CIONET

# COHESITY SURVEY

## SICUREZZA INFORMATICA E CYBER RESILIENCE:
## ANALISI DELLE SFIDE, DELLE PRATICHE E DELLE OPPORTUNITA'

AI-powered data security and management

COHESITY

## OVERVIEW

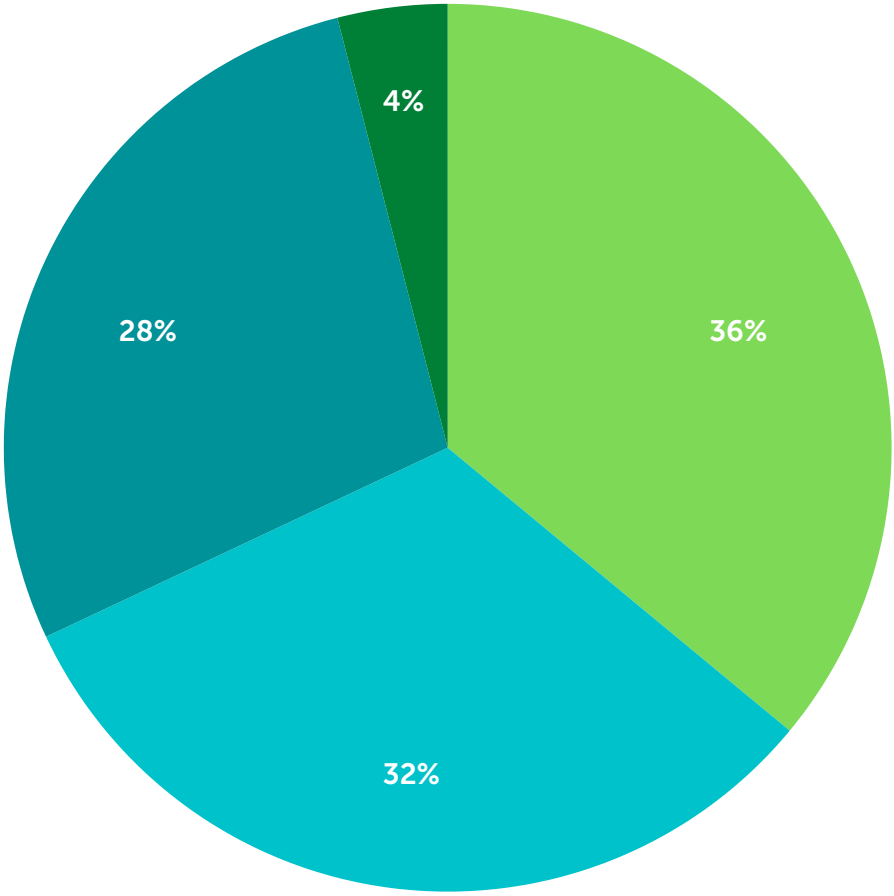
La Survey Sicurezza Informatica e Cyber Resilience: Analisi delle sfide, delle pratiche e delle opportunità è stata lanciata il 28 maggio 2024 ed è stata chiusa il 20 giugno 2024 con un numero di risposte pari a 75.

## PANEL

I rispondenti alla Survey sono Decision Maker dell'area IT e Security della propria organizzazione (CIO, ICT Manager, CTO, CIDO, CSO, CISO, Head of security, Risk, Business Continuity Director, ). Di seguito sono rappresentante le industry delle realtà rispondenti alla Survey.

