Deloitte.

Una visione cyber-first per la sicurezza e la creazione di valore

Future of Cyber: il punto di vista delle aziende italiane

Indice

Introduzione

I **dati** sono un elemento vitale ed imprescindibile per il business e una risorsa chiave per lo sviluppo delle aziende. **Garantire la loro sicurezza** e la conseguente **fiducia dei clienti** diventa imperativo per le organizzazioni per svolgere la loro attività in modo profittevole. Le organizzazioni, infatti, gestiscono una moltitudine di dati, sia proprietari che personali dei clienti[a], e una loro eventuale **perdita o violazione** comporta **gravi ripercussioni**. Quasi 8 clienti su 10 non acquisterebbero prodotti o servizi da un'azienda qualora non si fidassero di come questa gestisce e custodisce i loro dati[1].

I clienti, infatti, si accorgono sempre più che i dati personali hanno un valore intrinseco e ne esigono la protezione. Soddisfare questa aspettativa diventa fondamentale per le aziende nell'ottica di massimizzare la propria performance economica e i relativi margini. Quando i clienti si fidano di un'azienda, aumenta il loro grado di fidelizzazione, sono più propensi a riacquistare i suoi prodotti o servizi, provarne di nuovi e spendere in media di più rispetto a un nuovo cliente[2].

Si pensi che quasi il 90% dei clienti, che hanno un elevato grado di fiducia nei confronti di un brand, ha acquistato di nuovo da quel marchio e il 62% dei clienti fidelizzati acquista quasi esclusivamente da quel brand[3].

Alla luce della crescente importanza della cybersecurity nel contesto di business attuale, Deloitte ha condotto la ricerca "**2023 Global Future of Cyber Survey**", all'interno della quale sono state intervistate anche aziende italiane. Attraverso l'analisi dei dati italiani, il seguente report intende fornire un quadro più chiaro dello scenario attuale e futuro in materia di cybersecurity nel nostro Paese, cercando di dare risposta a domande quali: come stanno agendo le aziende italiane a fronte di un contesto competitivo in continua evoluzione?
Quale valore stanno traendo dall'adozione di approcci sempre più incentrati sulla cybersecurity? E quali sono le strade che stanno percorrendo per generare questo valore e avere successo nel lungo periodo?

[a]Fanno parte della categoria dei dati proprietari, fra gli altri: i dati finanziari, le credenziali e la proprietà intellettuale. Sono, invece, dati personali dei clienti: i dati anagrafici come nome e cognome, fotografie identificative, numeri di identificazione univoci come il codice fiscale, gli indirizzi IP, etc.

Le ripercussioni delle violazioni informatiche sul business: frequenza, intensità e ambiti maggiormente a rischio

Garantire la sicurezza dei dati e mantenere la fiducia è sempre più complesso nel contesto attuale. Oggi, infatti, ci troviamo in un mondo iperconnesso e l'avvento di **tecnologie digitali** sempre nuove, reso necessario dalle esigenze aziendali in continua evoluzione, **amplia la superficie di attacco** alla portata dei criminali informatici e **accresce il rischio** che le organizzazioni subiscano **attacchi cyber**.

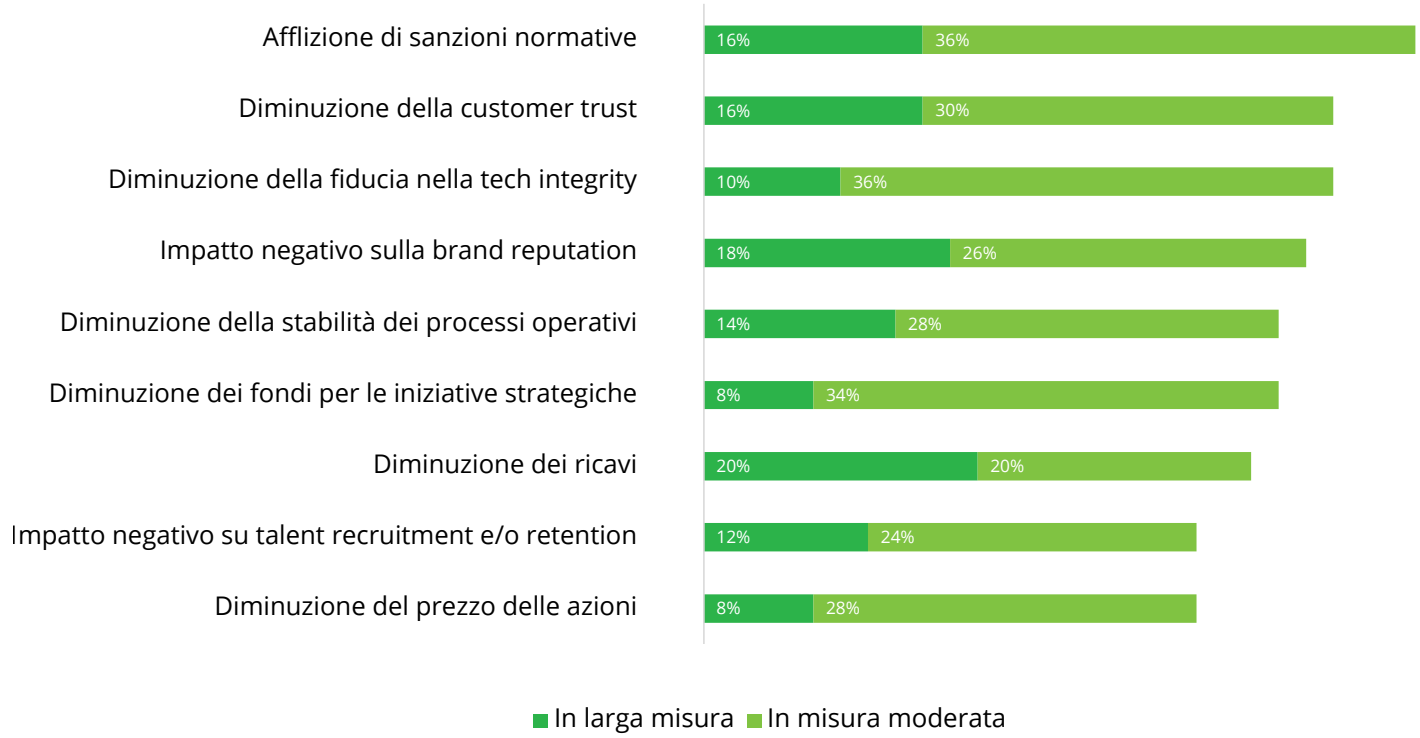
Secondo la 2023 Global Future of Cyber Survey di Deloitte, il **98%** delle aziende italiane ha riportato **almeno una violazione negli ultimi 12 mesi**. Nella maggior parte dei casi (62%), questi attacchi si sono manifestati con tecniche di phishing che, attraverso e-mail, messaggi di testo, telefonate o siti web fraudolenti, inducono a scaricare malware o ransomware, a condividere informazioni sensibili o a intraprendere altre azioni che espongono le organizzazioni alla criminalità informatica. E questo, secondo circa **2 intervistati su 3**, porta spesso a **danni di entità grave o estremamente grave**. A tal proposito, si pensi che, nel 2022, l'Italia si è classificata tra i primi 10 Paesi a livello mondiale per il valore medio del danno derivante da una violazione dei dati, stimato in 3,74 milioni di dollari, di poco inferiore alla media globale (4,35 milioni di dollari)[4].

Tuttavia, lo studio Deloitte evidenzia che le conseguenze negative di un attacco cyber non si limitano alla **sfera economica**, come la **perdita di fatturato (40%)** e la **riduzione del valore di mercato dell'azienda (36%),** ma possono incidere sulle organizzazioni sotto **molteplici profili**. In particolare, quello:

- **Normativo**, in termini di **multe e sanzioni** per inadempienza rispetto alle procedure in essere o per le violazioni dei regolamenti sulla cybersecurity **(52%)**. Si pensi, ad esempio, all'impatto del GDPR sulle attività delle organizzazioni oppure alla frammentazione e alla complessità normativa che un'azienda con operation in più Paesi deve fronteggiare.
- **Reputazionale**, in termini di ripercussioni negative sull'**immagine** dell'azienda **(44%)**, con il conseguente crollo della **fiducia** della clientela **(46%)** e anche della **capacità di attrarre e/o trattenere talenti (36%).**
- **Tecnologico**, in termini di minore fiducia nella **"tech integrity"**[b] **(46%).**
- **Strategico e operativo**, in termini di minori fondi resi disponibili per il **finanziamento delle iniziative strategiche (42%)** e di **interruzione delle attività**, ad esempio, nel più ampio ecosistema di business **(42%).**

Alla luce di ciò, per le organizzazioni italiane è oggi più che mai importante porre il tema della **cybersecurity al centro della propria strategia**.

Figura 1 | Conseguenze attese da violazioni della cybersecurity



D: Su una scala da 1 (per nulla) a 4 (in larga misura), quanto la sua organizzazione ha subito conseguenze negative in ognuna delle seguenti aree riconducibili a violazioni della cybersecurity?
Deloitte, 2023.

