CYBER INDEX PMI

RAPPORTO CYBER INDEX PMI 2025

La cultura digitale protegge la tua impresa

Promosso da:

GENERALI

CONFINDUSTRIA

Partner scientifico:

POLIMI SCHOOL OF MANAGEMENT

osservatori.net digital innovation

Partner Istituzionale:

ACN

EXECUTIVE SUMMARY

Nel 2025, il panorama della cybersecurity per le PMI italiane ha raggiunto un livello di complessità senza precedenti. Non siamo più di fronte a una sfida puramente tecnologica, ma a una pressione multidimensionale: le tensioni geopolitiche ridefiniscono le strategie di sourcing e il nuovo quadro normativo impone standard di adeguamento che richiedono trasformazioni strutturali profonde. In questo scenario, assistiamo al preoccupante allargamento tra la velocità esponenziale con cui crescono le minacce e la più lenta capacità di miglioramento e reazione delle aziende. A testimoniarlo sono i numeri: nel 2025, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha registrato un'impennata degli eventi cyber, con 1.549 episodi nel primo semestre (+53% rispetto al primo semestre 2024) e 1.253 nel secondo semestre (+30% sul secondo semestre 2024). L'incremento a doppia cifra dimostra che la minaccia viaggia a una velocità che le PMI faticano a inseguire.

Nel terzo anno di rilevazione, il Cyber Index PMI – indice che misura la consapevolezza delle PMI italiane in materia di cybersecurity su un campione di 1500 imprese – ha raggiunto il valore di 55 punti, segnando un incremento di 3 punti rispetto alla rilevazione del 2024, e di 4 punti rispetto al 2023. Sebbene questo dato indichi un'accelerazione nella velocità del miglioramento, esso nasconde una polarizzazione sempre più marcata tra un nucleo ristretto di eccellenze e una vasta platea di realtà ancora profondamente vulnerabili. Ciò emerge chiaramente osservando l'evoluzione delle imprese lungo i quattro profili di maturità: principianti, informate, consapevoli e mature. Ad oggi, solo il 16% del campione esprime una postura di sicurezza adatta, una quota ancora contenuta ma rilevante: per la prima volta, le aziende "mature" superano numericamente le "principianti" (14%), categoria in calo di 6 punti rispetto alla prima rilevazione. Questo sorpasso rappresenta un traguardo solo simbolico e non racconta certo di un'effettiva inversione di rotta: il restante 70% delle PMI, infatti, rimane arenato nei due livelli centrali – distribuendosi rispettivamente in un 32% di aziende "consapevoli" e in un 38% di "informate". Queste imprese possiedono una sufficiente conoscenza della materia che, tuttavia, non si traduce in una capacità di difesa efficace.

55
SU 100

CYBER INDEX PMI 2025

VS 52 DEL 2024
E 51 DEL 2023

Tralasciando quindi le realtà più virtuose, rimane evidente il gap in termini di security readiness riscontrato gli scorsi anni. Ciò è alimentato da una percezione distorta della realtà: un terzo delle PMI "principianti" afferma esplicitamente che gli attacchi informatici non rappresentano un rischio concreto per la propria attività, mentre il 39% di imprese "informate" nutre una fiducia eccessiva e spesso infondata nella propria capacità di difesa. La realtà racconta, però, uno scenario del rischio diverso da quello presunto dalle imprese. Nel 2025, quasi una PMI italiana su quattro ha dichiarato di aver subito almeno un attacco informatico negli ultimi tre anni. Nella rilevazione passata, lo stesso dato era tre volte inferiore. Ad aumentare non è solo la frequenza, ma anche l'impatto: il 2,5% ha infatti subito conseguenze operative o finanziarie in seguito all'incidente, mentre il 6% afferma che si

INDICE

sono comunque rese necessarie importanti azioni di risposta. Lo scenario della minaccia sta continuando a generare forte pressione sulle infrastrutture critiche e sulle Istituzioni: grandi imprese e pubbliche amministrazioni stanno progressivamente integrando requisiti di sicurezza informatica nei processi di selezione dei fornitori, preferendo partner che possano dimostrare una postura difensiva solida. Emerge quindi un rischio concreto di esclusione da filiere produttive strategiche per tutte quelle piccole e medie imprese che non garantiscono un adeguato dialogo sulla materia e, ovviamente, standard minimi di sicurezza.