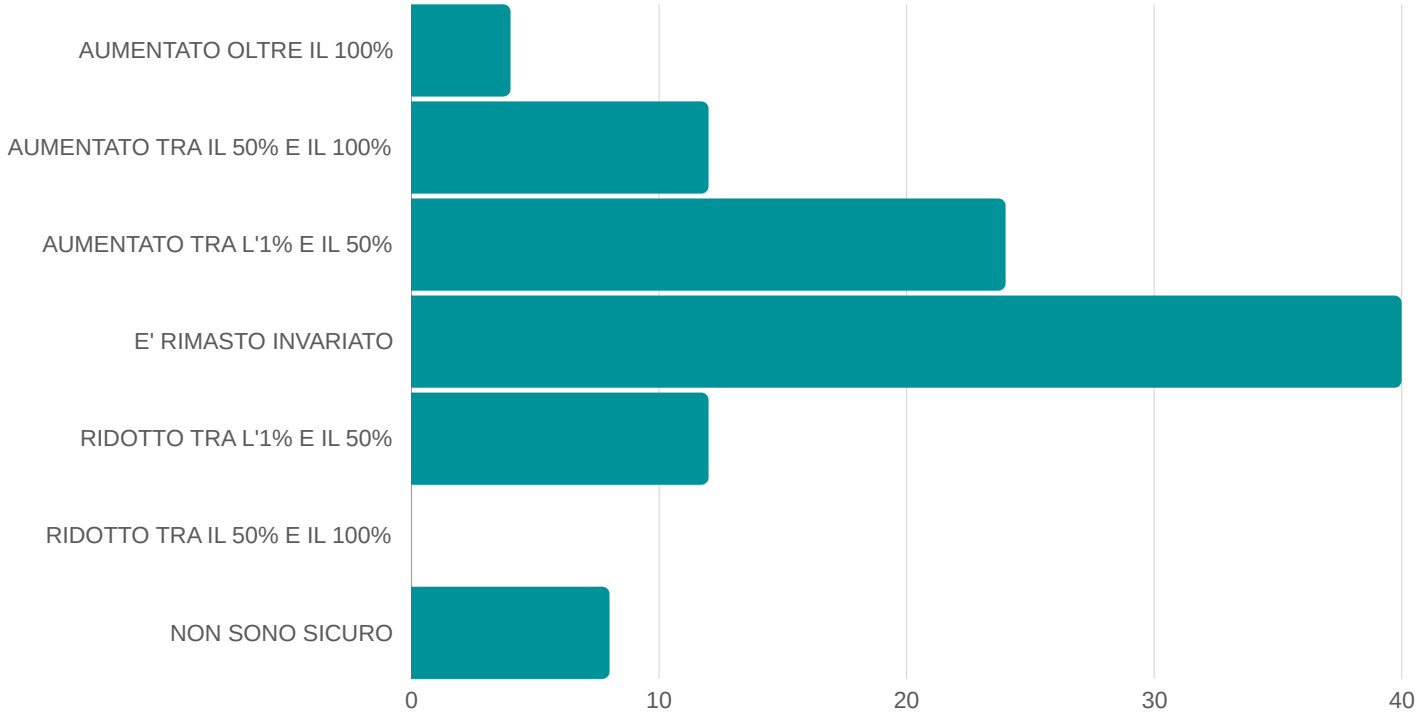
- 29% MANUFACTURING
- 18% FSI
- 12% UTILITIES
- 10% TRANSPORTATION & LOGISTICS
- 9%. PA
- 7% GDO
- 6% WHOLESALE & RETAIL
- 4% HEALTHCARE & PHARMA

## D1. Ritenete che la vostra azienda disponga di una strategia di cyber resilience concepita per affrontare le sfide e le minacce informatiche odierne?

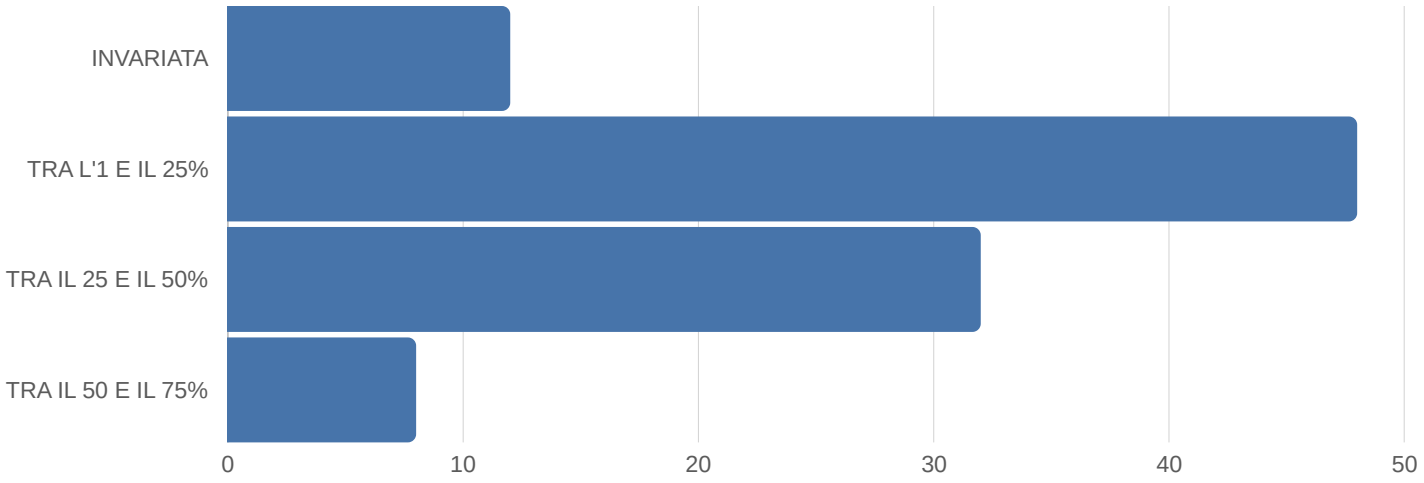



- MI SENTO PERLOPIÙ FIDUCIOSO NELLA NOSTRA STRATEGIA DI CYBER RESILIENCE
- HO PIENA FIDUCIA NELLA NOSTRA STRATEGIA DI CYBER RESILIENCE
- ABBIAMO UNA STRATEGIA DI CYBER RESILIENCE MA POTREBBE ESSERE MIGLIORATA
- TEMO CHE LA NOSTRA STRATEGIA DI CYBER RESILIENCE PRESENTI DELLE LACUNE

## D2. Il rischio di sicurezza dei dati della vostra organizzazione è aumentato o diminuito rispetto alla crescita del patrimonio di dati?