[b]*Per "tech integrity" si intende la fiducia nella capacità delle soluzioni tecnologiche di prevenire il furto o la modifica non autorizzata delle informazioni e di proteggere la riservatezza e l'integrità del dato.*

Cybersecurity, strumento fondamentale per la creazione di valore

Da tema IT a business enabler: l'evoluzione della cybersecurity

Le organizzazioni identificano **già oggi** la cybersecurity come un **tema prioritario e centrale** e dichiarano di comprendere in modo sempre più chiaro la sua evoluzione futura. Come emerge dalla 2023 Global Future of Cyber Survey di Deloitte, i leader aziendali stanno valutando la tematica della cybersecurity sotto una **nuova luce**, che va oltre l'essere un problema solo IT. Oggi, più che mai, la cybersecurity è percepita come un **driver fondamentale** affinché le aziende possano **raggiungere il successo** e **creare valore** per i propri stakeholder. Questo si riflette anche sulle strategie d'investimento delle aziende stesse: infatti, si registra un **aumento della propensione ad investire in questo ambito** da parte delle organizzazioni italiane, come suggerito dai **due terzi** del campione intervistato da Deloitte nel nostro Paese – un trend più marcato rispetto alla dinamica rilevata a livello globale (55%).

Questa maggiore inclinazione a investire nella cybersecurity accompagna la corsa al digitale che sta rivoluzionando il modo in cui le aziende operano nel mercato. Infatti, molti leader aziendali stanno rivolgendo e continueranno a dedicare molta attenzione alla **trasformazione digitale** nei **prossimi 3 anni**, con **investimenti** destinati in particolare all'adozione di soluzioni di **Cloud Computing**, considerato **prioritario** da **più di un'azienda su 2**, di **Intelligenza Artificiale (38%)**, di **IoT (38%)** e di **Data Analytics (36%)**.

Figura 2 | Aree prioritarie di trasformazione digitale e importanza attesa della cybersecurity

	Cloud	IoT	AI	Data Analytics	5G	Operational Technology
Priorità per il business nei prossimi 3 anni	54%	38%	38%	36%	34%	32%
Impatto della cybersecurity nei prossimi 3-5 anni	86%	80%	76%	80%	76%	80%

D1: Nei prossimi 3 anni, a quali iniziative di trasformazione digitale la sua organizzazione darà la massima priorità?
D2: Nei prossimi 3-5 anni, crede che la cybersecurity giocherà un ruolo cruciale in queste priorità di trasformazione digitale?
Deloitte, 2023.

Una visione cyber-first per la sicurezza e la creazione di valore

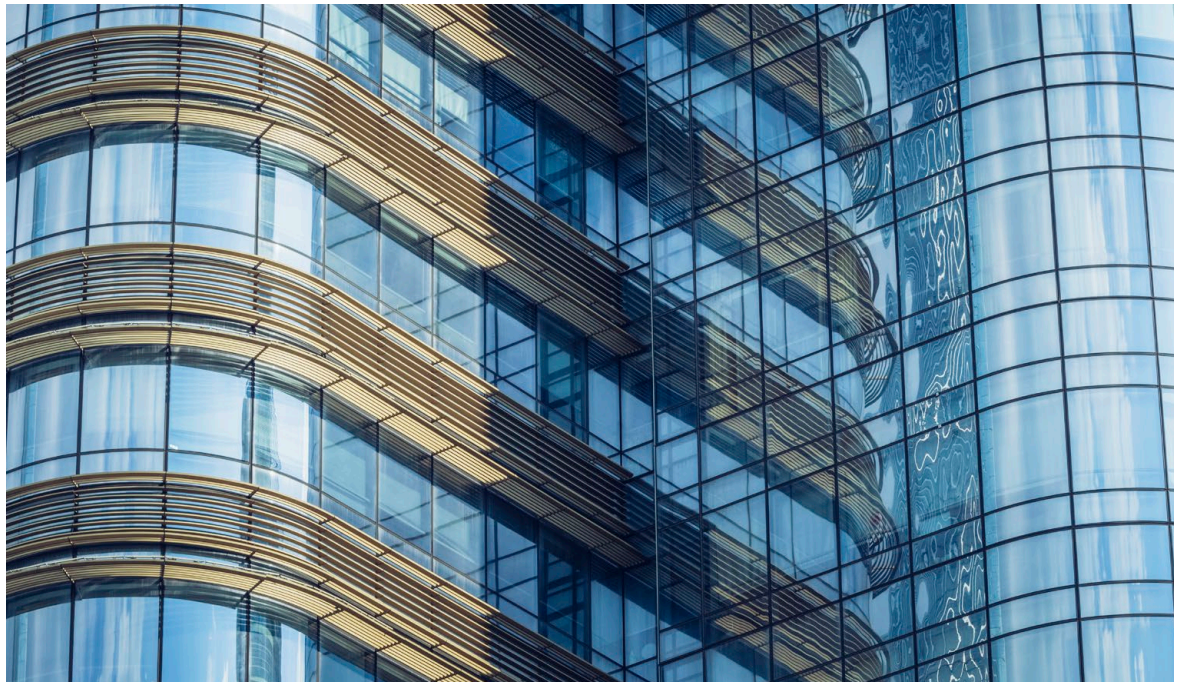
Adattarsi a questa fase di profonda trasformazione digitale, saperne sfruttare le opportunità e mitigarne i rischi è una necessità imprescindibile per ogni azienda. Per questo motivo, la **maturità delle strategie** e **degli approcci alla cybersecurity** ricopre un **ruolo centrale nel processo di digitalizzazione** delle organizzazioni. In particolare, si registra una coerenza circa le intenzioni d'investimento delle imprese italiane nelle principali aree tecnologiche e la centralità della componente cyber come prerequisito per un'implementazione di successo. Si pensi, ad esempio, come il Cloud porti con sé tutta la complessità delle problematiche IT associate all'hosting di dati e applicazioni in ambienti spesso eterogenei ed esterni all'azienda; in tale situazione, le organizzazioni devono essere in grado di bilanciare i benefici associati all'utilizzo di questa specifica tecnologia con le potenziali minacce ad essa associate[5].

Il contributo dei Consigli d'Amministrazione alla cybersecurity

Vista la crescente centralità della cybersecurity nelle strategie delle aziende, si riscontra una maggiore e più significativa attenzione verso questa tematica. In passato la responsabilità era del dipartimento IT ma oggi l'argomento è sempre più discusso a livello di **Consiglio d'Amministrazione** (CdA), anche in virtù delle possibili conseguenze che un attacco cyber potrebbe generare: si pensi, ad esempio, al fallimento dell'azienda stessa a causa di danni finanziari riconducibili alla violazione dei dati.

Nel proprio ruolo di indirizzo, supervisione e monitoraggio, il CdA si trova di fronte a una serie di opportunità legate all'evoluzione tecnologica e digitale, che sono inevitabilmente accompagnate da nuove sfide e rischi connessi alla cybersecurity[6]. L'azienda nel suo complesso è consapevole del rischio che corre nel campo della cybersecurity? Sono **9 su 10** i dirigenti italiani intervistati da Deloitte che hanno dichiarato che le questioni legate alla **cybersecurity** sono **regolarmente all'ordine del giorno del loro CdA**, con cadenza settimanale (36%), mensile (30%) o trimestrale (24%).

In effetti, i CdA delle aziende desiderano essere sempre più coinvolti in questa fase di pianificazione, tanto che, come emerge dal 2023 Global Future of Cyber Survey di Deloitte, **in 3 casi su 4 il Board riceve aggiornamenti regolari** in merito allo stato dei programmi di cybersecurity. Questo modus operandi consente all'organo direttivo di essere messo nelle migliori condizioni possibili per definire le traiettorie di sviluppo di strategie future e degli investimenti e integrare quanto meglio il Risk Management nei processi aziendali quale catalizzatore della performance, sempre nel rispetto degli interessi dei propri stakeholder e del complessivo "risk appetite" dell'azienda. Non è un caso che addirittura **8 aziende su 10** tra quelle intervistate da Deloitte stiano rivedendo la **composizione del loro CdA**, così da garantire all'interno dell'assemblea un'adeguata **presenza di professionalità** con una solida base di **conoscenze tecnico-specialistiche** in grado di fare challenge allo status quo e una forte capacità d'interazione ed indirizzo nelle discussioni consiliari.



In un contesto dove le innovazioni digitali sono sempre più pervasive all'interno dell'azienda, emerge la necessità di avere – anche a livello di Governance – una conoscenza approfondita e completa delle potenzialità e dei rischi delle stesse. A tal proposito, si riscontra sempre più una presenza di Chief Information Security Officer (CISO) e/o Chief Information Officer (CIO) all'interno del CdA: questi, infatti, sono in grado di mettere a disposizione dell'azienda non solo le proprie conoscenze e competenze tecniche ma anche una differente "forma mentis", più focalizzata sulla tecnologia. Inoltre, la presenza di tali figure nel CdA va a rafforzare il messaggio che la sicurezza informatica trascende i confini del dipartimento IT e permea tutta l'azienda con un approccio top-down. Tuttavia, a questo proposito, c'è ancora strada da fare soprattutto in quei settori regolamentati, quale quello dei servizi finanziari, dove la cybersecurity è assai rilevante e le competenze specifiche nei CdA non risultano e meno frequenti in materia di IT e risk management[7].

Focus on

Digital Operation Resilience Act: Sviluppi regolamentatori della cybersecurity nel settore finanziario

La minaccia cyber è particolarmente rilevante per il settore finanziario, in ragione delle motivazioni economiche degli attaccanti, della numerosità e diversificazione dei soggetti che vi operano, della stretta interconnessione tra i diversi nodi del sistema: è molto elevata la possibilità che un malfunzionamento o un grave attacco a un singolo operatore possa trasmettersi ad altri compromettendo la stabilità del sistema finanziario, la continuità dei servizi finanziari, la sicurezza del sistema dei pagamenti e la fiducia di cittadini e aziende.

