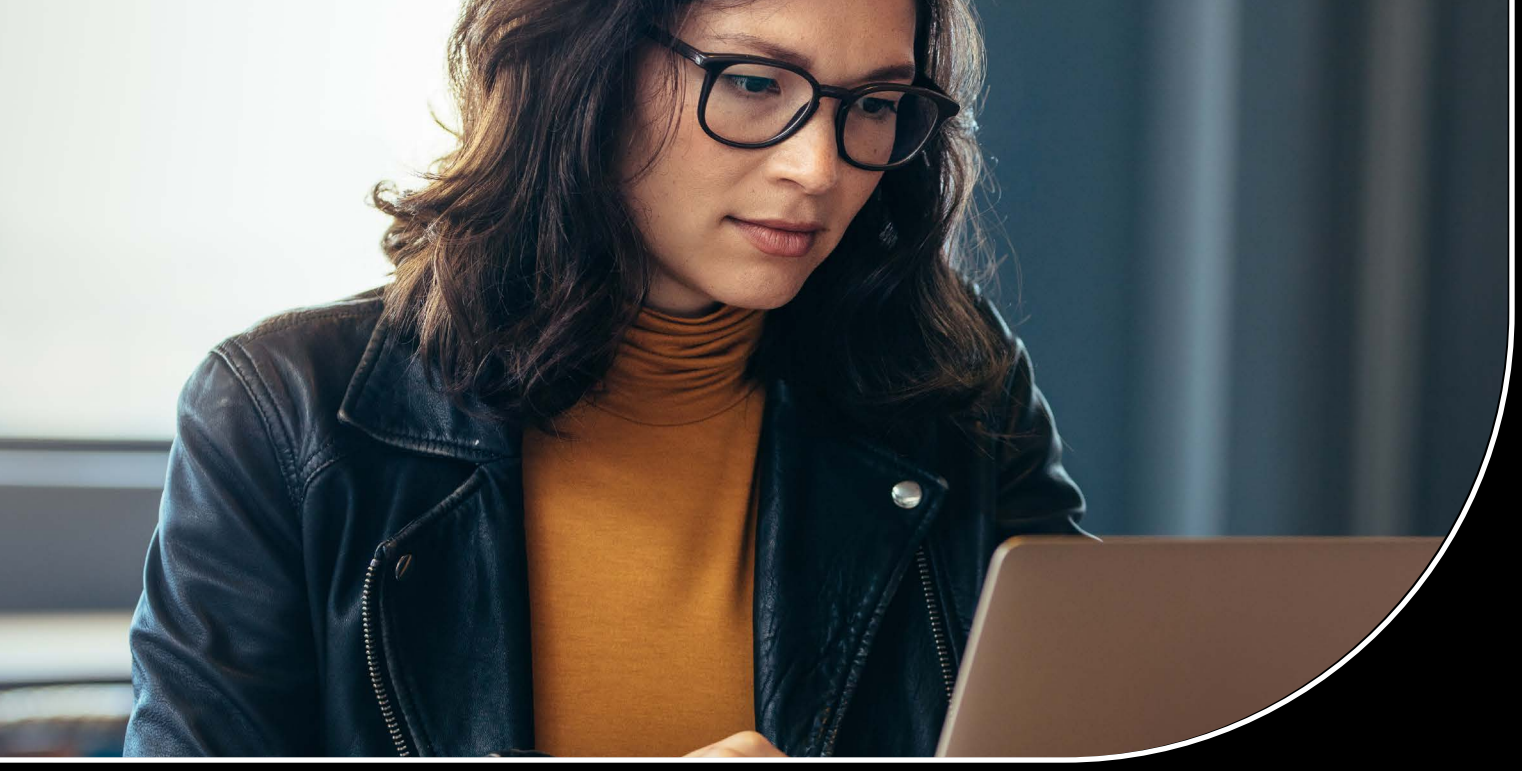
pwc

Playbook
per il Top Management:

La sicurezza come epicentro dell'innovazione

Global Digital Trust Insights 2024



La sicurezza come epicentro dell'innovazione: non è il mondo in cui viviamo oggi, ma se lo fosse?

Nonostante l'entusiasmo e lo stanziamento di budget sui programmi di sicurezza all'avanguardia, il progresso effettivo è lento, se non stagnante.

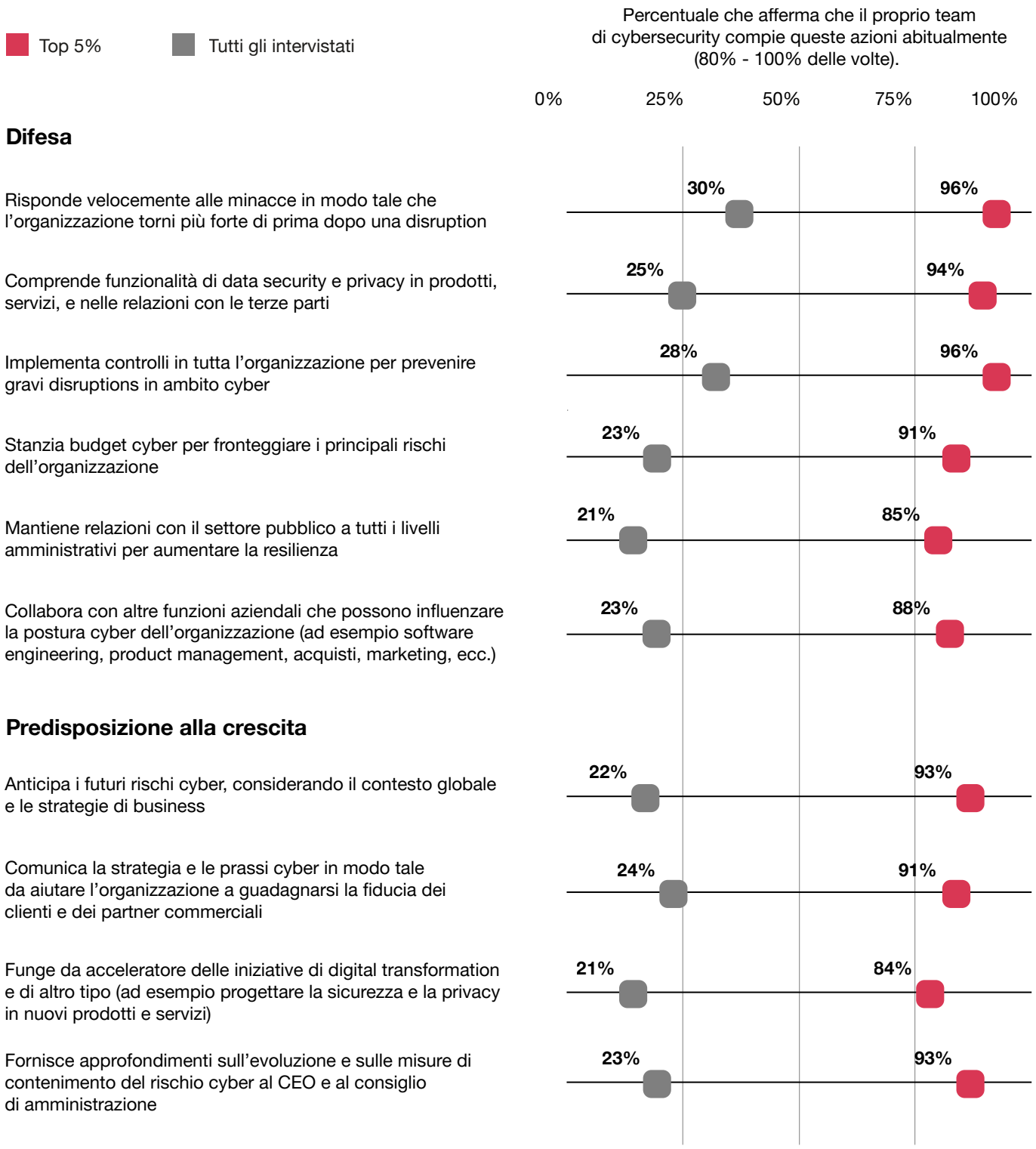
Il sondaggio di PwC "Global Digital Trust Insights 2024", che ha visto il coinvolgimento di 3.876 executives (tra business e tech) delle più grandi organizzazioni globali – il 30% dei quali detiene un fatturato da oltre 10 miliardi di dollari – suggerisce che vi sia un considerevole margine di miglioramento per quanto riguarda la cybersecurity.