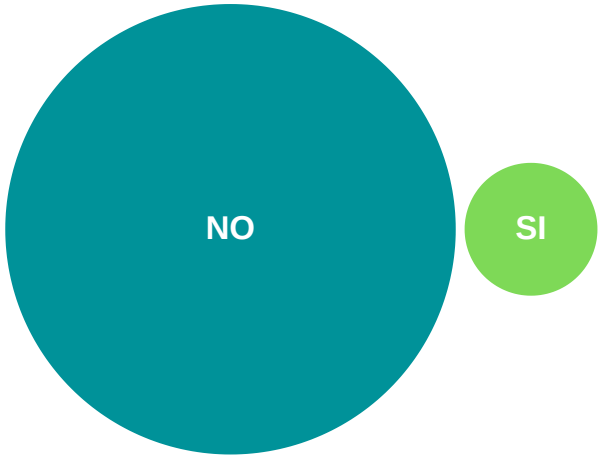

## D3. Riflettendo sul panorama delle minacce informatiche e della sicurezza dei dati nel 2024 rispetto al 2023, ritiene che la minaccia di attacchi informatici al suo settore aumenterà nel 2025?



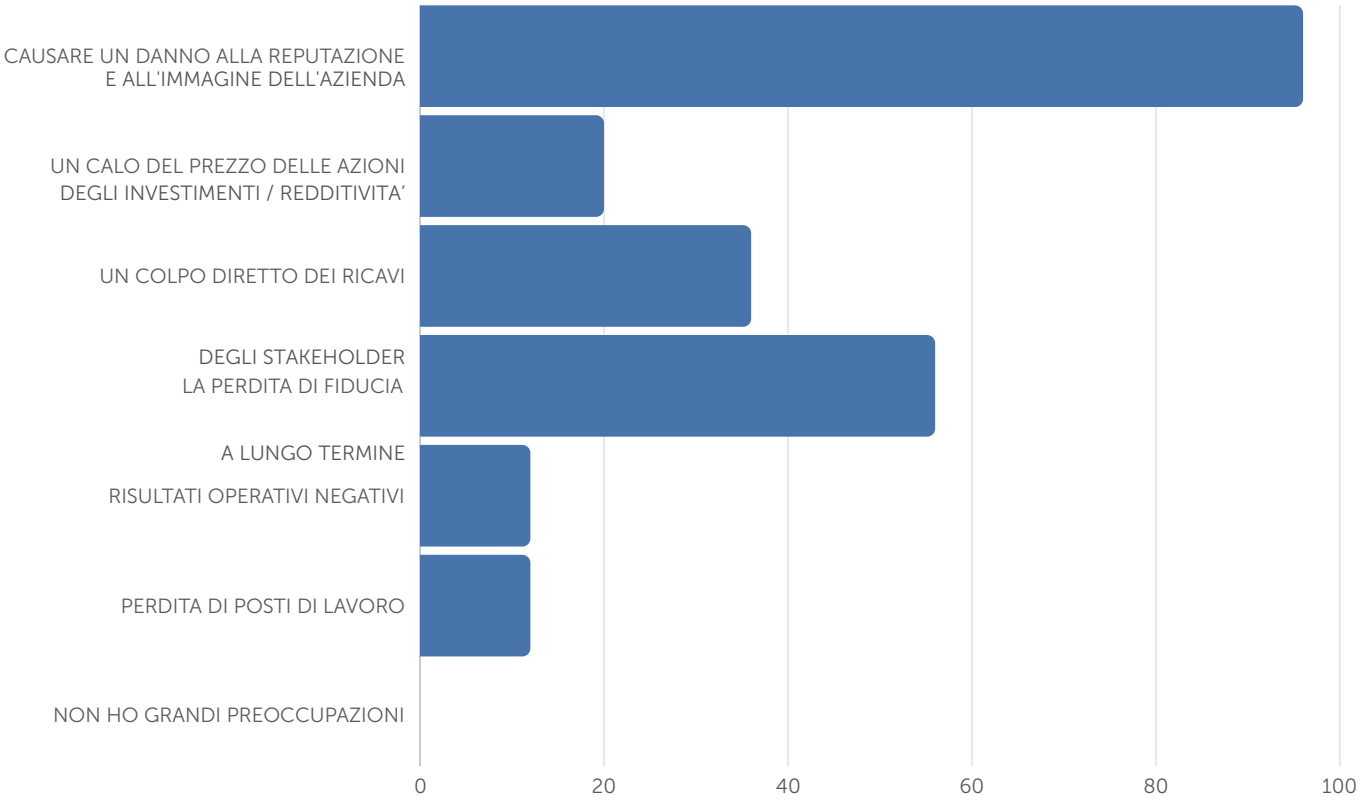
## D4. La vostra organizzazione è stata vittima di un attacco ransomware negli ultimi 6 mesi?

