CYBER INDEX PMI

RAPPORTO LAZIO 2024

La cultura digitale protegge la tua impresa

Unindustria, Roma, 1° aprile 2025

Promosso da:

GENERALI

CONFINDUSTRIA

Partner scientifico:

POLIMI SCHOOL OF MANAGEMENT

osservatori.net digital innovation

Partner Istituzionale:

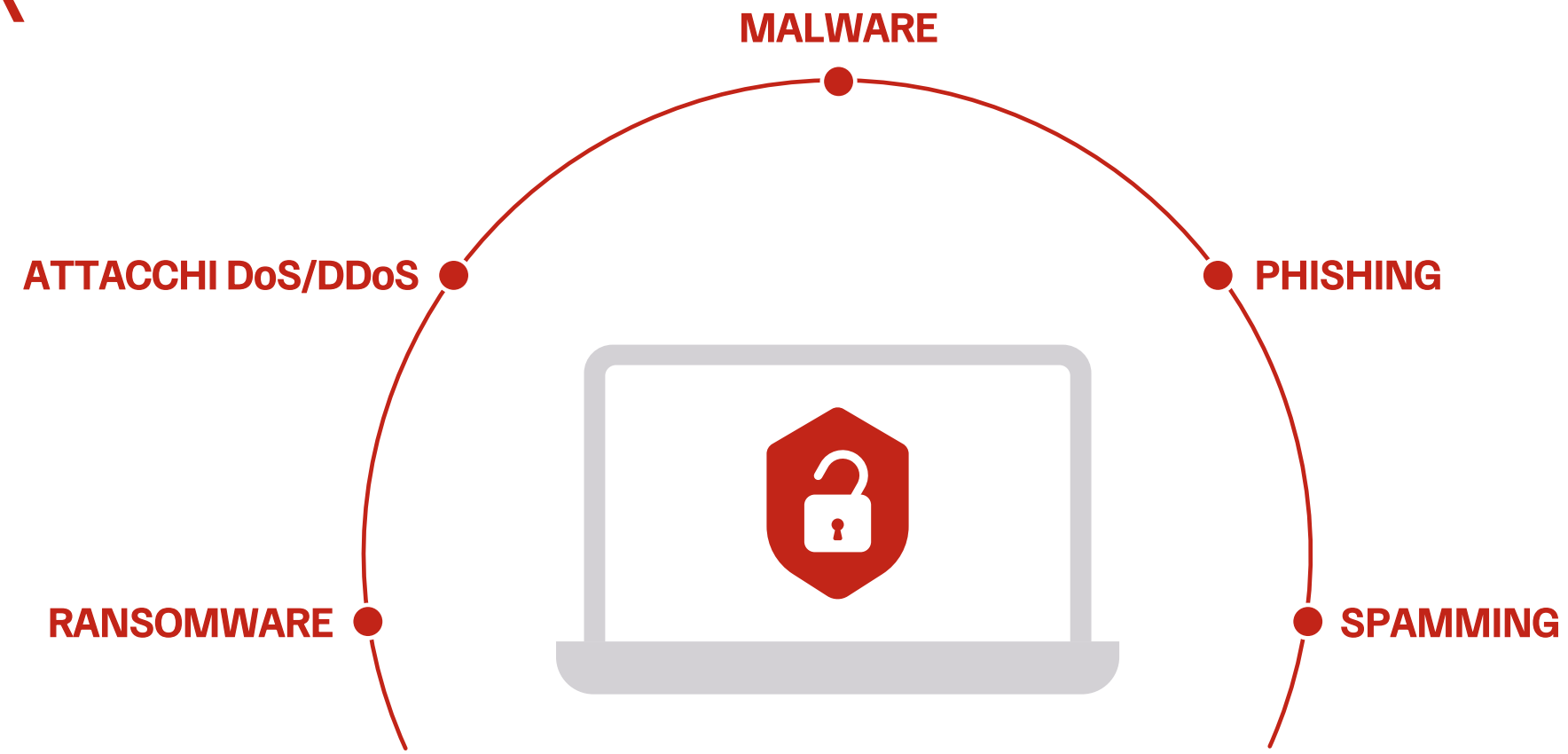
ACN

CYBER RISK: DEFINIZIONE

Cosa si intende per Cyber Risk

Per ”Cyber Risk" si intende qualsiasi rischio di perdita finanziaria, interruzione o danno alla reputazione di un'organizzazione derivante da un malfunzionamento dei suoi sistemi informatici.

