

# ***CYBER RISK MANAGEMENT 2025 SURVEY***

SFIDE E OPPORTUNITÀ NEI PROGRAMMI DI  
CYBERSECURITY DELLE AZIENDE ITALIANE

**CYBERSECURITY SUMMIT 2025  
SECURING THE FUTURE: PROGETTARE LA  
SICUREZZA DEL DOMANI**

**ELENA VACIAGO**, RESEARCH MANAGER, TIG – THE INNOVATION GROUP

MILANO, 19 MARZO 2025

# SECURING THE FUTURE: COME STA EVOLVENDO LO SCENARIO DELLE MINACCE DI CYBERSECURITY?

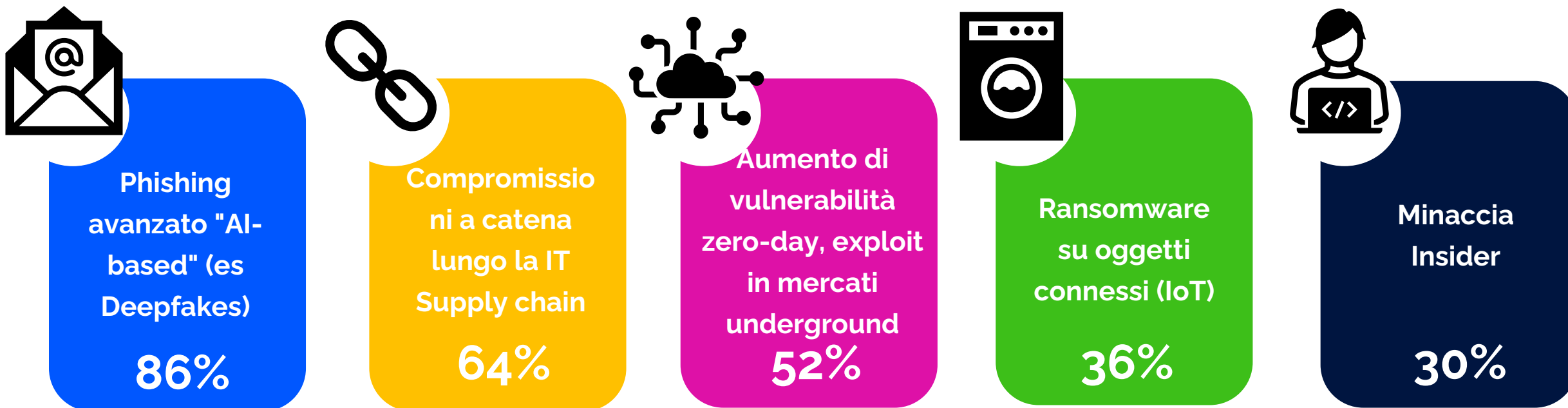
# RISCHI FUTURI DI CYBERSECURITY: PHISHING AI-BASED E IT SUPPLY CHAIN



**CSA**  
Cyber Security Angels

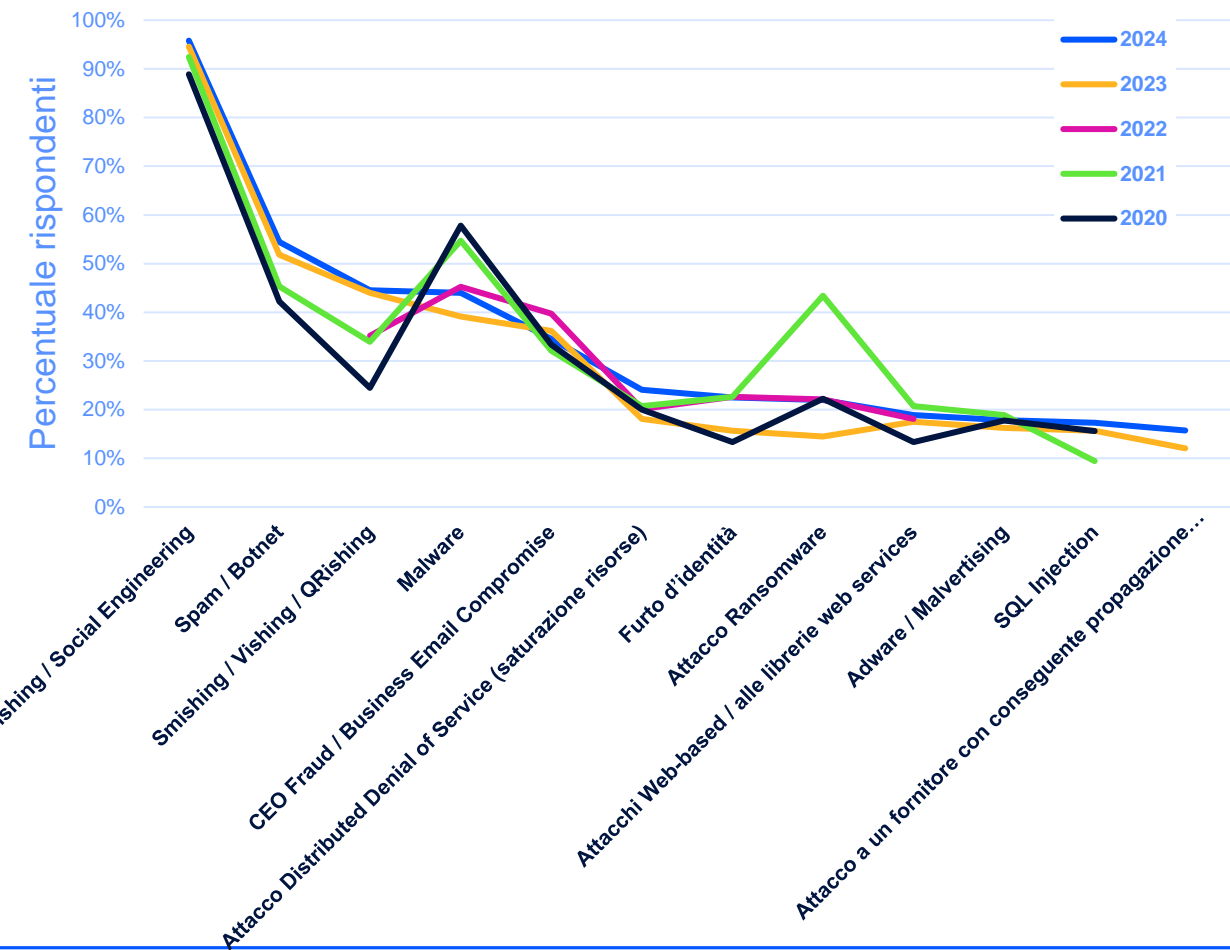
**TIG** | THE  
INNOVATION  
GROUP

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



# EVOLUZIONE DELLO SCENARIO DEGLI ATTACCHI CYBER, ANDAMENTO IN 5 ANNI

Nel corso degli ultimi 12 mesi, quali dei seguenti tentativi di attacco / tecniche di attacco avete rilevato nella Vostra azienda? (confronto su 5 anni)



FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025, CONFRONTO CON CYBER RISK MANAGEMENT 2024, 2023, 2022, 2021 SURVEY

Quali delle seguenti attività avete condotto nel 2024 per identificare i rischi cyber riguardanti la vostra organizzazione?