8% SI

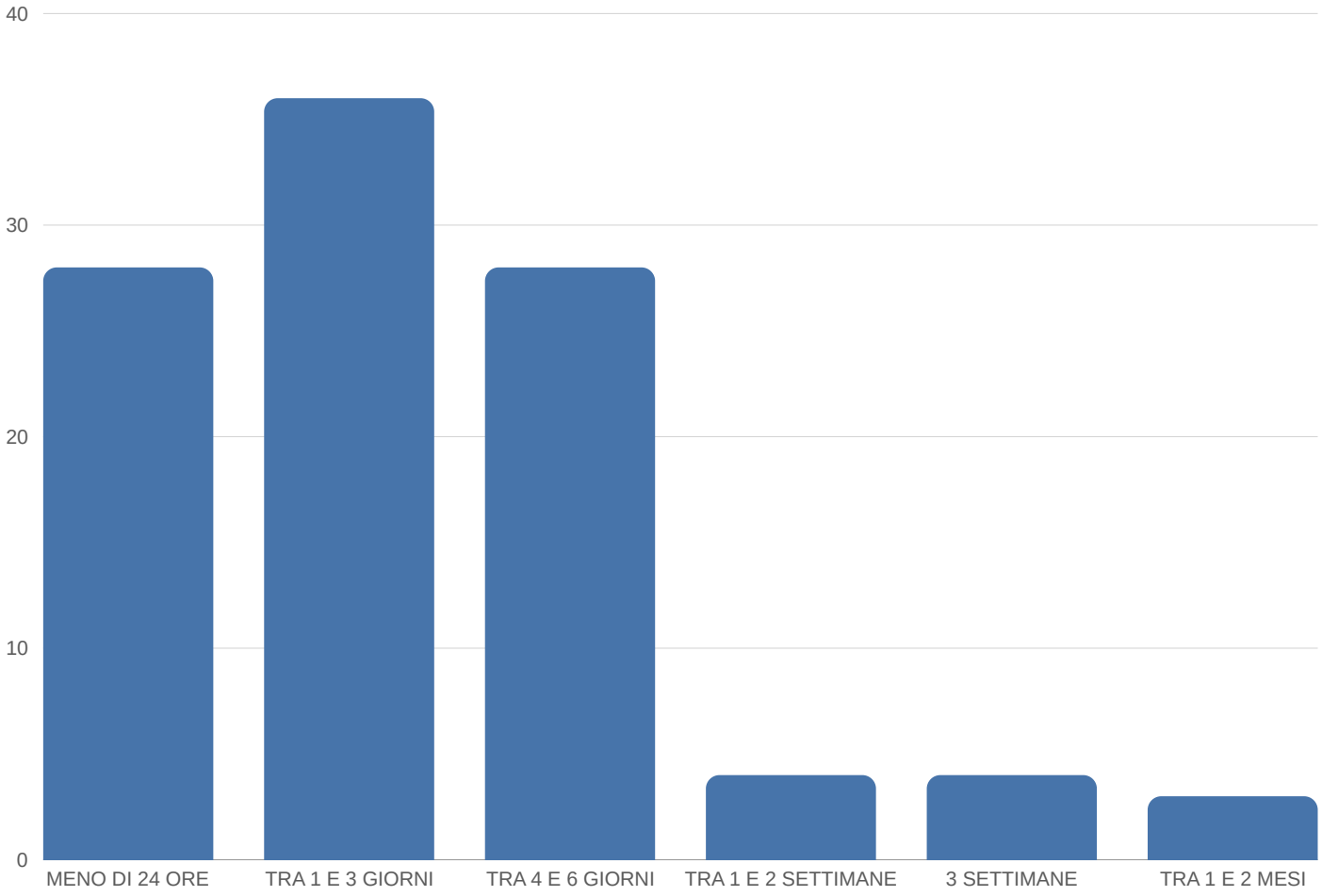
92% NO




## D5. Quali sono, eventualmente, le sue maggiori preoccupazioni in caso di violazione dei dati o di attacco informatico? (Risposta multipla)

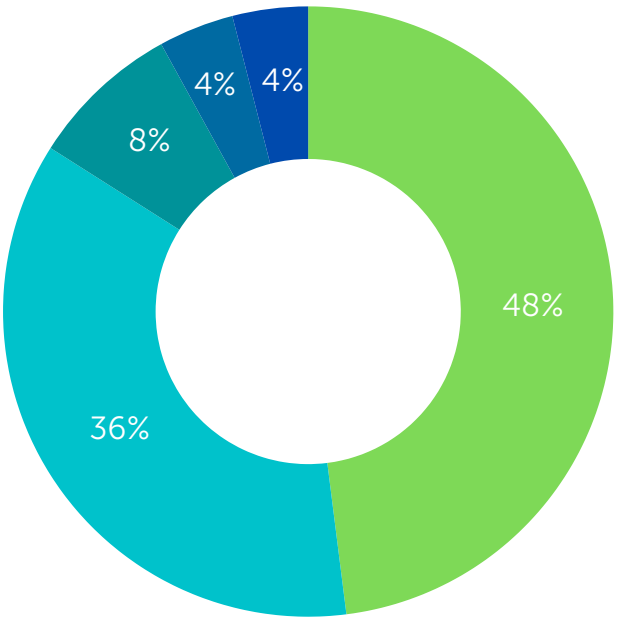


## D6. Quanto tempo impiegherebbe in media la sua azienda per ripristinare i dati e i processi aziendali in caso di attacco informatico?



