

CYBER RISK MANAGEMENT SURVEY 2025

CYBERSECURITY SUMMIT 2025 MILANO

**SESSIONE PLENARIA 4 – IL FUTURO È OGGI:
PREPARARSI AD AFFRONTARE I NUOVI RISCHI DEL
DIGITALE, DEI SOCIAL, DELL'AI, DELLA GEOPOLITICA,
DEL QUANTUM COMPUTING**

ELENA VACIAGO, RESEARCH MANAGER, TIG – THE INNOVATION GROUP

MILANO, 20 MARZO 2025

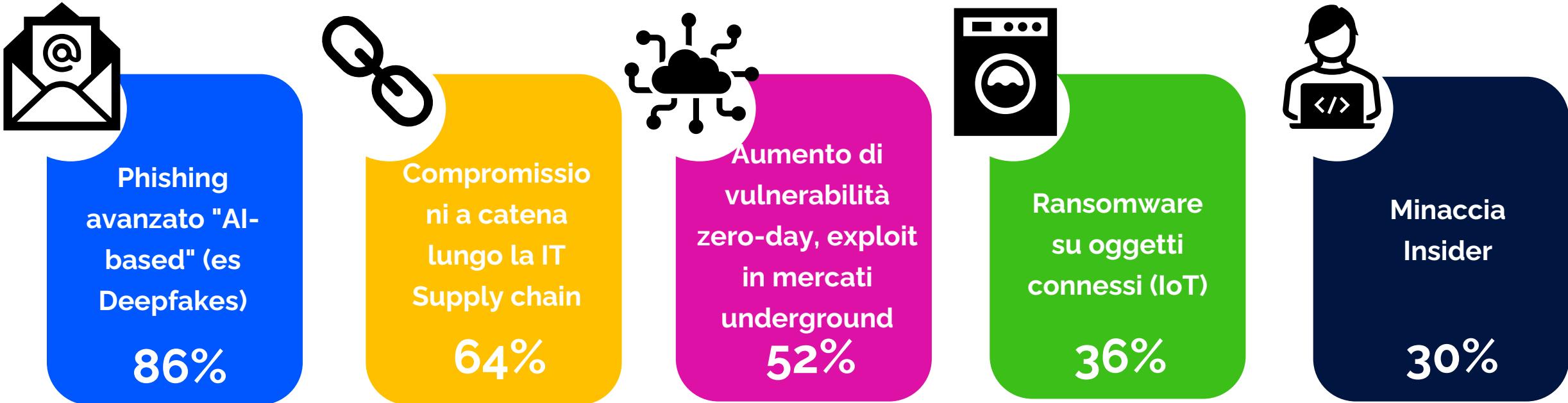


COME LE AZIENDE SI STANNO PREPARANDO AD AFFRONTARE I NUOVI RISCHI ?