Secondo i risultati, sia i costi delle violazioni che il numero di violazioni costose per le organizzazioni continuano ad aumentare incessantemente. Sebbene gli attacchi al cloud siano la principale preoccupazione in ambito cyber, circa un terzo delle organizzazioni non ha un piano di risk management per indirizzare i rischi provenienti dai fornitori di servizi cloud. Solo la metà è "molto soddisfatta" delle proprie capacità tecnologiche nei settori chiave della cybersecurity. Oltre il 30% delle organizzazioni non segue in maniera sistematica quelle che dovrebbero essere le prassi standard di cyber defence.

Immaginate un mondo in cui la sicurezza è l'epicentro dell'innovazione – il campo in cui fioriscono idee brillanti e ambizioni audaci. Immaginate il CISO impegnato a proteggere le grandi ambizioni e le risorse più preziose dell'organizzazione.

Abbiamo individuato 179 intervistati che sembrano fare esattamente questo. Il 5% degli intervistati – i nostri custodi della digital trust – stanno cogliendo opportunità che ad altri sfuggono. Loro registrano meno violazioni, e, quelle che si verificano, non sono eccessivamente onerose. Gestire il rischio è più facile perché loro hanno semplificato le soluzioni di sicurezza. Inoltre, si sono preparati per una maggiore produttività e per una crescita più rapida, superando la concorrenza, mentre esplorano e adottano nuove tecnologie con la certezza di essere adeguatamente protetti.

Conosci i nostri custodi della digital trust



Q26. Indicate quanto costantemente il team di cybersecurity della vostra organizzazione svolge le seguenti attività.
Base: All respondents= 3876
Source: PwC, 2024 Global Digital Trust Insights.

Con la tecnologia ormai al centro delle attività di business, salvaguardarla equivale a proteggere l'intera organizzazione. Ecco perché nel 2023, PwC ha creato un playbook per il Top Management per aiutare ogni singolo executive a focalizzarsi sui temi ai quali deve rispondere con il proprio CISO.

Abbiamo aggiornato il Playbook per il 2024. Questo sarà probabilmente un anno cruciale. La cybersecurity sta affrontando 4 importanti cambiamenti, ognuno dei quali potrebbe introdurre innovazioni significative.

- La volontà del Top Management di modernizzare, migliorare e investire in tecnologie e strumenti cyber in un anno di incertezza macroeconomica e spending review.
- L'aumento di minacce cyber di natura ibrida e l'assottigliamento del confine tra spionaggio e cybercrime, rendendo la cyber defence una questione di sicurezza nazionale.
- Una nuova tecnologia rivoluzionaria – IA Generativa – che porta con sé nuove minacce ma anche opportunità senza precedenti per la difesa.
- Normative che richiedono chiarezza sugli incidenti cyber e sulle prassi di risk management che potrebbero inaugurare una nuova era di trasparenza e collaborazione.

Le imprese si stanno reinventando. I legislatori stanno pensando a nuovi approcci normativi. I vostri executive sono altrettanto innovativi nel modo in cui proteggono le loro organizzazioni? Quanto siete audaci e cosa potreste fare di diverso?

9 gradi di separazione: Top performers VS gli altri

I top 5% sono:

6 volte più propensi ad implementare iniziative trasformative di cybersecurity dalle quali trarre benefici.

5 volte più propensi ad essere soddisfatti dello stato attuale delle proprie capacità tecnologiche informatiche.

4 volte più propensi ad avere un continuo aggiornamento del proprio risk management plan per mitigare i rischi legati al cloud.

9 volte più propensi ad essere maturi in ambito resilienza informatica.

Source: PwC, 2024 Global Digital Trust Insights.

I top 5% sono più propensi a:

Investire maggiormente nel cyber budget, con **l'85% degli intervistati che ha intenzione di aumentare il proprio cyber budget nel 2024** (vs il 79% totale), di cui il 19% ha intenzione di aumentarlo del 15% o più, rispetto al 10% complessivo.

Affermare che la **violazione cyber più dannosa** degli ultimi tre anni gli è costata meno di 100.000$ (28% vs 19% del totale).

Concordare fermamente che la loro **organizzazione svilupperà nuove linee di business utilizzando l'IA Generativa (GenAI)** (49% contro il 33% del totale).

Pianificare l'implementazione di strumenti GenAI per la cyber defence (44% contro il 27% del totale).

Essere in disaccordo sul fatto che la GenAI porterà ad attacchi cyber catastrofici (33% vs 22% del totale).

Cyber risk management: Pronti a reinventarsi

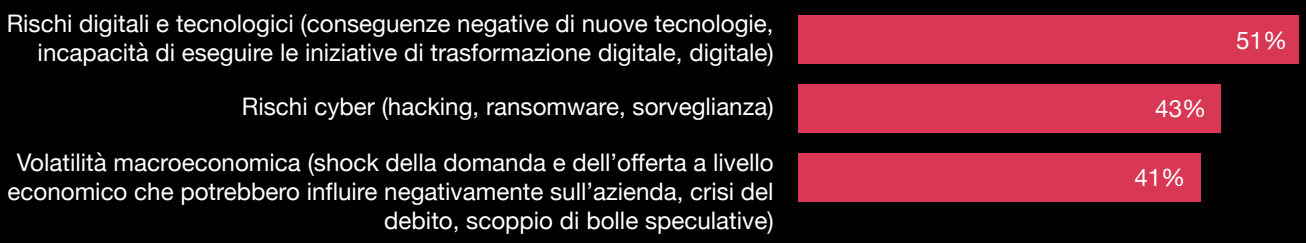
Innovare implica adottare decisioni determinanti e non vi è niente di più rassicurante che sapere di aver adottato tutte le misure necessarie per garantire la sicurezza, valutando e affrontando con determinazione i rischi cyber più rilevanti.

Secondo il Global Digital Trust Insights 2024 di PwC, il contenimento del rischio cyber è una priorità assoluta per l'anno 2024. Dopo essere sceso al quarto posto nella CEO Survey di PwC dello scorso anno, occupa ora il secondo posto per i nostri intervistati nella lista delle minacce più rilevanti, dietro soltanto ai rischi digitali e tecnologici. Inoltre, per i nostri intervistati, i rischi digitali e tecnologici sono inestricabili dal rischio cyber.

Nell'attuale panorama aziendale, non si può semplicemente parlare di trasformazione o di reinvenzione digitale senza menzionare la cybersecurity. Gli attacchi al cloud e gli attacchi ai dispositivi connessi a quest'ultimo – i quali rappresentano due tecnologie al centro della trasformazione aziendale contemporanea – sono le minacce che destano maggior preoccupazione tra i nostri intervistati.

