY

Quali sono i vantaggi dell'AI in cybersecurity?

FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

SFIDE NELL'ADOZIONE DELL'AI IN CYBERSECURITY

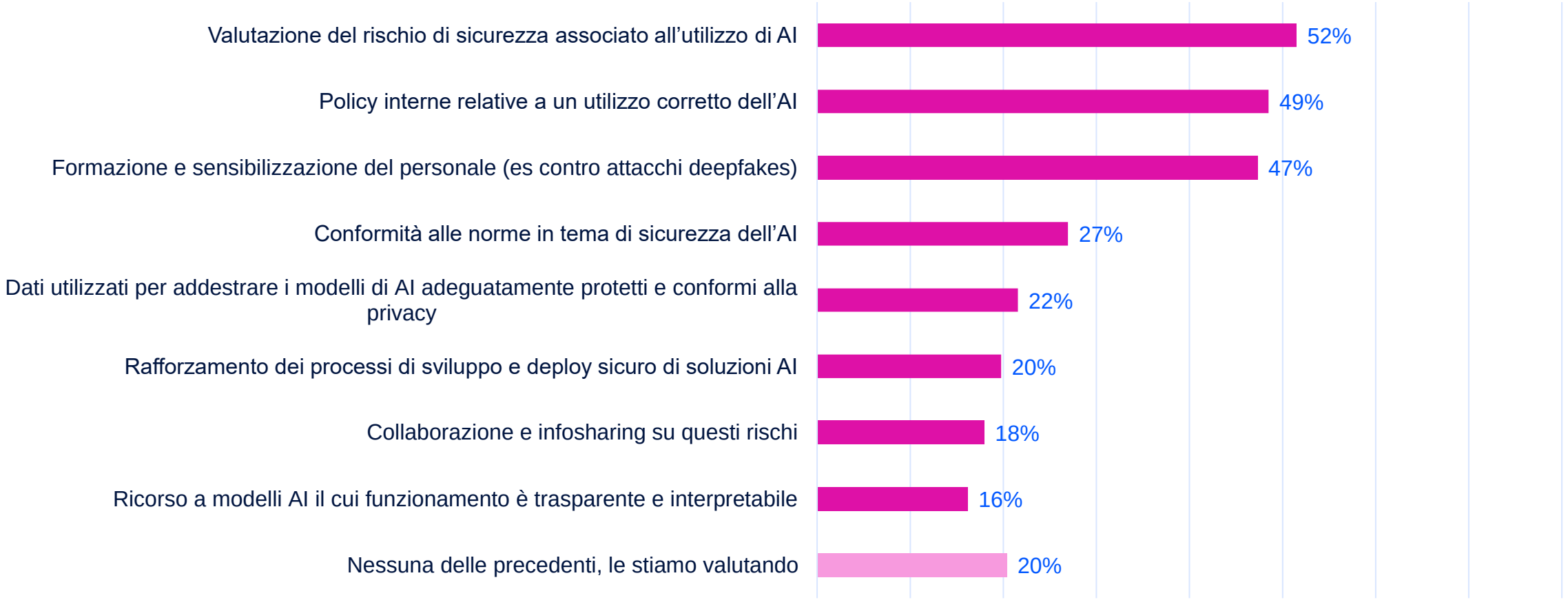
Quali le problematiche dell'AI in cybersecurity?



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

METTERE IN SICUREZZA I NUOVI SVILUPPI AI E GLI UTILIZZI DELL'AI IN AZIENDA

Considerando qualsiasi utilizzo dell'AI in azienda, nel business e non solo nella cybersecurity, quali delle seguenti azioni per mitigarne i rischi avete adottato o prevedete di adottare in azienda?



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

ALTRO: DEFINIZIONE DI CLAUSOLE CONTRATTUALI SPECIFICHE NEI CONTRATTI CON TERZE PARTI (14%); CONTROMISURE DI CYBERSECURITY PER MODELLI AI (ES. fiRME DIGITALI, CRITTOGRAfiA, PATCHING) (13%); MONITORAGGIO PER RILEVARE COMPORTAMENTI ANOMALI NEI MODELLI DI AI (11%); MITIGAZIONE DEI BIAS: MISURE PER GARANTIRE LA DIVERSITÀ E L'EQUITÀ NEI DATI DI ADDESTRAMENTO (9%); PREVENZIONE DEGLI ATTACCHI DI ADVERSARIAL MACHINE LEARNING (8%); NESSUNA DELLE PRECEDENTI, NON SONO PREVISTE (5%)

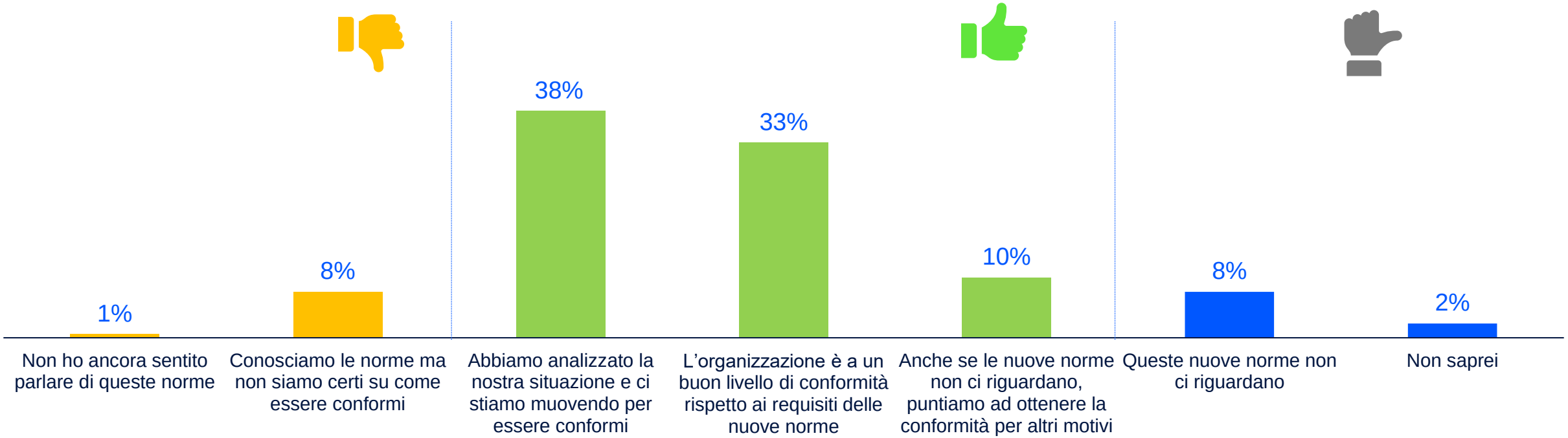
TIG | THE INNOVATION GROUP

WE DRIVE **TRANSFORMATION**

NIS2: A CHE PUNTO SIAMO?