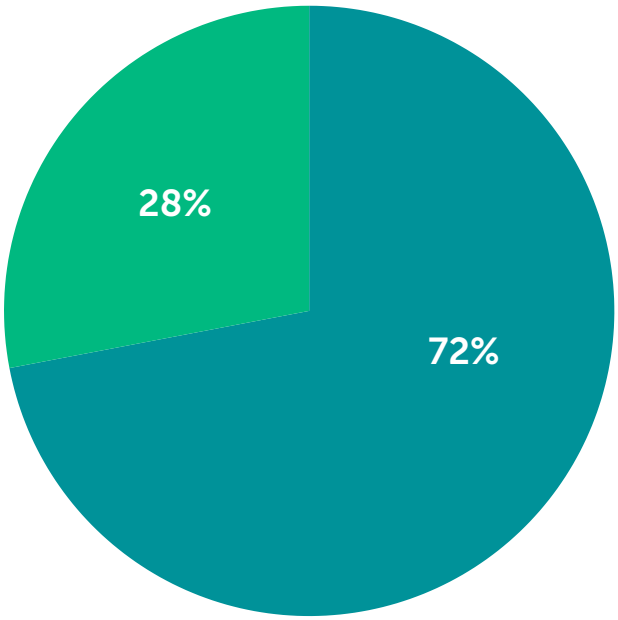

*Nessuno dei rispondenti ha indicato che il tempo necessario è oltre i 2 mesi o che non sarebbero in grado di ripristinare i dati e i processi aziendali se si verificasse un attacco informatico.

**D7. Avete sottoposto a stress test i vostri processi o soluzioni di sicurezza, gestione e ripristino dei dati negli ultimi due anni?**



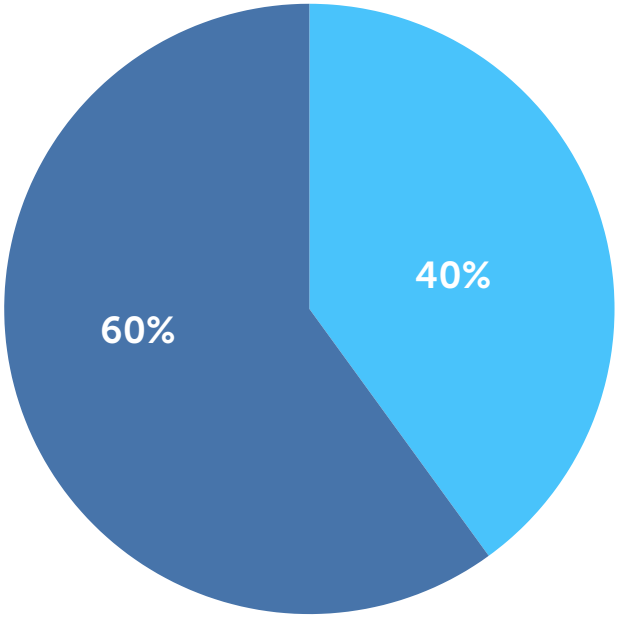

| | |
|---|---|
| 48% | SI, ABBIAMO TESTATO QUESTI PROCESSI E SOLUZIONI NEGLI ULTIMI 0-6 MESI |
| 36% | SI, ABBIAMO TESTATO QUESTI PROCESSI E SOLUZIONI NEGLI ULTIMI 7-12 MESI |
| 8% | SI, ABBIAMO TESTATO QUESTI PROCESSI E SOLUZIONI NEGLI ULTIMI 13-18 MESI |
| 4% | NO, SONO PASSATI PIÙ DI DUE ANNI DALL'ULTIMA VOLTA CHE ABBIAMO TESTATO QUESTI PROCESSI E SOLUZIONI |
| 4% | NO, NON ABBIAMO ANCORA ESEGUITO UNA SIMULAZIONE O UNO STRESS TEST DI QUESTI PROCESSI E SOLUZIONI |

**D8. Pensate che la vostra organizzazione pagherebbe un riscatto se questo significasse recuperare i vostri dati e processi aziendali (o farlo più velocemente), specialmente se è necessario un ripristino completo?**




| | |
|---|---|
| 72% | NO |
| 28% | FORSE, DIPENDE DALL'ENTITA' DEL RISCATTO |

D9. La vostra organizzazione ha una politica o un protocollo definito per non pagare riscatti?



