

The Deloitte logo is positioned in the top left corner. It consists of the word "Deloitte" in a white, bold, sans-serif font, followed by a small green dot. The background of the entire slide is a dark green gradient with several large, overlapping, semi-transparent green circles of varying sizes, creating a sense of depth and movement.

**Deloitte.**

# Future of Cyber Survey 2025

La cybersecurity come chiave per la creazione del  
valore aziendale, nel percepito delle imprese italiane

# Contenuti

- 4 La cybersecurity come chiave per presidiare il valore di business dell'impresa
- 13 L'evoluzione e l'importanza crescente del ruolo CISO
- 16 Accelerare la trasformazione digitale dell'impresa grazie alla cybersecurity
- 24 Nota Metodologica
- 25 Contatti

## Executive Summary

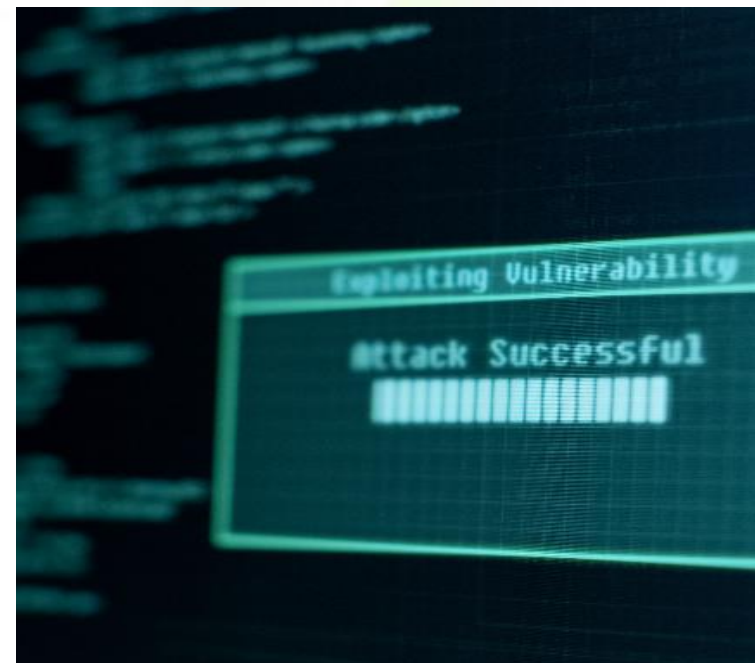
Nel contesto di mercato odierno, la cybersecurity è diventata un **elemento imprescindibile per il valore di business** delle organizzazioni, influenzando sia i **risultati** che i potenziali **costi** aziendali. Lo scenario globale, sempre più digitalizzato, ma anche più complesso e caratterizzato da repentini cambiamenti, rende la cybersecurity un fattore essenziale per la difesa delle infrastrutture digitali. La cybersecurity può fungere da **fattore abilitante per la digitalizzazione** delle imprese e delle istituzioni, oltre che **strategico** per garantire la competitività aziendale, ove la **protezione dei dati critici** e il mantenimento della **reputazione e fiducia dei clienti** rivestono un ruolo cruciale, con impatti diretti sul successo delle imprese.

Per esplorare e valorizzare il percepito delle aziende leader di mercato, la **Global Future of Cyber Survey** di Deloitte, giunta alla sua quarta edizione, ha raccolto le opinioni di ruoli apicali e opinion maker circa le sfide e le opportunità connesse all'evoluzione della cybersecurity. Tra le principali evidenze che emergono dallo studio, la cybersecurity risulta anzitutto **sempre più integrata nelle discussioni del Board aziendale**, acquisendo una maggiore **valenza strategica**. Inoltre, **le imprese stanno incrementando i loro investimenti** in quest'ambito non solo per una questione di conformità normativa, ma anche come misura proattiva al fine di prevenire costi significativi e possibili danni reputazionali.

Un altro aspetto da sottolineare è poi l'importanza crescente del **Chief Information Security Officer (CISO)**, con un aumento significativo in termini di coinvolgimento nelle discussioni strategiche ai vertici delle organizzazioni, soprattutto per quanto riguarda la **valutazione, analisi e comprensione delle capacità e competenze tecnologiche** dell'organizzazione.

Infine, ma non meno importante, la survey evidenzia il legame sempre più stretto fra cybersecurity e **trasformazione digitale** che, se adeguatamente gestito e valorizzato, può fungere da acceleratore in termini di **innovazione e capacità di resilienza**: non a caso, più della metà dei partecipanti italiani prevede un aumento degli investimenti nel prossimo biennio. Risulta poi cruciale la necessità di sviluppare competenze e governance efficaci riguardo alle tecnologie emergenti, come ad esempio nel caso dell'**Intelligenza Artificiale Generativa (GenAI)** o – in prospettiva – delle potenzialità connesse al **quantum computing**.

In sintesi, la cybersecurity può rivelarsi in diversi settori di mercato una chiave del **successo aziendale** e un chiaro **vantaggio competitivo**, richiedendo tuttavia un **approccio olistico e trasversale** per garantire la resilienza, protezione e crescita consolidata alle organizzazioni.



La 4ª edizione della Global Future of Cyber Survey di Deloitte ha coinvolto circa **1.200 decision-maker in ambito Cyber di imprese di grandi dimensioni** (con almeno 1.000 dipendenti e un fatturato annuale di 500 milioni di dollari), distribuite in **43 Paesi a livello mondiale**. Il presente report approfondisce le evidenze raccolte dal campione di imprese italiane, per i cui dettagli si rinvia alla nota metodologica di pag. 24.

# La cybersecurity come chiave per presidiare il valore di business dell'impresa

In un mondo sempre più complesso e digitalizzato, la cybersecurity diventa un elemento cruciale per prevenire e gestire i rischi aziendali, rappresentando così un fattore chiave per il valore di business, la competitività e il successo delle imprese.

## Valore di business e competitività

La cybersecurity è sempre più un elemento essenziale per il successo e il valore aziendale, influenzando sia i risultati sia i potenziali costi per l'intera organizzazione

In un mondo sempre più digitalizzato, la cybersecurity è divenuta una variabile fondamentale nella gestione dei molteplici rischi aziendali. Come tale, essa rappresenta per diverse imprese un **elemento chiave per il successo dell'impresa**, influenzando direttamente sia sul preservare i **risultati** sia sull'evitare (o minimizzare) i potenziali **costi** derivanti da vulnerabilità o incidenti informatici. Nell'attuale contesto di mercato – sempre più volubile e soggetto a cambiamenti repentini di natura economica, sociale e tecnologica – essa non può più essere concepita come un mero strumento di difesa dei sistemi e delle infrastrutture informatiche. Al contrario, in un mondo digitale in cui le minacce informatiche sono diventate una realtà quotidiana per le aziende di ogni settore, la cybersecurity richiede di essere riconosciuta come un **fattore essenziale di competitività**, in un contesto di mercato profondamente diverso rispetto al passato.

In altre parole, la protezione dei dati sensibili, delle infrastrutture IT, dell'operatività e della continuità aziendale non è più solo una questione tecnica, bensì una componente determinante per il successo o il fallimento di un'impresa.

Di conseguenza, la cybersecurity può svolgere una **funzione strategica** che guida ed influenza il **raggiungimento degli obiettivi di business**, coinvolgendo tutte le aree aziendali in modo trasversale. Pertanto, oggi le imprese sono chiamate a riflettere e comprendere a fondo come gli **investimenti in cybersecurity** possano **ottimizzare, preservare e generare valore** per l'intera organizzazione. Si tratta di predisporre una solida base per la **crescita futura** attraverso l'adozione di **best practice e strategie** orientate non solo alla sicurezza dei dati, ma anche al **mantenimento dell'integrità tecnologica** delle infrastrutture e dei processi aziendali. La cybersecurity non è dunque solo una necessità, ma può anche rappresentare un chiaro **vantaggio competitivo**.

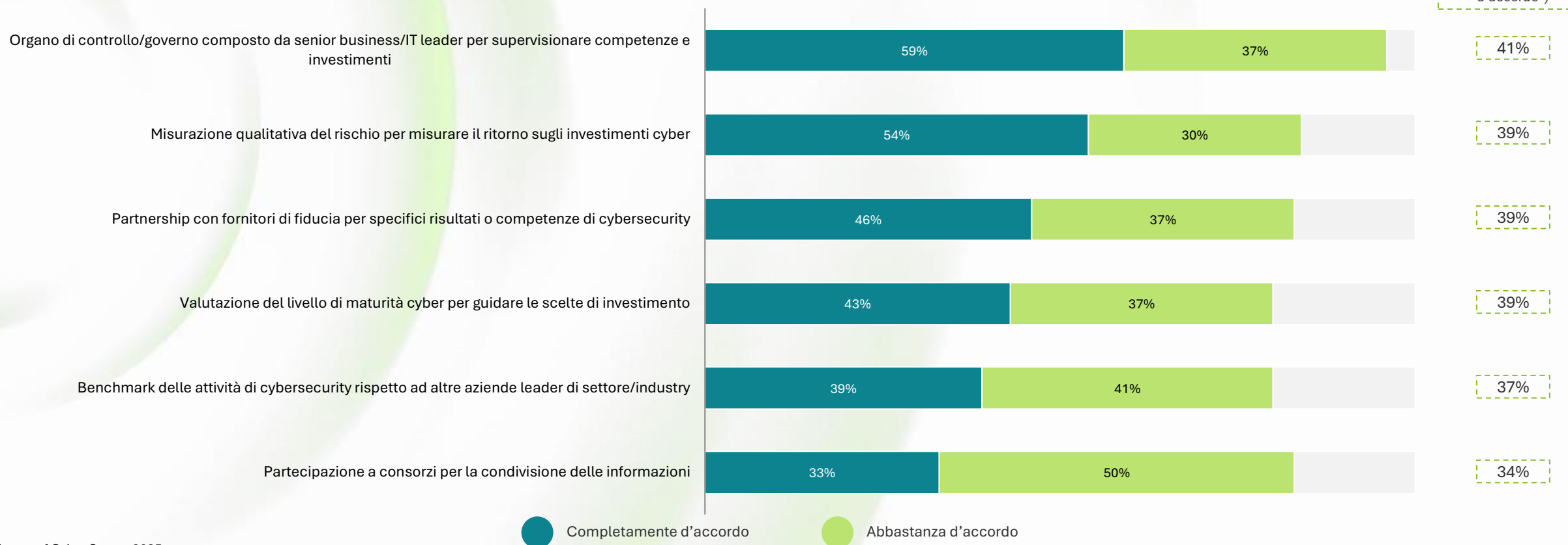


## Le strategie di cybersecurity attuate dalle aziende

Tra le evidenze della quarta edizione della survey – che Deloitte conduce annualmente a livello globale per valorizzare il percepito e il sentiment delle imprese leader di mercato – emerge anzitutto come **più di un'azienda su tre in Italia** sta attuando diverse **azioni strategiche** per rafforzare il proprio livello di cybersecurity. In primo luogo, 6 intervistati su 10 (59%) dichiarano di avere pienamente attivato uno **specifico organo di governance** (costituito da senior IT

e business leader) con l'obiettivo di supervisionare costantemente gli investimenti e le proprie competenze in ambito cyber. Circa un'impresa su due utilizza poi strumenti qualitativi (54%) per **misurare i ritorni degli investimenti** ed ha attivato **partnership con fornitori di fiducia** (46%). Circa 4 imprese su 10, inoltre, stanno esaminando il proprio livello di maturità per **ottimizzare le scelte di investimento** (43%) o effettuano **benchmark** rispetto alle imprese leader nel proprio settore di riferimento (39%).