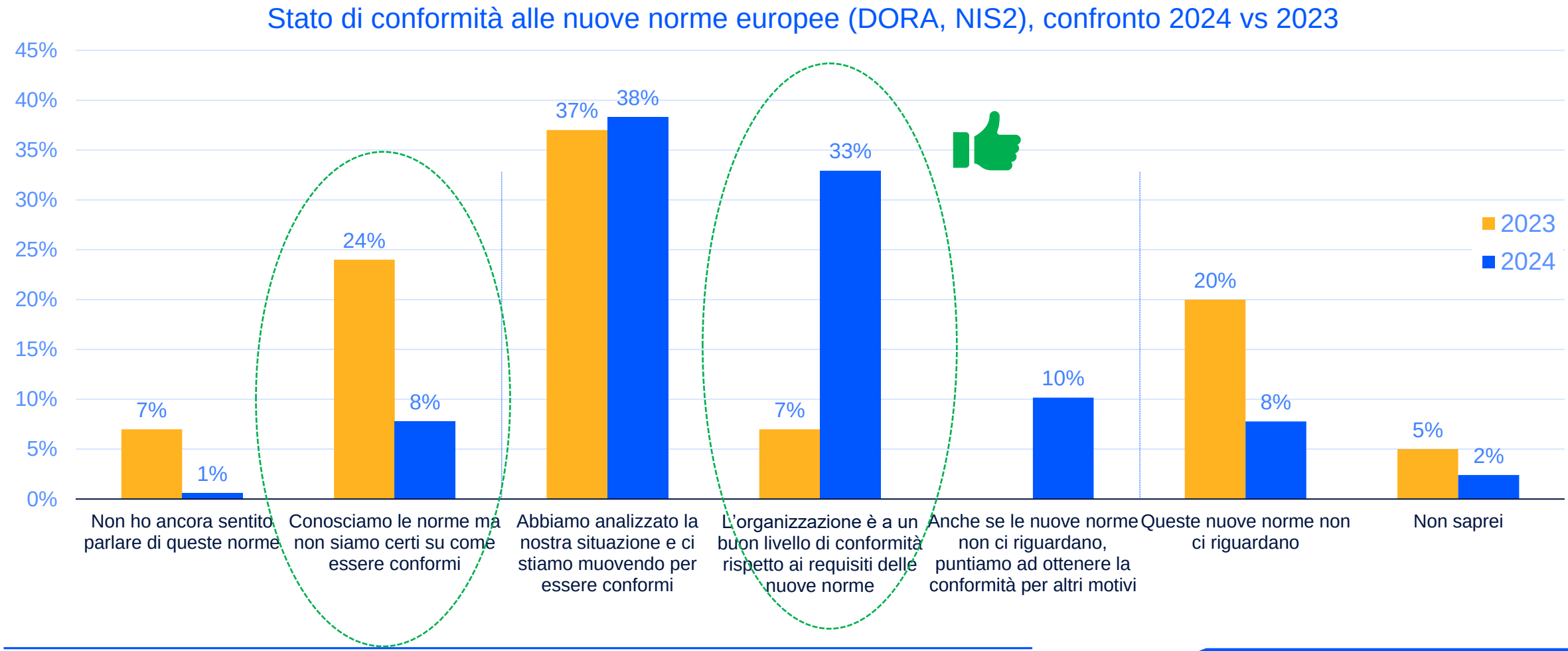
LA MAGGIOR PARTE DELLE ORGANIZZAZIONI (81%) È IMPEGNATA NELLA COMPLIANCE ALLA NIS2

Nel 2024 sono entrate in vigore le nuove norme europee (DORA, NIS2) che richiedono più elevati livelli di cyber resilienza, come il controllo della sicurezza dei fornitori e una migliore gestione degli incidenti informatici. Qual è la situazione della Sua



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

IL CONFRONTO CON IL 2023 MOSTRA UN MIGLIORAMENTO DELLA PREPARAZIONE E DELLA CONOSCENZA SUI REQUISITI DELLE NORME



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025, CONFRONTO CON CYBER RISK MANAGEMENT 2024 SURVEY, GENNAIO 2024

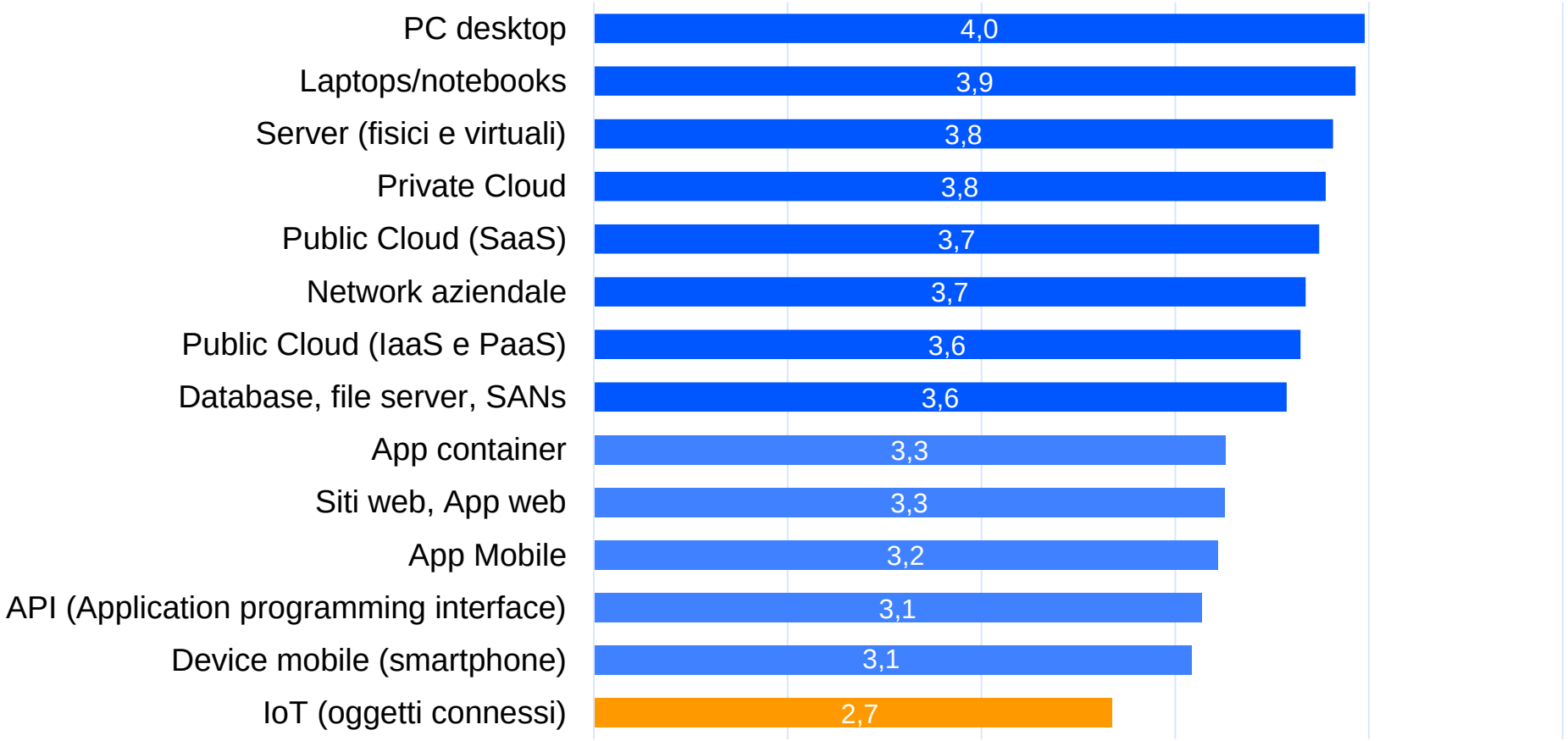
TIG THE INNOVATION GROUP

WE DRIVE **TRANSFORMATION**

QUAL E' LA MATURITÀ DELLA SECURITY POSTURE DELLE ORGANIZZAZIONI ITALIANE?