Il digitale è in cima alla classifica dei rischi in due modi

Priorità di contenimento del rischio nei prossimi 12 mesi (classifica dei primi tre)



Q1. Quali tra i seguenti rischi la vostra organizzazione intende affrontare prioritariamente nei prossimi 12 mesi? (Classifica dei primi tre)
Base: All respondents= 3876
Source: PwC, 2024 Global Digital Trust Insights.

Queste stesse minacce informatiche sono interconnesse tra loro. Una volta che gli attaccanti si introducono nei sistemi informatici e nelle reti, provocano disordini in ogni modo possibile.

Ciò che potrebbe iniziare come una violazione del cloud potrebbe facilmente trasformarsi in una minaccia persistente avanzata (Advanced Persistent Threat – APT), mentre gli attaccanti si aggirano all'interno del sistema raccogliendo dati e cercando altri modi per creare danni. Potrebbero esfiltrare i vostri dati, poi lanciare un attacco ransomware, quindi divulgare i dati ('hack and leak') nonostante il pagamento del riscatto.

Ognuno di questi incidenti è problematico di per sé. Insieme, possono compromettere gravemente la reputazione e le operazioni della vostra organizzazione. Le violazioni massicce (mega breaches) sono in aumento per numero e magnitudo, oltre che per costi. La percentuale di coloro che hanno dichiarato costi pari o superiori a 1 milione di dollari a causa della più grave violazione subita negli ultimi tre anni è salita al 36% rispetto al 27% dello scorso anno.

Ma il ritmo dell'innovazione e della reinvenzione del business non rallenta, specialmente quando il 40% dei CEO ritiene che le proprie aziende potrebbero non essere più economicamente sostenibili da qui a un decennio qualora continuassero in questa direzione. La sfida per il Top Management è la seguente: il cyber risk management della vostra organizzazione è al pari con i cambiamenti?

Tutto è interconnesso, incluso gli attacchi cyber

Le principali minacce informatiche per i prossimi 12 mesi

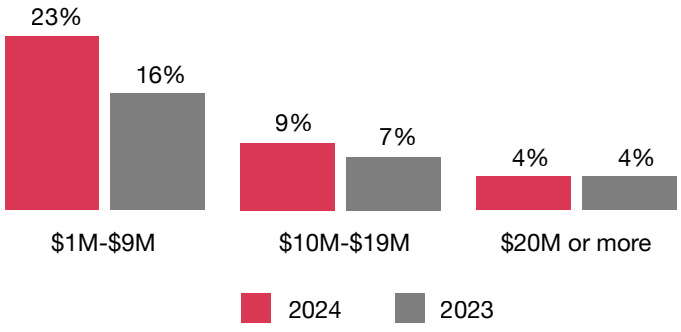
Q3. Nei prossimi 12 mesi, quali delle seguenti minacce cyber preoccupano maggiormente la sua organizzazione? (Classifica delle prime tre)
Base: All respondents=3876
Source: PwC, 2024 Global Digital Trust Insights.

La sfida per il Top Management è la seguente:
il cyber risk management della vostra azienda è al pari con i cambiamenti?

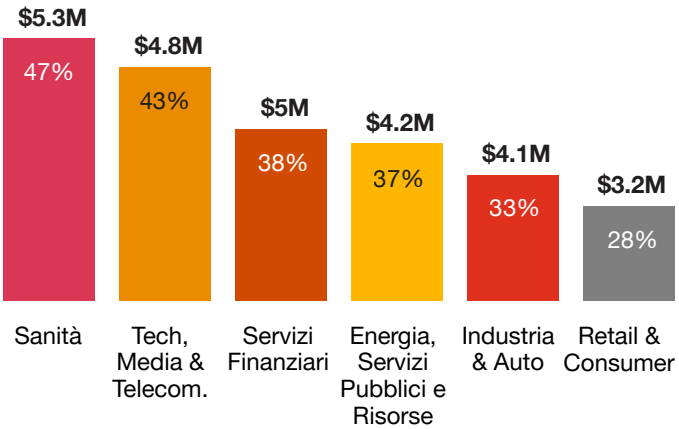
Le violazioni stanno diventando sempre più onerose

Costi stimati per le organizzazioni a causa dei data breach più onerosi negli ultimi tre anni

Percentuale di chi afferma che ha subito violazioni da più di 1 milione di dollari: Totale 2024= 36%, totale 2023= 27%



Costo medio delle violazioni in milioni e percentuale delle violazioni più dannose che sono costate $1 milione o più, per settore



Q5. Prendendo in considerazione il data breach più grave che ha subito negli ultimi tre anni, le chiediamo di fornire una stima del costo sostenuto dalla sua organizzazione.
Source: PwC, 2024 Global Digital Trust Insights.

Semplificazione degli strumenti cyber: un danno per gli attaccanti

La modernizzazione e l'ottimizzazione rappresentano le priorità assolute per quanto riguarda gli investimenti in ambito informatico nel 2024. Quasi la metà (49%) degli executive ha optato per la modernizzazione tecnologica, compresa l'infrastruttura cyber, mentre il 45% ha scelto l'ottimizzazione delle tecnologie e degli investimenti già esistenti.

Nel nostro sondaggio del 2022, abbiamo riscontrato che i CEO erano molto preoccupati che le proprie organizzazioni fossero diventate troppo complesse per essere messe in sicurezza. Nel momento in cui è stato condotto il sondaggio, il 32% delle organizzazioni aveva preso l'iniziativa di consolidare i propri fornitori tecnologici con l'obiettivo di semplificare e ristrutturare la propria combinazione di servizi gestiti esternamente e internamente.

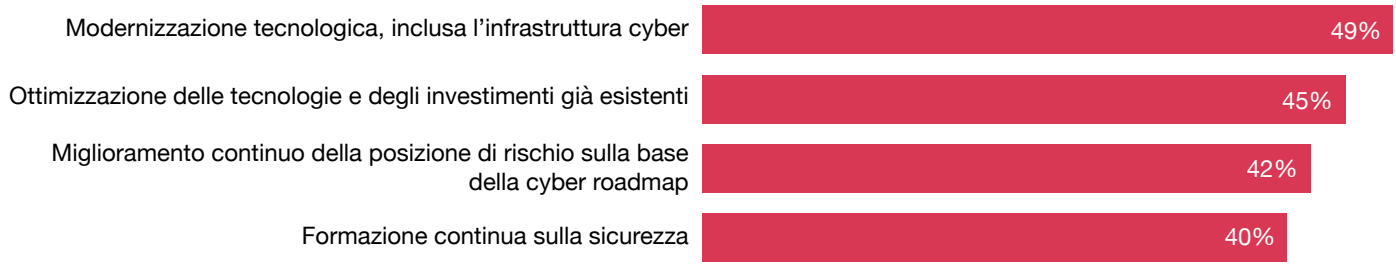
Nel sondaggio del 2024, il 44% dichiara di utilizzare una suite integrata di soluzioni cyber tech, mentre il 39% afferma di avere intenzione di adottarne una entro i prossimi due anni. Quasi un quinto, il 19%, dichiara di avere troppe soluzioni cyber e di aver bisogno di consolidarle.

La sovrabbondanza di point solution può essere una delle ragioni per cui solo il 5% degli intervistati dei settori IT e Tech dichiara di essere "molto soddisfatto" delle capacità tecnologiche delle proprie soluzioni cyber in tutte e otto le aree chiave. Un software non integrato correttamente può ostacolare le prestazioni, richiedere maggior tempo per la gestione e impedire una visione d'insieme, essenziale per il cyber risk management.