MINACCE CYBER



I RISCHI PER LE IMPRESE

- Downtime di rete/interruzione del servizio
- Estorsione digitale
- Perdita, alterazione o distruzione di dati aziendali
- Perdita, alterazione o distruzione di dati di terzi
- Perdita, alterazione o distruzione di proprietà intellettuale
- Danno di immagine
- Sanzioni normative
- Danni materiali a infrastrutture IT
- Danni a sistemi industriali o dispositivi connessi
- Diffamazione
- Trasmissione di virus a computer o sistemi di terzi

CONTESTO DI RIFERIMENTO

Nel 2024 sono stati registrati 3.541 attacchi gravi verso organizzazioni in tutto il mondo, dato in crescita del 27% rispetto all'anno precedente[1].

In Italia, solo nell'ultimo semestre del 2024 sono stati individuati 977 eventi cyber: di questi, 405 sono classificati quali incidenti con impatto confermato[2].

Lo scenario del rischio cyber si caratterizza per gli sviluppi tecnologici, guidati in primis dall'intelligenza artificiale, e per l'evoluzione del quadro normativo, con l'entrata in vigore della NIS2.

La piena fruibilità dell'AI da parte di chiunque (anche cyber-criminali) rischia di creare nuove vulnerabilità e minacce alle imprese

La Direttiva NIS2 entra finalmente in scena con l'obiettivo di stabilire un livello comune di cyber-resilienza tra le organizzazioni europee

A **livello italiano** cresce l'interesse verso le **tematiche cyber**: è la **priorità di investimento in digitale per PMI per il terzo anno di fila**.

Questo interesse viene anche evidenziato dalla **crescita del valore del mercato cyber italiano** per il 2024, che ha raggiunto il livello record di **2.48 mld di euro**, registrando un **+ 15% rispetto al 2023**[3].

Le PMI, necessitano di strumenti per migliorare la gestione dei rischi cyber

1. Fonte: Rapporto Clusit 2024
2. Fonte: Operational Summary, Agenzia per la Cybersicurezza Nazionale, Dicembre 2024
3. Fonte: Osservatorio Cybersecurity & Data Protection – School of Management del Politecnico di Milano

CYBER INDEX PMI: RICERCA E METODOLOGIA

APPROCCIO STRATEGICO

Formalizzazione della **responsabilità** della sicurezza informatica e definizione degli **investimenti** a lungo termine.

IDENTIFICAZIONE

Capacità di comprendere il **dominio aziendale** e la **filiera**, identificare le risorse e gli asset aziendali e le possibili implicazioni sul **rischio cyber** e adeguamento ai **requisiti normativi**.

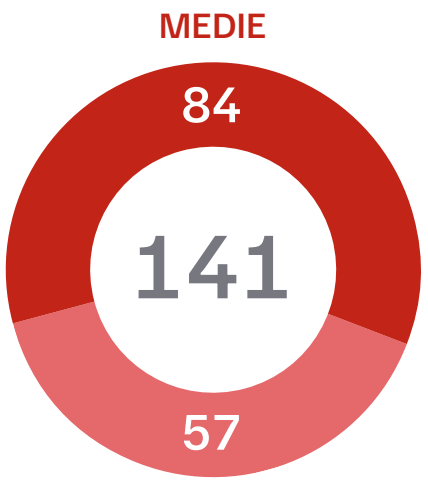
ATTUAZIONE

Capacità di selezionare il corretto **mix di competenze e modelli organizzativi** e di implementare iniziative concrete in termini di **persone, processi e tecnologie**.

AREE DI ANALISI

- Commitment della proprietà
- Presidio organizzativo
- Budget
- Certificazioni aziendali
- Piano di sicurezza aziendale
- Mappatura degli asset informatici
- Valutazione delle vulnerabilità
- Auditing & Compliance
- Misurazione del rischio cyber
- Valutazione delle terze parti
- Cyber risk management
- Fattore umano
- Formazione
- Tecnologie
- Assicurazioni
- Gestione patch
- Figure specializzate
- Gestione degli incidenti
- Gestione delle terze parti
- Programmi di info-sharing