Il rapido mutamento dello scenario di mercato ha reso evidente l'importanza e la centralità di creare un quadro normativo comunitario che guidasse verso la gestione armonizzata del rischio ICT e promuovesse la resilienza operativa digitale nel settore finanziario. A tal proposito, Digital Operation Resilience Act (DORA) è la più importante iniziativa UE in materia di resilienza operativa digitale e sicurezza informatica per il settore finanziario e ha l'obiettivo di trasformare i processi di gestione dei rischi ICT dei player finanziari per sviluppare elevati livelli di resilienza ai gravi incidenti di sicurezza.

L'avvio delle consultazioni per il suo sviluppo ha avuto luogo nel Dicembre 2019 e l'atto è entrato in vigore a partire dal Gennaio 2023[11], andando ad arricchire e rafforzare ulteriormente il framework regolamentare già attualmente esistente[c]. Il framework alla base di DORA si articola in 5 elementi costitutivi (ICT Governance & Risk Management; Incident Management & Reporting; Digital Operational Resilience Testing; ICT Third-party Risk Management; ICT Threat Intelligence & Information Sharing), che prevedono un rafforzamento dei requisiti rispetto agli standard regolamentari vigenti.

Tale normativa impatta in modo trasversale ed "end-to-end" sulle aziende finanziarie richiedendone una trasformazione della governance (e.g., Top Management, funzioni di controllo, funzioni operative, business) e del modello operativo, e l'adozione di un nuovo approccio di gestione strategica del rischio. Sebbene ciò comporti per le organizzazioni dei costi di adeguamento, tale atto garantisce anche molteplici benefici, i più rilevanti dei quali includono:

- L'efficientamento e la razionalizzazione del sistema di governance dei rischi informatici e il risk reporting, rafforzando le capabilities ICT a tutti i livelli e i processi di risk reporting
- La minimizzazione degli impatti derivanti da eventi critici sulle operazioni rilevanti per il business, attraverso la predisposizione di adeguate strategie e processi di identificazione, valutazione, mitigazione e gestione dei rischi connessi e il rafforzamento dei processi di monitoraggio e segnalazione nel continuo degli incidenti ICT in ottica end-to-end
- Il maggior presidio delle componenti gestite da terze parti, attraverso la ricostruzione degli elementi chiave della catena del valore, con focus su funzioni e servizi critici, catena tecnologica e adeguati meccanismi di monitoraggio dei fornitori critici
- L'ammodernamento e l'evoluzione dell'infrastruttura, dei sistemi e degli applicativi IT attraverso soluzioni Cloud che non solo mitighino i rischi connessi all'infrastruttura IT ma anche migliorino la scalabilità delle soluzioni e la data protection
- Il potenziamento dei meccanismi di apprendimento continuo di tipo "threat intelligence", così da avere maggiore flessibilità nell'adattamento ad un contesto in continua e sempre più rapida evoluzione

[c]Sono già molteplici e diverse le iniziative regolamentari che sollecitano i player di sistema ad attivarsi per rafforzare consapevolezza, strategie e presidi organizzativi e operativi a fronte dei rischi attuali e prospettici connessi alle tecnologie e alla complessità della catena del valore. A livello comunitario si ricordano, fra gli altri: la direttiva PSD2, il Cybersecurity Act "CSA", la direttiva resilienza operativa del settore finanziario, la direttiva NIS 2, la direttiva CER, il regolamento "CRA", il TIBER-EU e il GDPR. A livello italiano, si ricordano: la Circolare n. 285/2013 (40° agg.) e il TIBER-IT.

Figura 3 | DORA: i 5 elementi costitutivi e le più importanti implicazioni

GLI ELEMENTI COSTITUTIVI DI DORA

	ICT Governance & Risk Management	Incident Management & Reporting	Digital Operational Resilience Testing	ICT Third-party Risk Management	ICT Threat Intelligence & Information Sharing
Obiettivi	Creazione di un quadro comune per **la gestione armonizzata dei rischi ICT applicabile a tutte le istituzioni finanziarie in scope**	Armonizzazione logiche di **classificazione e segnalazione degli incidenti ICT** con tempi rapidi di notifica (**entro il giorno stesso** dell'evento)	Standard armonizzati a livello UE per i **test di resilienza operativa digitale in maniera proporzionale (basic vs advanced testing)**	Coprire gli elementi contrattuali minimi per permettere un **monitoraggio completo delle terze parti ICT**	Promuovere la **consapevolezza** e la **conoscenza delle minacce ICT attraverso la condivisione di informazioni a livello di sistema**
Implicazioni	• Rafforzamento compiti e **responsabilità dell'organo di gestione** in riferimento alla gestione dei rischi ICT e cyber • Definizione di una strategia di **resilienza operativa digitale** • **Evoluzione del Framework per la gestione dei rischi informatici** che permetta l'**individuazione ex ante** dei rischi con **focus sulle «critical functions»** • **Istituzione di una Funzione di controllo di II livello per la gestione dei rischi ICT**	• Definizione e implementazione processo di **gestione degli incidenti ICT e dei c.d. 'significant cyber threat'** • Adozione di **indicatori di allarme rapido** e classificazione degli incidenti ICT su criteri prescritti • Armonizzazione **segnalazioni** (formati, modelli etc.) **all'AAVV nazionale competente degli incidenti ICT** rilevanti per il sistema finanziario e possibilità di flussi di ritorno e riscontri (c.d. Supervisory Feedback)	• Conduzione, con frequenza almeno annuale, di **test di resilienza operativa digitale** proporzionati a seconda delle dimensioni, del business e dei profili di rischio delle entità finanziarie • Conduzione, con frequenza triennale, di **test di penetrazione basati sull'analisi della minaccia - TLPT**, per le entità significative e con un livello adeguato di maturità cyber	• Armonizzazione degli standard contrattuali funzionali a consentire un adeguato **monitoraggio dei TPPs ai fini della gestione del rischio** delle diverse fasi del rapporto con il fornitore terzo • **Nuovo framework di supervisione** sui fornitori ICT «critici» (CTPPs Oversight Framework) identificati secondo criteri di rilevanza che saranno declinati dai Regulators	• Promozione dell'**Information Sharing**, tra istituzioni finanziarie per la condivisione di informazioni e dati a livello di sistema, come elemento chiave per rafforzare la **prevenzione e risposta alle minacce connesse al continuo evolversi del contesto**
Tempi	**Grace period di 2 anni per adeguarsi** ai nuovi standard regolamentari	**Grace period di 2 anni per adeguarsi** ai nuovi standard regolamentari	**Grace period di 3 anni per adeguarsi** ai nuovi standard regolamentari	**Grace period di 2 anni per adeguarsi** ai nuovi standard regolamentari	**In attesa di indicazioni** da parte del Regolatore sui meccanismi di attuazione

L'importanza di adottare un nuovo approccio strategico e integrato alla cybersecurity

I benefici di una strategia di una cybersecurity di successo

Le aziende italiane, intervistate nella 2023 Global Future of Cyber Survey, considerano il **contributo della cybersecurity** come fondamentale per assicurare e proteggere la **"brand reputation" (92%)** e preservare il più possibile la **fiducia** dei clienti **(92%)**, soprattutto con un esplicito riferimento alla **"digital trust"[8d] (80%)** e alla **"tech integrity" (78%)**.

Accanto a queste considerazioni, il campione intervistato enfatizza anche l'importanza della cybersecurity a supporto di un modello di business fondato sui concetti di **"resilienza" (82%)** e **"agilità" (80%)**, che si caratterizzi per una forte propensione al cambiamento proattivo e talvolta radicale di fronte ad eventi potenzialmente avversi o imprevisti[9].

Questo scenario è coerente con il nuovo approccio delle aziende italiane alla cybersecurity, che si ritiene possa generare **valore non solo in termini di crescita dei ricavi**, come indicato dal **78%** dei rispondenti, ma anche attraverso diversi elementi che, direttamente o indirettamente, possono contribuire a ottimizzare i margini nel lungo periodo.

Figura 4 | Contributo positivo atteso della cybersecurity

D: Su una scala da 1 (per nulla) a 4 (in larga misura), quanto le iniziative di cybersecurity della sua organizzazione hanno dato un contribut
nelle seguenti aree?
Deloitte, 2023.

[d] *Per "digital trust" si intende la fiducia delle persone nella capacità dell'organizzazione di gestire i dati in modo sicuro e responsabile all'interno dell'ambiente digitale.*

Integrare la cybersecurity nella strategia aziendale per realizzare le priorità di business

Nel panorama moderno, la cybersecurity acquisisce un **valore più elevato**, passando dall'essere considerata una pura ed efficace risposta alle minacce informatiche al diventare un **vero e proprio fattore abilitante** per il raggiungimento degli obiettivi aziendali.