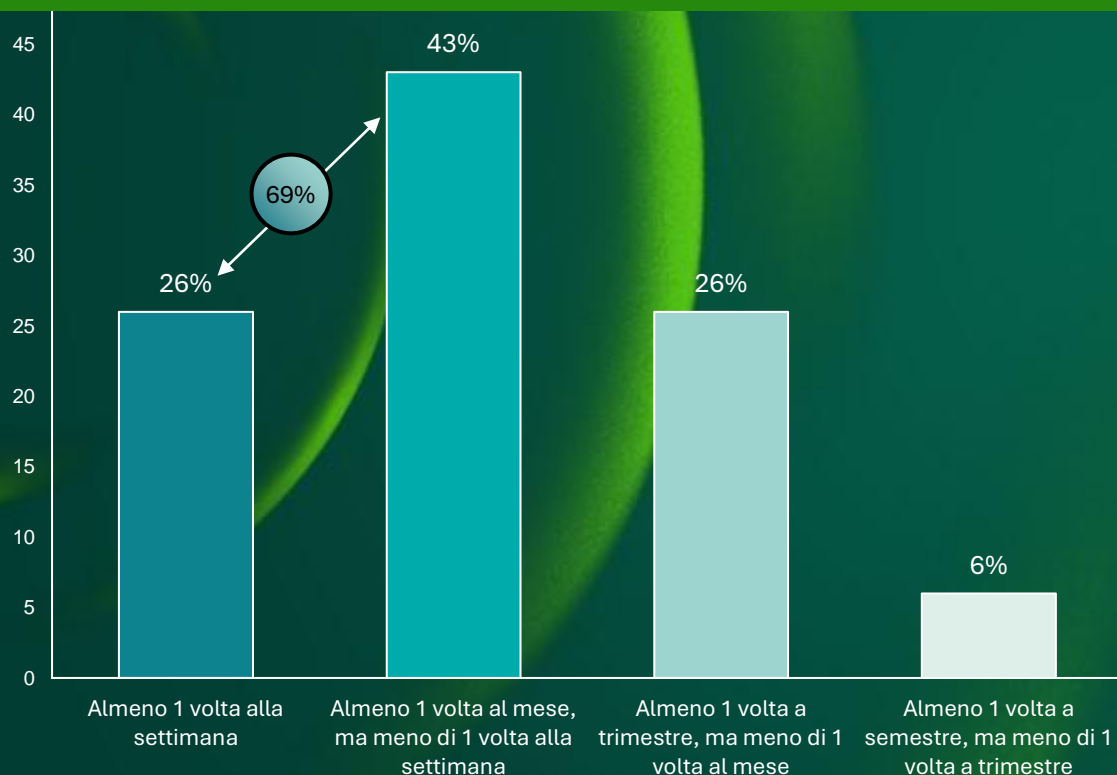
### Leve strategiche per la cybersecurity dell'organizzazione



## Focus: il coinvolgimento del Board aziendale

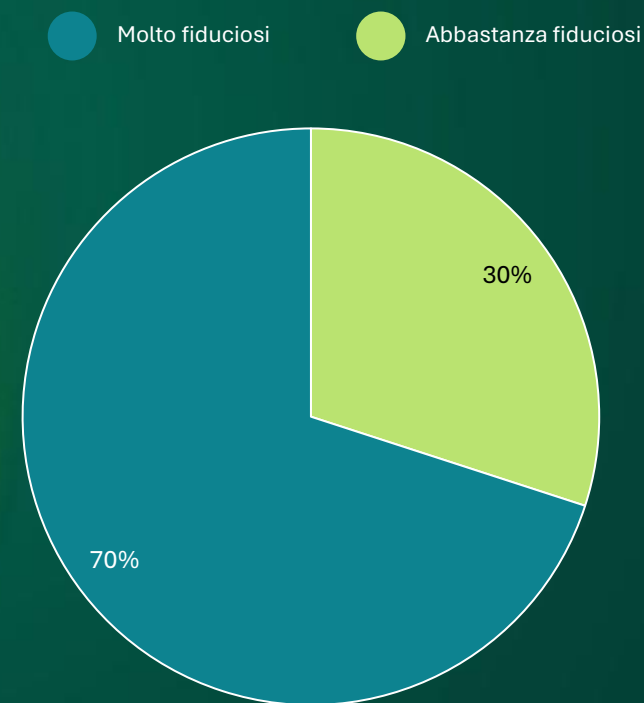
È ormai evidente che la cybersecurity non sia più percepita come una questione solamente tecnica, ma **una priorità strategica all'attenzione del Board aziendale**. Lo conferma la survey evidenziando come **il 69% delle imprese discuta di cybersecurity almeno mensilmente con il Board**, alcuni arrivando a parlarne settimanalmente (26%). Questo sarà ulteriormente accentuato con l'introduzione delle responsabilità in capo ai membri del Organi di amministrazione e direttiva, come regolamentato dalla **nuova direttiva NIS2**.

Frequenza con cui il Board aziendale discute tematiche di cybersecurity



Il **70%** dei partecipanti si dichiara **molto fiducioso** riguardo alla **preparazione del proprio Board per affrontare le sfide della cybersecurity**. Si direbbe che questa buona percezione in termini di preparazione del Board sia frutto del dialogo con i CISO instaurato negli scorsi anni e delle azioni di sensibilizzazione e formazione sulle tematiche di cybersecurity. Questi sforzi hanno infatti reso il Board capace di discutere in maniera consapevole dei rischi di cybersecurity che l'organizzazione si trova ad affrontare.

Fiducia nel grado di preparazione del Board su tematiche cyber

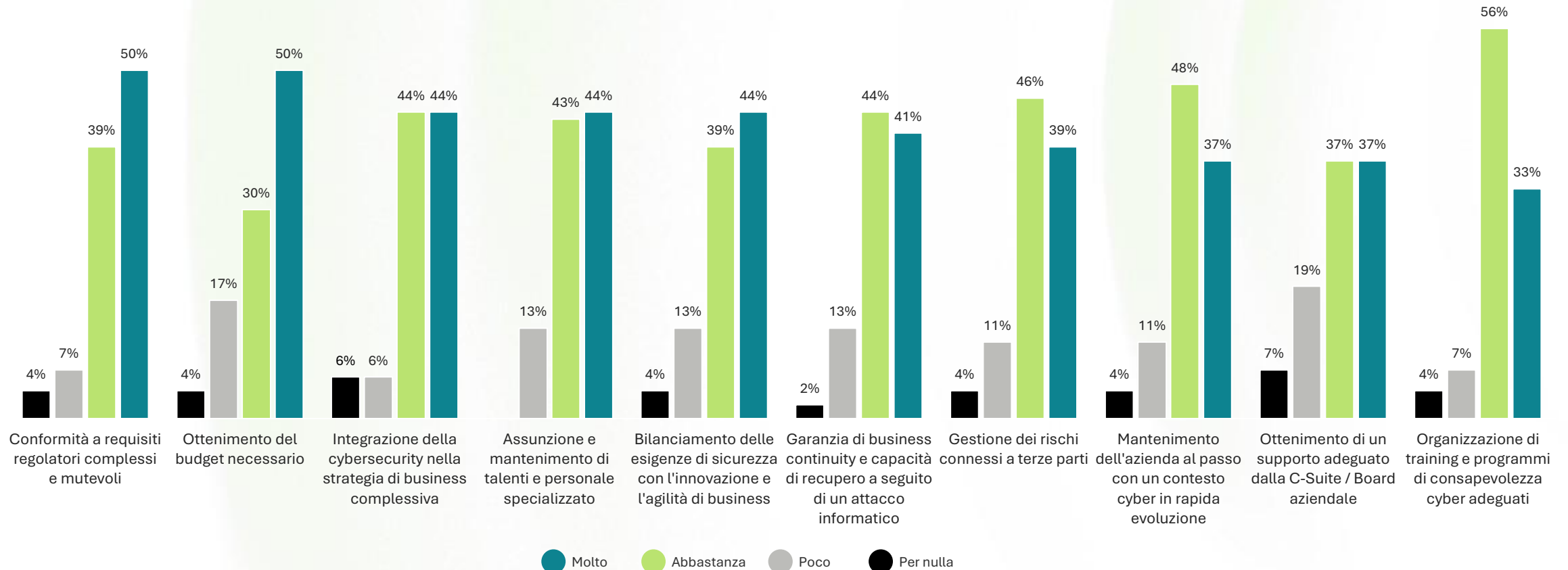


# Come le sfide possono agire da barriere all'implementazione della strategia cyber

Tuttavia, l'adozione di un'adeguata ed efficace strategia di cybersecurity richiede di superare molteplici **sfide**, le quali possono rappresentare delle vere e proprie **barriere** al raggiungimento di questo obiettivo. In Italia, nel percepito delle imprese, le criticità maggiormente diffuse (50%) risultano la necessità di adeguarsi a **requisiti normativi complessi e mutevoli** e di assicurare il **budget necessario**.