LA POSTURA DI SICUREZZA DEGLI AMBIENTI ICT NELLE ORGANIZZAZIONI ITALIANE È SUFFICIENTEMENTE BUONA

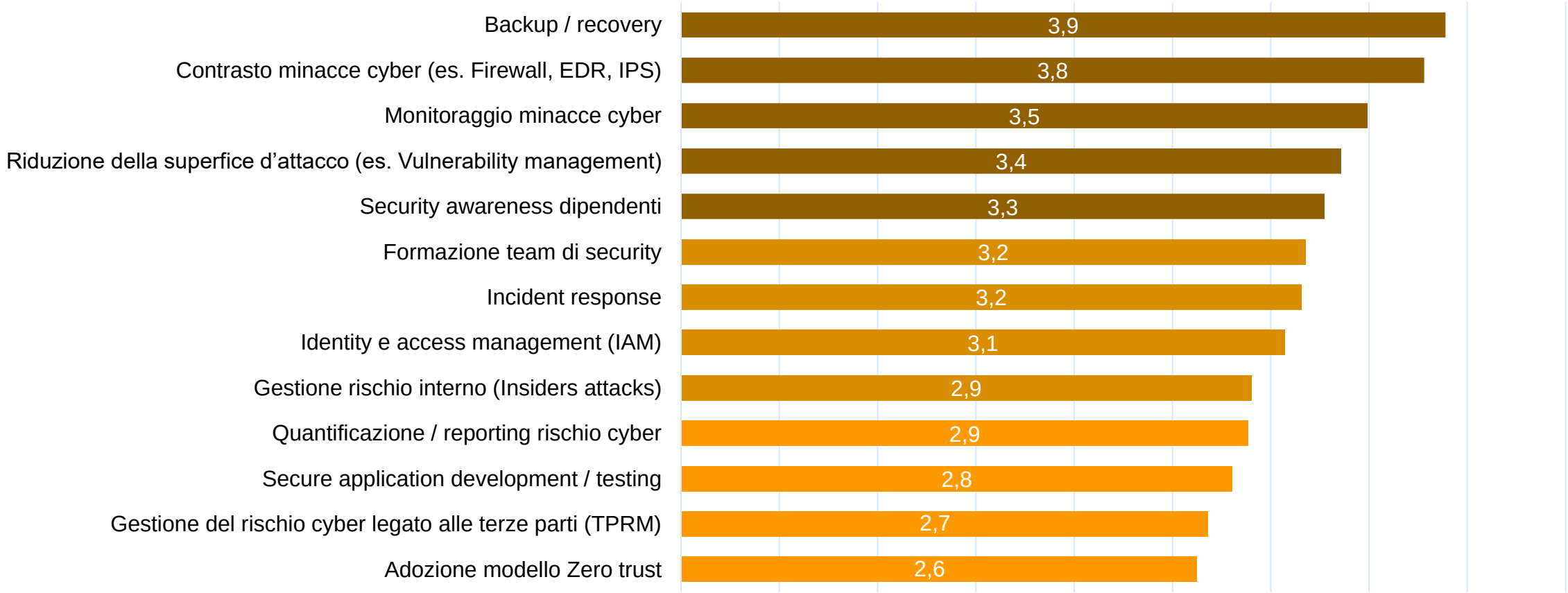
Come valuta la postura di sicurezza dei seguenti ambienti IT della Sua organizzazione? (in una scala da 1 a 5)



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

I PROCESSI DI CYBER RISK MANAGEMENT HANNO UN LIVELLO DI SUFFICIENTE ADEGUATEZZA

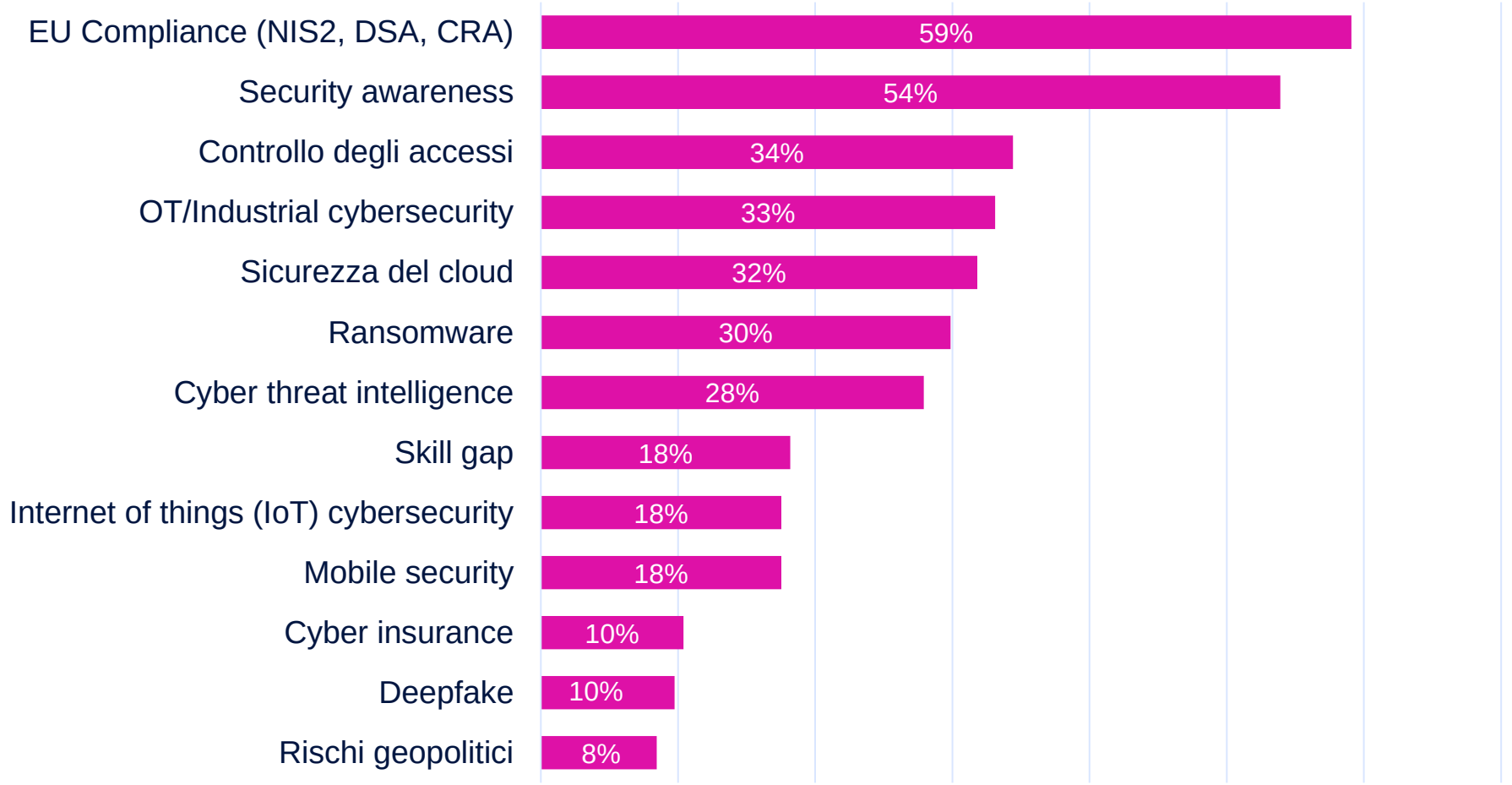
Adeguatezza dei processi di cybersecurity (in termini di persone, processi, tecnologie adottate) (in una scala da 1 a 5)