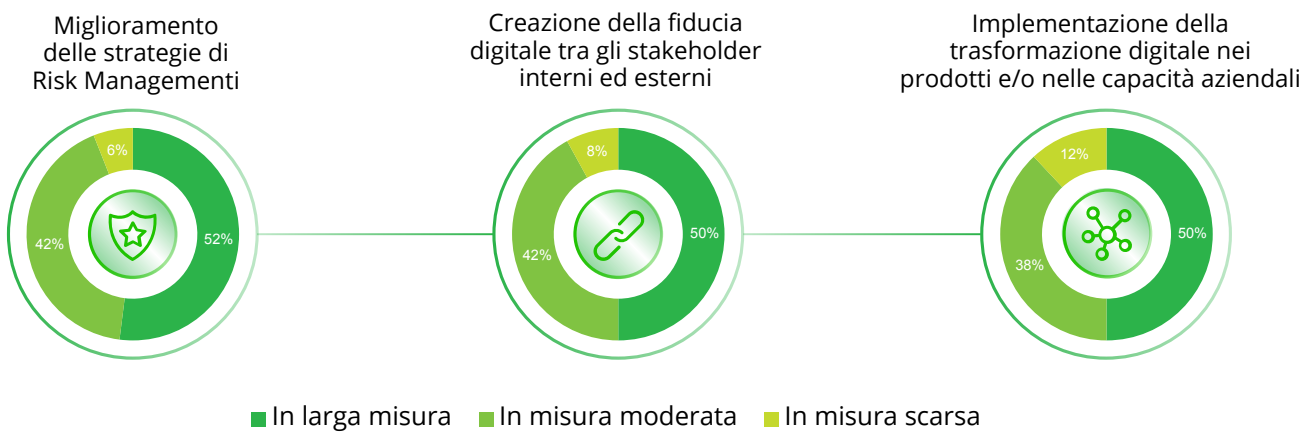
La cybersecurity, infatti, diventa una grande occasione per **esplorare in modo sicuro nuove opportunità di business** un tempo considerate rischiose. Tuttavia, per sfruttare appieno il suo potenziale, la cybersecurity deve essere integrata nella più ampia strategia di business. Infatti, è solo se inserita all'interno della pianificazione aziendale e opportunamente supportata in termini di risorse e competenze che la cybersecurity consente alle aziende di beneficare di nuove opportunità di crescita e sviluppo.

Secondo le organizzazioni italiane intervistate nella 2023 Global Future of Cyber Survey di Deloitte, seguire un **approccio strategico e integrato alla cybersecurity** consente di **migliorare l'efficienza** nella gestione delle **priorità di business (62%)**, in termini di strategie di:

- **Risk management**, poiché le aziende, integrando la cybersecurity nella strategia dell'organizzazione, possono mitigare i rischi di natura informatica, contribuendo al potenziamento della gestione del rischio complessivo a cui esse sono esposte **(94%)**.
- Creazione di **digital trust**, poiché le aziende, considerando la cybersecurity come un investimento prioritario, migliorano la propria immagine e preservano il rapporto di fiducia con tutti gli stakeholder, rafforzando il loro senso di fiducia nei confronti di una gestione sicura e responsabile dei dati nell'ambiente digitale **(92%)**.
- **Trasformazione digitale**, poiché le aziende, integrando la cybersecurity con la strategia aziendale, possono intraprendere percorsi di digitalizzazione con una maggiore sicurezza, confidando nella loro maggiore capacità di proteggere gli asset materiali e immateriali e di prevenire i rischi associati che potrebbero danneggiare l'organizzazione, i dipendenti e i clienti **(88%)**.

Oltre a migliorare l'efficienza nella gestione delle priorità di business, le aziende intervistate dichiarano che un approccio strategico e integrato alla cybersecurity affina la capacità delle organizzazioni di **anticipare l'identificazione dei rischi (54%)**, di **prendere decisioni in modo rapido e agile (48%)** e di **adattarsi prontamente** all'evoluzione del contesto competitivo **(46%)**. Questo risulta coerente con quanto evidenziato in precedenza circa l'importanza della cybersecurity nel supportare l'adozione di un modello di business resiliente e agile, che sia in grado di garantire la creazione di valore anche in un contesto di elevata incertezza.

Figura 5 | Principali benefici di un approccio strategico e integrato alla cybersecurity



D: Su una scala da 1 (per nulla) a 4 (in larga misura), quanto l'adozione di un approccio strategico e integrato alla cybersecurity consente di raggiungere con successo le seguenti priorità di business?
Deloitte, 2023.

Tra strategia e operatività: la risposta delle aziende italiane all'esigenza di integrare la cybersecurity nella strategia di business

La fase di pianificazione strategica della cybersecurity

La cybersecurity è una sfida complessa per le organizzazioni e non può essere improvvisata; al contrario, vista anche la sua crescente centralità nelle strategie di business, richiede un'attenta **pianificazione strategica** della stessa e delle attività ad essa riconducibili: secondo Deloitte, sono **8 su 10** le aziende italiane che **rivedono e aggiornano i propri piani di cybersecurity su base annua**. Sono, di solito, i CISO o i CIO, vista la propria competenza, a guidare e svolgere questo tipo di attività al fine di garantire la massima protezione degli asset aziendali e la mitigazione dei rischi cyber in un contesto altamente mutevole sia per quanto riguarda il tipo di minacce da fronteggiare sia per l'evoluzione degli aspetti normativi.

Affinché una strategia di cybersecurity risulti essere efficiente ed efficace, non deve solo essere propriamente pensata e disegnata, coerentemente con le proprie priorità di business, ma deve poi essere **implementata**. Questo richiede la predisposizione di idonei budget e piani operativi da parte delle aziende. Al fine di guidare le decisioni di investimento, i CISO sono soliti condurre analisi di vario tipo. Le aziende italiane rispondenti, ad esempio, misurano il ritorno degli investimenti in cybersecurity utilizzando sia **strumenti quantitativi per la valutazione del rischio**[e] **(88%)**, sia metodi **qualitativi**[f] **(72%)**. **Oltre 8 organizzazioni su 10** dichiarano di svolgere anche un **assesment complessivo della maturità** della propria azienda in termini di cybersecurity. Questa maturità, in molti casi, viene analizzata anche in relazione a quella dei principali competitor attraverso **attività di benchmarking**, come indicato da oltre **7 organizzazioni su 10**. Oltre alle analisi e alle valutazioni sopracitate, l'**84%** del campione intervistato dichiara che, durante la fase di pianificazione degli investimenti cyber, si premura di utilizzare tecniche di **"analisi di scenario"** (Fire Drill, Table Top Exercise)[10] , attraverso cui testare e valutare la reale adeguatezza ed efficacia dei piani esistenti, nonché la capacità e la reattività delle aziende di reagire di fronte a inattesi eventi di disruption informatica.

[e]Si pensi ai metodi basati sulla statistica bayesiana, fra gli altri i modelli FAIR (Factor Analysis of Information Risk) e CIS RAM (Center for Internet Security Risk Assessment Method).
[f]Ad esempio, le matrici di valutazione del rischio bidimensionale.

Le attività chiave in ambito cybersecurity

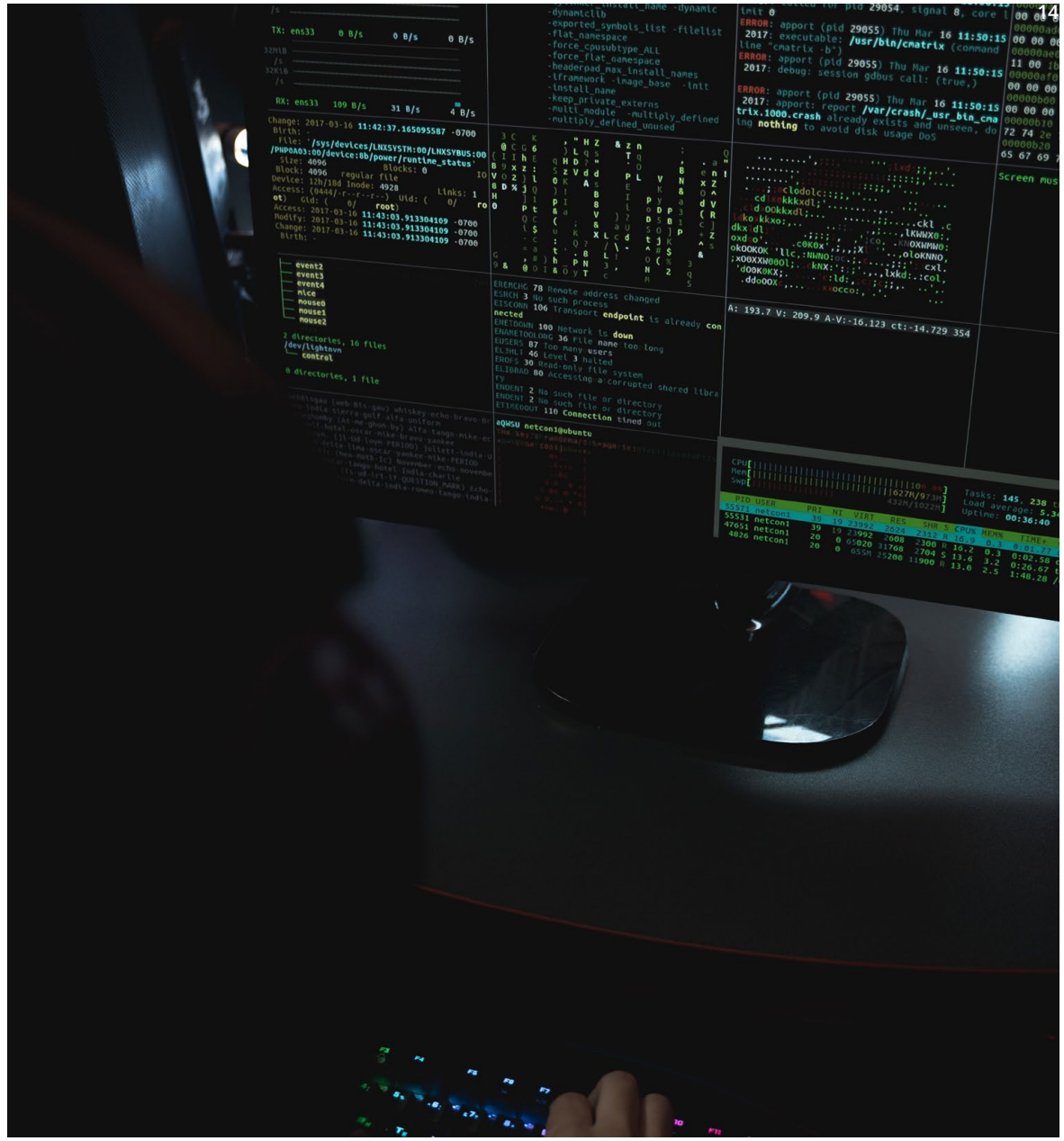
Una volta definita la strategia cyber, le organizzazioni devono poi implementarla attraverso la predisposizione di un **dettagliato piano operativo**.