Una quota di poco inferiore (44%) richiama l'attenzione anche sulla **difficoltà di integrare la cybersecurity nella strategia di business complessiva**, nonché di assumere e mantenere i **talenti** e il **personale specializzato** e di armonizzare le esigenze di cybersecurity con quelle relative all'**agilità** e alla **capacità di innovazione** dell'impresa.

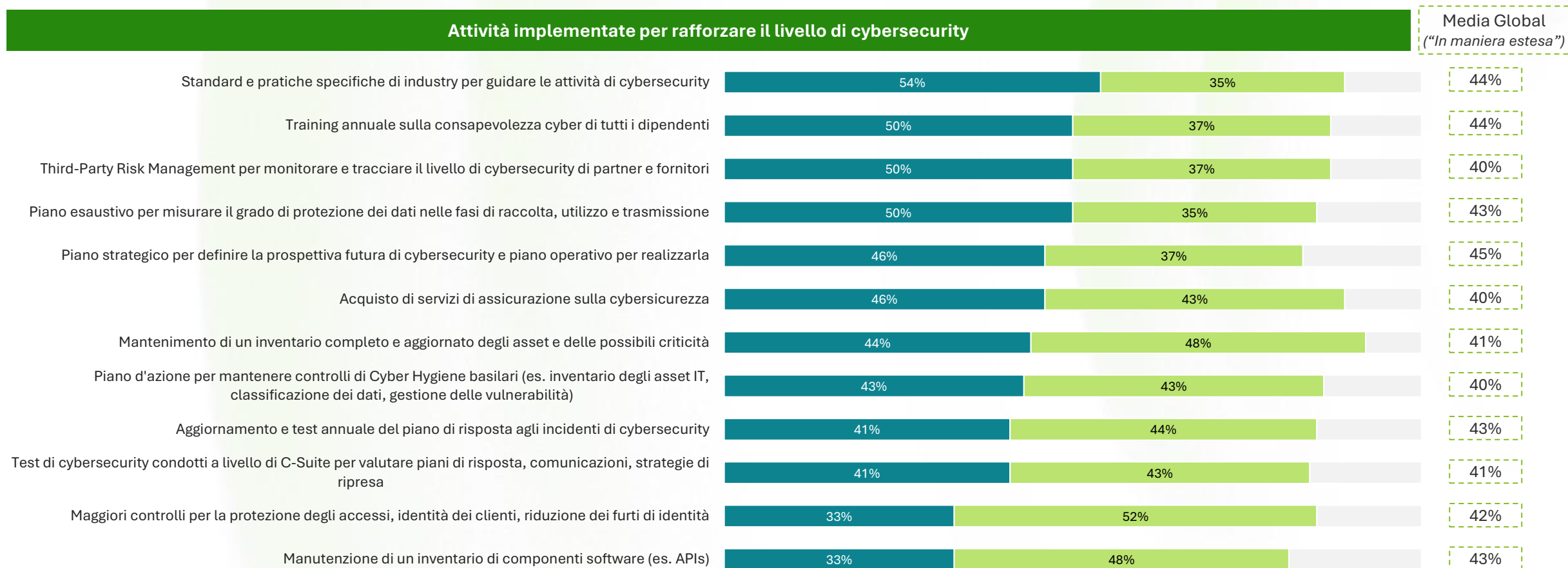
## Principali sfide nell'implementazione della strategia cyber



## Le principali attività volte a incrementare il livello di cybersecurity

Il presidio degli standard di sicurezza attuali non è sufficiente a mantenere un'adeguata competitività sul mercato anche in prospettiva futura. In uno scenario di mercato sempre più incerto e soggetto a cambiamenti repentini ed evoluzioni complesse – anche a causa delle dinamiche geopolitiche – diventa quantomai necessario **incrementare il livello di cybersecurity** dell'organizzazione, al fine di essere preparati anche alle sfide emergenti o minacce impreviste.

A questo proposito, dalle interviste raccolte emerge come più della metà delle imprese si definisca pienamente d'accordo riguardo alla necessità di **adottare specifici standard e pratiche settoriali** (54%), mentre una quota analoga (50%) fornisce attività di **formazione e training** a tutti i dipendenti, oltre a monitorare il livello di sicurezza delle **terze parti** (come partner commerciali o fornitori) e adottare un piano dettagliato per misurare la **protezione dei dati** laddove vengono custoditi, processati o trasmessi.

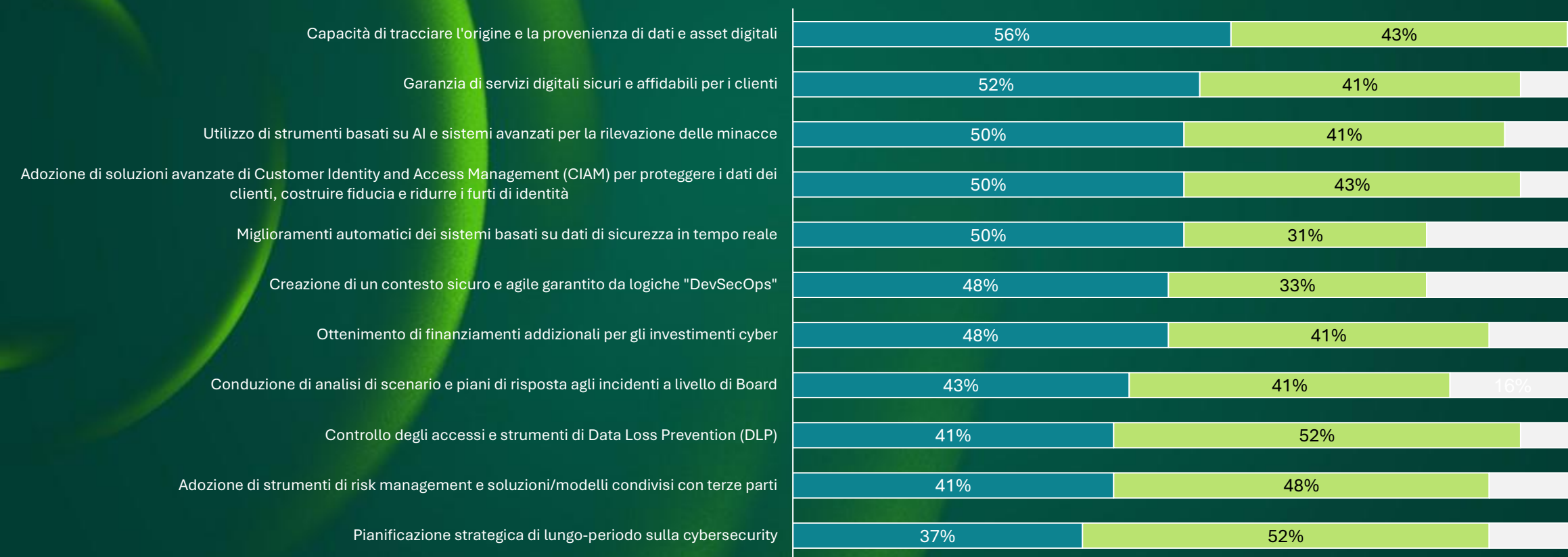


## Focus: lo sviluppo delle competenze e capacità di cybersecurity

L'evoluzione del contesto di mercato e la molteplicità delle sfide che le imprese si trovano a fronteggiare implicano la necessità di **sviluppare adeguate capacità e competenze** in materia. Quelle su cui le imprese stanno puntando maggiormente includono la capacità di **tracciare i dati e le origini degli asset digitali** (56%) e di **garantire la sicurezza e l'affidabilità dei servizi digitali per i clienti** (52%).

Altrettanto importante (50%) risulta poi la capacità di **implementare tool di intelligenza artificiale e sistemi avanzati** per la rilevazione delle minacce, soluzioni **CIAM** (Customer Identity & Access Management) per proteggere i dati dei clienti e rafforzarne la fiducia, insieme ai miglioramenti dei **sistemi automatizzati** basati su dati in tempo reale.

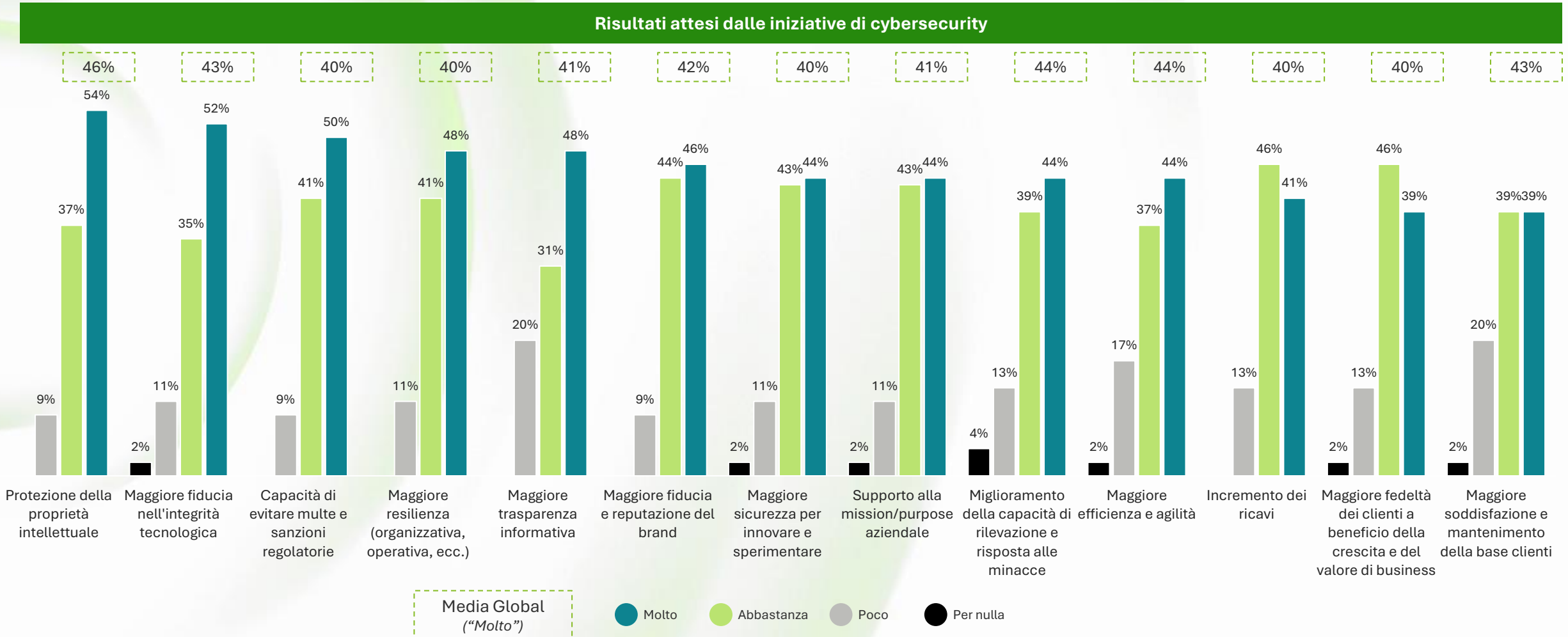
### Competenze/capacità cyber da sviluppare in via prioritaria