76%

Monitoraggio di sicurezza con strumenti specifici (es. IDS, Intrusion Detection Systems)

65%

Test di conoscenza e capacità di risposta delle persone (es. simulazione phishing)

62%

Vulnerability audit

61%

Penetration test

59%

Risk assessment per misurare il rischio cyber per l'impresa

48%

Cyber threat intelligence

42%

Deep web / dark web intelligence

29%

Supply chain risk analysis (es. questionari)

# 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%**

**Mail di phishing scritte meglio / più efficaci**

**53%**

**Audio e video deepfake per impersonare dirigenti aziendali o altri**

**45%**

**Attacchi potenziati da ricognizione sofisticata basata su AI**

**43%**

**Capacità più avanzate nella scoperta di vulnerabilità della difesa / zero days**

**43%**

**Incremento del volume degli attacchi**

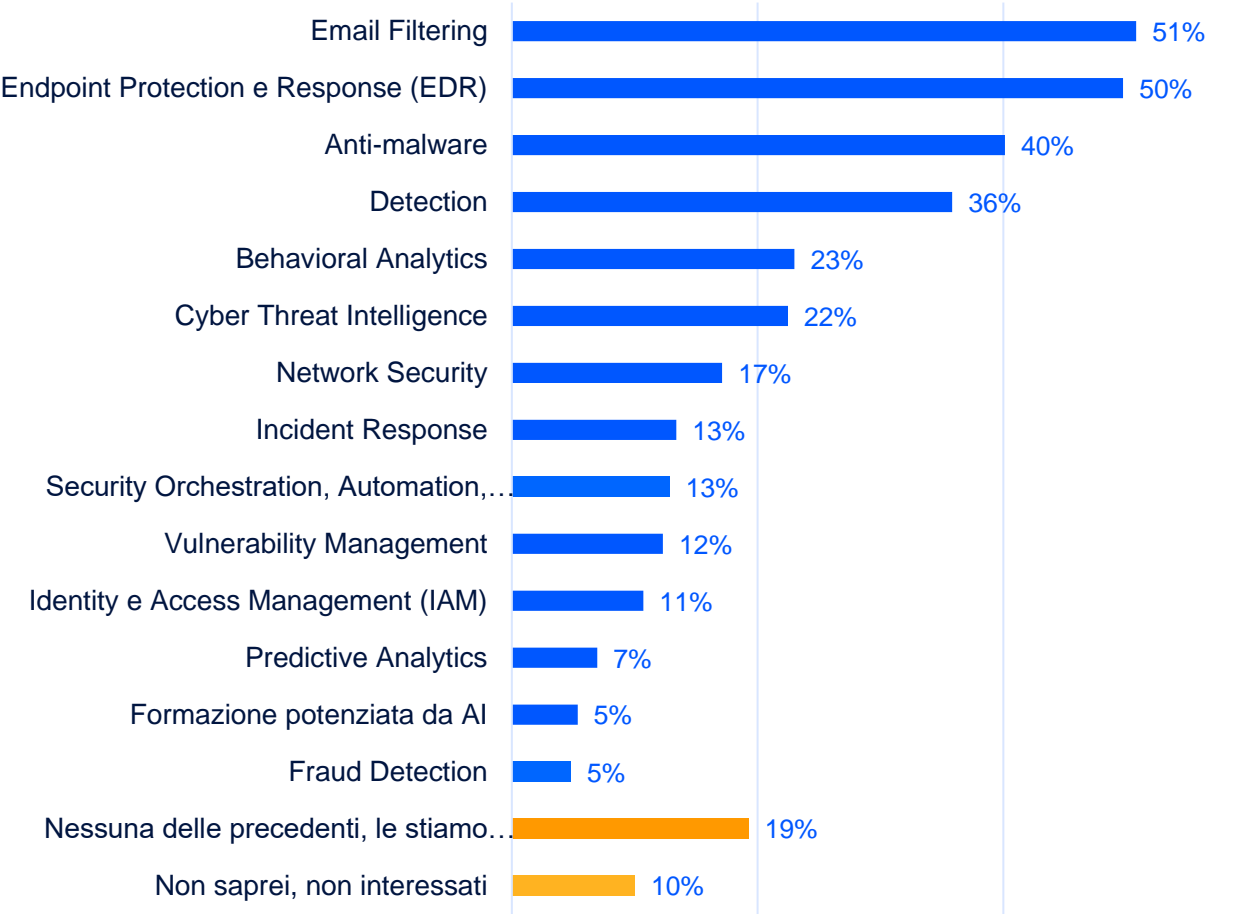
**42%**

**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%)

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

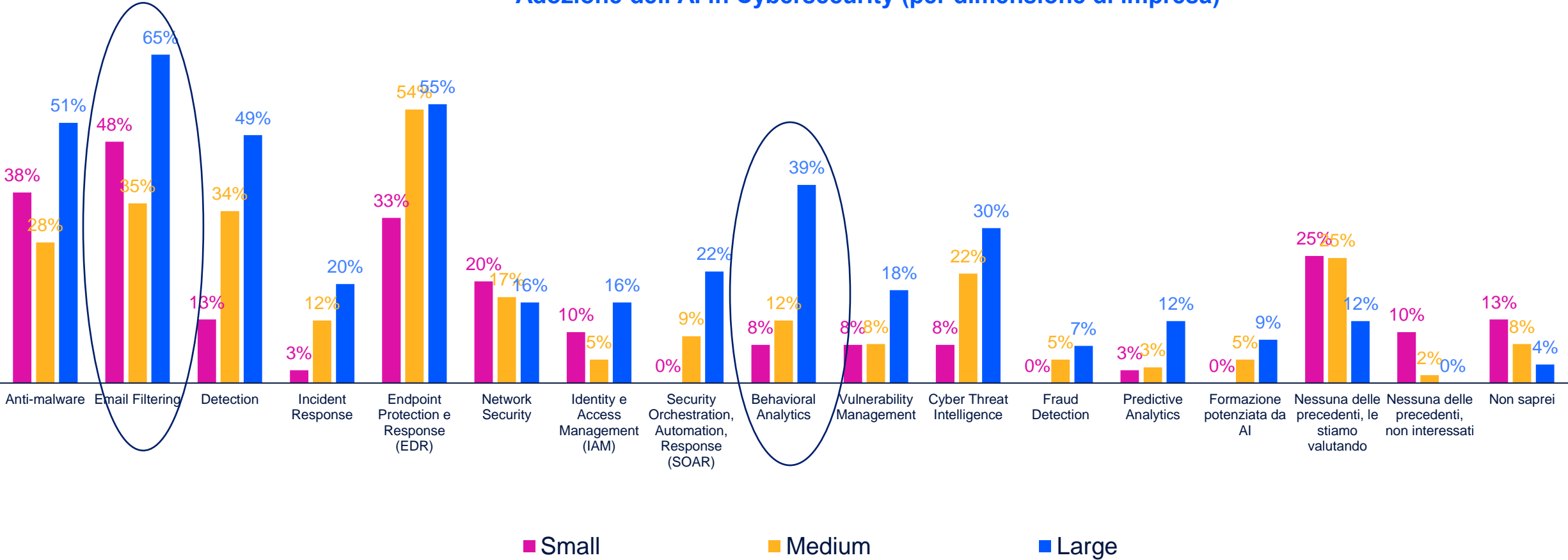




# UTILIZZO PIÙ AVANZATO DELL'AI IN CYBERSECURITY NELLE GRANDI ORGANIZZAZIONI



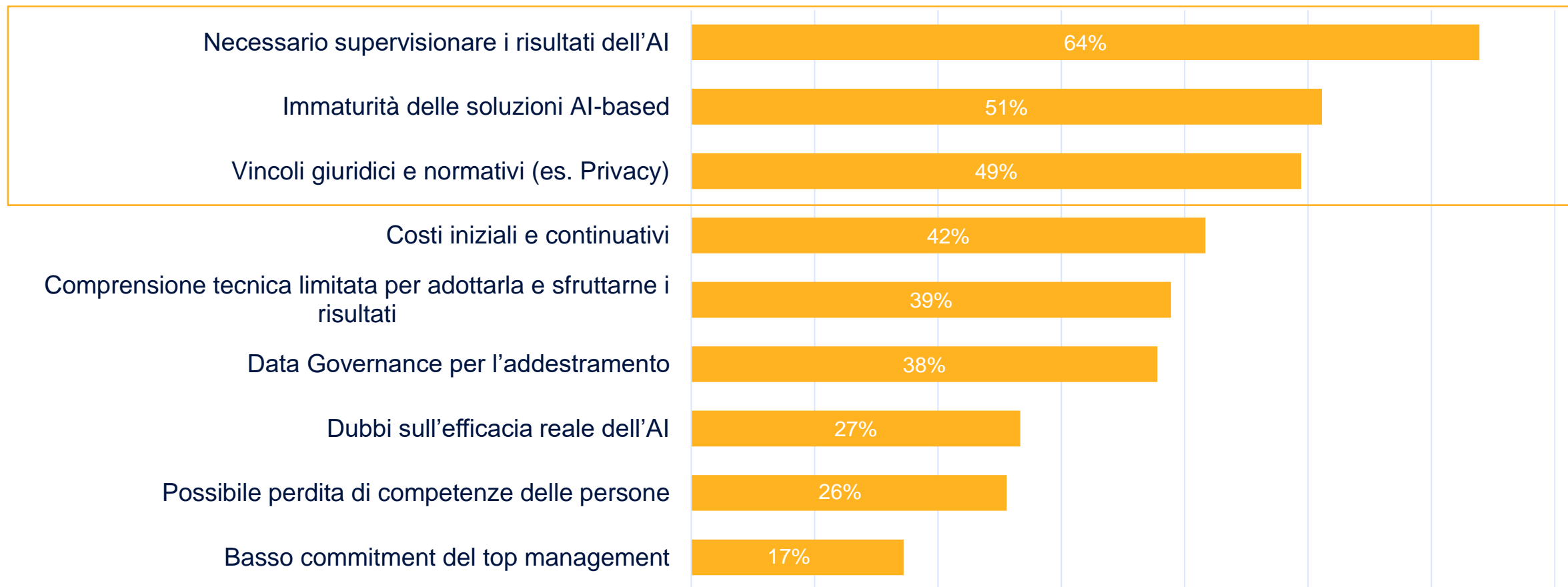
Adozione dell'AI in Cybersecurity (per dimensione di impresa)



## Quali sono i vantaggi dell'AI in cybersecurity?



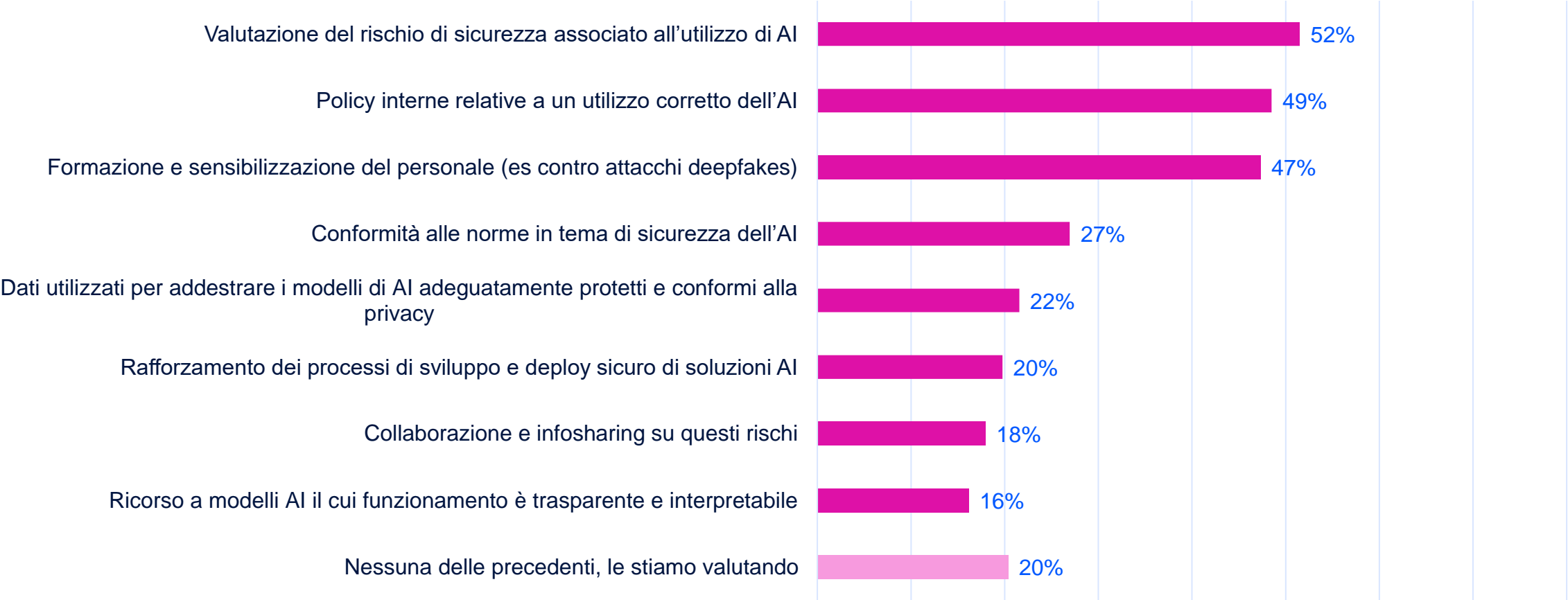
## Quali le problematiche dell'AI in cybersecurity?