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

COMPLIANCE E AWARENESS AI PRIMI POSTI NELLE PRIORITÀ 2025 DEL CISO

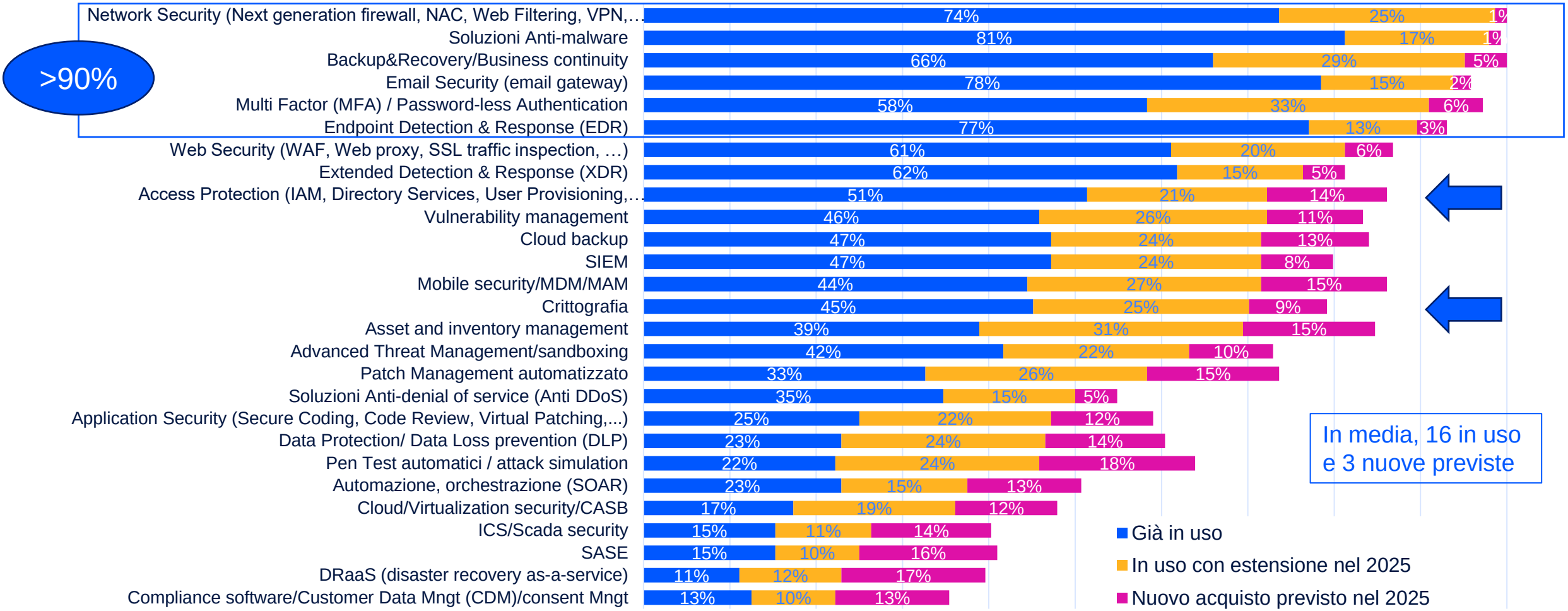
Gli Hot Topic 2025 per il CISO



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

OLTRE IL 90% DELLE AZIENDE SI È DOTATA DELLE PRIME 6 SOLUZIONI DI CYBERSECURITY

Quali tecnologie/ soluzioni di cybersecurity utilizzate già/ prevedete di estendere a più ambiti/ andrete a dotarvi ex novo nel 2025, per aspetti legati alla protezione di dati e infrastrutture?



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

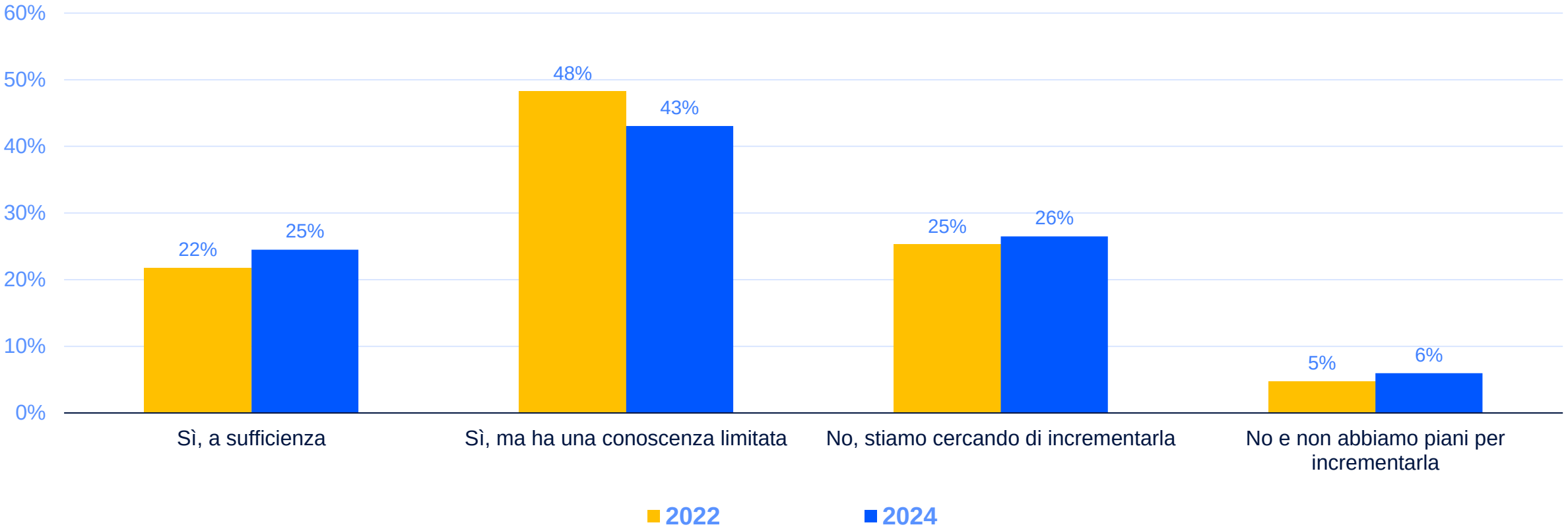
TIG | THE INNOVATION GROUP

WE DRIVE **TRANSFORMATION**

QUANTO E' AVANZATO IL LIVELLO DI COMUNICAZIONE CON IL BOARD/CDA SULLA CYBERSECURITY?

