COMPETENZE CYBER PER LE IMPRESE: FORMAZIONE, AWARENESS E INIZIATIVE DI SISTEMA

Valentina Lo Voi
Capo Divisione formazione

3 giugno 2026

COMPETENZE CYBER E RESILIENZA DELLE IMPRESE: IL NUOVO CONTESTO DI RIFERIMENTO

TRASFORMAZIONE DIGITALE

- Cloud
- AI
- Automazione industriale
- Servizi interconnessi

AMPLIAMENTO DELLA SUPERFICIE DI ATTACCO PER LE IMPRESE

EVOLUZIONE DEL QUADRO NORMATIVO

Il nuovo paradigma normativo europeo non si limita più a richiedere misure tecniche di sicurezza, ma attribuisce **centralità alla governance, alla consapevolezza del management, alla formazione continua del personale e allo sviluppo di competenze specialistiche.**

UN SISTEMA PRODUTTIVO IN CRESCITA, MA A PIÙ VELOCITÀ

L'Italia continua a essere tra i Paesi maggiormente colpiti dagli attacchi cyber gravi a livello globale.

PROGRESSI	CRITICITÀ
Maggiore attenzione alla consapevolezza del top management	Carenza di professionalità specialistiche cyber
Cybersicurezza integrata nella governance	Limitata diffusione di programmi strutturati di formazione continua
Crescita degli investimenti	Ruoli, processi e responsabilità ancora poco formalizzati
Approccio più strutturato alla gestione del rischio	Approccio ancora «reattivo» in molte realtà

L'APPROCCIO DELLE IMPRESE ITALIANE NEL 2025

Governance & Dati Chiave

83% Delle grandi imprese italiane gestisce il rischio cyber come parte integrante della governance aziendale.

60% Ha formalizzato il processo interno di gestione del rischio, mostrando una crescita positiva.

57% Dei CISO dichiara che i vertici aziendali (Board) sono chiamati a essere parte attiva dei processi decisionali.

Sfide & Criticità Persistenti

Linguaggio non allineato

Il linguaggio tecnico della cybersecurity non è integrato nel Board; il dialogo con i vertici rimane complesso.

Solo il 9% misura il ROI

La maggioranza (53%) si concentra ancora solo su metriche prettamente tecniche anziché finanziarie.

Centro di costo, non di valore

La sicurezza è vista come un costo e non come abilitatore di business, rendendo critica la difesa dei budget.

Controllo attività

ATTIVITÀ CORE — GESTIONE INTERNA

90%	72%	71%
Definizione Strategie	Analisi del Rischio	Compliance Normativa

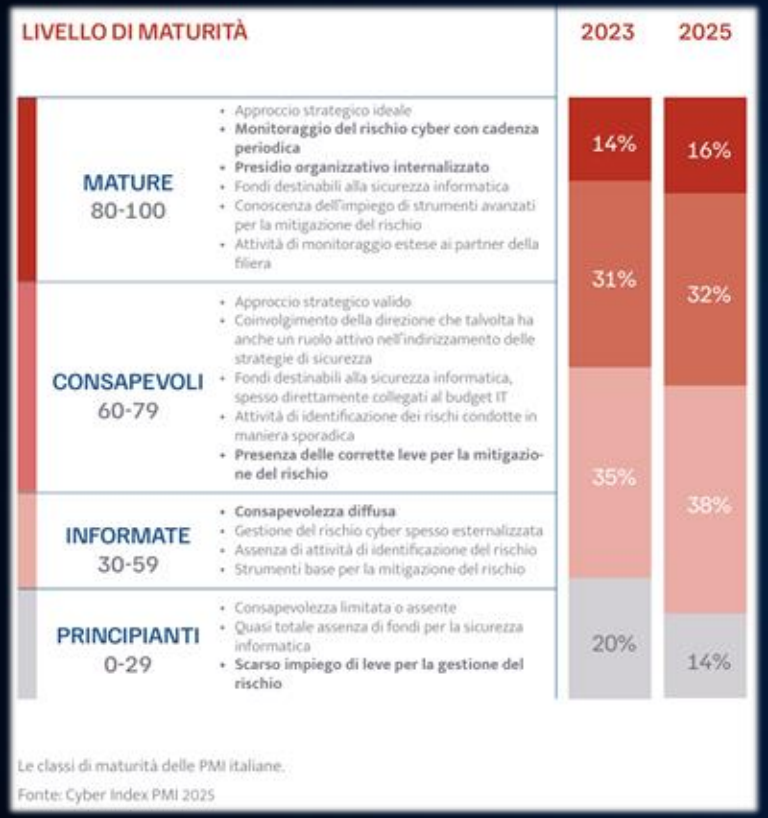
TALENT & RISORSE UMANE

88%	49%
delle imprese fatica a reclutare le competenze	cerca profili ibridi tecnici + business + risk

ATTIVITÀ OPERATIVE ANCORA TROPPO SPESSO ESTERNALIZZATE

Presenza nella filiera di attori che non presentano livelli di sicurezza adeguati.
Con l'aumento degli attacchi, l'anello debole della filiera rappresenta un potenziale punto di ingresso, un vettore per accedere all'infrastruttura critica e sferrare l'attacco.

LA MATURITÀ CYBER DELLE PMI ITALIANE: PROGRESSI, MA *GAP* ANCORA SIGNIFICATIVI



Le classi di maturità delle PMI italiane.
Fonte: Cyber Index PMI 2025

55
SU 100

CYBER INDEX PMI 2025

VS 52 DEL 2024
E 51 DEL 2023

- Cresce la consapevolezza cyber delle PMI italiane
- Approccio strategico in miglioramento (62/100)
- Persistono difficoltà nell'attuazione concreta delle misure di sicurezza
- Oltre il 70% permane nei livelli intermedi di maturità

LE PRINCIPALI INIZIATIVE DI SISTEMA A SUPPORTO

FORMAZIONE E DIFFUSIONE CULTURA CYBERSICUREZZA

- Campagne di sensibilizzazione
- Linee guida
- Aggiornamento continuo

UNIVERSITÀ E FORZA LAVORO ALLINEATA AL MERCATO

- Partnership
- ITS
- Tirocini
- Corsi qualificati
- Premi di laurea

GOVERNANCE

- Formazione del management
- Accountability
- Gestione del Rischio

SUPPORTO ALLE IMPRESE

- **E-academy**
- **Progetto Secure**
- **Accompagnamento alla compliance (NIS2)**

La cybersicurezza non rappresenta più soltanto una misura tecnica di protezione, ma una leva strategica per la competitività, la resilienza e la sicurezza economica del sistema Paese.