# Risultati attesi dalle iniziative di cybersecurity

La forte relazione tra cybersecurity e valore aziendale è evidenziata anche dai **risultati più significativi** che le imprese confidano di ottenere proprio grazie alle iniziative implementate in questo ambito. Tra quelli più diffusi, gli intervistati italiani citano al primo posto la **protezione della proprietà intellettuale** (54%), seguita dal

**rafforzamento dell'integrità dei dati / tecnologica** (52%), dalla prospettiva di **evitare sanzioni normative** (50%), dal rafforzamento della **resilienza operativa** (48%) e dalla maggiore **trasparenza delle informazioni** (48%). Poco meno della metà, inoltre, si aspettano anche un **incremento dei ricavi** (41%).



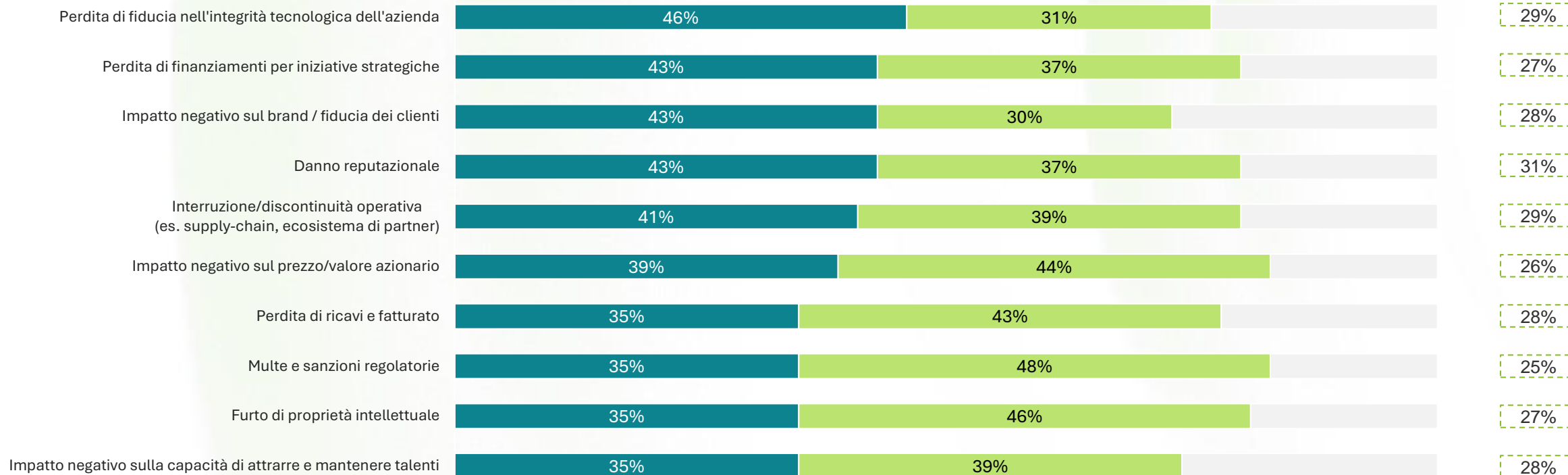
## Le conseguenze negative degli incidenti o violazioni informatiche

In parallelo, la cybersecurity consente alle imprese di **prevenire importanti costi e perdite** che possono impattare significativamente la profittabilità aziendale. La vulnerabilità agli attacchi cyber espone infatti un'organizzazione a una molteplicità di rischi di diversa natura. Pensando alle **conseguenze negative più rilevanti** per la propria azienda, gli intervistati citano la **perdita di fiducia nell'integrità tecnologica** (46%), la **perdita di finanziamenti per un'iniziativa strategica** (43%), i **danni reputazionali** (43%) e la **disruption dei processi operativi** (41%) estesi all'ecosistema

composto da partner o altri attori della supply-chain. È importante notare, tuttavia, come **più di un'impresa su tre** riveli un **impatto significativo e diffuso per tutte le possibili tipologie di rischio**, a dimostrazione della complessità e dell'effetto interdependente delle minacce cyber. Oltre alla possibile perdita di valore azionario per le aziende quotate (39%), per più di un terzo rimangono pressanti i rischi legati alla **perdita di ricavi e fatturato** (35%), a **multe e sanzioni regolatorie**, al **furto di proprietà intellettuale**, nonché alla **capacità di attrarre e mantenere talenti**.

### Principali impatti negativi derivanti da incidenti cyber

Media Global  
("In maniera estesa")



# L'evoluzione e l'importanza crescente del ruolo CISO

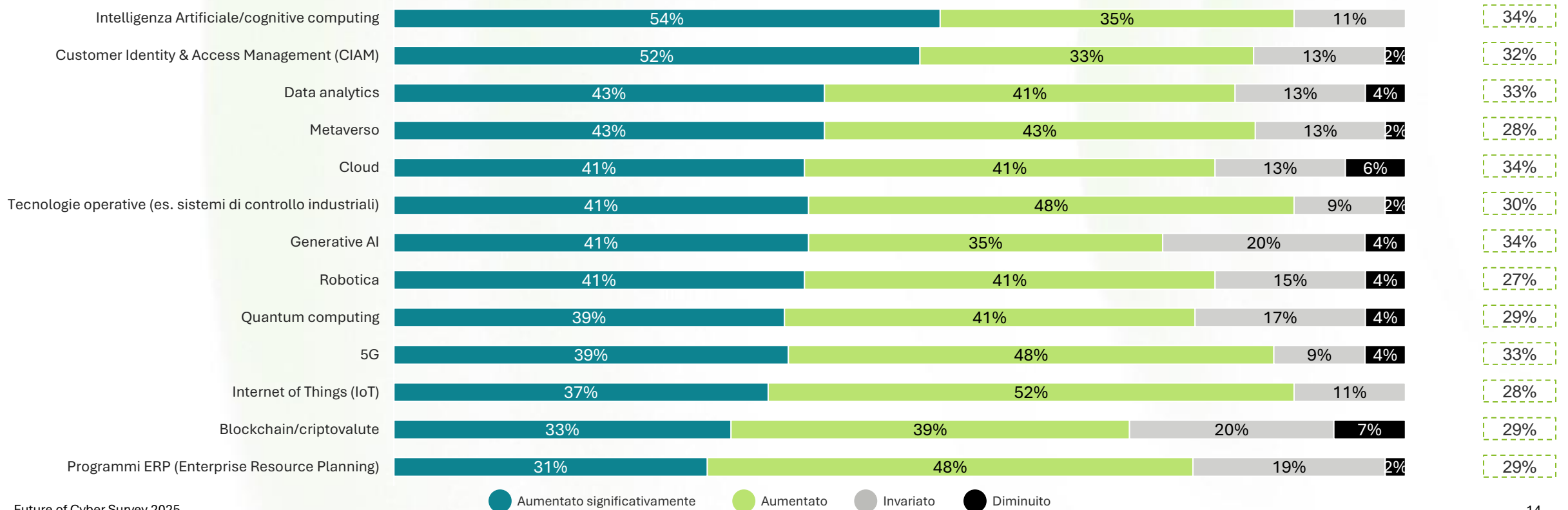
La cybersecurity è sempre più vista come una responsabilità condivisa che richiede una forte collaborazione tra le diverse funzioni aziendali. Il ruolo del CISO emerge come un punto di riferimento e di coordinamento per le strategie cyber dell'impresa.

# Le aree e il coinvolgimento del CISO nelle discussioni sulle tecnologie critiche

Il ruolo del CISO sta acquisendo un'importanza destinata a crescere ulteriormente nei prossimi anni, con lo sviluppo di tecnologie critiche per le attività di business delle imprese. Non a caso, per circa il 40% degli intervistati nazionali (rispetto a circa un terzo della media internazionale), nel corso dell'ultimo anno è **significativamente aumentato il coinvolgimento del CISO nelle discussioni strategiche**, in particolare con riferimento a quelle incentrate sulle **competenze** e sulle **capacità tecnologiche dell'impresa**. Più nello specifico, gli ambiti tech in cui i CISO sono chiamati a

valorizzare la propria expertise includono: Intelligenza Artificiale e tecnologie cognitive (54%), Customer Identity & Access Management (CIAM) (52%), data analytics (43%) e metaverso (43%). Una quota analoga (41%) si registra poi per Cloud, tecnologie operative (es. sistemi di controllo industriale), Gen-AI e robotica. In generale, vale la pena sottolineare che, per circa un terzo degli intervistati, il coinvolgimento è **aumentato significativamente** in almeno un ambito specifico, a conferma dello **stretto legame tra evoluzione tecnologica e cybersecurity**.

Aree e grado di coinvolgimento del CISO nelle discussioni sulle tecnologie critiche



## La collaborazione con la C-Suite e gli impatti sull'innovazione e la sicurezza aziendale



L'evoluzione tecnologica sta chiaramente trasformando le logiche e le modalità con cui le imprese operano sul mercato. Pertanto è quantomai cruciale che le imprese includano nelle proprie riflessioni strategiche **gli impatti dell'innovazione tecnologica sul proprio livello di cybersecurity**. I cambiamenti indotti dal continuo sviluppo di nuove soluzioni e strumenti tecnologici richiedono, infatti, un'attenzione crescente a livello apicale da parte dei C-level, consentendo al ruolo del **CISO** di emergere come una sorta di **coordinatore in ambito cyber tra le diverse aree di business**.