CREARE CONSAPEVOLEZZA NEL VERTICE: SI FA ANCORA TROPPO POCO

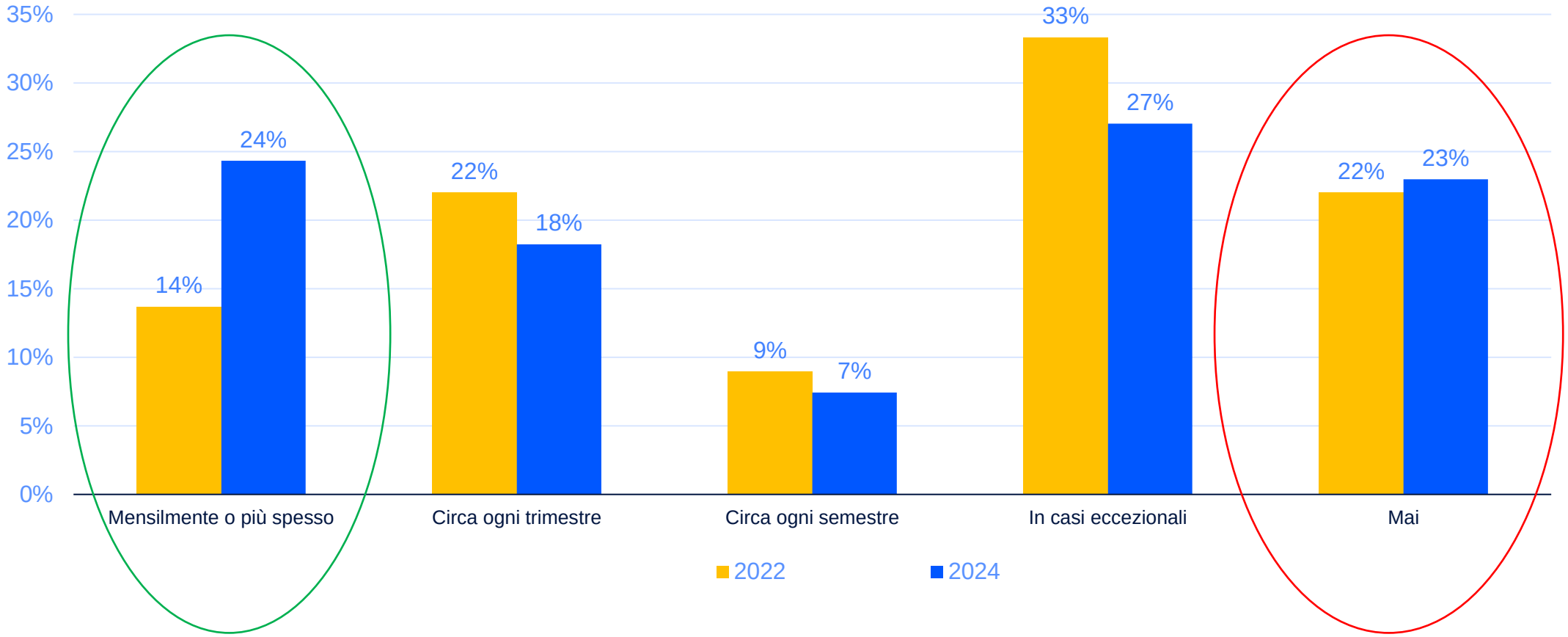
Il Board / il top management della Sua azienda ha una conoscenza adeguata dell'ICT Security, è in grado di valutarne rischi e contromisure? (2024 vs 2022)



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025 – CONFRONTO CON SURVEY 2023

AUMENTANO GLI INCONTRI TRA IL CISO E I VERTICI AZIENDALI

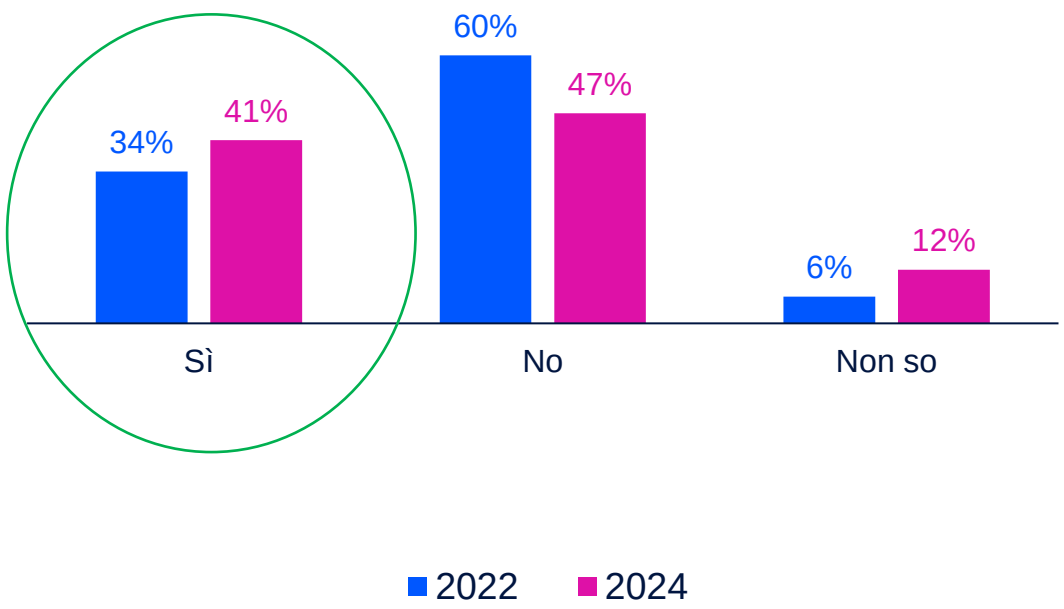
Quanto spesso il CISO / ruolo equivalente della Sua azienda partecipa ad incontri con il CEO/CDA durante l'anno? (2024 vs 2022)



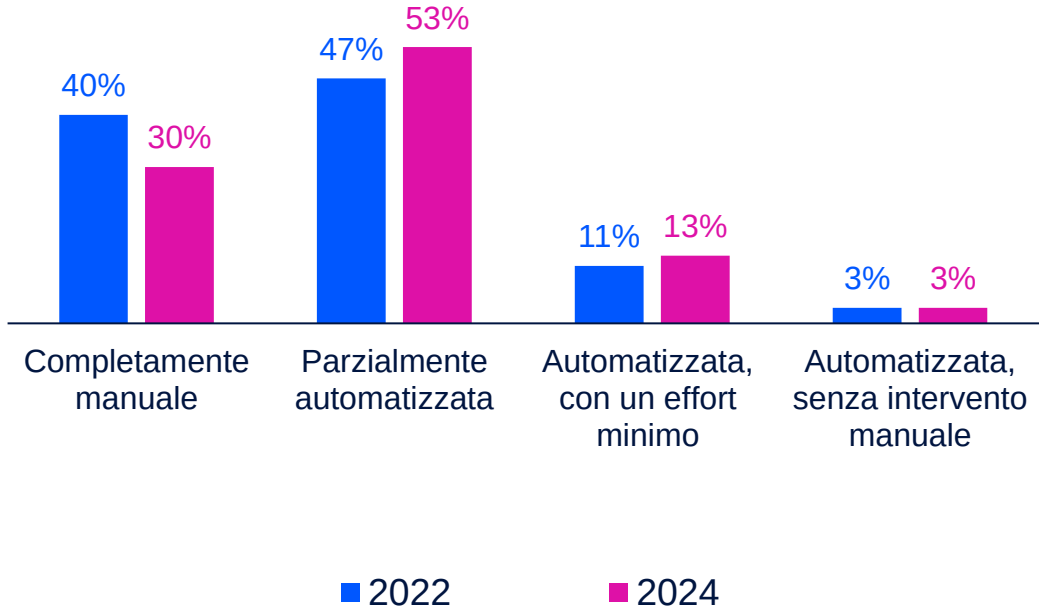
FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025 – CONFRONTO CON SURVEY 2023