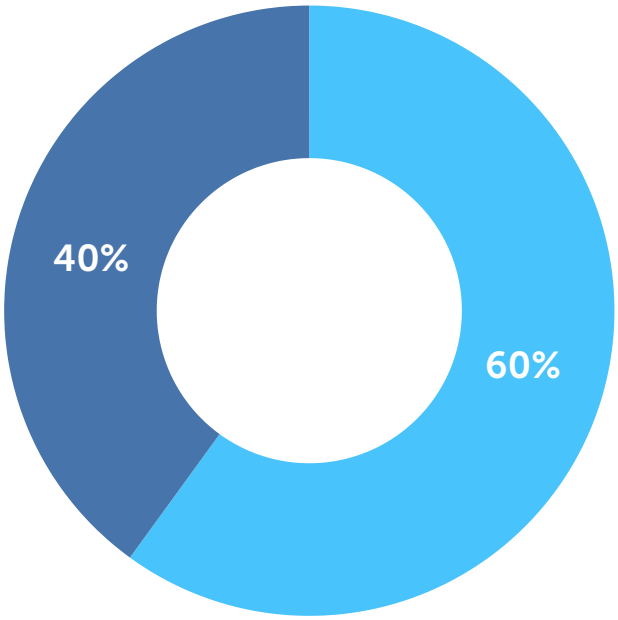

40% SI

60% NO

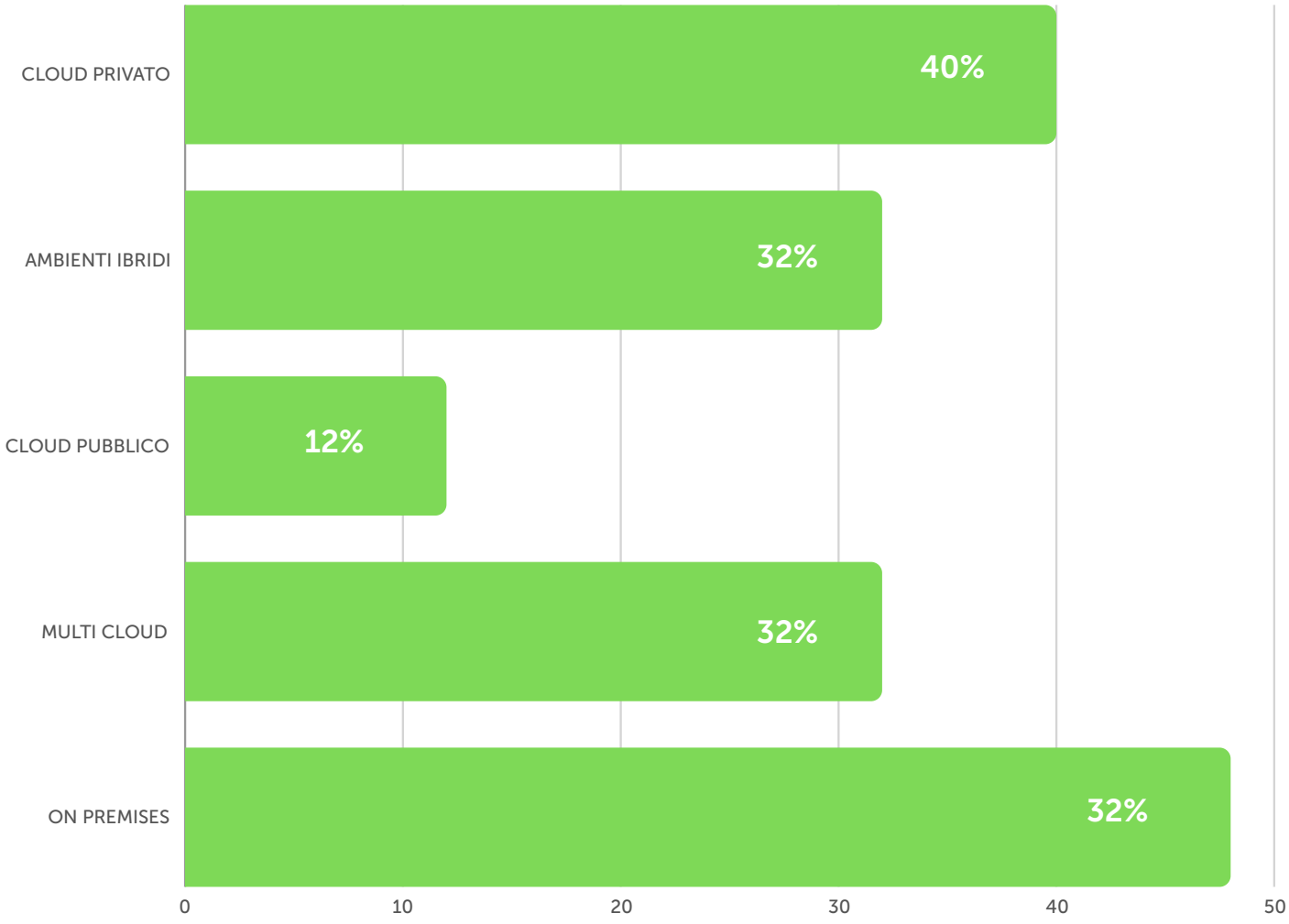
D10. Avete un'assicurazione informatica per coprire i costi di incidenti informatici come i pagamenti di ransomware?