# 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?



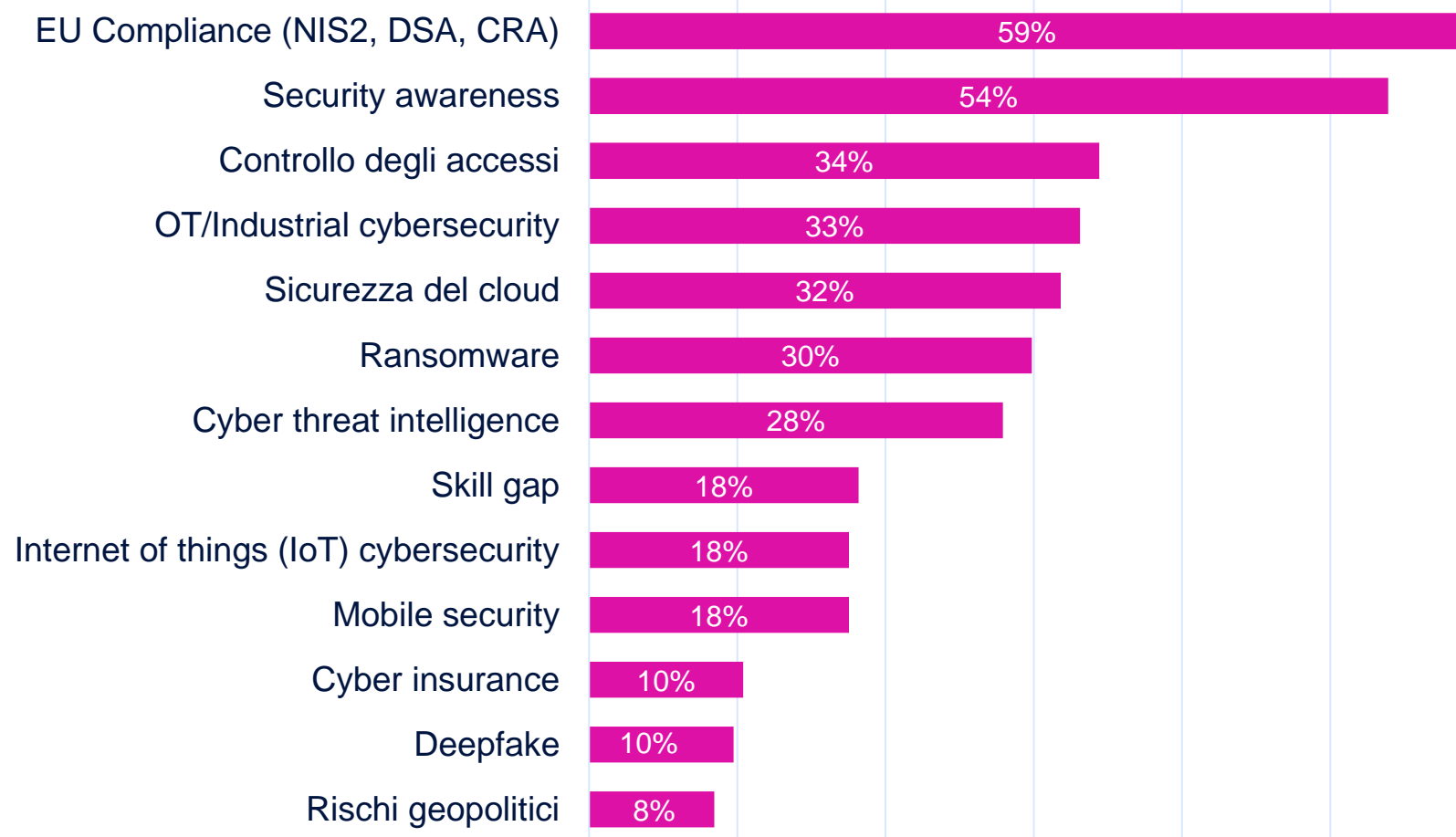
FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025  
ALTRO: DEFINIZIONE DI CLAUSOLE CONTRATTUALI SPECIFICHE NEI CONTRATTI CON TERZE PARTI (14%); CONTROMISURE DI CYBERSECURITY PER MODELLI AI (ES. FIRME DIGITALI, CRITTOGRAFIA, PATCHING) (13%); MONITORAGGIO PER RILEVARE COMPORTAMENTI ANOMALI NEI MODELLI 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%)