La quasi totalità delle aziende italiane **(94%)**, incluse nella 2023 Global Future of Cyber Survey, ha già definito o sta definendo un **piano olistico per la protezione da minacce cyber** e riferisce di aver già in essere anche un piano ad hoc d'intervento, aggiornato e testato con frequenza annuale, per rispondere a possibili attacchi informatici di varia natura.

Le imprese italiane intervistate da Deloitte affermano di sviluppare e implementare piani operativi che **valutano le modalità di protezione dai rischi cyber in ogni fase della gestione del trattamento di dati sensibili (96%)** e che favoriscono il **continuo miglioramento della "cyber hygiene"** dell'organizzazione **(90%)**. Accanto a questi, si registra anche un crescente interesse, confermato dal **82%** del campione intervistato, per l'**acquisto di prodotti assicurativi** in grado di coprire i danni diretti e indiretti derivanti da un attacco cyber ai sistemi aziendali.

Considerata la natura stessa della cybersecurity, ogni valutazione operativa relativa alla cybersecurity deve **andare oltre i meri confini aziendali**, includendo la **più ampia rete di stakeholder** con cui ciascuna organizzazione si relaziona nello svolgimento delle sue attività.
A tal proposito:

- il **92%** delle aziende consultate dichiara che i propri programmi di valutazione del rischio cyber includono già, o lo faranno presto, il **monitoraggio della "security posture" di partner e fornitori**.
- **Circa 9 organizzazioni su 10** collezionano regolarmente le preferenze dei propri clienti rispetto ai temi di privacy e protezione dei dati sensibili attraverso **programmi di "voice of the customer"**.



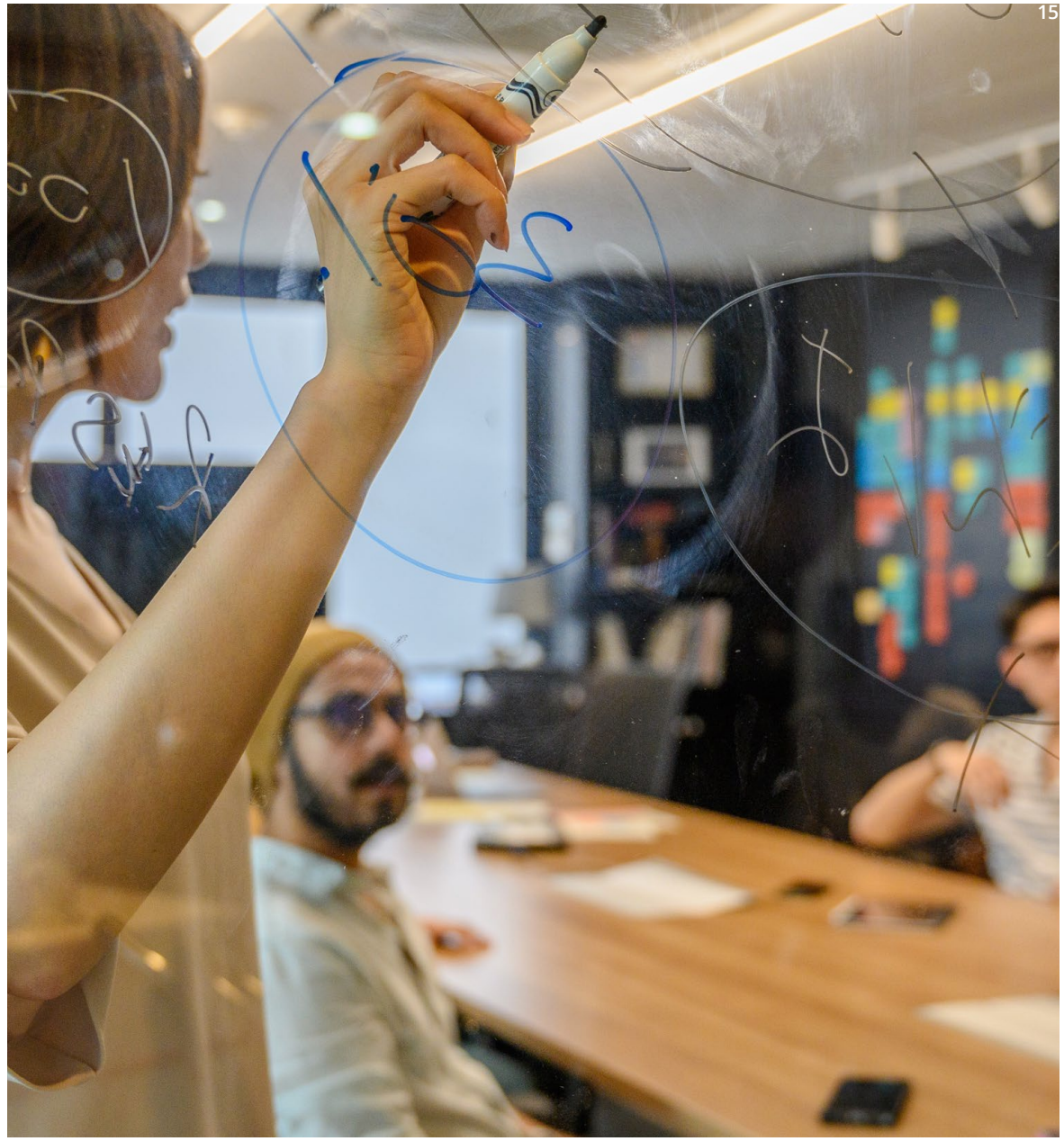
Coinvolgere, sviluppare e trattenere i talenti in ambito cybersecurity

Nel contesto odierno, occorre prestare grande attenzione al tema della **formazione delle professionalità qualificate** nel campo della cybersecurity. Avere un team competente, esperto e focalizzato sul tema della sicurezza cyber, è un prerequisito fondamentale per affrontare con successo le sfide a cui le organizzazioni sono esposte.

La **mancanza di talenti** in questa area, riconosciuta da **4 leader italiani su 10 intervistati**, è una delle **questioni più complesse da risolvere**, richiedendo lo sforzo e la collaborazione di un ampio ecosistema di attori nel pubblico e nel privato.

Da un lato, le aziende possono ovviare a tale criticità **guardando oltre i profili tradizionali** dei potenziali dipendenti. La cybersecurity, pur richiedendo profili altamente tecnici, può **includere anche molti ruoli non tecnici**: i migliori team di cybersecurity sono spesso costituiti da un mix di persone con competenze trasversali, opportunamente formati. Riconoscere questo aspetto può ampliare notevolmente il bacino di talenti per un'organizzazione e rendere molto più semplice il loro reclutamento[12]. Si pensi, ad esempio, a profili come il "customer experience designer", che potrebbe apportare intuizioni alle iniziative cyber identificando potenziali vulnerabilità nei processi di raccolta di dati o tutela della privacy.

D'altro canto, la quasi totalità delle aziende italiane intervistate riconosce che **formare le proprie risorse è più che mai cruciale** per affrontare la sfida della cybersecurity e dichiara di aver **già implementato** dei **programmi a riguardo (92%)**. La formazione è sicuramente un potente strumento, che le imprese devono utilizzare, per minimizzare la propria esposizione al rischio cyber. Affinché sia efficace, però, le organizzazioni devono garantire che tale formazione sia **erogata in modo continuativo**, sia **sempre aggiornata** rispetto agli sviluppi del mercato, sia **coerente al "risk appetite"**