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



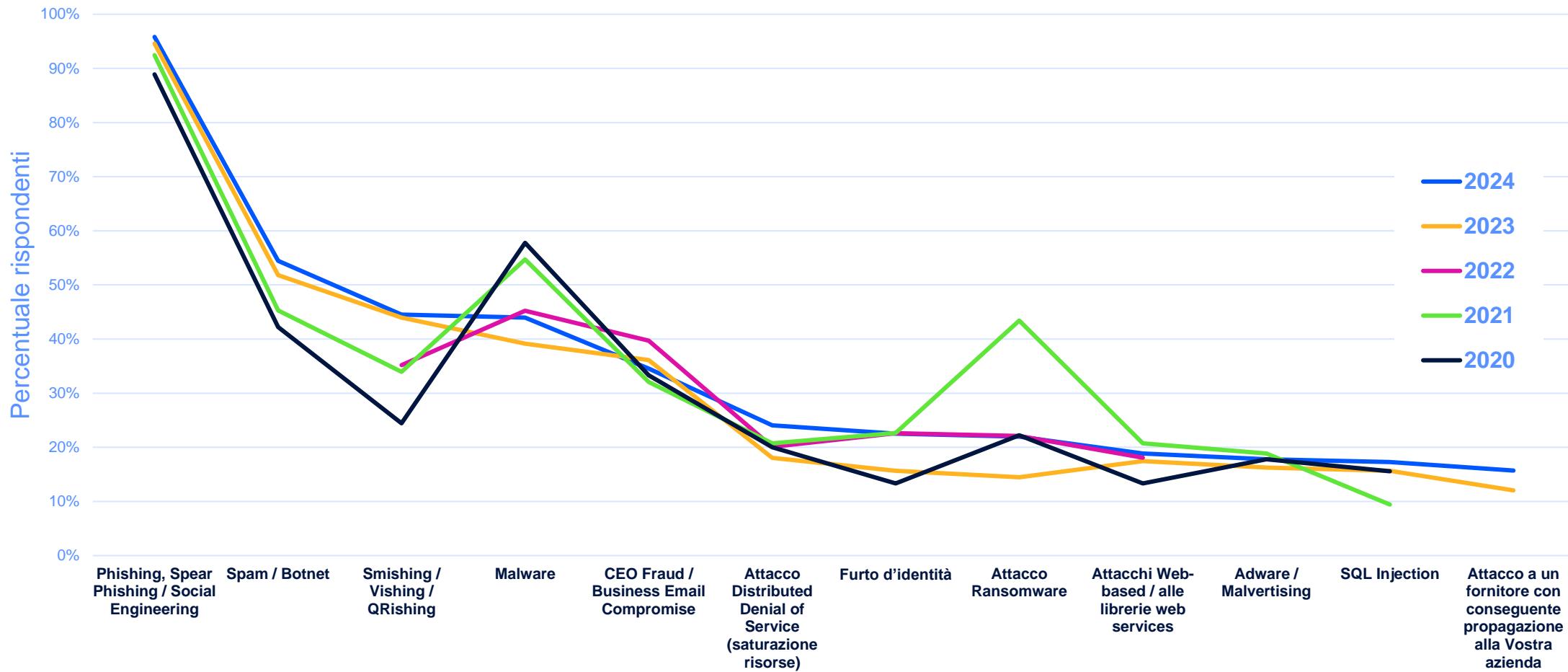
Con riferimento ai rischi futuri di cybersecurity, quali sono le minacce da monitorare già oggi?



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 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

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

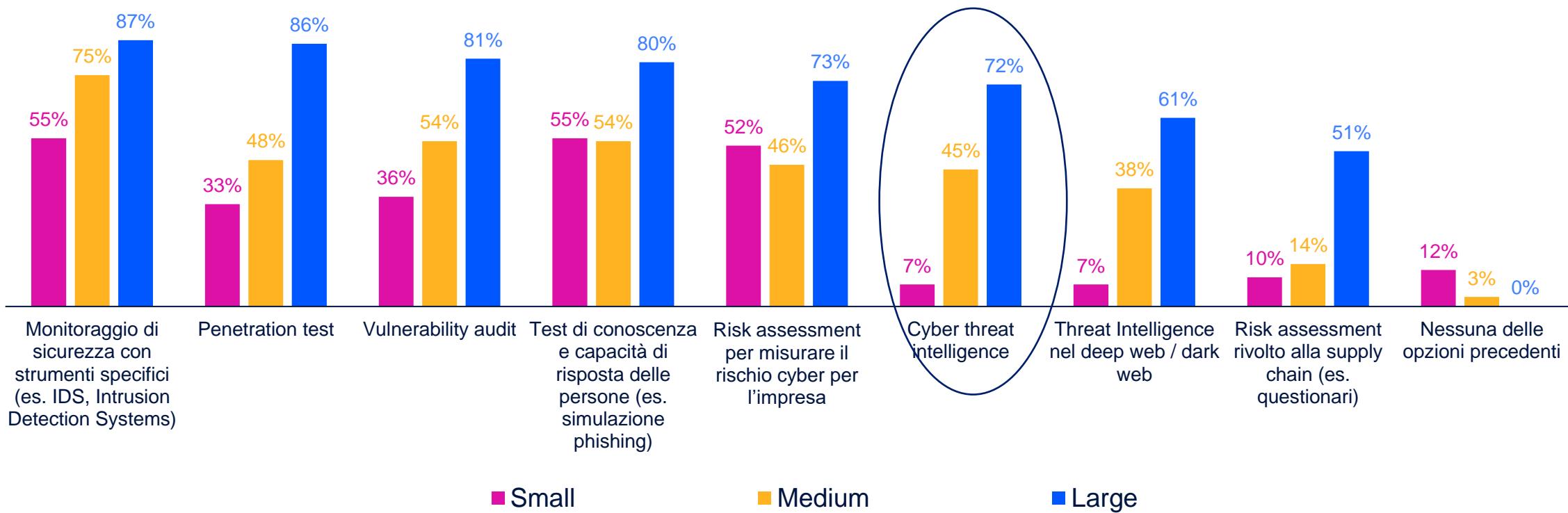
29%

Supply chain risk analysis (es. questionari)