In altre parole, il ruolo del CISO è destinato a diventare un partner essenziale per **sensibilizzare e orientare le scelte del Board e del top management** aziendale, ad esempio riguardo alle possibili **vulnerabilità di sicurezza**, agli **scenari di rischio**, alle potenziali **minacce emergenti**, nonché alle **azioni necessarie** per incrementare ulteriormente la resilienza e la reattività dell'organizzazione.

In senso esteso, la **cybersecurity** diventa infatti **una responsabilità condivisa dall'intera organizzazione** che, come tale, richiede una forte collaborazione tra tutti i dipendenti e un approccio olistico e trasversale tra le diverse funzioni.

È dunque lecito attendersi che, in prospettiva futura, il CISO non si limiterà a gestire i piani di cybersecurity dell'impresa, ma fornirà anche una **guida** e un **orientamento strategico** ai vertici aziendali, collaborando in modo sempre più stretto e sistematico con altri CxO per ottimizzare e allineare le iniziative di sicurezza con i rispettivi obiettivi di business. Inoltre, il suo ruolo dovrà fungere da garante sul fatto che **la cybersecurity continui a ricevere l'attenzione e le risorse necessarie**, quale area strategica che richiede costantemente investimenti adeguati. Non meno rilevante è poi il fatto che l'evoluzione delle responsabilità e del ruolo del CISO dovrà **mantenersi al passo con l'evoluzione della natura stessa delle minacce cyber**, a fronte di sviluppi e cambiamenti tecnologici spesso repentini o imprevedibili.

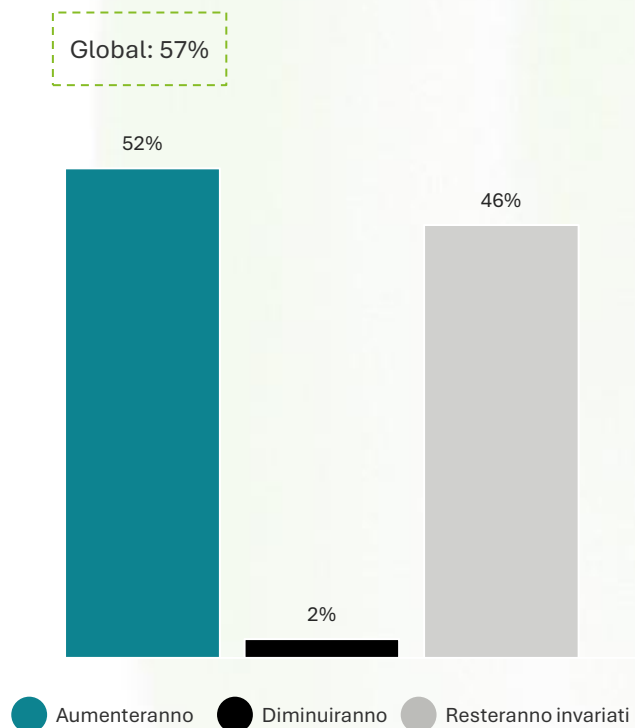
# Accelerare la trasformazione digitale dell'impresa grazie alla cybersecurity

La crescente digitalizzazione richiede maggiori investimenti in cybersecurity, con un focus sulla protezione dei dati e sulla rilevazione delle minacce in tempo reale. Anche le imprese italiane stanno rispondendo a questa sfida aumentando il proprio livello di investimenti.

## Gli investimenti previsti

Alla luce della progressiva digitalizzazione delle imprese, l'importanza crescente della cybersecurity è confermata anche dalle maggiori risorse che le imprese dichiarano di destinare alle iniziative su questo ambito. Tra gli intervistati italiani, più della metà (52%) prevede infatti un **aumento degli investimenti entro i prossimi due anni**, con un incremento medio del 2%.

### Previsione degli investimenti cyber nei prossimi 2 anni



Inoltre, un maggiore livello di cybersecurity all'interno dell'organizzazione consente, a sua volta, di **supportare e incentivare maggiormente gli investimenti destinati a tecnologie potenzialmente "critiche"** che, altrimenti, potrebbero esporre le imprese a possibili vulnerabilità e minacce alla sicurezza.

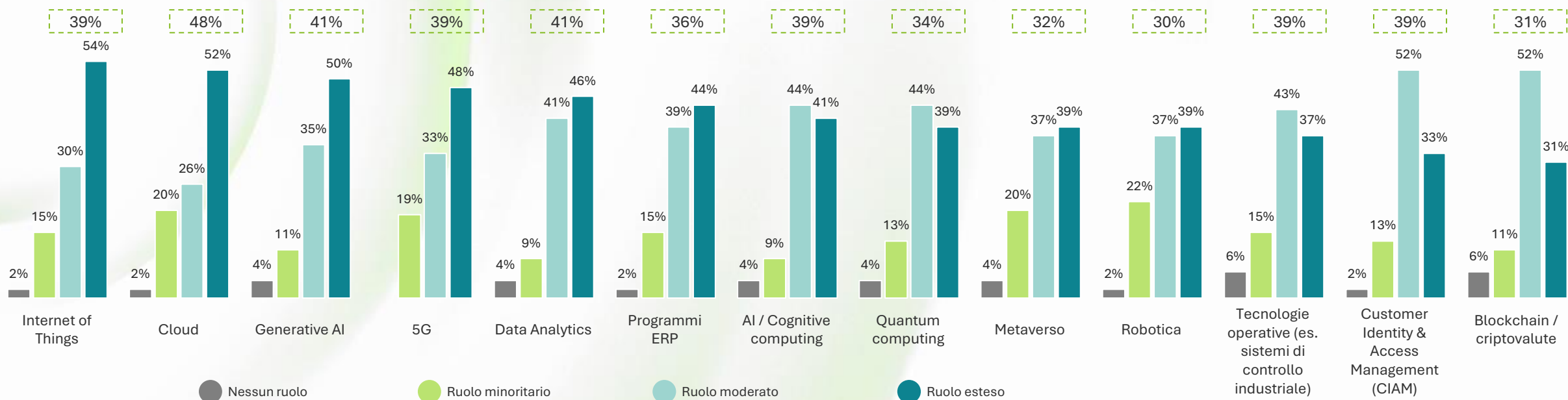


## Gli investimenti previsti

In altre parole, un adeguato livello di cybersecurity consente alle organizzazioni di **garantire e assicurare gli investimenti volti ad acquisire o rafforzare gli asset tecnologici**, abilitando a sua volta molteplici benefici in termini di integrità tecnologica, produttività e capacità di innovazione, ricerca e sviluppo. Da questo punto di vista, circa la metà degli intervistati italiani riconosce alla cybersecurity un ruolo maggiormente incisivo anzitutto sugli investimenti destinati alle tecnologie relative a Internet of Things (54%), Cloud (52%) e GenAI (50%), seguiti a breve distanza da 5G (48%), data analytics (46%) e sistemi ERP (44%).

L'importanza di questi ambiti risulta confermata anche dalla media internazionale, dove tuttavia l'influenza maggiore è attribuita agli investimenti relativi al Cloud e assumono più importanza, rispetto all'Italia, quelli destinati a tecnologie operative e CIAM. In ogni caso, il punto centrale è che la sicurezza delle infrastrutture e la protezione dagli attacchi cyber **favoriscono l'adozione di nuovi asset tecnologici** e la progressiva **digitalizzazione dei processi aziendali**, per i quali diventa cruciale la preparazione e la capacità di risposta ai potenziali incidenti di sicurezza. Anche questa prospettiva conferma, peraltro, l'importanza dei CISO nel supportare l'innovazione e la trasformazione digitale delle imprese, garantendo che le nuove tecnologie siano implementate in modo sicuro.