Chi lo ha già sperimentato lo sa bene. Gli intervistati al nostro sondaggio che hanno subito un data breach dal costo di 1 milione di dollari o più negli ultimi tre anni sono più propensi a riconoscere di avere troppe soluzioni di cybersecurity e di doverle integrare. Diversamente, le organizzazioni che utilizzano suite di soluzioni cyber integrate sono più spesso in grado di evitare violazioni costose e di ampia portata.

I cyber budget per il 2024 puntano a sfruttare al meglio gli strumenti già a disposizione

Top Management – Priorità di investimento in cybersecurity nei prossimi 12 mesi (Classifica dei primi tre)



Q14b. A quale dei seguenti investimenti darà priorità nell'allocazione del budget cyber della sua organizzazione nei prossimi 12 mesi? (Ranked in top three). Base: Business respondents= 1925
Source: PwC, 2024 Global Digital Trust Insights.

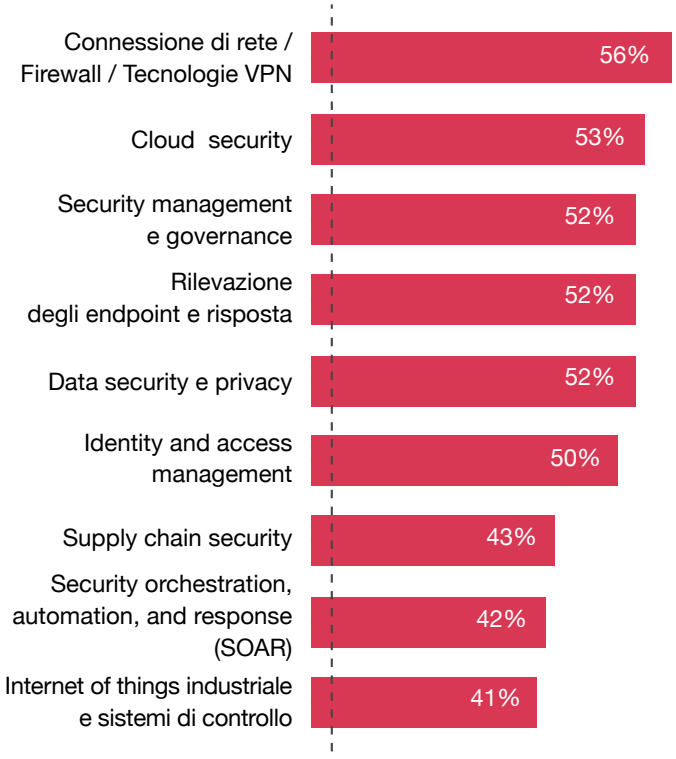
Tuttavia, gli intervistati non stanno rinunciando a spendere. Più di tre quarti (79%) affermano che aumenteranno le spese nell'ambito cyber nel 2024 (rispetto al 64% dello scorso anno), soprattutto le grandi organizzazioni con un fatturato di 5 miliardi di dollari o superiore. Le organizzazioni che prevedono aumenti di budget del 15% o più tendono ad essere quelle con un fatturato da 50 miliardi di dollari o superiore, oppure che operano nel settore tecnologico, dei media e delle telecomunicazioni, o quelle che prevedono una maggiore crescita dei ricavi nel prossimo anno.

Anche gli investimenti nell'ambito cyber costituiscono una parte sempre maggiore del budget per IT, OT e automation. Si assiste ad un aumento medio complessivo del 14% nel 2024, rispetto all'11% del 2023.

La vera sfida per il Top Management non è la mancanza di strumenti o investimenti. Consiste piuttosto nel comprendere come l'organizzazione possa trarre vantaggio dai propri investimenti. L'architettura IT dell'azienda è troppo complessa per essere difesa adeguatamente? State agevolando involontariamente gli attaccanti nel trovare punti deboli nella vostra difesa?

Solo la metà degli intervistati è soddisfatta delle proprie capacità di cyber-tech

Capacità tecnologiche dell'azienda nelle aree chiave della cybersecurity



Solo il 5% degli intervistati dei settori security e IT sono molto soddisfatti in tutte le aree

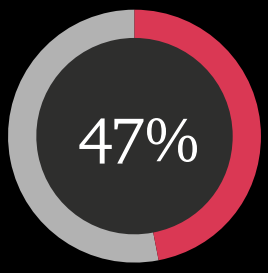
Q23. Quanto è soddisfatto delle capacità tecnologiche della sua organizzazione nelle seguenti aree?
Base: Security and IT respondents= 1517
Source: PwC, 2024 Global Digital Trust Insights.

Cloud security: un’attenzione che non si vedeva da tempo

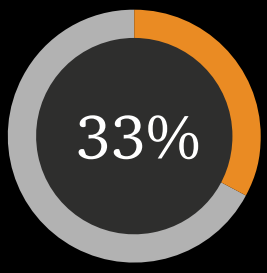
L’utilizzo del cloud è sempre stato una parte fondamentale dell’innovazione aziendale, come consentire agli sviluppatori di collaborare ovunque si trovino nel mondo, adottare nuovi modi più flessibili di lavorare, inventare nuovi modelli di business, coordinare nuove tecnologie per migliorare il funzionamento del business, fornire servizi migliori ai clienti, e così via.

La cloud security è il rischio informatico numero 1 per quasi la metà (47%) degli intervistati. I modi in cui gli attaccanti possono accedervi appaiono virtualmente illimitati. Le aziende dovrebbero predisporre controlli in ogni ambito: su identità ed accessi, lateral movements, account di posta elettronica, portali web, applicazioni, informazioni proprietarie, interazioni coi clienti, sistemi operativi, connected devices, e l’elenco continua.

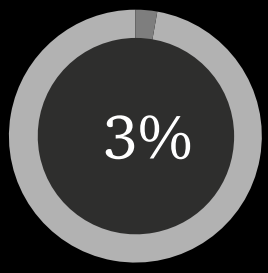
Cloud security: minaccia principale, investimento principale – ancora mal gestito