AZIENDE INTERVISTATE



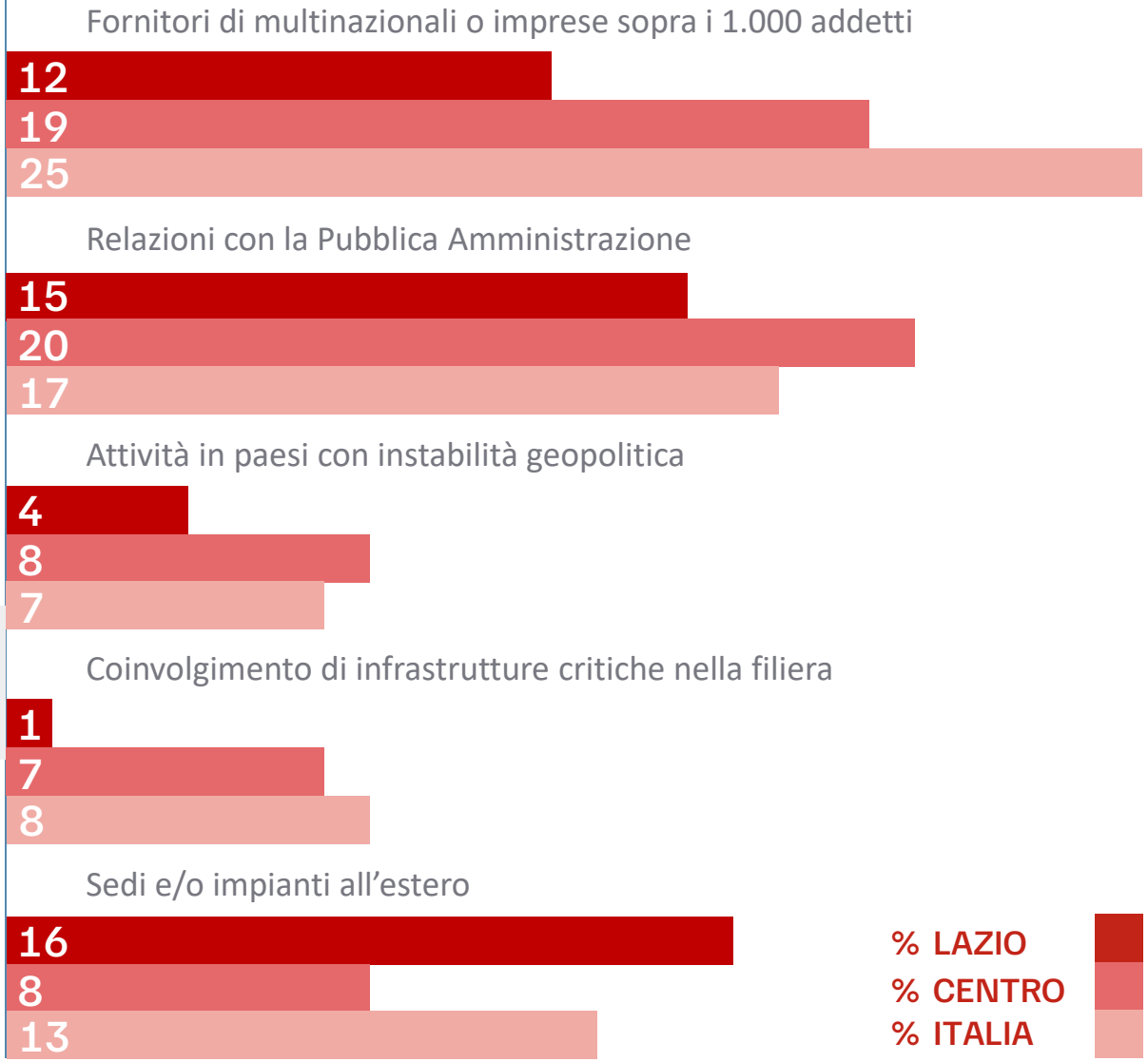
	LAZIO	CENTRO	ITALIA
PMI che fanno ricorso a strumenti digitali per supportare l'attività aziendale	60%	80%	86%
Gestione di dati confidenziali e di interesse nazionale	23%	19%	24%
PMI che dichiarano di aver subito una violazione negli ultimi 4 anni	4%	4%	9%

ESPOSIZIONE AI RISCHI

// LE PMI DEL LAZIO SONO ESPOSTE A RISCHI LEGATI ALLE TERZE PARTI

ATTACCO A TERZE PARTI

Un **attacco alla supply chain** è un attacco informatico che **prende di mira la catena di fornitura** dell'impresa per **compromettere la sicurezza** di un **sistema** o di un'**organizzazione**.



INDICE SINTETICO DEL LAZIO E CENTRO ITALIA

Le PMI del **Lazio** dimostrano un **basso livello** di consapevolezza sui rischi cyber

La media del Lazio è in linea con alla media del Centro Italia **(41)**, ma inferiore alla media nazionale **(52)**

Evidenze analoghe emergono dal confronto tra le singole dimensioni

APPROCCIO STRATEGICO

L'approccio strategico rappresenta la capacità di formalizzare internamente o esternamente la **responsabilità** della sicurezza informatica, coinvolgendo i vertici aziendali, e di definire **investimenti** a lungo termine.