60% SI

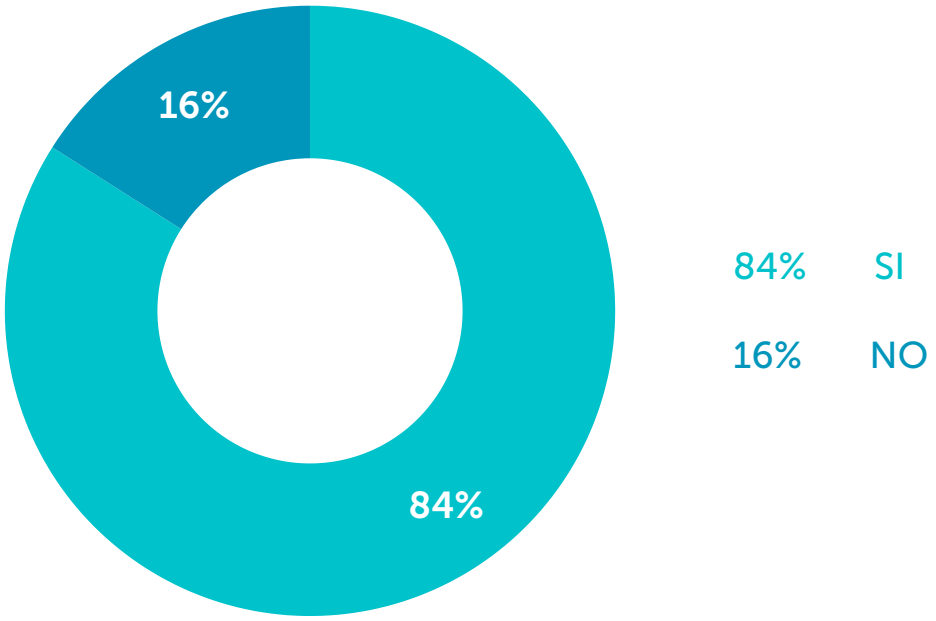
40% NO



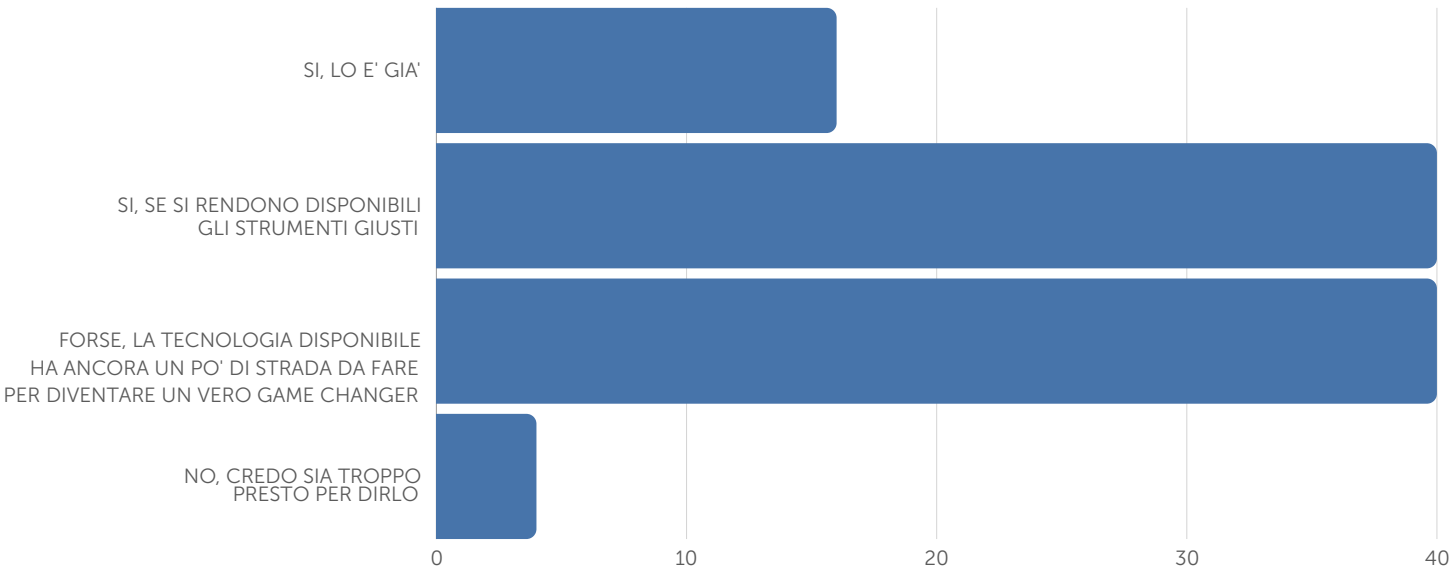
**D11. Dove sono conservati i dati della vostra organizzazione?**
E' possibile selezionare più di una risposta.