# NIS2: A CHE PUNTO SIAMO?

# COMPLIANCE E AWARENESS AI PRIMI POSTI NELLE PRIORITÀ 2025 DEL CISO



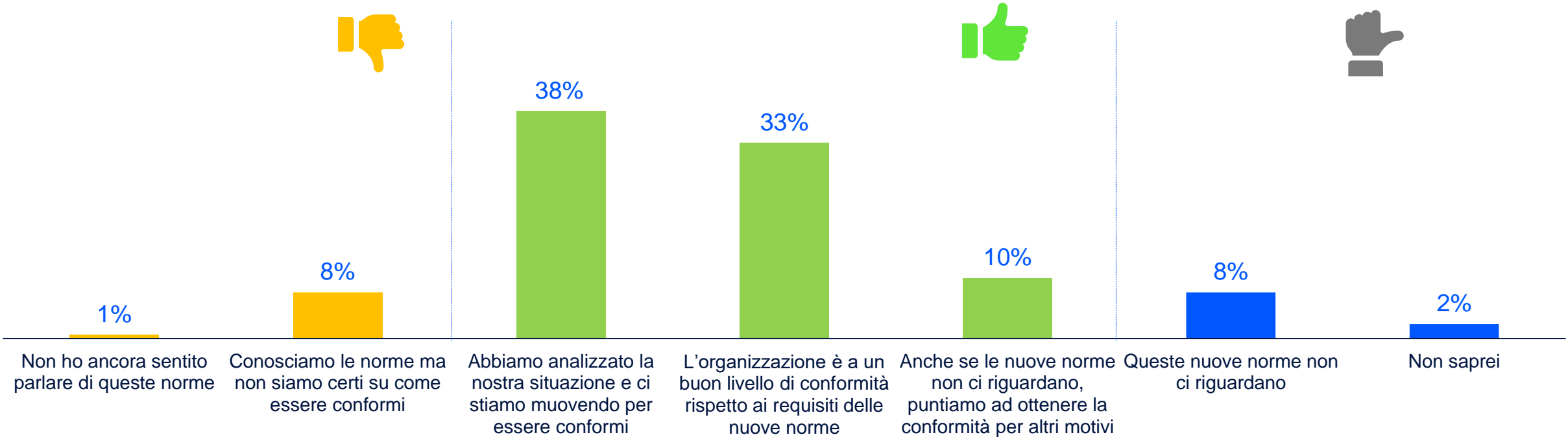
## Gli Hot Topic 2025 per il CISO



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



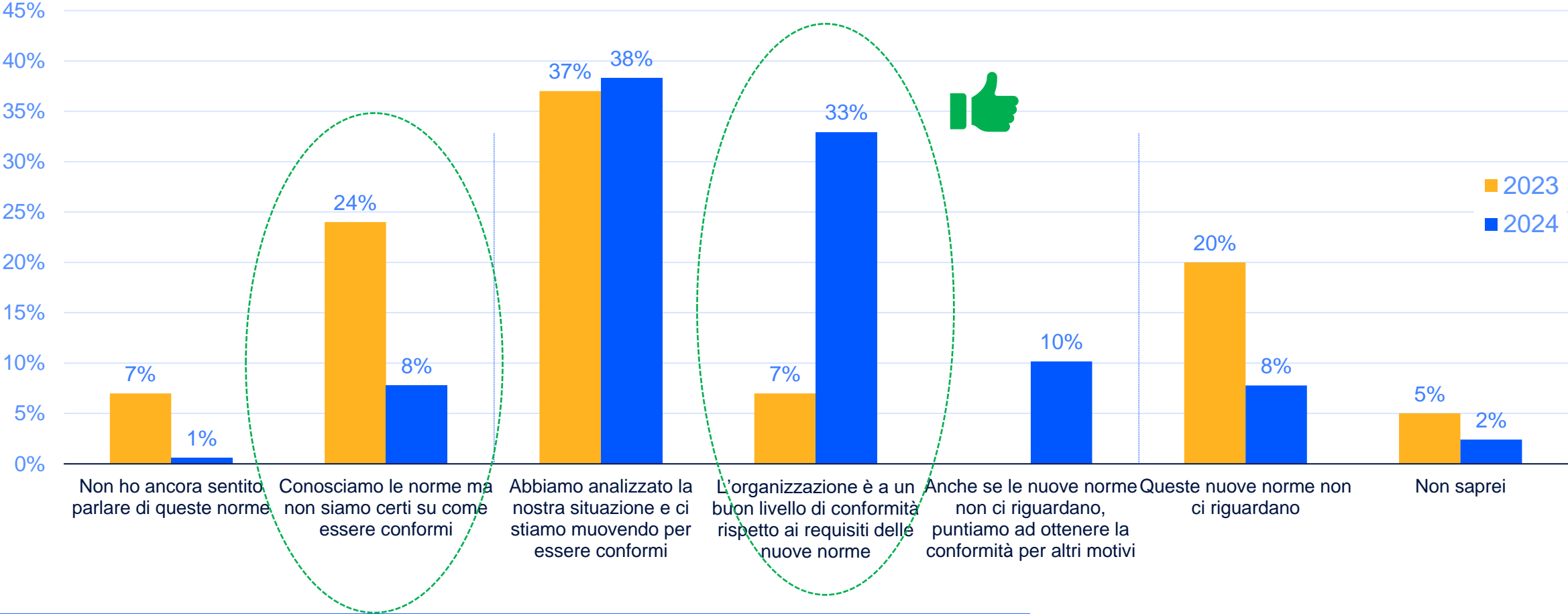
Nel 2024 sono entrate in vigore le nuove norme europee (DORA, NIS2) che richiedono più elevati livelli di cyber resilienza, come il controllo della sicurezza dei fornitori e una migliore gestione degli incidenti informatici. Qual è la situazione della Sua



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



Stato di conformità alle nuove norme europee (DORA, NIS2), confronto 2024 vs 2023



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



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

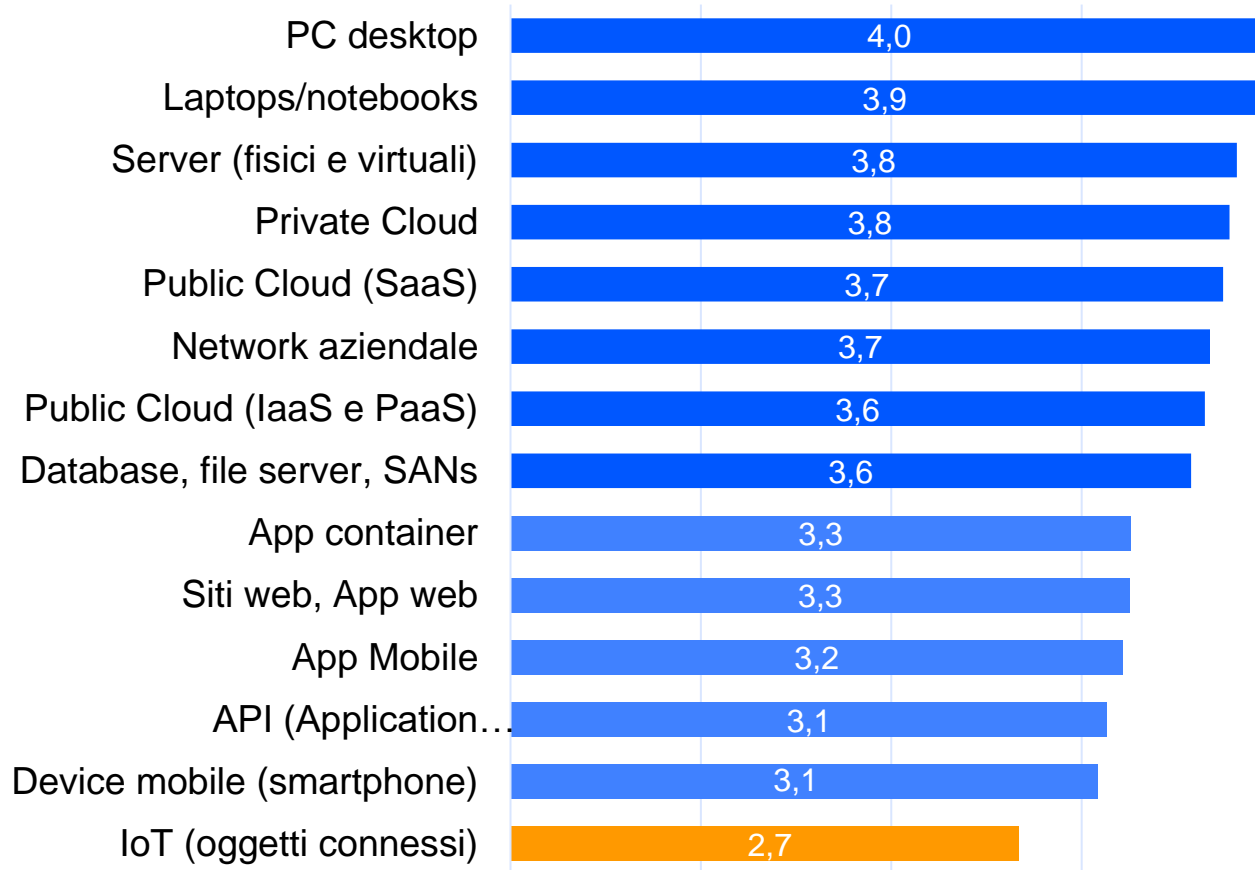
# LA POSTURA DI SICUREZZA DEGLI AMBIENTI ICT NELLE ORGANIZZAZIONI ITALIANE È SUFFICIENTEMENTE BUONA