47% degli imprenditori, o dei vertici aziendali, si interessa al tema della sicurezza informatica

29% delle PMI ha previsto fondi per l'acquisto di soluzioni e servizi per affrontare i rischi informatici

39% delle PMI ha definito un presidio interno, il 41% ha affidato la responsabilità a un Partner esterno

LIVELLO APPROCCIO STRATEGICO

48 LAZIO
53 CENTRO
56 ITALIA

AREE DI ANALISI

- Commitment della proprietà
- Presidio organizzativo
- Budget
- Certificazioni aziendali
- Piano di sicurezza aziendale

// PMI POCO PROPENSE ALL'APPROCCIARSI IN MANIERA STRATEGICA ALLA SICUREZZA INFORMATICA

IDENTIFICAZIONE

L'identificazione rappresenta la capacità di comprendere il **dominio aziendale** e la **filiera**, monitorando le risorse e gli asset aziendali, le possibili relative implicazioni sul **rischio cyber** e le necessità di adeguamento ai requisiti **normativi**.

LIVELLO IDENTIFICAZIONE

43 LAZIO
41 CENTRO
45 ITALIA

AREE DI ANALISI

- Mappatura degli asset informatici
- Cyber risk management
- Auditing & Compliance
- Misurazione del rischio cyber
- Valutazione delle terze parti
- Valutazione delle vulnerabilità

52% delle PMI prevede un processo di mappatura degli asset informatici

46% delle PMI svolge attività di auditing sugli aspetti di sicurezza informatica

// SCARSO LIVELLO DI CONOSCENZA DEL DOMINIO CYBER AZIENDALE

ATTUAZIONE

L'attuazione rappresenta la capacità di selezionare il corretto **mix di competenze e modelli organizzativi** e di implementare **iniziative concrete** in termini di **persone, processi e tecnologie**.

30% delle PMI dispone di tecnologie di base per la protezione dei dati, 60% dispone di tecnologie di base per la protezione delle reti, 33% dispone di tecnologie di base per l'identificazione delle anomalie

75% delle PMI ha definito diritti e modalità di accesso ai dati, 35% eroga corsi di formazione sulla cybersecurity

LIVELLO ATTUAZIONE

51 LAZIO
52 CENTRO
57 ITALIA

AREE DI ANALISI

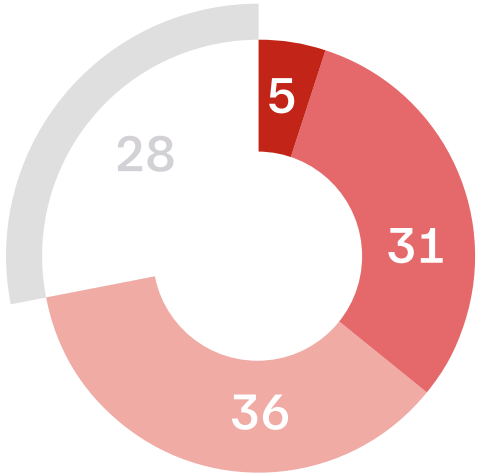
Fattore umano	Formazione
Tecnologie	Assicurazioni
Gestione patch	
Figure specializzate	
Gestione degli incidenti	
Gestione delle terze parti	
Programmi di info-sharing	

// SCARSA DIFFUSIONE DI LEVE TECNOLOGICHE PER LA GESTIONE DEL RISCHIO CYBER

FOCUS PROTEZIONE LAZIO

Le PMI del Lazio sono poco consapevoli dei benefici delle polizze assicurative.

// IL TRASFERIMENTO DEL RISCHIO CYBER RESIDUO È UNA POSSIBILITÀ ANCORA POCO ESPLORATA DALLE PMI. SOLO IL 5% HA GIÀ INTRODOTTO POLIZZE ASSICURATIVE



Già attive coperture assicurative per trasferire il rischio cyber

In valutazione l'introduzione di coperture assicurative per trasferire il rischio cyber

Non sono state stipulate polizze assicurative per trasferire il rischio cyber

Non a conoscenza della possibilità di stipulare polizze per trasferire il rischio cyber

LIVELLO DI MATURITÀ

MATURE
80-100

- Approccio strategico ideale
- Monitoraggio del rischio cyber con cadenza periodica
- Presidio organizzativo internalizzato
- Fondi destinabili alla sicurezza informatica
- Conoscenza dell'impiego di strumenti avanzati per la mitigazione del rischio
- Attività di monitoraggio estese ai partner della filiera