### Ruolo della cybersecurity nell'assicurare gli investimenti su tecnologie chiave/emergenti

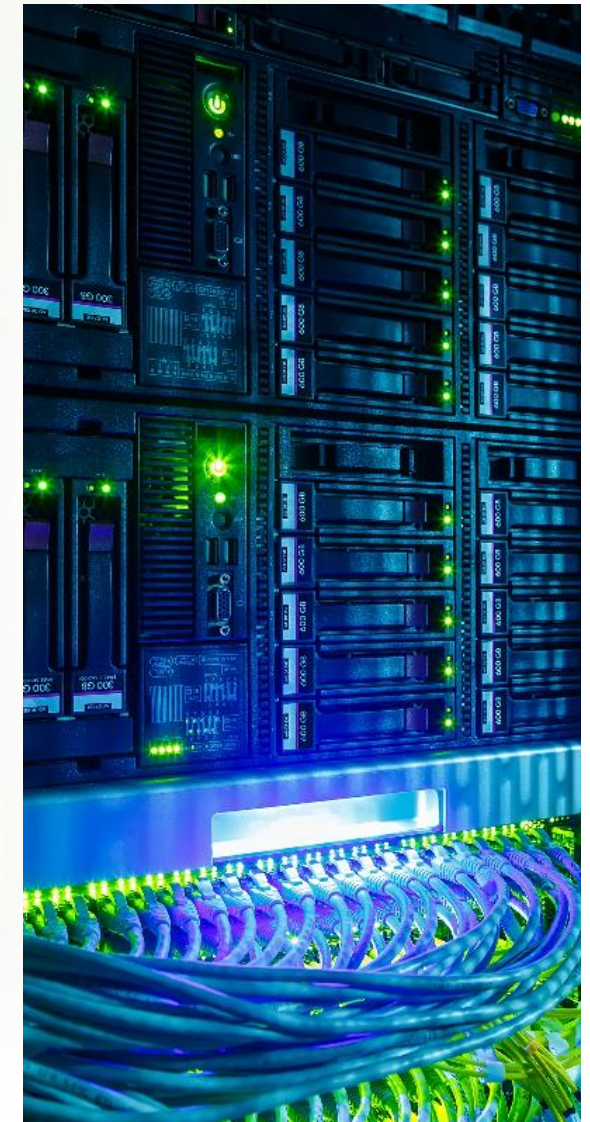
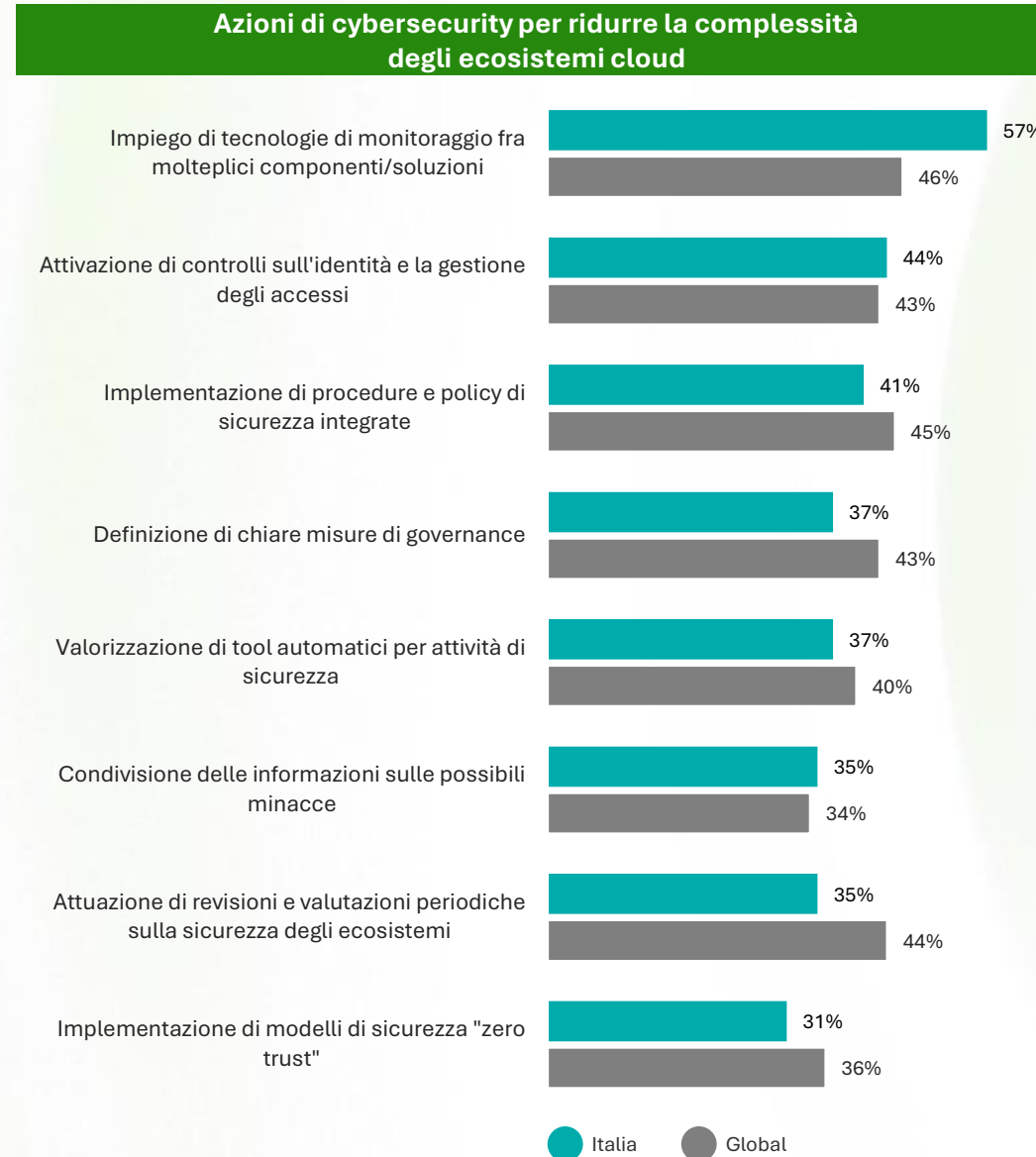


# Il ruolo della cybersecurity per gli ecosistemi cloud

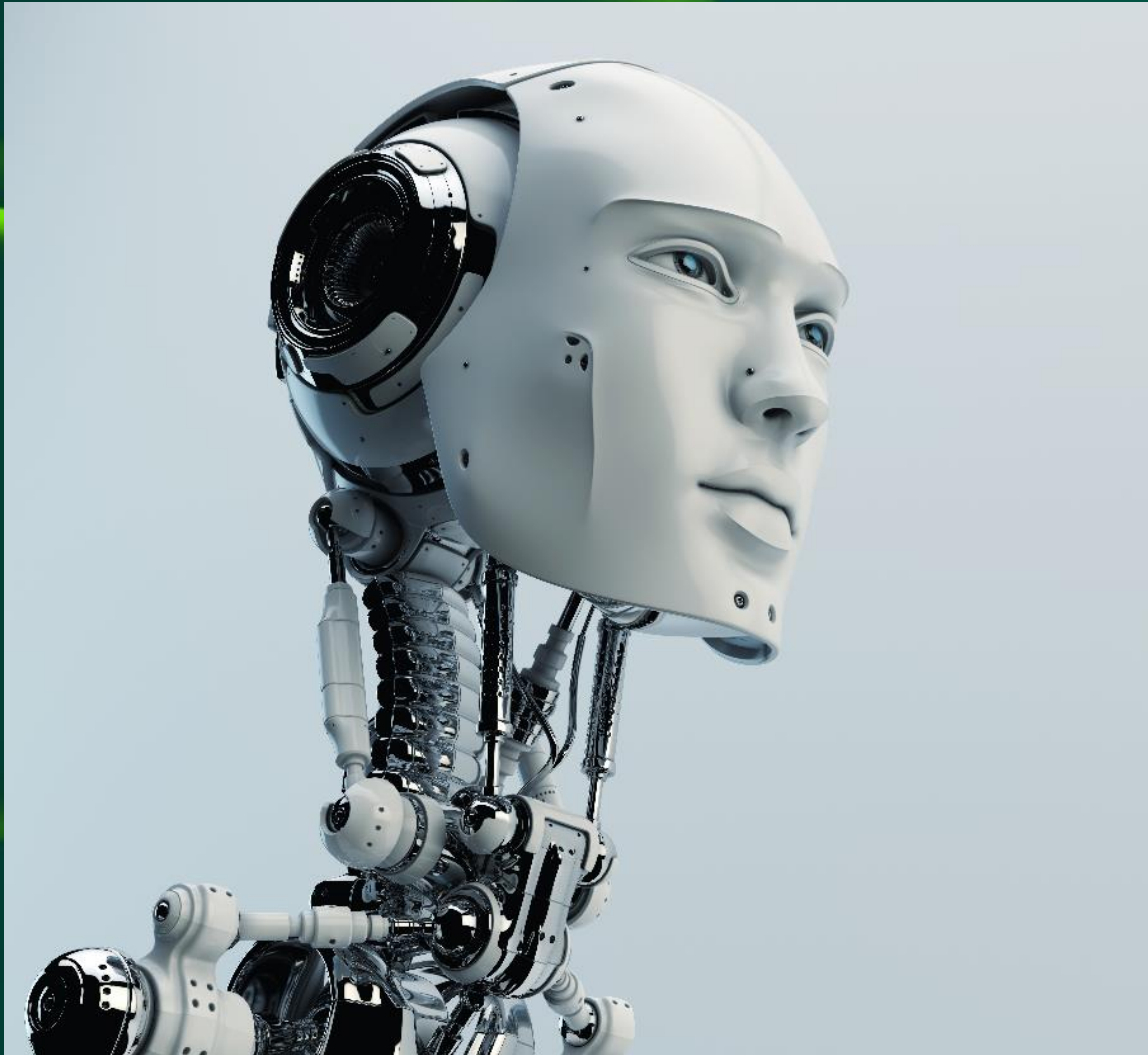
Altri due fattori di rilievo per la trasformazione digitale sono riconducibili al fatto che, da un lato, la cybersecurity aiuta le imprese a **ridurre la complessità degli ecosistemi Cloud** e, dall'altro, consente di **sfruttare le nuove tecnologie di Intelligenza Artificiale** per rispondere in maniera più rapida ed efficace ad attacchi sempre più complessi e sofisticati.

Con riferimento al primo punto, secondo le imprese italiane intervistate, le azioni di cybersecurity possono contribuire a diminuire la complessità impiegando anzitutto **tecnologie di monitoraggio** (57%), seguite da **controlli di identificazione e gestione degli accessi** (44%) e **procedure/policy di sicurezza** (41%) che siano fortemente integrate tra loro.

Per più di un terzo degli intervistati, inoltre, risulta importante stabilire **chiare misure di governance** (37%), valorizzare **tool di automazione** per compiti relativi alla sicurezza (37%), condurre regolarmente all'interno dell'ecosistema processi di **valutazione e revisione degli standard di sicurezza** (35%), nonché **condividere le informazioni** sulle possibili minacce con altre parti (35%).



# Cybersecurity e Intelligenza Artificiale



Per quanto riguarda invece la diffusione delle tecnologie più innovative nel campo dell'**Intelligenza Artificiale**, come ad esempio quelle relative alla **GenAI**, le imprese si trovano oggi ad affrontare **rischi inediti e sempre più sofisticati**.

Tradizionalmente, le tecnologie di machine learning ed apprendimento automatico sono state già a lungo utilizzate per **rilevare vulnerabilità informatiche**, attraverso attività di monitoraggio delle potenziali minacce su larga scala. Esse, tuttavia, richiedono un **elevato livello di competenza tecnica** e **notevoli investimenti** per addestrare il modello di un'organizzazione a individuare "pattern", comprenderne le correlazioni sottostanti e rilevare anomalie nei dati.

I **sistemi tradizionali di intelligenza artificiale**, basati su regole pre-determinate, presentano tuttavia il limite di poter individuare unicamente

tipologie di **attacchi già noti** e di funzionare in **casi d'uso molto specifici per l'organizzazione**.