Minaccia prioritaria



Principale investimento cyber



Implementazione e continuo aggiornamento di piani di gestione del rischio cloud

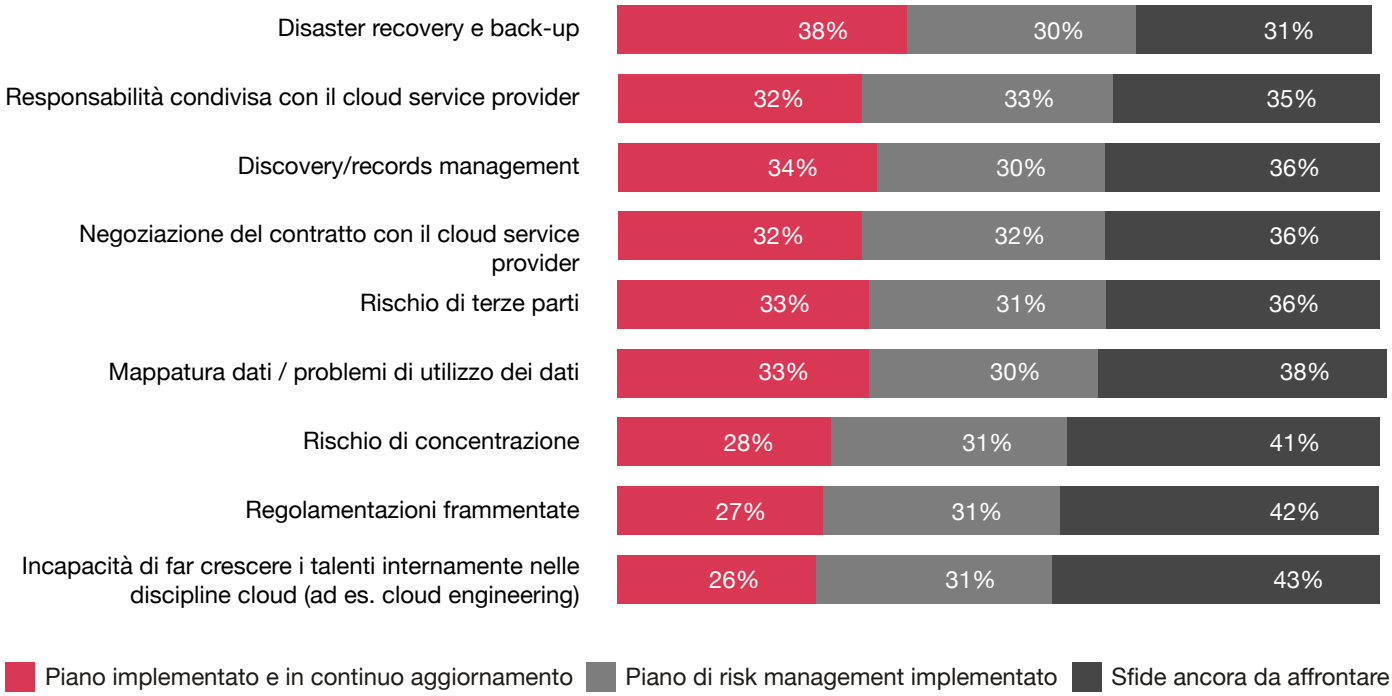
Q3. Nei prossimi 12 mesi, quali delle seguenti minacce cyber preoccupano maggiormente la sua azienda? (Classifica delle prime tre)
Base: All respondents= 3876
Q14a. Quale dei seguenti investimenti state prioritizzando nell'allocazione del budget cyber della vostra organizzazione nei prossimi 12 mesi? (classifica delle prime tre) Base: IT respondents= 1919
Q19. In quale modo la sua organizzazione ha affrontato le seguenti sfide con i fornitori di servizi cloud? Base: Cloud provider users= 3648
Source: PwC, 2024 Global Digital Trust Insights.

Molti degli intervistati (42%) utilizzano più di un servizio cloud, e le preoccupazioni sulla cloud security aumentano tra coloro che utilizzano più di un cloud, anche ibridi. Il 54% di questi intervistati cita il cloud come il rischio più rilevante per la cybersecurity. Gli utilizzatori di cloud ibridi sono anche i più propensi a scegliere il cloud tra la lista delle tre priorità per gli investimenti in ambito security nel prossimo anno (36% rispetto al 33% totale).

Ma quasi tutte le aziende (il 97%) hanno delle lacune nel proprio piano di cloud risk management. Solo il 3% possiede piani aggiornati che rispondono a tutte le esigenze delle nove aree di sicurezza relative al cloud. I rischi posti dalla frammentazione delle normative, ad esempio, non sono ancora stati affrontati dal 42%; il 41% non ha un piano per affrontare il rischio di concentrazione dei servizi su un unico cloud provider, il 36% non ha ancora affrontato il rischio legato al cloud di terze parti.

Tanti rischi legati al cloud, pochi piani per contrastarli

L'opinione delle aziende circa le sfide dei fornitori di servizi cloud



Q19. In quale modo la sua azienda ha affrontato le seguenti sfide con il suo fornitore di servizi cloud?
Base: Cloud provider users= 3648
Source: PwC, 2024 Global Digital Trust Insights.

Il top 5% – i nostri "custodi della digital trust" – è quattro volte più propenso ad aggiornare continuamente il proprio piano di risk management per contrastare i rischi relativi al cloud. Il resto dei nostri intervistati, tuttavia, deve ancora svolgere gran parte di questo lavoro cruciale.

La sfida per il management è la seguente:
Qual è la strategia ottimale per collaborare con i fornitori di soluzioni per la cloud security al fine di migliorare la difesa dei principali punti di accesso ai sistemi e agli asset aziendali attraverso il cloud?

La crescita dell'utilizzo della Generative AI per la cyber defence

Quasi sette intervistati su dieci affermano che la propria organizzazione utilizzerà la generative AI (GenAI) per la cyber defence. Gli strumenti GenAI possono essere un valido supporto per i team di cybersecurity che affrontano una crescente mole di attacchi cyber, sempre più numerosi e complessi.

GenIA per la cyber defence

69%

Più di due terzi (69%) affermano che utilizzeranno la GenIA per la cyber defence nei prossimi 12 mesi.

47%

Quasi metà (47%) già la utilizzano per rilevamento e mitigazione del rischio cyber.

21%

Un quinto (21%) afferma di vedere già i benefici apportati dalla GenAI ai propri programmi informatici – a distanza di pochi mesi dal suo debutto.

Q7. In quale modo è d'accordo o in disaccordo con le seguenti affermazioni riguardo la Generative AI?
Q10. In che modo la sua organizzazione sta implementando o ha in programma di implementare le seguenti iniziative di cybersecurity?
Base: All respondents= 3876
Source: PwC, 2024 Global Digital Trust Insights.

Le piattaforme stanno concedendo in licenza i loro grandi modelli di linguaggio (LLM) insieme alle loro soluzioni tecnologiche per la cybersecurity. Microsoft Security Copilot intende offrire funzionalità GenAI per la gestione della postura di sicurezza, la risposta agli incidenti e la generazione di report di security. Allo stesso modo, Google ha presentato Security AI Workbench per finalità analoghe.

Molti fornitori stanno testando i limiti dell'GenAI, cercando di capire come sia possibile utilizzarla concretamente. Potrebbe passare del tempo prima di assistere ad un utilizzo su vasta scala dei sistemi di defenceGPT. Nel frattempo, ecco le tre aree dove l'utilizzo della GenAI per la cyber defence potrebbe introdurre un cambiamento concreto.

- **Threat detection and analysis.** La GenAI ha un potenziale inestimabile per quanto riguarda il rilevamento proattivo delle vulnerabilità, la valutazione rapida della loro entità – cosa è a rischio, cosa è già compromesso e quali siano i danni, per poi presentare opzioni collaudate per la difesa ed il ripristino. La GenAI può aiutare ad identificare schemi, anomalie e indicatori di compromissione (IOC) che sfuggono ai tradizionali sistemi di rilevamento.
- **Cyber risk and incident reporting.** La GenAI potrebbe anche semplificare la segnalazione dei rischi cyber e degli incidenti. Con l'aiuto del natural language processing (NLP), la GenAI può trasformare i dati tecnici in contenuti concisi che possono essere compresi anche dai non-addetti ai lavori. Può essere d'aiuto con la segnalazione degli incidenti, fornire informazioni sulle minacce, dare valutazioni sui rischi, audit e conformità alle normative vigenti. Inoltre, può fornire raccomandazioni in termini che chiunque possa comprenderle, anche traducendo grafici complessi in testi di facile accesso.
- **Adaptive controls.** Mettere in sicurezza il cloud richiede un costante aggiornamento dei criteri di funzionamento e dei controlli di sicurezza, un compito, ad oggi, ancora arduo. Gli algoritmi di apprendimento automatico e gli strumenti GenAI potrebbero presto essere in grado di consigliare, convalidare e redigere politiche di sicurezza e automatizzare controlli adattati al profilo delle minacce, alle tecnologie e agli obiettivi aziendali di un'organizzazione.

La sfida per il management è la seguente:
Come gestire i nuovi strumenti a disposizione senza apportare nuovi rischi per l'azienda e la società? Come fare per utilizzare la GenAI in modo etico e responsabile?