GRANDI ORGANIZZAZIONI PIÙ AVANZATE SUL FRONTE DELL'IDENTIFICAZIONE E COMPRENSIONE DEI RISCHI, IN PARTICOLARE NELL'ADOZIONE DI THREAT INTELLIGENCE



Identificazione dei rischi, per dimensione di impresa



COME 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 mitigare i rischi avete adottato o prevedete di adottare in azienda?



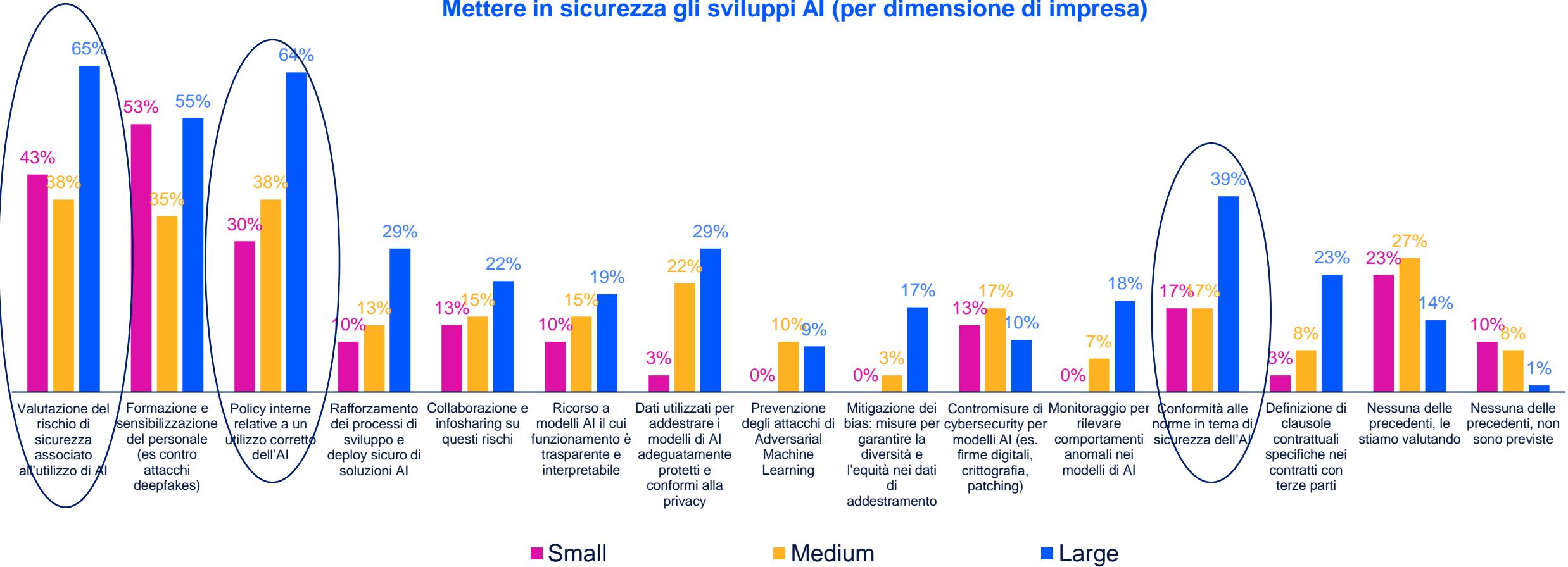
FONTE: CYBER RISK MANAGEMENT 2025 SURVEY, GENNAIO 2025

ALTRI: 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%)

LE GRANDI ORGANIZZAZIONI SONO PIÙ AVANZATE NEL PERCORSO DI MESSA IN SICUREZZA DEGLI SVILUPPI AI



Mettere in sicurezza gli sviluppi AI (per dimensione di impresa)



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