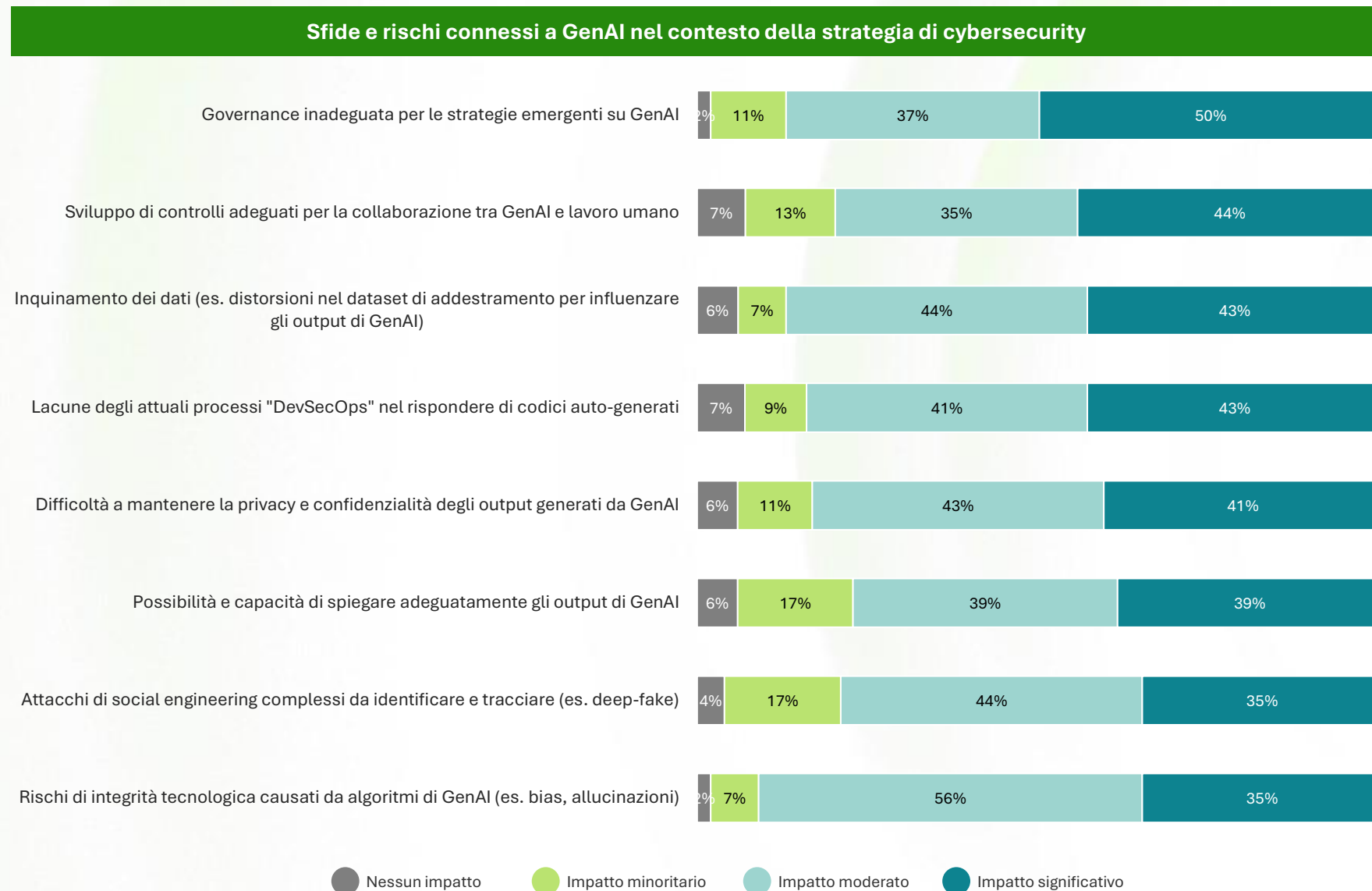
Viceversa, con l'avvento dei sistemi di **Intelligenza Artificiale Generativa** e dei **modelli LLM (Large-Language Models)**, lo scenario è cambiato profondamente. I sistemi di GenAI utilizzano infatti modelli basati su reti neurali e addestrati su quantità di dati estremamente elevate, che consentono di individuare risultati e pattern nuovi, al di là dei dataset originali o di regole pre-determinate.

Altrettanto rilevante è poi il fatto che l'utilizzo di un **linguaggio "umano"** nelle interazioni con i sistemi di controllo può fornire agli analisti un metodo più comprensibile, immediato e naturale per **identificare, sintetizzare e riassumere le informazioni** relative alle **potenziali minacce informatiche**, con evidenti vantaggi in termini di rapidità e precisione.

# Cybersecurity e Intelligenza Artificiale

Ma se da un lato la GenAI crea nuove opportunità per prepararsi e difendersi dagli attacchi informatici con più efficienza e tempestività, dall'altro lato (come ogni nuova tecnologia) essa presenta **rischi inediti**, oltre al potenziale di amplificare quelli esistenti, ad esempio tramite attacchi più sofisticati.

A fronte di questo nuovo scenario, qual è dunque il percepito delle imprese italiane? Tra i **rischi più significativi**, esse indicano anzitutto una **governance inadeguata delle iniziative emergenti in ambito GenAI** (50%), seguita dalla necessità di sviluppare controlli efficaci sulle modalità di interazione tra umani e sistemi di GenAI (44%) e dal possibile inquinamento degli output prodotti dall'IA generativa (43%) a causa della manipolazione delle banche dati utilizzate per addestrare gli algoritmi.



# Grado di utilizzo delle capacità offerte dall'AI per il piano di cybersecurity dell'organizzazione

Al tempo stesso, naturalmente, le nuove soluzioni di Intelligenza Artificiale offrono anche **opportunità per rafforzare il livello di cybersecurity** delle imprese stesse. A questo proposito, più di 9 aziende su 10 citano la possibilità di **rispondere più rapidamente alle minacce informatiche** (94%) e di **monitorare in modo**

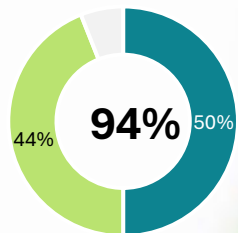
**continuativo l'integrità dell'infrastruttura digitale** (92%). Leggermente inferiore, ma comunque ampiamente diffusa, risulta invece la quota di chi indica la possibilità di **analizzare serie storiche e dati in tempo reale** (89%) per comprendere pattern complessi e individuare possibili attacchi inediti.

## Grado di utilizzo delle capacità di AI nella strategia di cybersecurity dell'organizzazione

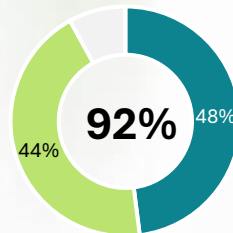
● Utilizzo ampiamente esteso

● Utilizzo moderatamente esteso

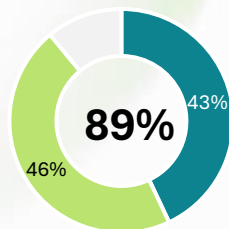
Attivare risposte più tempestive a potenziali minacce alla sicurezza



Attivare tool AI per monitorare costantemente l'infrastruttura digitale dell'organizzazione



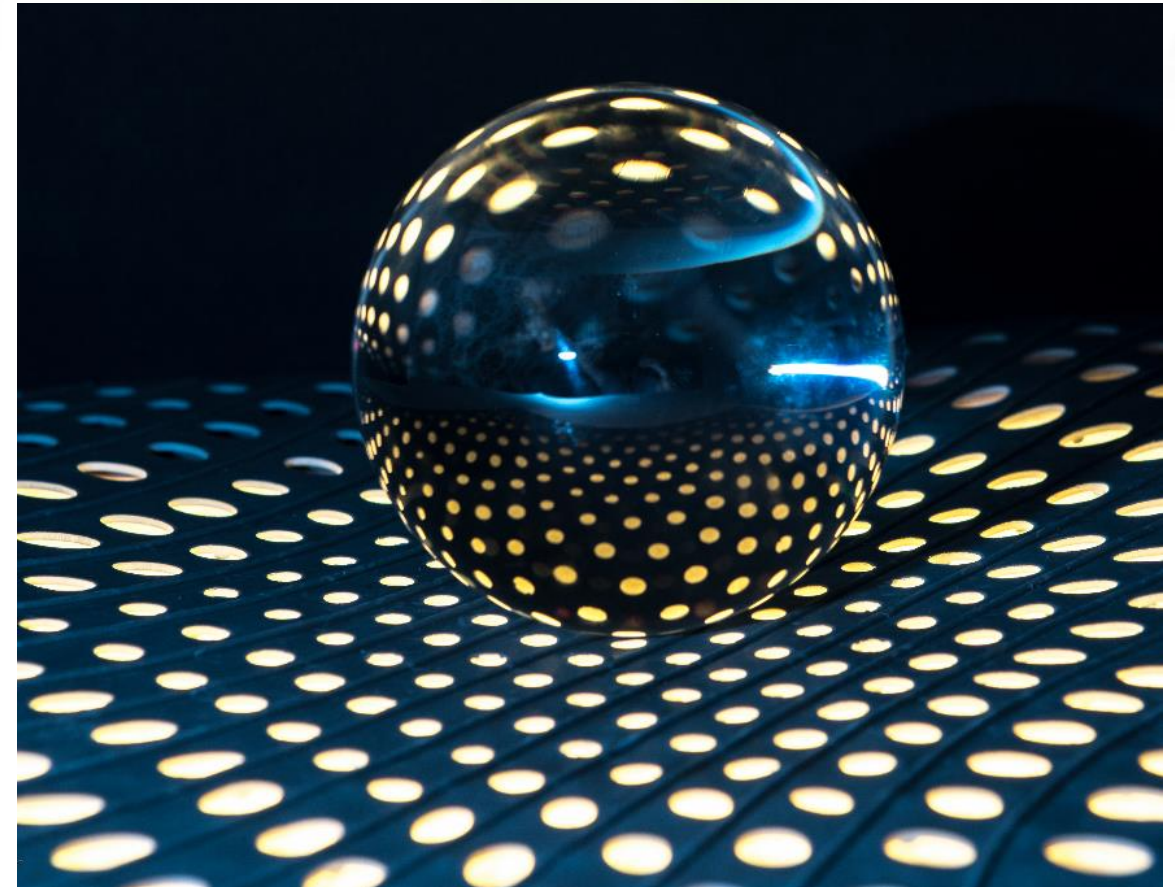
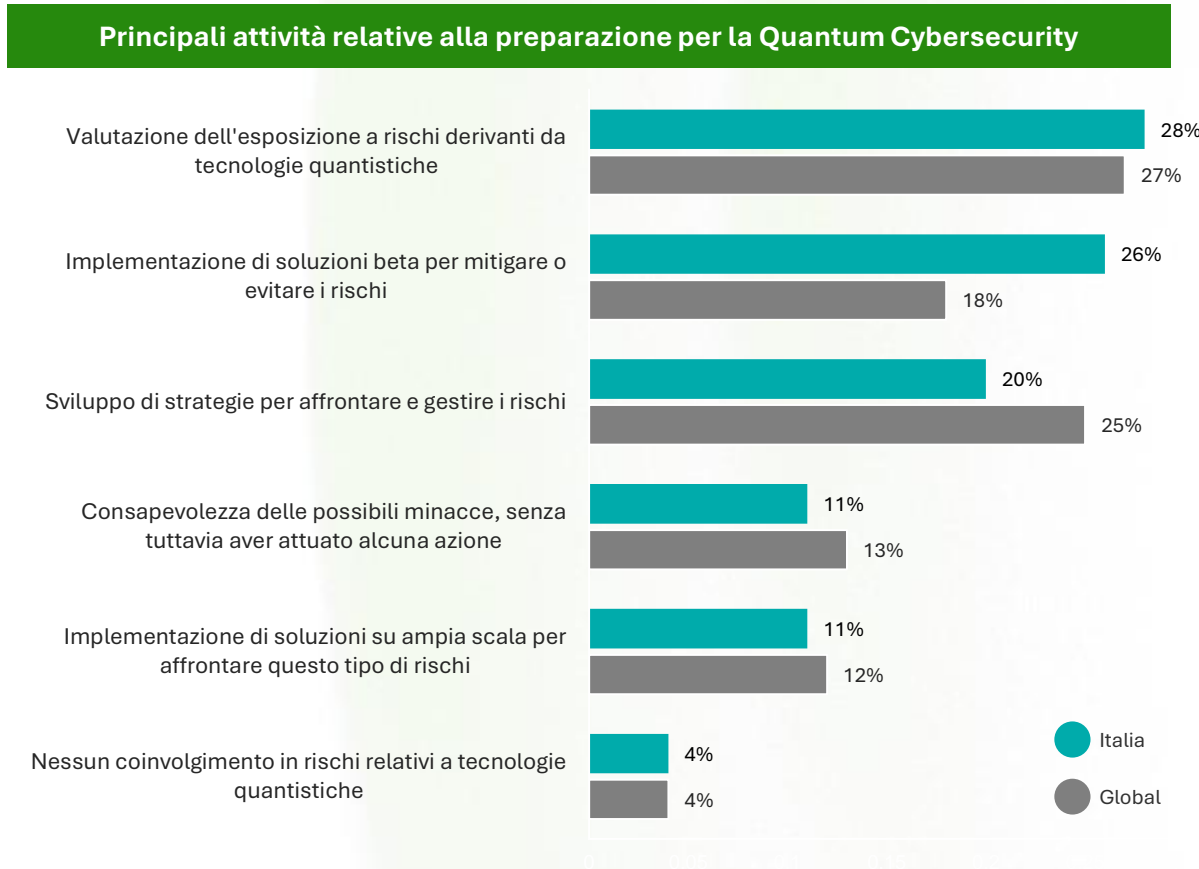
Analizzare dati storici e identificare potenziali minacce e vulnerabilità