SI OSSERVA UN INCREMENTO (DAL 34% DEL 2022 AL 41% NEL 2024) DEL NUMERO DI AZIENDE CHE INCLUDONO METRICHE NEL REPORTING DI CYBERSECURITY

Il reporting al CEO/ Board comprende metriche che misurano la situazione dell'ICT Security? (2024 vs 2022)



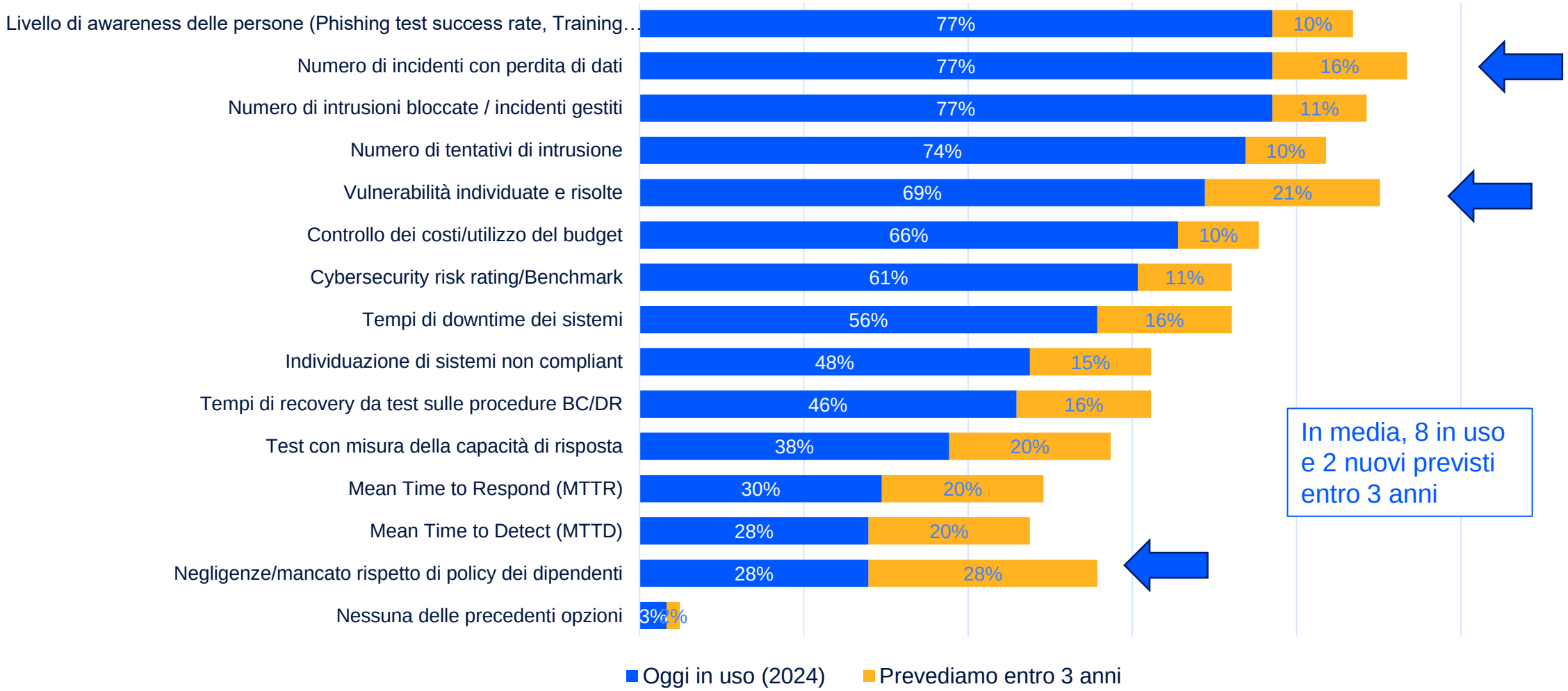
Come avviene la misurazione degli indicatori/metriche oggetto di reporting? (2024 vs 2022)



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025 – CONFRONTO CON SURVEY 2023

IN MEDIA, SI UTILIZZANO 8 DIVERSI INDICATORI NEL REPORTING DI CYBERSECURITY E NE INTRODURRANNO ALTRI 2 NEI PROSSIMI 3 ANNI

Quali indicatori/ metriche utilizzate oggi per il reporting interno, quali potreste introdurre entro 3 anni?