CONSAPEVOLI
60-79

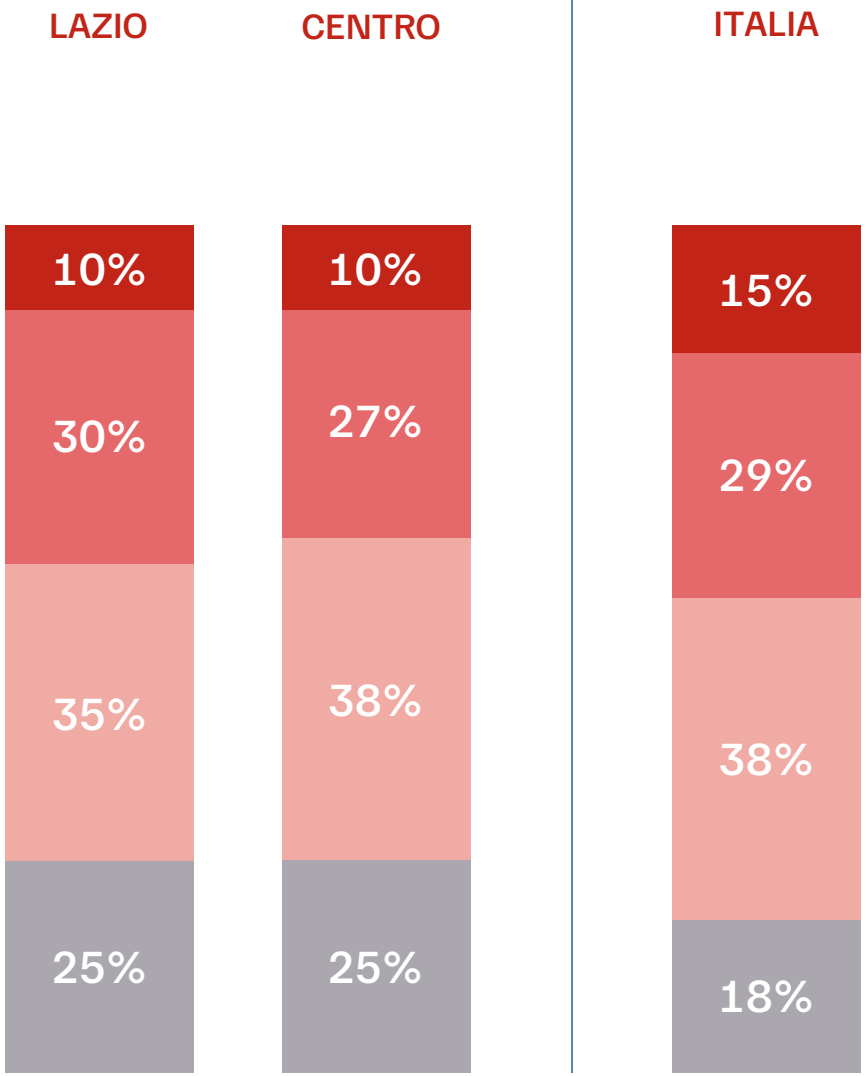
- Approccio strategico valido
- Coinvolgimento della direzione che talvolta ha anche un ruolo attivo nell'indirizzamento delle strategie di sicurezza
- Fondi destinabili alla sicurezza informatica, spesso direttamente collegati al budget IT
- Attività di identificazione dei rischi condotte in maniera sporadica
- Presenza delle corrette leve per la mitigazione del rischio

INFORMATE
30-59

- Consapevolezza diffusa
- Gestione del rischio cyber spesso esternalizzata
- Assenza di attività di identificazione del rischio
- Strumenti base per la mitigazione del rischio

PRINCIPIANTI
0-29

- Consapevolezza limitata o assente
- Quasi totale assenza di fondi per la sicurezza informatica
- Scarso impiego di leve per la gestione del rischio



SCARICA IL REPORT CYBER INDEX PMI 2024

Bit.ly/CIPMI2024

Eventuali informazioni o chiarimenti in merito all'indagine e ai risultati possono essere richiesti al Dott. Nicola Ciani (nicola.ciani@polimi.it)

CYBER INDEX PMI

Grazie

Promosso da:

GENERALI

CONFINDUSTRIA

Partner scientifico:

POLIMI SCHOOL OF MANAGEMENT

osservatori.net digital innovation

Partner Istituzionale:

ACN