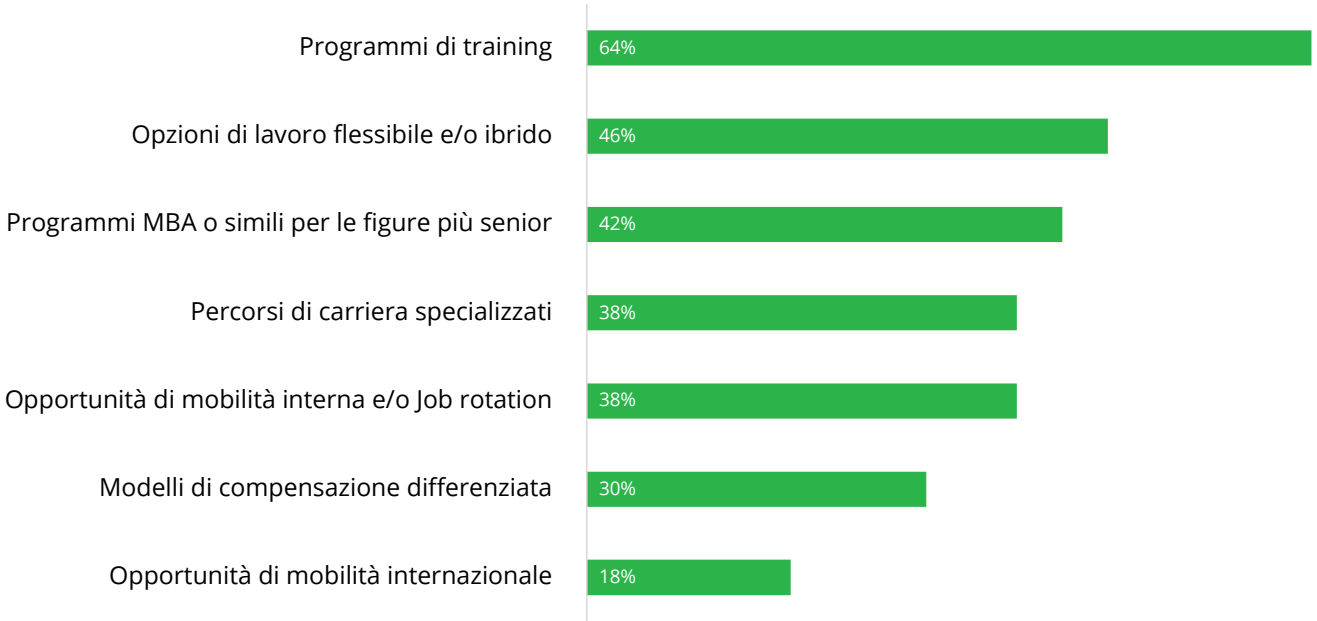


dell'azienda e offra **percorsi differenziati e personalizzati**. I programmi di formazione sono sì utili per dotare le aziende delle giuste competenze, ma sono anche uno dei principali strumenti per **coinvolgere**, **trattenere** e **sviluppare i talenti**, come indicato da **circa 2 aziende italiane su 3**.

Al fine di completare il proprio organico, oltre all'offrire percorsi di training, le organizzazioni italiane hanno indicato, nell'ambito della 2023 Global Future of Cyber Survey di Deloitte, di puntare sul **work-life balance** con modalità di lavoro più flessibili **(46%)**, e sull'offerta di una molteplicità di opportunità di crescita e sviluppo del potenziale attraverso **programmi di formazione di alto profilo (42%)**, **percorsi di carriera specializzati (38%)** e programmi di **mobilità interna (38%)**. Accanto a queste strategie, poi, circa un terzo delle aziende intervistate cerca di implementare **modelli di retribuzione differenziati (30%)**[8].

In una professione tradizionalmente considerata poco dinamica e con contenute opportunità di carriera, una possibilità per trattenere i talenti è quella di offrire loro **nuove opportunità di lavoro in tempi sempre più brevi**, anche all'estero. Ciò mantiene i dipendenti coinvolti e permette loro di continuare a sviluppare nuove competenze, migliorando la soddisfazione sul lavoro e la fedeltà all'azienda. Combinando questa tattica con la flessibilità del lavoro, un maggiore equilibrio tra lavoro e vita privata, la formazione e una retribuzione competitiva, è possibile gettare le basi per affrontare la sfida della carenza di talenti[13].

Figura 6 | Strategie per sviluppare i talenti in ambito cybersecurity



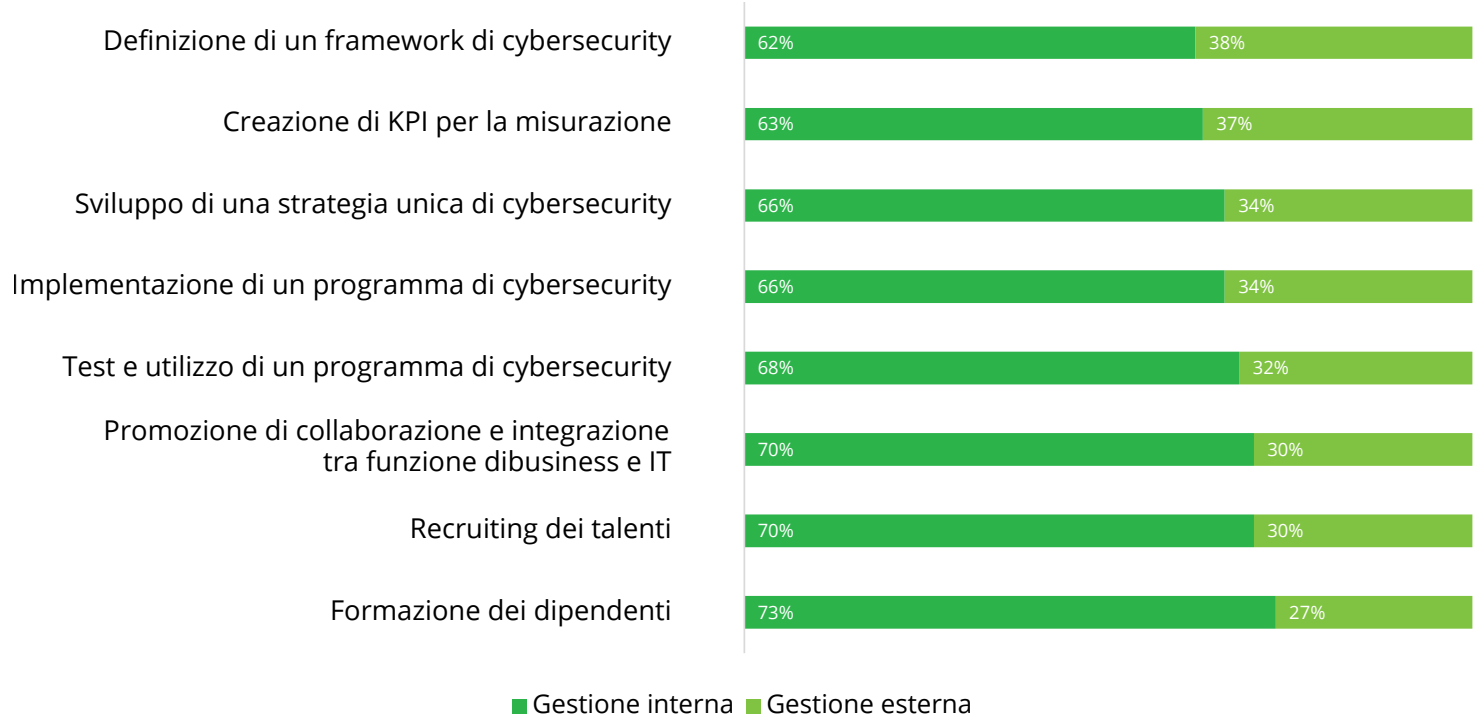
D: Considerando il contesto altamente competitivo per i talenti della cybersecurity, quali strategie vengono valutate dalla sua organizzazione per coinvolgere, trattenere e sviluppare i propri dipendenti?
Deloitte, 2023.

[8]Tali modelli possono includere, ad esempio, programmi di retribuzione variabile che comprendono: una "skill-based premium pay", utilizzato principalmente per reclutare e trattenere i talenti IT con competenze altamente richieste; un "signing bonus", finalizzato a incentivare un candidato ad accettare un'offerta di lavoro; un "retention bonus", impiegato per incoraggiare i talenti IT con competenze critiche a rimanere nell'organizzazione per un periodo specifico, ad esempio durante un'importante iniziativa di trasformazione digitale.

Implementare un ecosistema diversificato di strumenti e servizi a supporto della cybersecurity

Le aziende italiane intervistate, in relazione alle questioni strategiche in materia di cybersecurity, si dimostrano più inclini a internalizzare i propri processi operativi. Tuttavia, dalla 2023 Global Future of Cyber Survey di Deloitte emerge una **tendenza ad affidare parte della responsabilità** delle iniziative strategiche **a terze parti**, che si riscontra in tutte le aree indagate: **più di un quarto** di ciascuna attività (con punte fino al 38%), infatti, viene gestita da partner esterni.