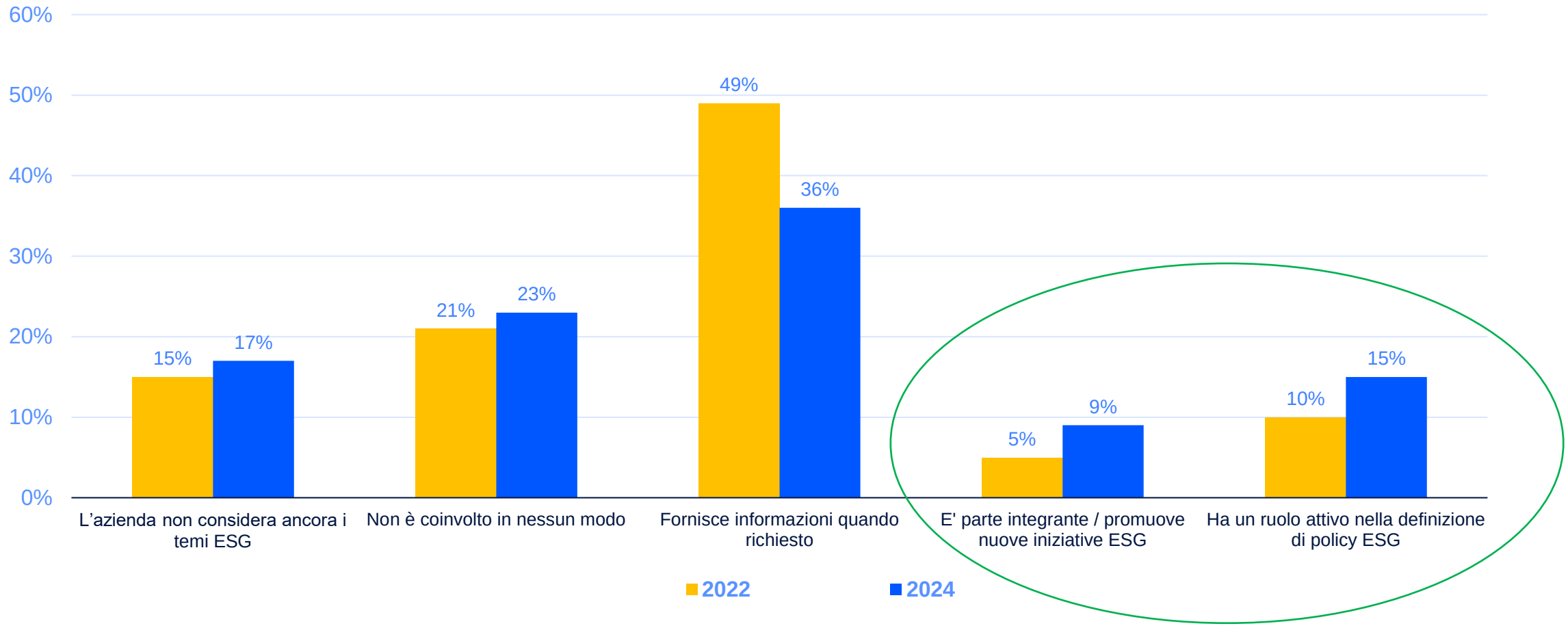


In media, 8 in uso e 2 nuovi previsti entro 3 anni

FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

IL COINVOLGIMENTO DEL CISO NELLE POLITICHE ESG

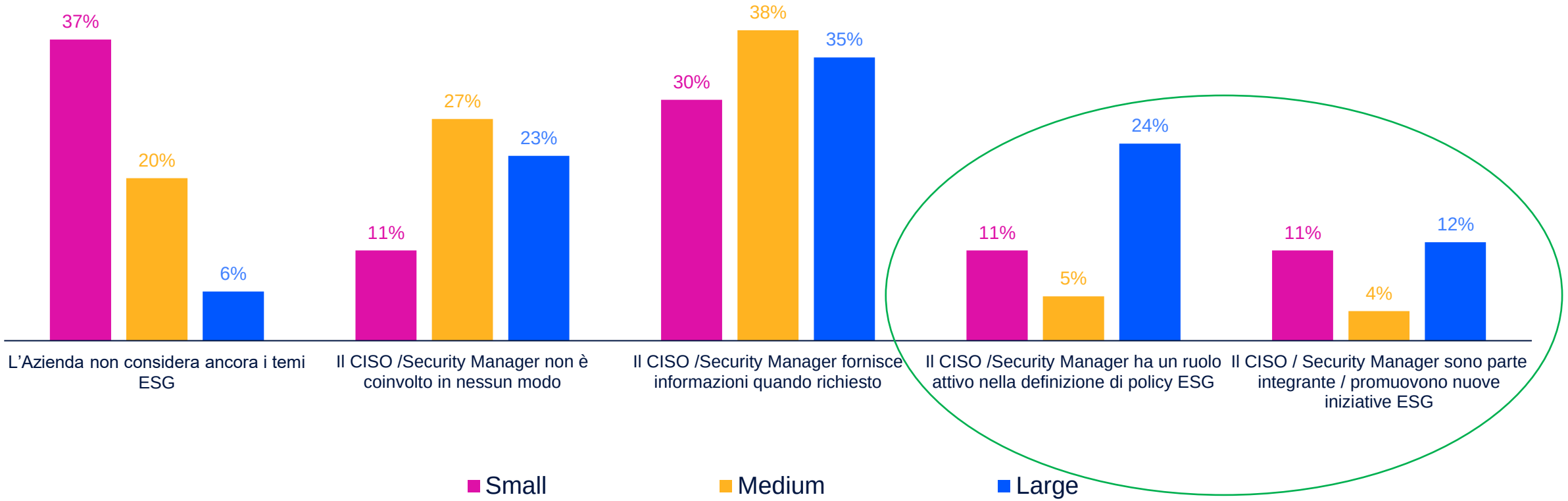
Come valuta il coinvolgimento del CISO / del Security Manager sui temi delle politiche ESG (Environmental, Social e Governance) nella Sua azienda? (2024 vs 2022)



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025 – CONFRONTO CON SURVEY 2023

NEL 36% DELLE GRANDI ORGANIZZAZIONI IL CISO È GIÀ OGGI MOLTO ATTIVO NELLA PROMOZIONE DI POLITICHE ESG

Coinvolgimento del CISO/ del Security Manager nelle politiche ESG (per dimensione di impresa)



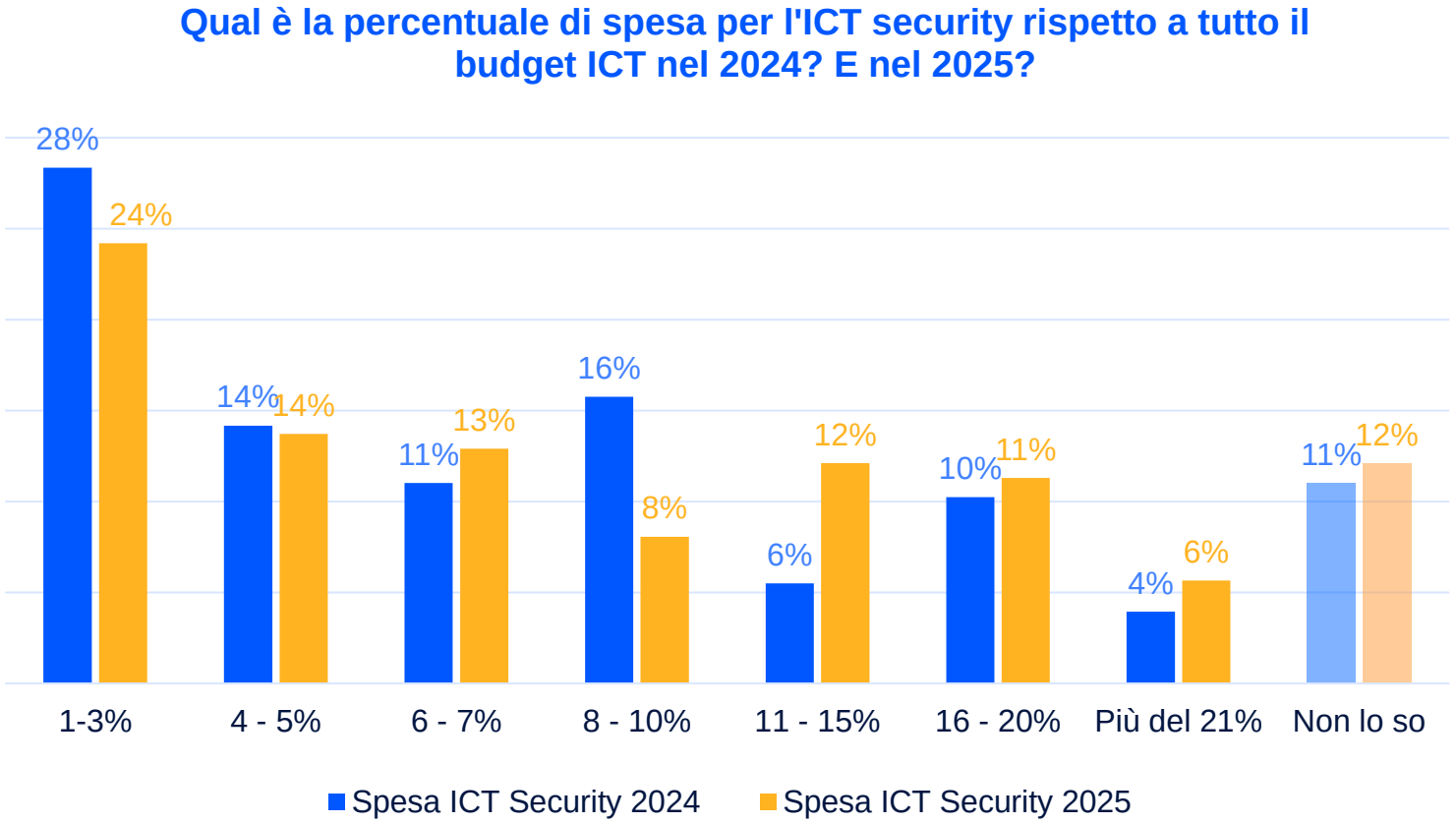
FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025 – PER DIMENSIONE AZIENDALE