**CSA**  
Cyber Security Angels

**TIG** | THE INNOVATION GROUP

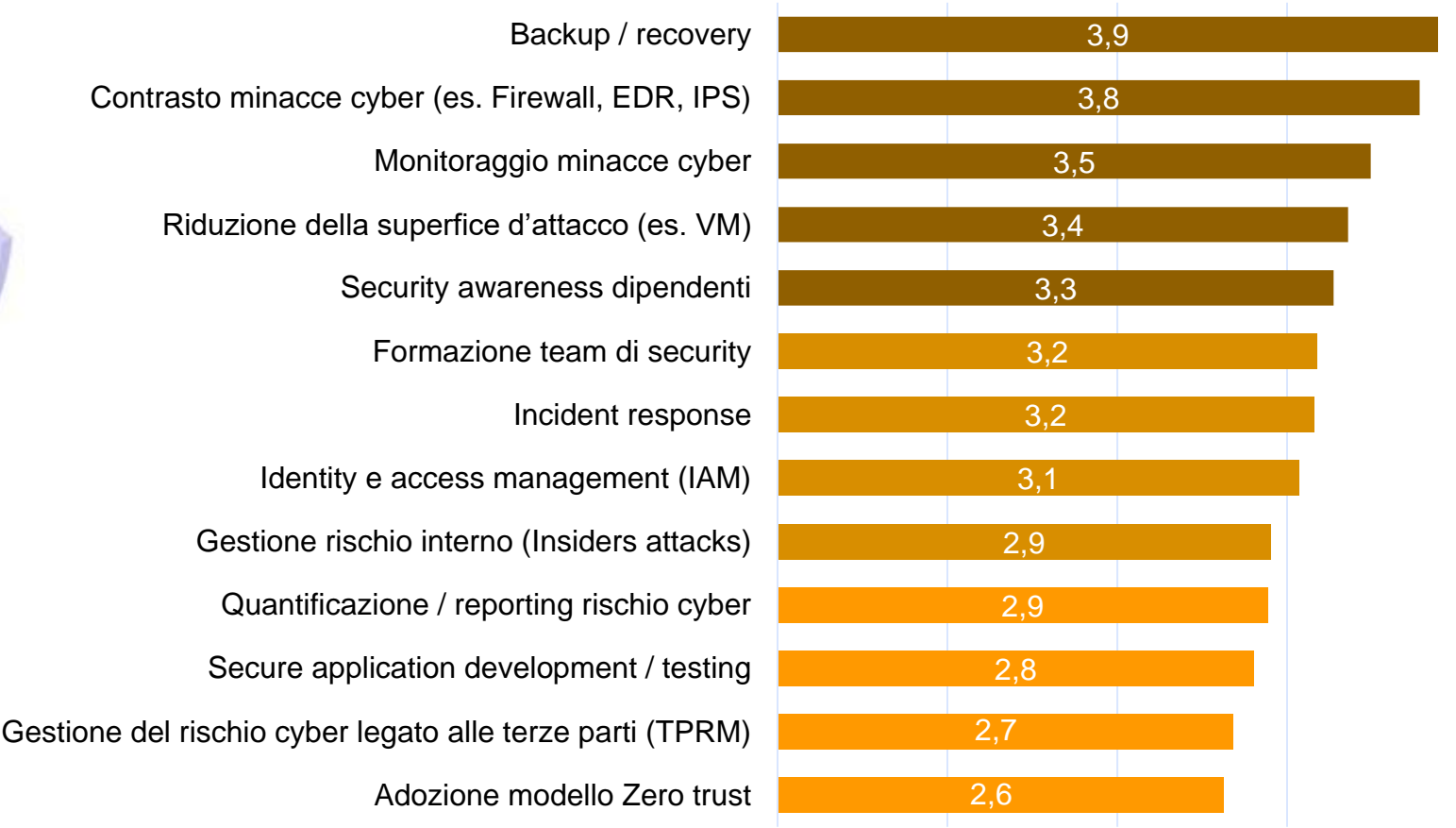
Come valuta la postura di sicurezza dei seguenti ambienti IT della Sua organizzazione? (in una scala da 1 a 5)



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

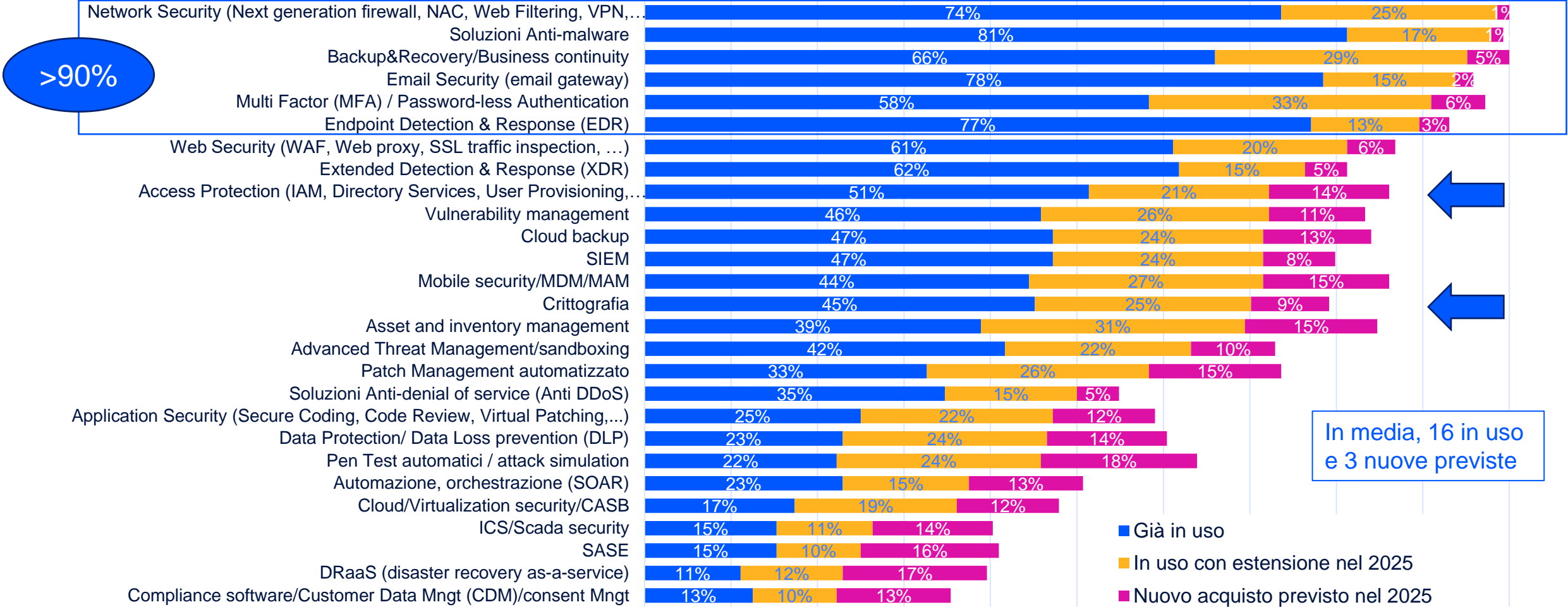


Adeguatezza dei processi di cybersecurity (in termini di persone, processi, tecnologie adottate) (in una scala da 1 a 5)