Figura 7 | La responsabilità dei servizi di cybersecurity



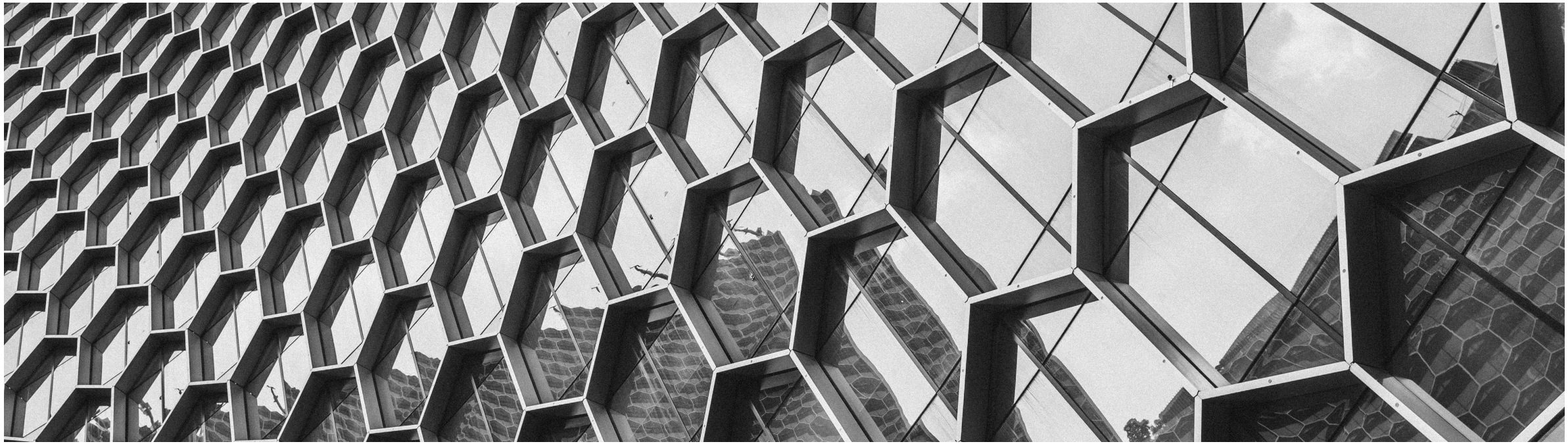
D: Quale percentuale di ciascuna delle seguenti attività, facenti parte di una strategia di cybersecurity viene gestita dalla sua organizzazione e quale è, invece, affidata a partner esterni? Deloitte, 2023.

Le organizzazioni italiane, quindi, denotano un certo grado di consapevolezza circa l'importanza di **creare un ecosistema di partner** per lo sviluppo e l'accesso a **strumenti e tecnologie di cybersecurity** che supportino la generazione di valore nel medio-lungo termine. In particolare, i servizi cyber più ricercati, secondo quanto riportato dai rispondenti allo studio, riguardano l'ambito del **Cloud Computing (80%)**. Ne sono un esempio i servizi di **Identity & Access management** (IAM) o di **Threat and incident response**.

Altri servizi di terze parti di cui oltre **7 aziende italiane su 10** si servono sono poi quelli di **Infrastructure security**, per garantire la sicurezza dell'intera infrastruttura IT e la tech-resiliency dell'organizzazione, e di **Application security**, per assicurare la massima sicurezza nelle fasi di progettazione, sviluppo e implementazione delle varie applicazioni.

A ulteriore dimostrazione di questa crescente sensibilità nei confronti dell'outsourcing, i leader aziendali intervistati prevedono che il **numero medio di fornitori di servizi cyber** utilizzati **aumenterà** nei prossimi due anni del **33%**, passando **da 6 a 8**

Per sfruttare il valore che i partner possono apportare, le organizzazioni devono però considerare come gestire la crescita e la complessità intrinseca dei loro ecosistemi di servizi. Se da un lato l'implementazione di strumenti e servizi aumenta la capacità delle organizzazioni di affrontare le minacce alla cybersecurity, dall'altro crea la **necessità di una forte pianificazione**, **gestione** e **operatività dell'ecosistema**. La **collaborazione con più fornitori** presenta una serie di **esigenze complesse**, che potrebbero potenzialmente aprire la strada a **nuovi rischi cyber**.



Conclusione

All'interno delle organizzazioni italiane si sta diffondendo una **nuova cultura** che considera la **sicurezza** e la **protezione dei dati** come un **fulcro** attorno al quale **ruota il loro stesso futuro**.

Nella realtà odierna, secondo la 2023 Global Future of Cyber Survey, dotarsi di una adeguata strategia di cybersecurity non è più visto come un'opzione tra cui le aziende possono scegliere o un insieme di pratiche di "igiene informatica" incentrate sulla tecnologia; piuttosto, **la sicurezza informatica trascende le sue tradizionali radici IT** e viene considerata come un'area funzionale distinta ed essenziale per la realizzazione dei risultati dell'azienda. Pertanto, oggi non rappresenta più un pro o un contro del modo in cui l'organizzazione svolge il proprio business; **la cybersecurity, piuttosto, "è" il business** e una conversazione sul futuro del cyber diventa una conversazione sul futuro dell'azienda.

Oggi, **sviluppare una visione "cyber-first"** – vale a dire, incorporare il pensiero, la pianificazione e l'azione in ambito cyber in tutte le iniziative aziendali – **è imperativo** per tutte le attività aziendali: nell'intraprendere nuove iniziative di trasformazione digitale, nello sviluppare nuovi prodotti e servizi, nel coinvolgere terze parti nel proprio ecosistema e nel fornire nuovi strumenti ai propri dipendenti. Diffondere questo nuovo modo di pensare nell'intera organizzazione consente di **favorire l'adozione di un approccio strategico e integrato alla cybersecurity** tale da determinare il successo di tutte le iniziative aziendali e il raggiungimento degli obiettivi di business in contesti sempre più mutevoli.

Per realizzare questa prospettiva, Deloitte raccomanda che le aziende agiscano lungo le seguenti direttrici:

- Promuovere un **impegno multidirezionale** che includa il **coinvolgimento dell'intera organizzazione** nelle iniziative di cybersecurity. In ogni azienda, infatti, il futuro della cybersecurity sarà determinato dall'impegno della C-suite e del CdA sul tema. In particolare, se maggiormente coinvolto, il Board può anticipare possibili conseguenze degli attacchi cyber e stimolare l'opportuno aggiornamento dei processi aziendali, assicurandosi di contribuire in modo significativo alla crescita dell'azienda, ponendo in primo piano la necessità di agire in modo conforme e sicuro.
- Sviluppare e implementare un **approccio di tipo zero-trust** rispetto alla cybersecurity, che rafforzi la sicurezza degli ambienti aziendali digitali, semplificandone anche la gestione, e migliori l'esperienza dell'utente finale. Il percorso verso lo zero-trust richiede una strategia allineata ai risultati di business, oltre a un impegno e a una pianificazione significativi, che comprendono la risoluzione di problemi informatici fondamentali, l'automazione dei processi manuali e la programmazione di cambiamenti radicali nell'organizzazione della sicurezza, nel panorama tecnologico e nell'azienda stessa.
- Implementare una **solida pianificazione** al fine di formulare strategie di cybersecurity in grado di mitigare efficacemente i rischi e generare valore aziendale. Questi piani possono includere, l'uso di strumenti di

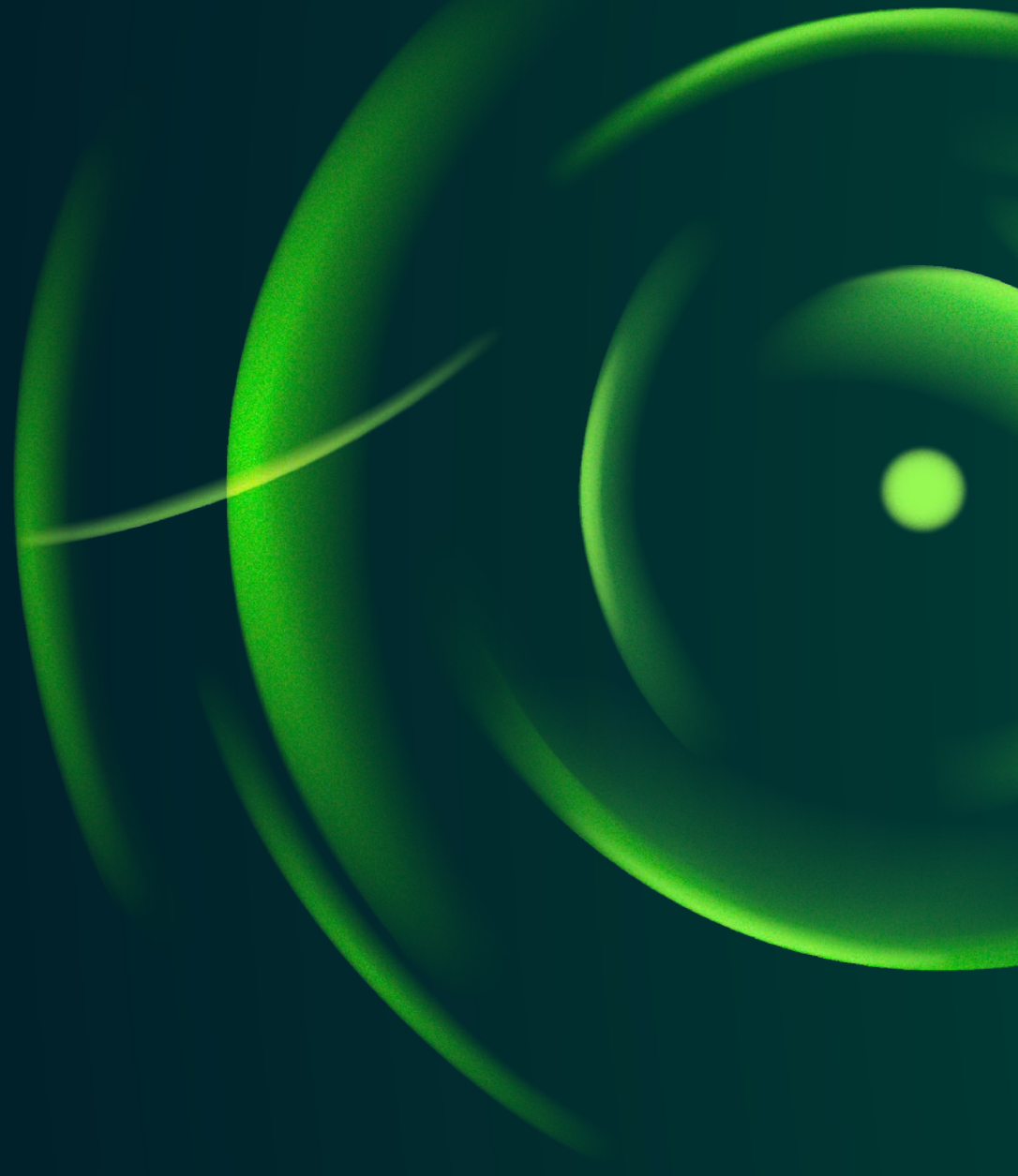
quantificazione del rischio per misurare e garantire il ROI delle iniziative di cybersecurity o valutazioni della maturità della cybersecurity stessa per meglio guidare le decisioni di investimento future.