TIG THE INNOVATION GROUP

WE DRIVE **TRANSFORMATION**

QUANTO CRESCONO IN MEDIA GLI INVESTIMENTI IN CYBERSECURITY?

IL BUDGET DI CYBERSECURITY È IN CONTINUA CRESCITA: NEL 2024 RAGGIUNGE UNA MEDIA DEL 8,4% CON UNA PREVISIONE DEL 9,5% PER IL 2025

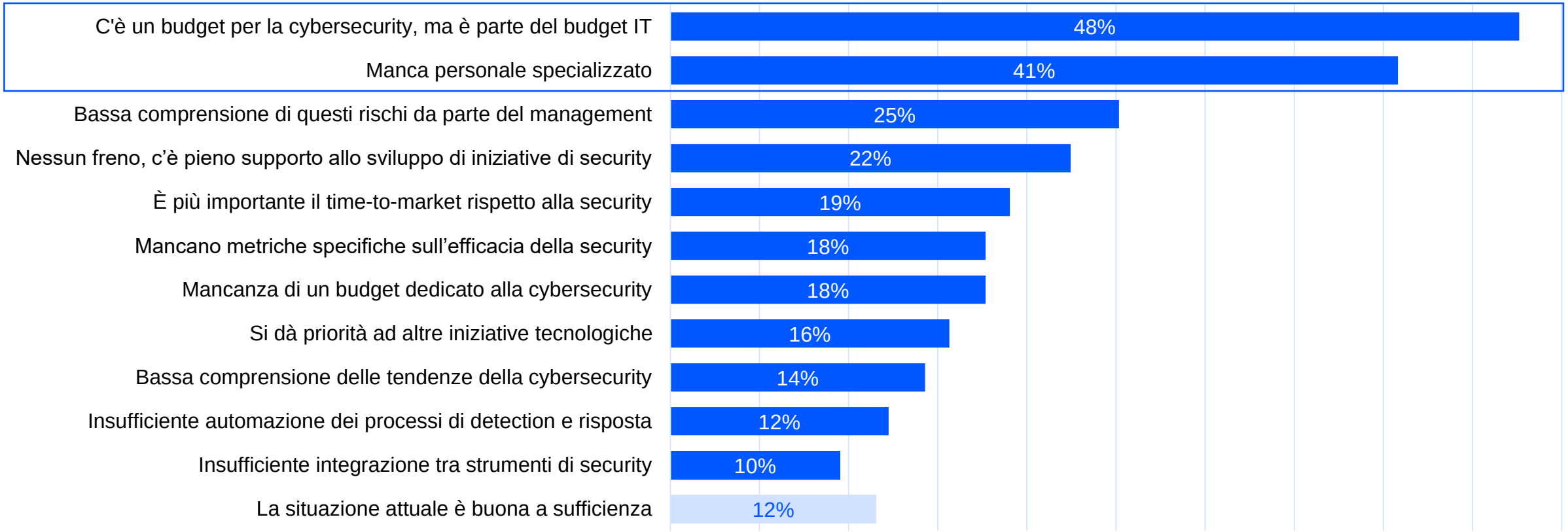


Indagine - Anno	% Spesa ICT Security rispetto a Budget ICT	
Indagine «Cyber Risk Management 2025»	2024	**8,4%**
	Previsione 2025	**9,5%**
Indagine «Cyber Risk Management 2024»	2023	**8,3%**
	Previsione 2024	**9,0%**
Indagine «Cyber Risk Management 2023»	2022	**7,2%**
	Previsione 2023	**8,6%**

FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

QUALI SONO I PRINCIPALI FRENI AGLI INVESTIMENTI IN CYBERSECURITY?

Quali fattori frenano nella Sua azienda una migliore gestione del rischio cyber?



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

CONCLUSIONI

- Gli **attacchi informatici continuano ad evolvere e a crescere in volume** sfruttando un contesto geopolitico frammentato e un'evoluzione tecnologica rampante. La digitalizzazione è diventata più diffusa, con il cloud e l'IoT è aumentata la superfice da proteggere, l'AI offre molte opportunità (in larga parte già sfruttate in cybersecurity) ma nel contempo **aumentano i rischi, di subire attacchi o di incrementare le vulnerabilità.** I **vertici aziendali sono più consapevoli rispetto al passato**, ma la comunicazione interna alle organizzazioni richiede ulteriori sforzi.

- I risultati dell'indagine «Cyber Risk Management 2025» di TIG – The Innovation Group e CSA – Cyber Security Angels sui percorsi di Cyber Risk Management nelle aziende italiane, mostrano una combinazione di sfide tradizionali (es. ransomware, sicurezza del cloud) e nuove esigenze (compliance normativa, OT cybersecurity). **Nella lista delle priorità 2025 per i CISO, i due temi principali sono l'EU Compliance e la Security Awareness.**

- Il confronto con le survey degli anni scorsi indica in generale molti miglioramenti, in alcuni casi però a una velocità inferiore rispetto a quella che sarebbe necessaria: **alcune problematiche di fondo risultano infatti non risolte**. Sono stati indagati gli aspetti che frenano gli investimenti in cybersecurity: i risultati evidenziano che le principali barriere non sono strettamente tecnologiche, ma piuttosto legate a fattori organizzativi, culturali e di risorse.

- La dipendenza degli investimenti in cybersecurity dal budget IT (48% delle risposte) e la mancanza di personale specializzato (41%) riflettono una **gestione non autonoma della cybersecurity**. Nel confronto invece tra realtà di diversa dimensione, le grandi organizzazioni appaiono in generale più strutturate, con una maggior numero di processi e misure tecnologiche oltre che con un reporting più completo verso il vertice e una migliore compliance alle norme.

- In questo scenario, emergono le priorità:

  - uno sforzo più ampio per la **diffusione di competenze di sicurezza nell'organizzazione**;
  - un'azione più **coordinata tra i diversi attori dell'ecosistema digitale** in cui viviamo (e una IT supply chain più sicura);
  - la necessità di dotarsi di un **Integrated Risk Management** per gestire in modo integrato e risk-based aspetti come compliance, cyber resilienza e sicurezza delle terze parti.

Siamo The Innovation Group.
Progettiamo, raccontiamo e governiamo il cambiamento.

TIG THE INNOVATION GROUP

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

TIG Events s.r.l.
Via Ettore Romagnoli, 6
20146, Milano