Regolamenti e Normative: Fornire uno spazio sicuro per sperimentare e crescere

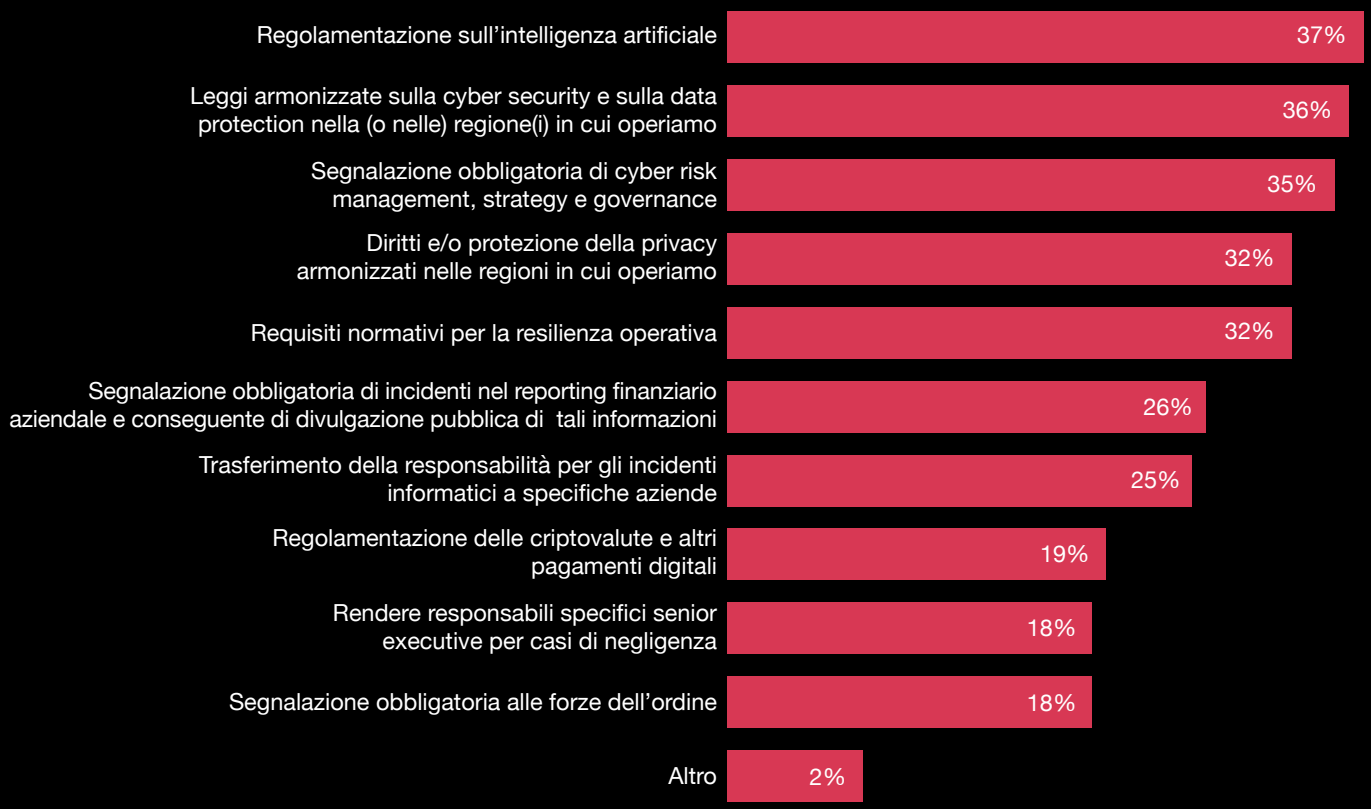
La visione mainstream è che le nuove regole e regolamentazioni ostacolino i ricavi, ma l'opinione di almeno un terzo degli intervistati è la seguente: Le barriere imposte dalle autorità di regolamentazione possono dare alle aziende una spinta maggiore per esplorare, sperimentare, inventare e competere. Navigare tra i requisiti regolamentari può diventare un vantaggio competitivo per le aziende leader.

Circa un terzo degli intervistati di quest'anno concorda sul fatto che sono quattro i tipi di regolamentazione più importanti per garantire la crescita futura delle proprie aziende: la regolamentazione dell'AI (37%), l'armonizzazione delle leggi sulla cyber security e sulla data protection, il reporting obbligatorio sui risultati di attività di cyber risk management, e su strategie e governance (35%), e i requisiti di operational resilience (32%).

La trasparenza è l'aspetto normativo più rilevante che assumerà sempre più importanza nelle regolamentazioni e livello internazionale. Le nuove regole SEC richiedono la divulgazione pubblica delle violazioni cybersecurity che si ritiene possano essere di rilevanza materiale per gli investitori. Il Digital Markets Act e il Digital Services Act impongono trasparenza nelle procedure di trattamento dati e di decision-making algoritmico. In più, all'orizzonte si profilano normative che regolino l'AI, tra cui una legge Europea sull'AI ed una sulla GenAI.

Regolamentazioni che potrebbero cambiare la cybersecurity

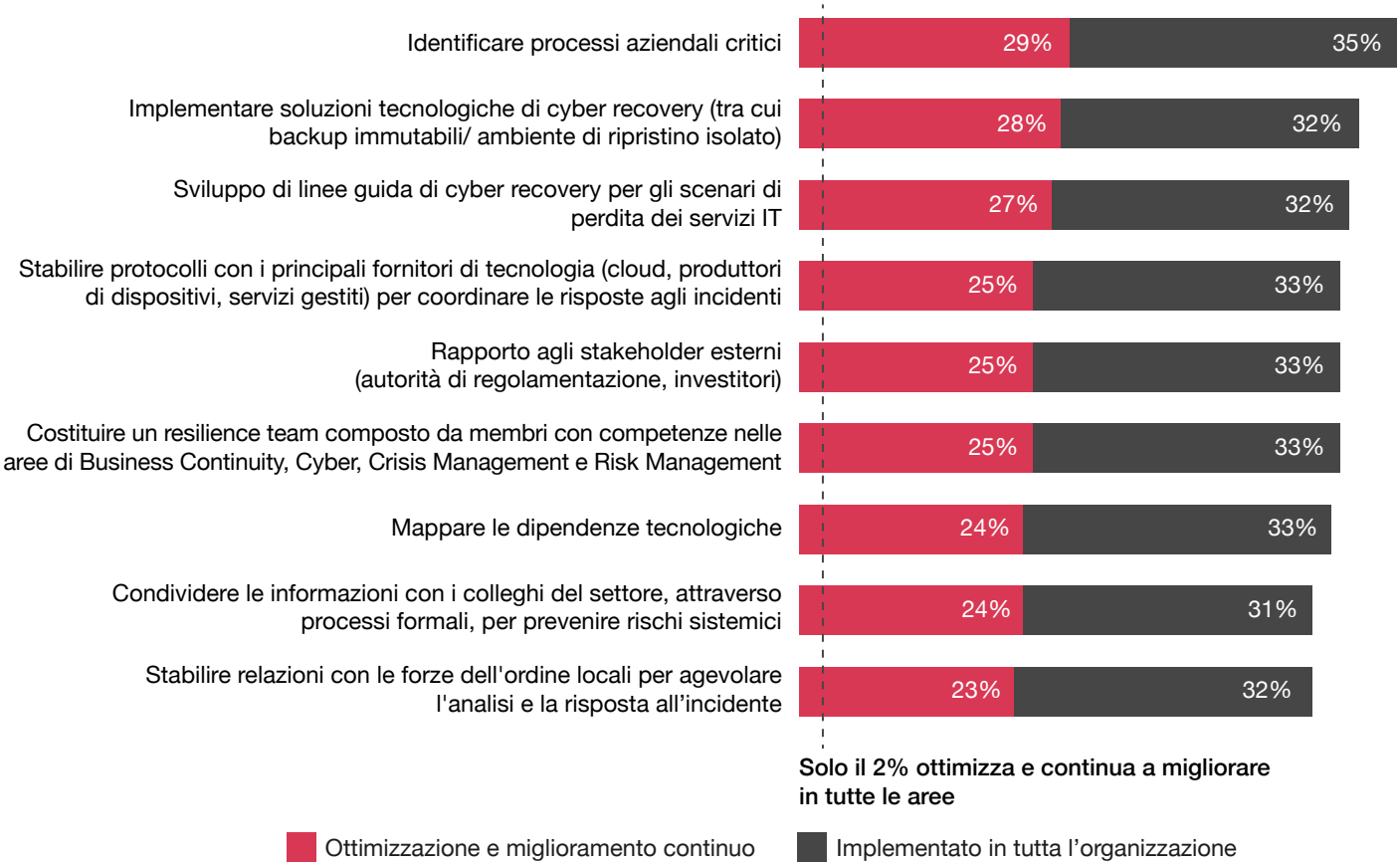
Obiettivi e principi regolamentari con il maggior impatto sulla crescita futura dei ricavi delle organizzazioni (Classificati tra i primi tre)