In questo contesto, l'evoluzione normativa agisce come un decisivo game-changer. La direttiva NIS2, in particolare, segna un cambio di paradigma: non si limita a imporre requisiti tecnici o protocolli di notifica, ma eleva la cybersecurity a pilastro della governance aziendale. Per la prima volta, la responsabilità ricade direttamente sugli organi amministrativi, chiamati a rispondere degli impatti che un incidente può generare su dipendenti, fornitori e clienti. Questo produrrà un effetto a cascata sui fondi destinati alla cybersecurity: nel 2025 il budget IT delle piccole imprese è cresciuto del 3,3%, quello delle medie imprese del 5,2%, di cui, mediamente, l'11% è destinato alla cybersecurity. Complessivamente, la maggior presenza di responsabilità e fondi destinabili alla sicurezza spingono l'indice che valuta l'approccio strategico a raggiungere i 62 punti (+6p.p. rispetto al 2024), rappresentando il principale elemento di miglioramento osservato nel 2025.

Un driver che può supportare le imprese nel calare a terra la maggior consapevolezza, oltre all'indirizzo istituzionale, è rappresentato dalle polizze assicurative. La possibilità di accesso a una copertura assicurativa che copra il rischio cyber è infatti vincolata al raggiungimento di standard minimi di sicurezza, imposti dalle imprese assicuratrici e valutati in fase di sottoscrizione: il rispetto di tali requisiti sta quindi guidando implicitamente le PMI verso una miglior postura. I dati, tuttavia, mostrano una diffusione delle coperture assicurative ancora troppo limitata nonostante le conseguenze economiche e operative derivanti da un incidente risultino mediamente inferiori, con danni rilevati nel 1% del campione assicurato, rispetto al 3% del campione non assicurato. Ciò che si vuole evidenziare, pertanto, non è solo il ruolo che ha l'assicurazione nel trasferimento del rischio residuo, quanto l'impatto positivo nell'indurre le imprese a introdurre processi e tecnologie per mitigare il rischio: ipoteticamente, l'obbligatorietà di una polizza sul rischio cyber darebbe un ulteriore spinta al miglioramento delle PMI.

L'ACCESSO A UNA COPERTURA CYBER INCENTIVA LE AZIENDE A INTRODURRE TECNOLOGIE DI PROTEZIONE E RISPOSTA AGLI INCIDENTI

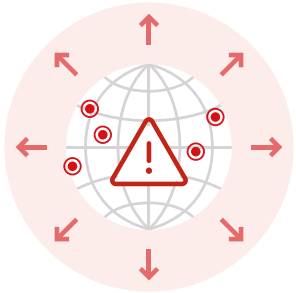
Il principale beneficio derivante da una maggior consapevolezza è un marcato miglioramento nella capacità di comprendere il rischio cyber. Per il secondo anno di fila, l'identificazione – componente dell'indice che rileva l'attenzione e la capacità di individuazione del rischio cyber delle imprese – cresce e raggiunge i 48 punti (+3 punti). Questo impulso è sostanziato dall'impressionante aumento di imprese che ha costituito un inventario degli asset informatici. Nel 2024, solo il 48% delle PMI ne disponeva di uno, nel 2025 la percentuale è salita al 70%. Inoltre, il 44% ha svolto auditing sulla sicurezza informatica – dato in crescita di 3 punti rispetto al 2024.

Ciò fa emergere criticità già note al mondo delle grandi imprese, ma rimaste nascoste dalla mancanza di attività di analisi. Le PMI italiane soffrono dell'eterogeneità e dell'obsolescenza infrastrutturale, e talvolta non hanno le competenze necessarie per gestire le vulnerabilità derivanti da errate

INDICE

configurazioni o mancati aggiornamenti: una PMI su tre, infatti, non ha adeguate competenze digitali e fatica a portare avanti anche tradizionali attività di IT Security, che favoriscono almeno la protezione degli asset digitali.

