

Deloitte: il 52% delle aziende italiane prevede un aumento degli investimenti in cybersecurity entro i prossimi due anni

- *Il 94% delle organizzazioni italiane ritiene che l'Intelligenza Artificiale contribuirà a rispondere più velocemente alle minacce informatiche*
- *6 imprese su 10 stanno potenziando la propria struttura di cybersecurity istituendo un organo di governance dedicato, che supervisioni gli investimenti e le competenze in ambito cyber*
- *Nel 69% dei casi, il tema cyber viene discusso a livello di Board su base almeno mensile*
- *Per circa 4 imprese su 10 è significativamente aumentato il coinvolgimento del Chief Information Security Officer (CISO)*

Milano, 9 giugno 2025 – Nel mondo delle imprese la cybersecurity sta diventando sempre più una leva strategica per la competitività e la creazione di valore, con più della metà (52%) delle aziende italiane che prevede un aumento degli investimenti entro i prossimi due anni e una sempre maggiore integrazione del tema cyber nelle discussioni del Board aziendale, che nel 69% dei casi viene affrontato su base almeno mensile (26% almeno settimanale).

Queste alcune delle principali evidenze che emergono dalla “**Global Future of Cyber Survey 2025**”, la quarta edizione della ricerca condotta da Deloitte a livello globale, che ha raccolto le opinioni di oltre 1.200 executive e C-level in ambito cyber, tra cui 54 top manager italiani appartenenti a grandi imprese attive in diversi settori.

*“In un contesto di mercato sempre più digitalizzato – commenta **Matthew Holt, Cyber Leader di Deloitte Central Mediterranean** – le imprese italiane devono operare in uno scenario di cybersecurity in continua evoluzione, contraddistinto da sfide complesse ma anche da nuove opportunità per incrementare ulteriormente il valore di business. Oggi la cybersecurity è riconosciuta non solo come un elemento di difesa delle infrastrutture digitali, ma anche in qualità di fattore abilitante per la digital transformation e la competitività delle imprese sul mercato: la protezione dei dati critici, degli asset e del know-how aziendale, insieme all’integrità della fiducia e della reputazione agli occhi dei clienti, sono infatti elementi determinanti per una crescita consolidata nel lungo periodo”.*

La Cybersecurity: da necessità a vantaggio competitivo strategico

Dalla survey emerge come la cybersecurity non venga più percepita esclusivamente come un sistema di difesa, ma come un fattore strategico determinante per la competitività delle imprese.

In particolare, in quasi 7 aziende italiane su 10, il tema cyber viene discusso a livello di Board almeno una volta al mese, e in oltre il 26% dei casi la discussione avviene su base settimanale. Un dato che conferma una gestione del rischio cyber sempre più strutturata e proattiva e che sarà ulteriormente accentuato con l’introduzione delle responsabilità in capo ai membri del Organi di amministrazione e direttiva, come regolamentato dalla nuova direttiva NIS2.

A rafforzare questa evidenza, il 70% dei rispondenti italiani si dichiara molto fiducioso nella preparazione del proprio Board nel trattare questioni legate alla cybersecurity. Questi risultati confermano che, per molte imprese, l’attenzione del top management è ormai orientata a integrare il tema cyber nella strategia complessiva, a tutela non solo della sicurezza, ma della sostenibilità e della reputazione aziendale.

Tra le barriere all’implementazione della strategia cyber, gli intervistati segnalano la difficoltà ad 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.

“Un aspetto cruciale emerso dal report Deloitte – aggiunge **Holt** – è l'integrazione della cybersecurity nelle agende e discussioni strategiche dei consigli di amministrazione, confermato dal fatto che le imprese stanno incrementando proattivamente i propri investimenti in questo ambito. E ciò non soltanto per un tema di conformità normativa, ma soprattutto per prevenire danni reputazionali e costi significativi, presidiando al tempo stesso la capacità di creare un valore distintivo. La cybersecurity è diventata pertanto un elemento chiave per il successo aziendale. E il suo stretto legame con la trasformazione digitale – se adeguatamente valorizzato – può incrementare sensibilmente la capacità di innovazione e resilienza delle aziende stesse.”

La sinergia tra Cybersecurity e Cloud per potenziare la competitività aziendale

Nel contesto della trasformazione digitale, la cybersecurity rappresenta un fattore abilitante fondamentale per la gestione degli ecosistemi cloud. Le aziende italiane riconoscono che soluzioni di sicurezza avanzate contribuiscono a ridurre la complessità del cloud, favorendo l'adozione di nuove tecnologie e garantendo una risposta tempestiva ad attacchi sempre più sofisticati. In particolare, le strategie più adottate includono l'impiego di tecnologie di monitoraggio degli ecosistemi cloud su diversi componenti e soluzioni (57%), l'attivazione di controlli sull'identità e la gestione degli accessi (44%) e l'implementazione di procedure e policy di sicurezza integrate (41%). Queste azioni permettono alle organizzazioni di rafforzare la governance, automatizzare i processi di sicurezza e condividere informazioni sulle minacce, assicurando così un ambiente cloud resiliente e competitivo.

Cybersecurity e Intelligenza Artificiale: nuovi orizzonti e sfide

L'adozione crescente di tecnologie di Intelligenza Artificiale, in particolare la Generative AI e i Large Language Models (LLM), sta trasformando il panorama della cybersecurity, introducendo rischi inediti ma anche opportunità significative. Secondo quanto emerso dalla ricerca di Deloitte, tra i rischi più impattanti generati da GenAI identificati dalle imprese intervistate spiccano una governance inadeguata delle iniziative GenAI (50%), la necessità di sviluppare controlli efficaci sulle interazioni tra umani e sistemi GenAI (44%), e il possibile inquinamento degli output a causa della manipolazione delle banche dati usate per l'addestramento degli algoritmi (43%).



Inoltre, tra le principali potenzialità dell'AI a supporto della cybersecurity, oltre 9 aziende su 10 citano la possibilità di rispondere più velocemente alle minacce informatiche (94%) e di monitorare continuamente l'integrità dell'infrastruttura digitale (92%). L'analisi di serie storiche e dati in tempo



reale per comprendere pattern complessi e individuare attacchi inediti è indicata dall'89% delle organizzazioni.

Il ruolo crescente del CISO

Per circa il 40% delle aziende intervistate è significativamente aumentato il coinvolgimento del Chief Information Security Officer (CISO), che il ruolo di emergere come una sorta di coordinatore in ambito cyber tra le diverse aree di business. Secondo il report di Deloitte, è 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.

*** **

Contatti

Ufficio Stampa Deloitte | Michele Pozzi

Tel: 335 148 9871

E-mail: mpozzi@deloitte.it

Omnicom PR Group | Tommaso Filippi, Michele Cartisano, Sante Di Giannantonio, Letizia Castiglioni, Davide Paolicchi, Giacomo Agostinelli, Rossella Primerano

Tel: 324 0021567, 340 852 4741, 338 887 2351, 389 450 7621, 389 595 9986, 333 283 8953

E-mail deloitte-ita@omnicomprgroup.com