Q24. Quali dei seguenti obiettivi e principi regolamentari proposti avranno il maggiore impatto sulla capacità della vostra organizzazione di garantire la crescita futura dei ricavi? (Classifica dei primi tre). Base: All respondents= 3876
Source: PwC, 2024 Global Digital Trust Insights.

Il lento progresso della cyber resilience

Livello di implementazione di azioni chiave di cyber resilience



Q8. In quale modo la sua organizzazione sta implementando o ha intenzione di implementare le seguenti azioni di cyber resilience?
Base: All respondents= 3876
Source: PwC, 2024 Global Digital Trust Insights.

La resilienza operativa è un altro tema importante. Le autorità di regolamentazione riconoscono la sfida di gestire rischi complessi e interconnessi, ma spesso le organizzazioni trattano tali rischi in modo frammentato, considerandoli separatamente per ciascuna unità operativa. I nuovi requisiti, come il Digital Operational Resilience Act, enfatizzano sempre di più la necessità di una resilienza integrata, incorporando elementi chiave che rendono l'organizzazione più adattabile, flessibile e più forte dopo ogni episodio di malfunzionamento.

Tre quarti dei soggetti intervistati prevedono che l'adeguamento a tali normative richiederà un considerevole investimento di risorse finanziarie e di tempo. L'implicazione di costi elevati e il potenziale impatto negativo sui ricavi potrebbero essere mitigati se le organizzazioni intraprendessero un approccio proattivo e costante verso i processi regolatori. Ad esempio, ciò potrebbe comportare la collaborazione con le forze dell'ordine, la partecipazione a discussioni pubbliche e persino l'interazione diretta con le autorità competenti al fine di contribuire alla creazione o all'influenza delle direttive proposte.

La sfida per il management è la seguente:
In un contesto di incertezza regolamentare, è possibile dare alla propria organizzazione l'opportunità di innovare, preservando al contempo il concetto di security e privacy by design? In che modo è possibile trarre vantaggio da questo nuovo contesto normativo per ottenere un vantaggio competitivo?

Interrompere il Cyber-as-usual: le linee guida 2024 per il management

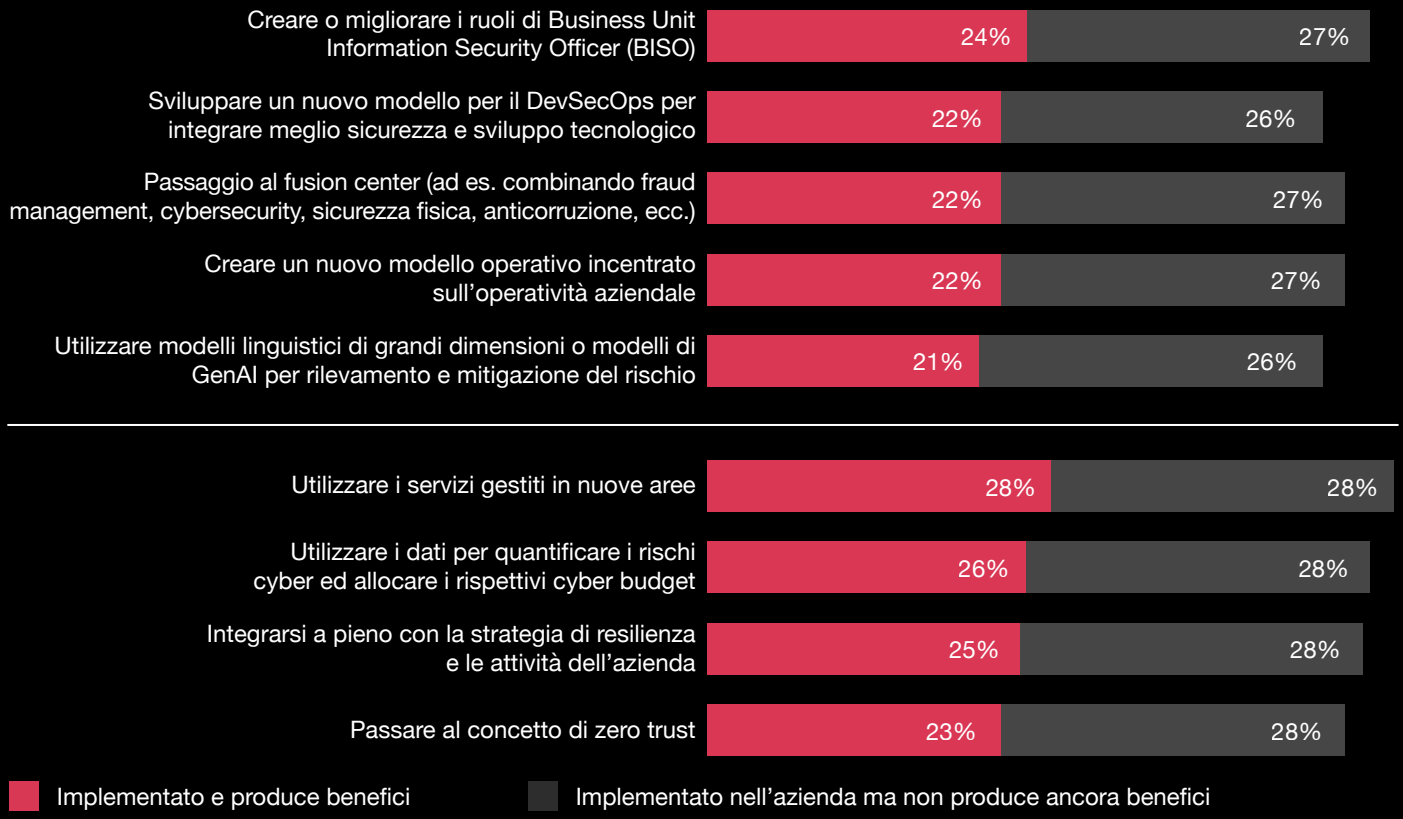
Le organizzazioni non seguono più il business-as-usual. Tuttavia, la maggior parte delle aziende è ancora bloccata nel cyber-as-usual, come dimostra la Global Digital Trust Insights 2024. Si osservano iniziative frammentate, una costante crescita di complessità tecnologica, e un programma di gestione del rischio che, a causa delle sue lacune, rappresenta di per sé un rischio.