# 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?



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

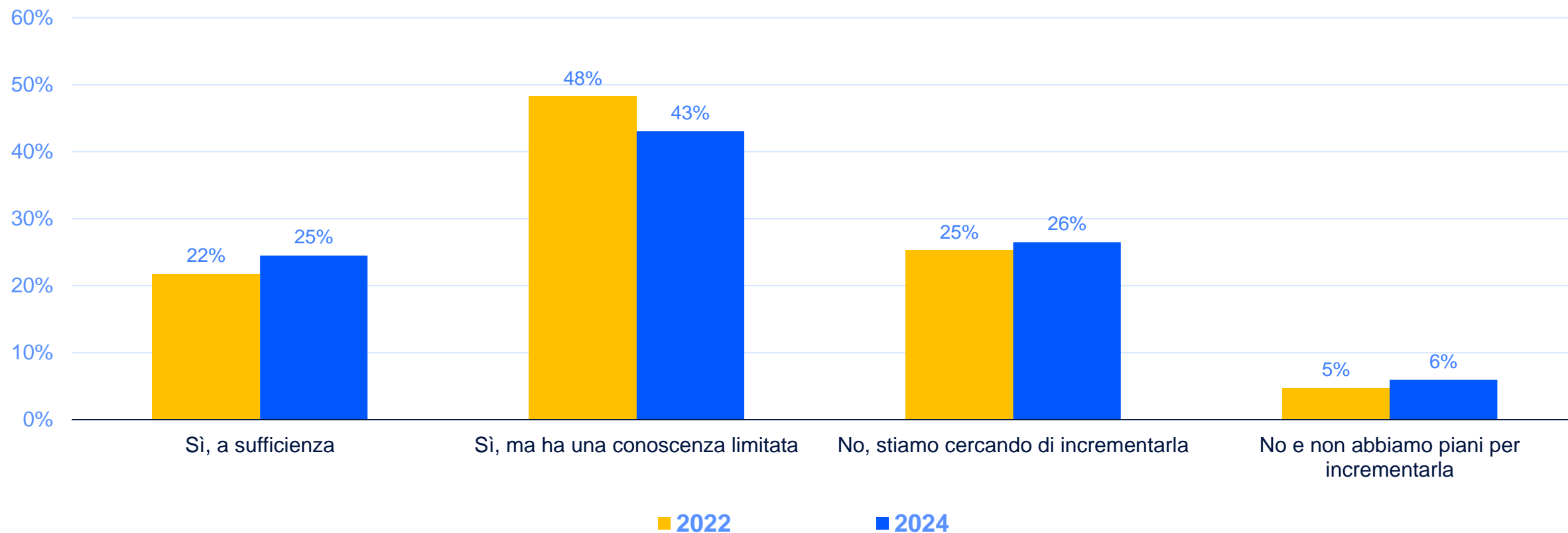
# CREARE CONSAPEVOLEZZA NEL VERTICE: SI FA ANCORA TROPPO POCO



**CSA**  
Cyber Security Angels

**TIG** | THE INNOVATION GROUP

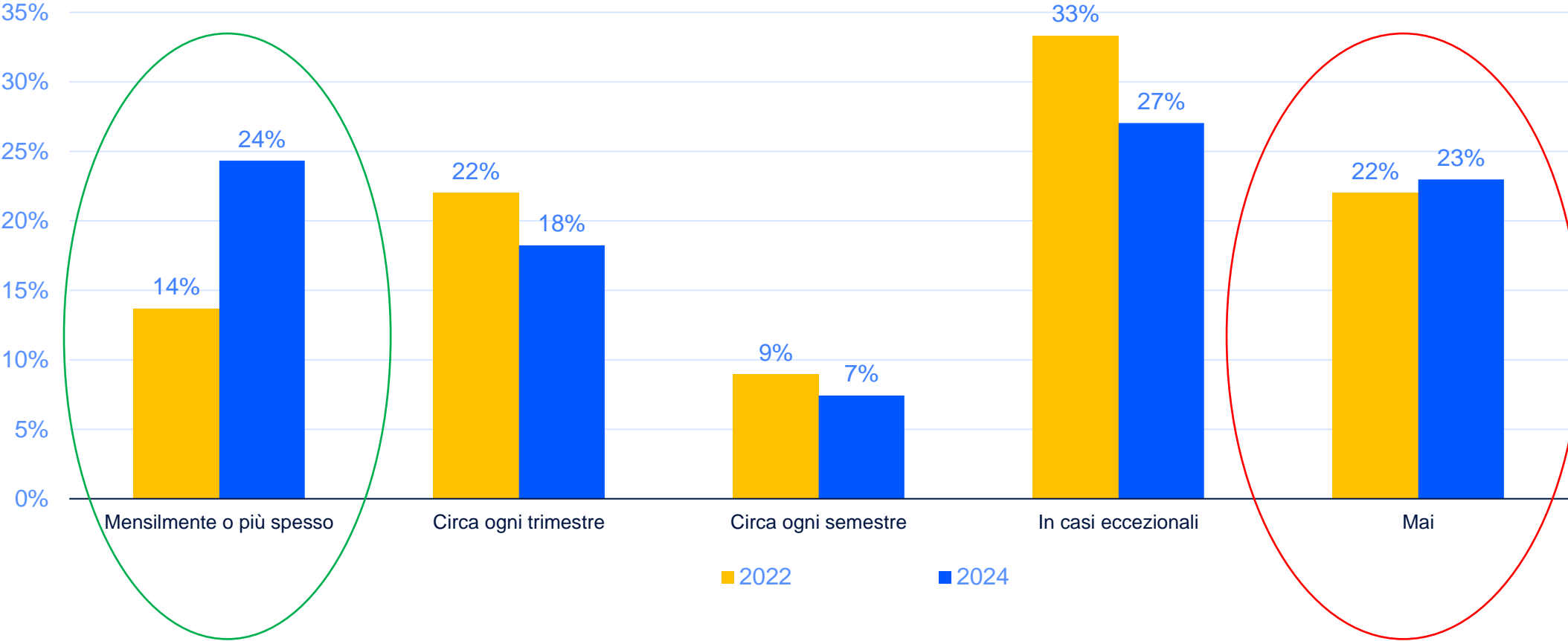
**Il Board / il top management della Sua azienda ha una conoscenza adeguata dell'ICT Security, è in grado di valutarne rischi e contromisure? (2024 vs 2022)**