**D12. Ritiene che la tecnologia basata sull'AI, o quella che sfrutta l'AI, aiuti o aiuterà i team IT e di sicurezza a lavorare insieme in modo più efficace?**

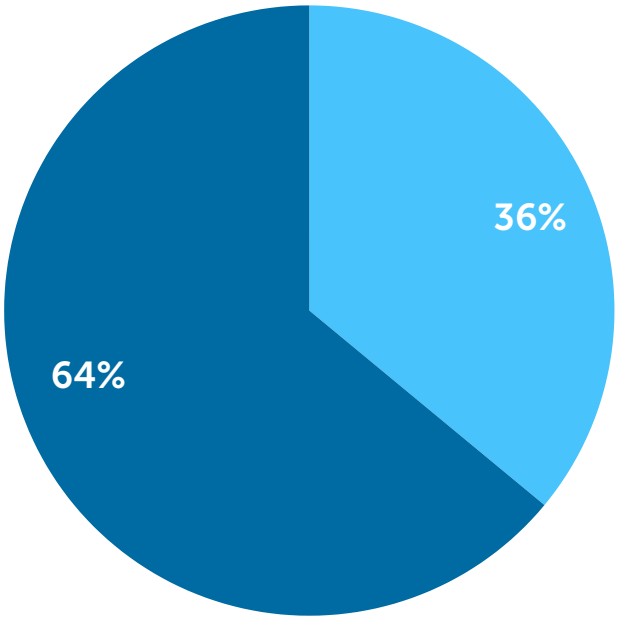



**D13. Ritenete che l'AI generativa e/o la tecnologia alimentata dall'AI (tecnologia che sfrutta l'AI) avranno un impatto sostanziale sui vostri processi e sull'efficacia dell'IT o della sicurezza nei prossimi 12-24 mesi?**




*Nessuno dei rispondenti ha indicato di disporre già di processi e strumenti efficaci.

D14. Attualmente utilizzate tecnologie basate sull'intelligenza artificiale per l'analisi dei dati o per la comprensione della vostra infrastruttura tecnologica?



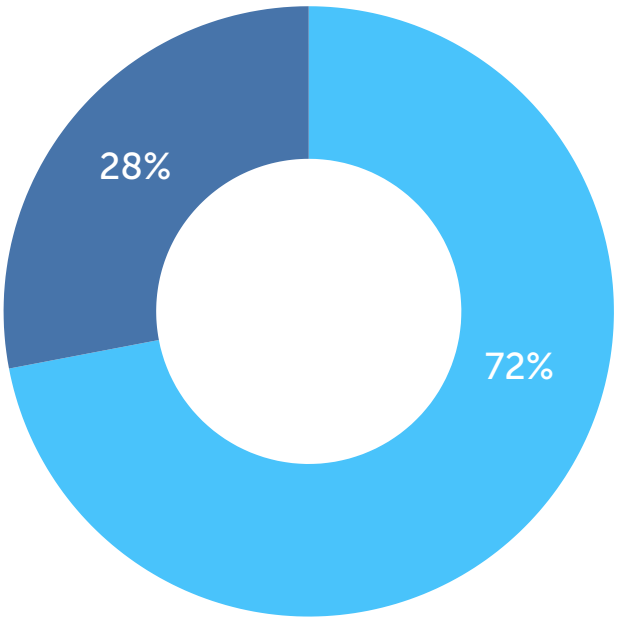

36% SI

64% NO

D15. Avete implementato e utilizzato tecnologie basate sull'intelligenza artificiale nella vostra infrastruttura di backup, gestione, protezione, sicurezza o ripristino dei dati?

72% SI

28% NO



CIONET

SI RINGRAZIANO TUTTE LE REALTÀ CHE HANNO PARTECIPATO ALLA SURVEY SICUREZZA INFORMATICA E CYBER RESILIENCE: ANALISI DELLE SFIDE, DELLE PRATICHE E DELLE OPPORTUNITÀ TRA CUI: ACEA, ACI INFORMATICA, ALLIANZ SPA, ANGELINI INDUSTRIES, ARCELORMITTAL, ARGOTRACTORS, ARIA SPA, BANCA MEDIOLANUM, BARILLA, BOLTON GROUP, BREMBO, CELLULARLINE GROUP, CERBA HEALTHCARE, CNH INDUSTRIAL, CNP VITA ASSICURA, CONAD, CORTE DEI CONTI, CREDEM, EDISON, ENEL, ESSILOR LUXOTTICA, FCA GROUP, FERRERO,FIDEURAM, FSTECHNOLOGY, GRUPPO HERA, INTERCOS. IVECO, LEONARDO, MAX MARA FASHION GROUP, MEDIASET, MENARINI, PIRELLI, PRYSMIAN, POSTE ITALIANE, PUBLIACQUA SPA, RAI, ROMAGNA ACQUE, SAIPEM, SECADVANCE SRLS, SKY, SNAM, WFP, YOOX NET-A-PORTER GROUP.