Inoltre, le trasformazioni e i progetti in corso spesso non producono i risultati desiderati. Questi ostacoli e altri ancora si frappongono alla realizzazione di una cybersecurity veramente affidabile.

Nel playbook 2023, abbiamo individuato le sfide critiche che il management aziendale dovrebbe affrontare. Queste sfide rimangono ancora rilevanti.

Regolamentazioni che potrebbero cambiare la cybersecurity

Le iniziative nella prima parte del grafico sono incentrate sull'aspetto cyber, quelle nella seconda parte sul business



Q10. In quale modo la sua azienda sta implementando o ha intenzione di implementare le seguenti iniziative di cybersecurity?
Base: All respondents= 3876. Analysis technique utilised is factor analysis
Source: PwC, 2024 Global Digital Trust Insights.

Nel 2024, rilanciamo la sfida:

In qualità di manager, ha la determinazione necessaria per compiere decisioni che avranno un impatto significativo sulla sua azienda?

Farebbe quel passo in avanti in più che potrebbe finalmente eliminare ciò che ostacola la vostra azienda dal raggiungere i propri obiettivi?

Notiamo che alcune imprese stanno già facendo delle scelte strategiche ponderate. Le opzioni disponibili sono molteplici.

Cosa è più giusto per la sua organizzazione?

Parlare una nuova lingua.

CISO CFO GC

Essere al centro dell'innovazione significa sostenere i propri team manageriali e aiutarli a superare eventuali timori nei confronti della vostra attività. Utilizzare termini come cyber landscape, superficie di attacco, e persino zero trust, non farà altro che confondere ulteriormente chi non pratica la vostra stessa professione.

Non abbiate paura a parlare di cyber quando parlate di affari, tecnologia, finanza o nelle conversazioni di tutti i giorni. Comunicate con i vostri clienti, investitori e partner commerciali durante i security reports annuali in modo tale da informare e coinvolgere. L'utilizzo di linguaggio comune può agevolare il management nel gestire le sfide, le tensioni e la confusione che inevitabilmente sorgono nel contesto dell'innovazione.

Provare nuovi modi coraggiosi di gestire il rischio cyber.

CISO CRO IA CCO COO

Adottare approcci più avanzati nella valutazione del rischio cyber, come l'analisi delle minacce mediante modelli specifici per il settore, la visione e la strategia aziendale. Implementare un sistema di incentivi legato alle prestazioni in termini di gestione del rischio per tutti i dipendenti al fine di promuovere una cultura del rischio. Innovare nell'individuazione e nel rafforzamento dei punti vulnerabili, magari attraverso l'implementazione di un programma di bug bounty volto a incoraggiare la ricerca indipendente sulla sicurezza. Infine, acquisire e implementare una soluzione di identità gestita centralmente, con un approccio orientato al cloud, per tutelare gli obiettivi di espansione aziendale.

Plasmate confini sicuri.

CISO CIO GC RA

È essenziale comunicare attraverso il linguaggio della fiducia, anziché limitarsi alla conformità normativa. Occorre un coinvolgimento proattivo, tempestivo e costante per massimizzare l'influenza nella definizione delle nuove policy, assicurando che queste siano allineate con il successo aziendale, piuttosto che rappresentare impedimenti. Temi normativi di grande attualità come l'intelligenza artificiale, il metaverso, le criptovalute e la privacy possono trarre beneficio dalla vostra esperienza e dalle vostre intuizioni. È importante ricordare che i regolatori, proprio come tutti gli altri, possono trovarsi disorientati dal complesso funzionamento della cyber-tech.

Lasciate i vostri team liberi di pensare (automation, GenAI, managed services)

CISO CIO CTO CRO COO

Tra i vantaggi dell'automation, della GenAI e dei servizi gestiti c'è la capacità di offrire assistenza 24 ore su 24. Questi consentono di eseguire operazioni di routine in modo da alleviare il carico di lavoro dei vostri team e permette ai vostri dipendenti di dedicare tempo ed energie alla riflessione sulle nuove minacce cyber e alla creazione di nuove strategie per contrastare le minacce in continua evoluzione.

Un benvenuto alla cyber nella meeting rooms.

CISO B CEO

Quello cyber è in cima alla lista dei rischi nella maggior parte delle aziende e in molti sondaggi effettuati tra il management. Ma è un argomento centrale nei meeting? State ottenendo informazioni di qualità, non solo su rischi e controlli di tipo cyber, ma anche sul modo in cui le principali iniziative strategiche stanno promuovendo la crescita del business e dei ricavi?

Il concetto di cybersecurity è alla base di tutte le attività dell'azienda: finanza, sviluppo, personale, tecnologia e altre aree di cui probabilmente parlate ogni volta che vi incontrate.

Pensa come se fossi il capo.

CISO CEO

La business transformatrion e la cyber transformation non sono due entità separate, ma una stessa realtà. Il CISO e il CEO devono affrontare il concetto di cyber come parte integrante del loro business, assumendo la prospettiva imprenditoriale. Non è forse nell'interesse di entrambi assicurarsi che ogni aspetto dell'azienda, come i documenti finanziari, la proprietà intellettuale, lo sviluppo di applicazioni e i dati dei clienti, sia protetto da accessi o utilizzi non autorizzati? Non vorrebbero tutelare la reputazione del marchio? E la cyber security non potrebbe essere un driver di innovazione, portando a risparmi finanziari e alla crescita aziendale? Questa è la ragione d'essere del cyber.

La Global Digital Trust Insights 2024 è un sondaggio condotto su 3.876 executive, del reparto di techonology e security (CEO, directors, CFO, CISO, CIO e manager) condotto nel periodo compreso tra maggio e luglio 2023.

Quattro manager su 10 appartengono a grandi aziende con un fatturato di 5 miliardi di dollari o più. Il 30% di essi lavora in aziende con ricavi pari o superiori a 10 miliardi di dollari.

Gli intervistati operano in diversi settori, tra cui industrial manufacturing (20%), servizi finanziari (20%), tech, media, telecom (19%), retail (17%), energy & utilities (11%), sanità (9%) e government e servizi pubblici (3%).

Gli intervistati provengono da 71 paesi diversi. La ripartizione regionale è Europa Occidentale (32%), Nord America (28%), Asia-Pacifica (18%), America Latina (10%), Europa Orientale (5%), Africa (4%) e Medio Oriente (3%).

La Global Digital Trust Insights era prima conosciuta come Global State of Information Security Survey (GSISS). Nel suo 26° anno di vita, questo sondaggio annuale rappresenta la più longeva e ampia indagine sulle tendenze della cybersecurity. È unico nel suo genere poiché coinvolge non solo professionisti della security e dell'information technology, ma anche manager di alto livello provenienti da varie aree aziendali.

L'indagine è stata condotta da PwC Research, il centro globale di eccellenza di PwC dedicato alla ricerca di mercato e all'analisi.

Contatti

Nicola Monti
Partner, Cyber Leader, PwC Italia
+39 348 2504036
nicola.monti@pwc.com

Giuseppe D'Agostino
Partner, PwC Italia
+39 347 6466747
giuseppe.dagostino@pwc.com

Paolo Carcano
Partner, PwC Italia
+39 334 6896335
paolo.carcano@pwc.com

Lorenzo Desidera
Partner, PwC Italia
+39 392 291 4959
lorenzo.desidera@pwc.com