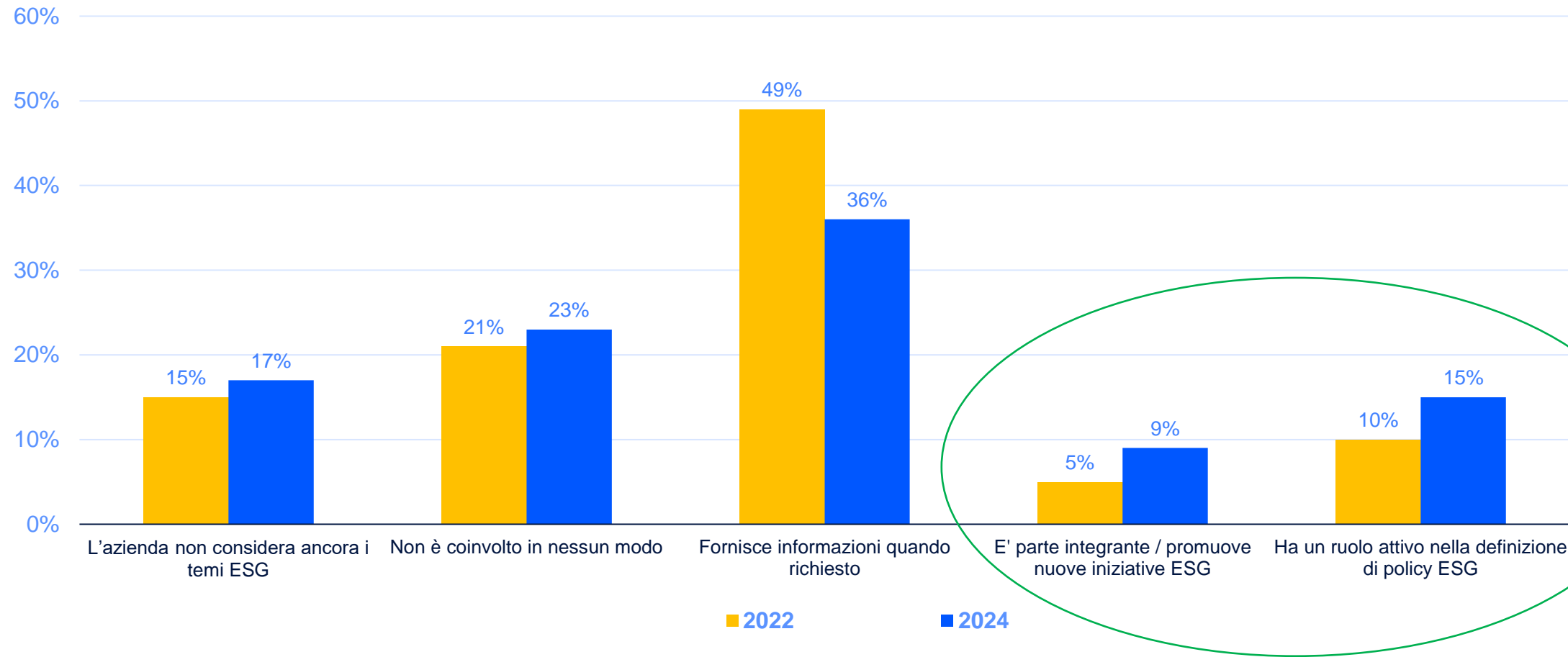
# AUMENTANO GLI INCONTRI TRA IL CISO E I VERTICI AZIENDALI



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



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



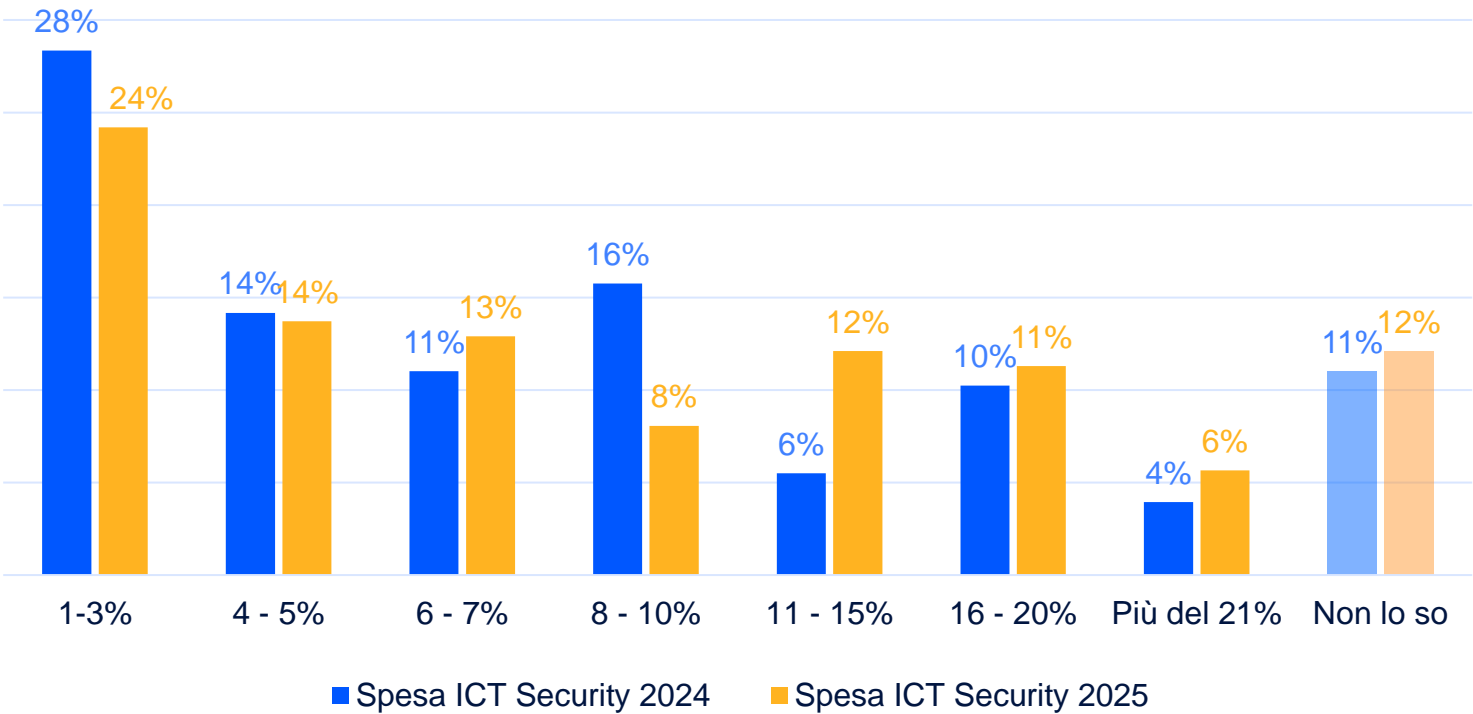


# QUANTO CRESCONO IN MEDIA GLI INVESTIMENTI IN CYBERSECURITY?

# 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



Qual è la percentuale di spesa per l'ICT security rispetto a tutto il budget ICT nel 2024? E nel 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%

# QUALI SONO I PRINCIPALI FRENI AGLI INVESTIMENTI IN CYBERSECURITY?



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



**Siamo The Innovation Group.**

Progettiamo, raccontiamo e governiamo il cambiamento.

---



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

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

---