- Riconoscere la **centralità della cybersecurity per le innovazioni tecnologiche a supporto della trasformazione digitale**. Se da un lato la loro adozione è essenziale per garantire l'agilità operativa e il successo aziendale, dall'altro è fondamentale tenere conto dei significativi rischi informatici che ciascuna di esse comporta.

- Sviluppare un'efficace **strategia di gestione dei talenti in ambito cyber**. Questo richiede alle aziende di dedicare tempo e risorse al recruiting dei talenti ma anche alla loro formazione e allo sviluppo della carriera. Investire nel talento è necessario per far fronte all'attuale carenza di professionalità qualificate e dotare l'organizzazione delle competenze necessarie per gestire le iniziative di cybersecurity, sempre più centrali per il successo e la generazione di valore. Affinché ciò possa risultare efficace, è opportuno che le aziende abbiano ben chiari quali sono i ruoli e le competenze più rilevanti in grado di garantire una consistente riduzione del complessivo rischio cyber a cui è esposta.

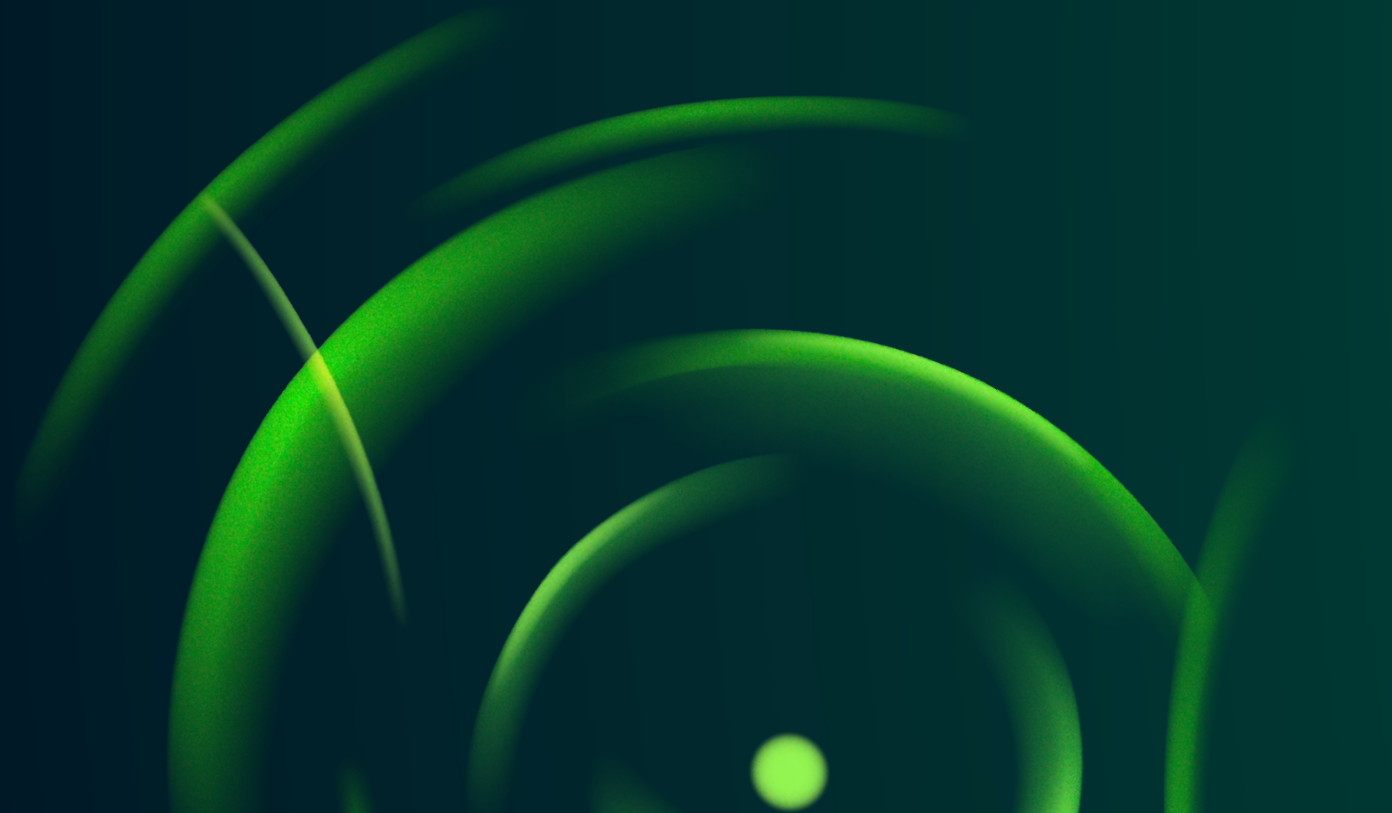
- Aprirsi alle potenzialità di un **ecosistema di partner** in grado di dare supporto nella pianificazione e implementazione di iniziative cyber a tutti i livelli. Nel contesto attuale, è sempre più importante che le organizzazioni pianifichino e gestiscano attentamente tale ecosistema, valutando come, quando e quanto esternalizzare bilanciando le sfide, anche cyber, che ciò comporta.

In un mondo sempre connesso, avere delle **strategie cyber solide** può ottimizzare l'utilizzo delle **nuove soluzioni tecnologiche** e garantire una s**icurezza maggiore** e un **più agevole mantenimento della fiducia** con tutti i propri stakeholder. In questo contesto, la necessità di una strategia informatica risk-based, che abbracci l'insieme di strategie, soluzioni e controlli informatici dell'organizzazione, è sempre più importante per il futuro della cybersecurity. Ma l'adozione di questa prospettiva va al di là dell'implementazione tecnologica; si tratta di una **vera e propria trasformazione aziendale e culturale**.



Metodologia

I dati presentati in questo report fanno riferimento alla “2023 Global Future of Cyber Survey” di Deloitte. L’obiettivo della ricerca è stato quello di definire la situazione attuale e le prospettive future della cybersecurity secondo il punto di vista delle aziende. Il campione analizzato si compone di oltre 1.000 responsabili aziendali (Proprietari/Presidenti, C-Level, Responsabili di Business Unit), provenienti da organizzazioni con almeno 1.000 dipendenti e 500 milioni di dollari di fatturato annuo. Per l’Italia sono state intervistate 50 aziende.



Contatti

Matthew Holt
Partner
DCM Cyber Strategy and Transformation Leader
Deloitte Risk Advisory
maholt@deloitte.it

Fabio Bonanni
Partner
DCM Cyber Digital Identity & Apps Leader,
Deloitte Risk Advisory
fbonanni@deloitte.it

Tommaso Stranieri
Partner
DCM Cyber Data & Privacy Leader,
Deloitte Risk Advisory
tstranieri@deloitte.it

Fabio Battelli
Partner
DCM Cyber Cloud & Infrastructure Leader,
Deloitte Risk Advisory
fbattelli@deloitte.it

Manuel Allara
Partner
DCM Cyber Detect & Respond Leader,
Deloitte Risk Advisory
mallara@deloitte.it

Research & Editorial

Luca Bonacina
Manager
DCM Growth
lbonacina@deloitte.it

Alberto Andria
Junior Specialist
DCM Growth
aandria@deloitte.it

Bibliografia

1 **Cisco**, *Data Transparency's Essential Role in Building Customer Trust*, 2022.
2 **Deloitte Insights**, *Can you measure trust within your organization?*, 9 Febbraio 2022.
3 **Deloitte HX** *TrustID survey*, May 2020.
4 **IBM**, *Cost of Data Breach 2022*, Luglio 2022.
5 **Deloitte**, *Closing the cloud strategy, technology, and innovation gap | Deloitte US Future of Cloud Survey Report*, 2022.
6 **Deloitte**, *The Board of the Future – Le sfide del Board nel definire l'evoluzione della Governance del futuro*, 2022.
7 **Banca d'Italia**, *Orientamenti della Banca d'Italia sulla composizione e sul funzionamento dei consigli di amministrazione delle LSI*, 29 Novembre 2022.
8 **Deloitte Insights**, *Digital Trust for the Future: Building cyber-security strategies for a trusted, digital future*, 18 Agosto 2021.
9 **Ahir H., Bloom N., and Furceri D.**, *World Uncertainty Index,* 2023.
10 **Harvard Business Review**, *Cyberattacks Are Inevitable. Is Your Company Prepared?*, 9 Marzo 2021.
11 **Gazzetta Ufficiale dell'Unione Europea**, *Regolamento (Ue) 2022/2554 Del Parlamento Europeo E Del Consiglio*, 14 Dicembre 2022.
12 **Deloitte**, *Finding cybersecurity talent in an altered world*, Febbraio 2023.
13 Ibidem

Deloitte.