Oltre alla carenza di competenze specifiche, le PMI italiane scontano un'incapacità strutturale nel presidiare l'intero ciclo del rischio, dalla rilevazione dell'attacco alla risposta. Nonostante l'indice dell'Attuazione rimanga stabile a 57 punti, si osserva una tendenza strategica incoraggiante: la quota di imprese che scelgono di affidarsi a partner esterni è infatti salita dal 25% del 2024 al 29% del 2025. Questa preferenza non solo riflette la crescente difficoltà nel selezionare le leve tecnologiche più adeguate, ma anche nell'integrarle efficacemente all'interno di infrastrutture IT sempre più stratificate. In questo scenario di incertezza tecnica, la provenienza geografica delle soluzioni emerge come un nuovo e determinante criterio di scelta: l'11% delle imprese identifica oggi nella dipendenza da attori extra-UE una vulnerabilità intrinseca, manifestando una sensibilità geopolitica che trasforma la fornitura in una questione di sicurezza.



LA DIPENDENZA DA ATTORI EXTRA-UE È PERCEPITA COME UNA VULNERABILITÀ STRATEGICA DALL'11% DELLE AZIENDE

In questo percorso di maturazione, i finanziamenti pubblici agiscono come un potente acceleratore. Sebbene solo il 12% delle PMI vi abbia avuto accesso, il fatto che il 42% dei beneficiari abbia raggiunto il profilo "maturo" conferma la validità della strategia adottata. Risulta dunque prioritario insistere su questa strada, colmando il deficit informativo che ancora impedisce al 39% delle imprese di conoscere e sfruttare tali opportunità strategiche. Passando poi alle misure di sicurezza specifiche, i progressi nella gestione degli accessi rappresentano uno dei segnali positivi della terza dimensione di analisi, con una PMI su due che ha introdotto strumenti di autenticazione a più fattori (MFA), quali ad esempio la biometria. Questa attenzione non si riflette invece nella protezione dell'infrastruttura: solo l'11% delle imprese ha predisposto attività sistematiche di identificazione e remediation delle vulnerabilità, lasciando sistemi e reti pericolosamente esposti a potenziali exploit. La protezione del dato tramite cifratura e l'adozione di logiche di segmentazione della rete — fondamentale per prevenire il movimento laterale dei cybercriminali e la conseguente propagazione dell'attacco — interessano appena il 30% delle aziende.

Ancor più critico appare lo scenario relativo alla rilevazione e alla risposta agli incidenti. Solo una PMI su quattro dispone di soluzioni capaci, almeno in minima parte, di identificare tempestivamente un'intrusione in corso, lasciando la maggior parte delle imprese cieca di fronte a una violazione già avvenuta. A chiudere questo quadro di fragilità è la gestione del post-incidente: il 36% delle PMI non ha proprio preso in considerazione l'ipotesi di un'interruzione operativa, omettendo di fatto qualsiasi programmazione per il ripristino delle attività. Tale carenza non è solo un problema interno, ma un rischio sistemico per le intere filiere produttive: l'incapacità di ripristinare i sistemi in tempi brevi può innescare un effetto domino devastante lungo la catena del valore, come drammaticamente evidenziato durante il 2025.

INDICE

L'orizzonte futuro è dominato dall'integrazione di tecnologie emergenti come l'Intelligenza Artificiale Generativa, che pone le PMI di fronte a nuove sfide. Se da un lato il progresso tecnologico corre spedito verso logiche di automazione nella ricerca delle vulnerabilità e nello sviluppo delle tecniche di attacco, dall'altro un'adozione precoce di soluzioni digitali potrebbe esporre le aziende a nuovi scenari di rischio, come l'esfiltrazione massiva di dati sensibili. Il bilancio di Cyber Index PMI 2025 suggerisce che, per garantire una sostenibilità digitale a lungo termine, le imprese debbano convertire la presa di consapevolezza sugli errori del passato in una capacità di rendere la cybersecurity aderente alle sfide correnti, spalmando l'onere economico e umano lungo l'intero ciclo di trasformazione digitale. Nel breve periodo, allinearsi ai requisiti richiesti in fase di underwriting assicurativo permette di ridurre drasticamente il rischio cyber: adottare queste misure consente infatti di mitigare sia l'entità degli impatti che la probabilità di accadimento.

INDICE