# Cybersecurity e Quantum Computing

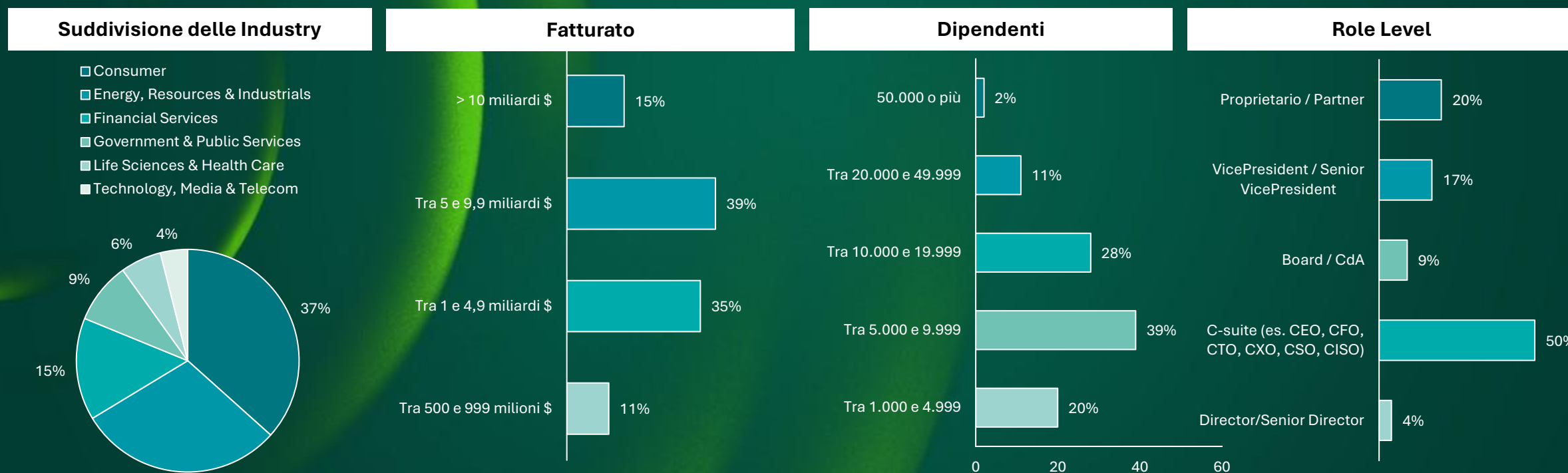
In prospettiva degli sviluppi tecnologici dei prossimi decenni, infine, una quota minoritaria di aziende sta cercando di prepararsi alla diffusione futura del **quantum computing**. Ad oggi, più di una su quattro sta conducendo valutazioni e assessment (28%) circa la propria esposizione a possibili rischi legati a questa nuova frontiera tecnologica e/o implementando soluzioni beta per evitarli o almeno mitigarli (26%).

Minore è invece la quota di chi sta sviluppando strategie strutturate per affrontarli (20%) o implementando soluzioni scalabili all'intera organizzazione (11%). Vale tuttavia la pena sottolineare che, nel complesso, quello dei rischi legati agli sviluppi del quantum computing rimane un tema importante per le imprese: solo una quota estremamente residuale (4%) dichiara di non tenere attualmente in considerazione questo argomento.



# Nota Metodologica | Profilazione del campione per l'Italia

Per la 4° edizione della *Global Future of Cyber Survey*, Deloitte ha messo in evidenza la complessità dell'attuale panorama tecnologico e di business, analizzando le esigenze espresse dalle aziende leader di mercato. La survey è stata condotta in 43 Paesi a livello globale ed esclusivamente su imprese di grandi dimensioni (con almeno 1.000 dipendenti e un fatturato annuale di 500 milioni di dollari), adottando una prospettiva cross-settoriale tra 6 principali Industry. In particolare, la ricerca ha coinvolto circa 1.200 decision-maker in ambito Cyber, con livello Director o superiore. Nelle interviste sono stati inclusi anche C-level e loro diretti collaboratori, garantendo così un buon mix tra aree di business e funzioni IT. La survey online è stata poi integrata da interviste qualitative in profondità con una selezione di opinion maker in ambito Cyber, al fine di raccogliere insight più dettagliati e validare ulteriormente i risultati dell'indagine. Tale approccio metodologico ha consentito così di coprire tutti gli aspetti più rilevanti riguardo al futuro del mondo Cyber: dalle strategie alle tattiche, alla cultura aziendale e alla consapevolezza della C-suite, fino all'implementazione delle nuove tecnologie. Lungo tutte le fasi della ricerca, Deloitte ha cercato di identificare insight preziosi per comprendere al meglio il valore di business derivante dall'ambito Cyber e le principali implicazioni per le imprese, nonché le strategie e le azioni più distintive che i leader di mercato stanno adottando per rafforzarsi e incrementare ulteriormente il valore stesso della cybersecurity. Di seguito si riporta la profilazione del campione italiano di intervistati.



# Contatti

## Matthew Holt

Partner  
DCM Cyber Leader  
Deloitte Technology & Transformation  
maholt@deloitte.it

## Manuel Allara

Partner  
DCM Cyber Defense & Resilience  
Technology & Transformation  
mallara@deloitte.it

## Fabio Battelli

Partner  
DCM Enterprise Security  
Technology & Transformation  
fbattelli@deloitte.it

## Fabio Bonanni

Partner  
DCM Digital Trust & Privacy  
Technology & Transformation  
fbonanni@deloitte.it

## Maurizio Costa

Partner  
DCM Cyber aaS / Operate  
Technology & Transformation  
maurcosta@deloitte.it

# Research & Editorial

## Luca Bonacina

Manager  
DCM Growth  
Deloitte Italy  
lbonacina@deloitte.it

## Marco Tirelli

Research & Market Insights  
DCM Growth  
Deloitte Italy  
mtirelli@deloitte.it

## Important notice

This document has been prepared by Deloitte Italy S.p.A. Società Benefit for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of Deloitte Italy S.p.A. Società Benefit to supply the proposed services.

The information contained in this document has been compiled by Deloitte Italy S.p.A. Società Benefit and may include material obtained from various sources which have not been verified or audited. This document also contains material proprietary to Deloitte Italy S.p.A. Società Benefit. Except in the general context of evaluating the capabilities of Deloitte Italy S.p.A. Società Benefit, no reliance may be placed for any purposes whatsoever on the contents of this document. No representation or warranty, express or implied, is given and no responsibility or liability is or will be accepted by or on behalf of Deloitte Italy S.p.A. Società Benefit or by any of its partners, members, employees, agents or any other person as to the accuracy, completeness or correctness of the information contained in this document.

Other than stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or insurance saving, no such conditions of confidentiality applies to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.

Deloitte Italy S.p.A. Società Benefit, a company, registered in Italy with registered number 04963170966 and its registered office at Via Santa Sofia no. 28, 20122, Milan, Italy, is an affiliate of Deloitte Central Mediterranean S.r.l., a company limited by guarantee registered in Italy with registered number 09599600963 and its registered office at Via Santa Sofia no. 28, 20122, Milan, Italy.

Deloitte Central Mediterranean S.r.l. is the affiliate for the territories of Italy, Greece and Malta of Deloitte NSE LLP, a UK limited liability partnership and a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL, Deloitte NSE LLP and Deloitte Central Mediterranean S.r.l. do not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.