CYBER INDEX PMI

RAPPORTO EMILIA-ROMAGNA 2023

La cultura digitale protegge la tua impresa

Confindustria Emilia, Bologna, 29 febbraio 2024

Promosso da:

GENERALI

CONFINDUSTRIA

Partner scientifico:

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT

osservatori.net digital innovation

Partner Istituzionale:

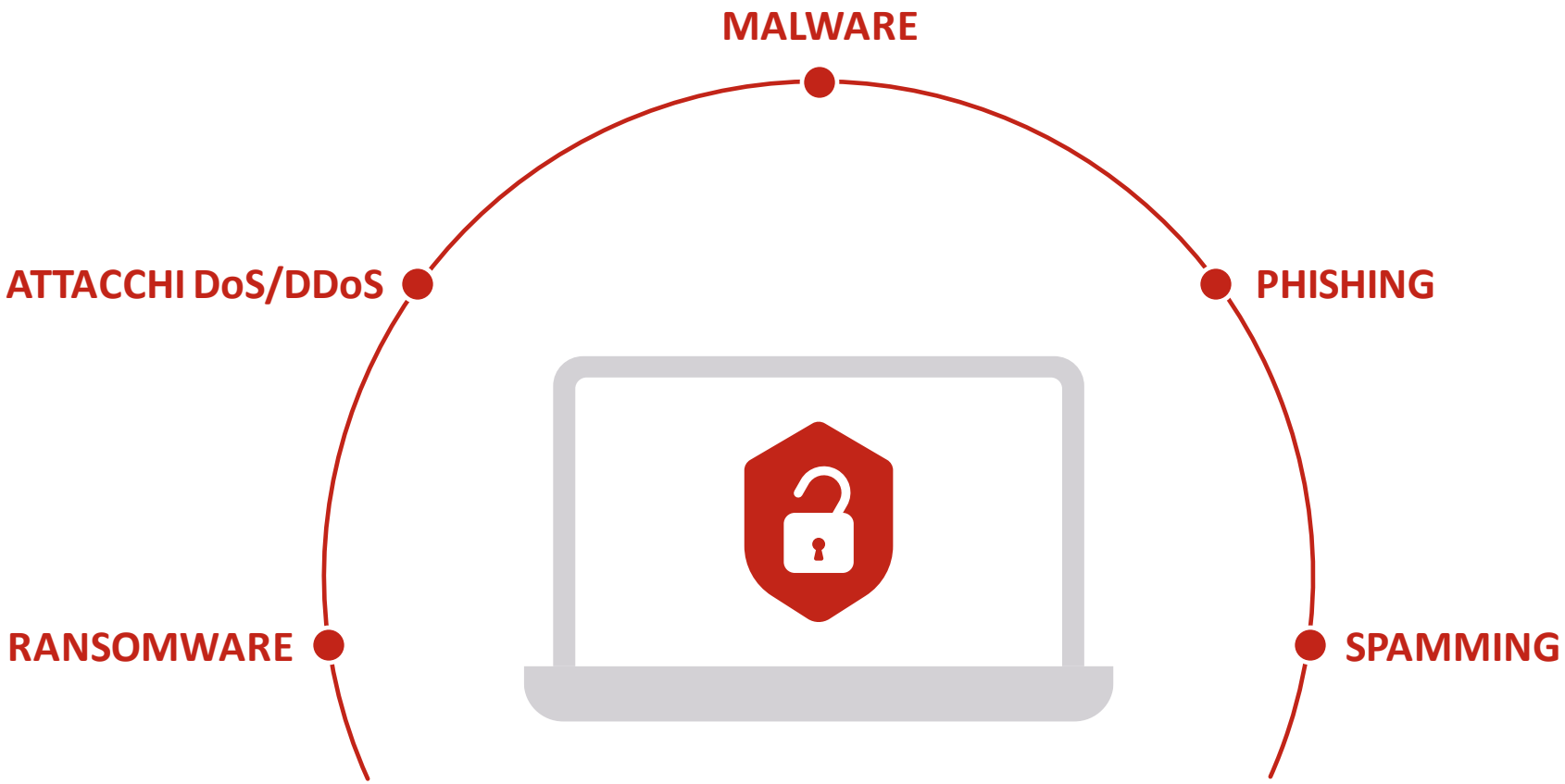
ACN

CYBER INDEX: DEFINIZIONE

Cosa si intende per Cyber Index

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

Il **panorama** di riferimento per la **sicurezza informatica** sta vivendo un **momento di grande turbolenza**: nella "**nuova normalità**" post-pandemia gli **attacchi informatici** sono sempre **più frequenti e significativi**.

Dal **2018 al 2022** si è rilevato un **aumento del 60% degli attacchi gravi** di dominio pubblico a livello mondiale[1].

A **livello italiano** cresce l'interesse verso le **tematiche cyber**: è la **priorità di investimento in digitale per PMI e grandi imprese** per due anni di fila.

Questo interesse viene anche evidenziato dalla **crescita del valore del mercato cyber italiano** per il 2022, che ha raggiunto il livello record di **1.86 mld di euro**, registrando un
+ 18% rispetto al 2021[2].

Si registra anche a **livello istituzionale un maggior interesse verso le tematiche cyber**: nel **PNRR** la sicurezza informatica ricopre un ruolo rilevante, con investimenti previsti nella Missione 1 e nella Missione 4. È stata inoltre introdotta l'**Agenzia per la Cybersicurezza Nazionale** (ACN), struttura che ha l'obiettivo di creare un fronte comune contro le minacce informatiche.

Le PMI necessitano di strumenti per aumentare la propria consapevolezza e migliorare la gestione dei rischi cyber

1. Fonte: Rapporto Clusit 2023
2. 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**.

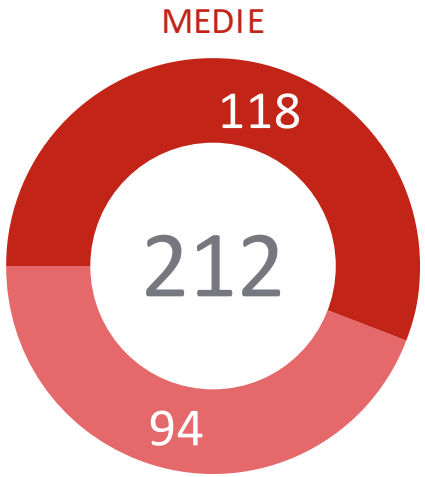
ATTUAZIONE

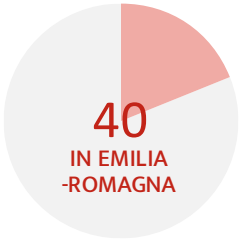
Capacità di selezionare il corretto **mix di competenze e modelli organizzativi** e di implementare iniziative concrete in termini di **persone, processi e tecnologie**.

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
- Processo di adeguamento normativo
- Fattore umano | Formazione
- Tecnologie | Assicurazioni
- Gestione delle terze parti
- Programmi di info-sharing

AZIENDE INTERVISTATE





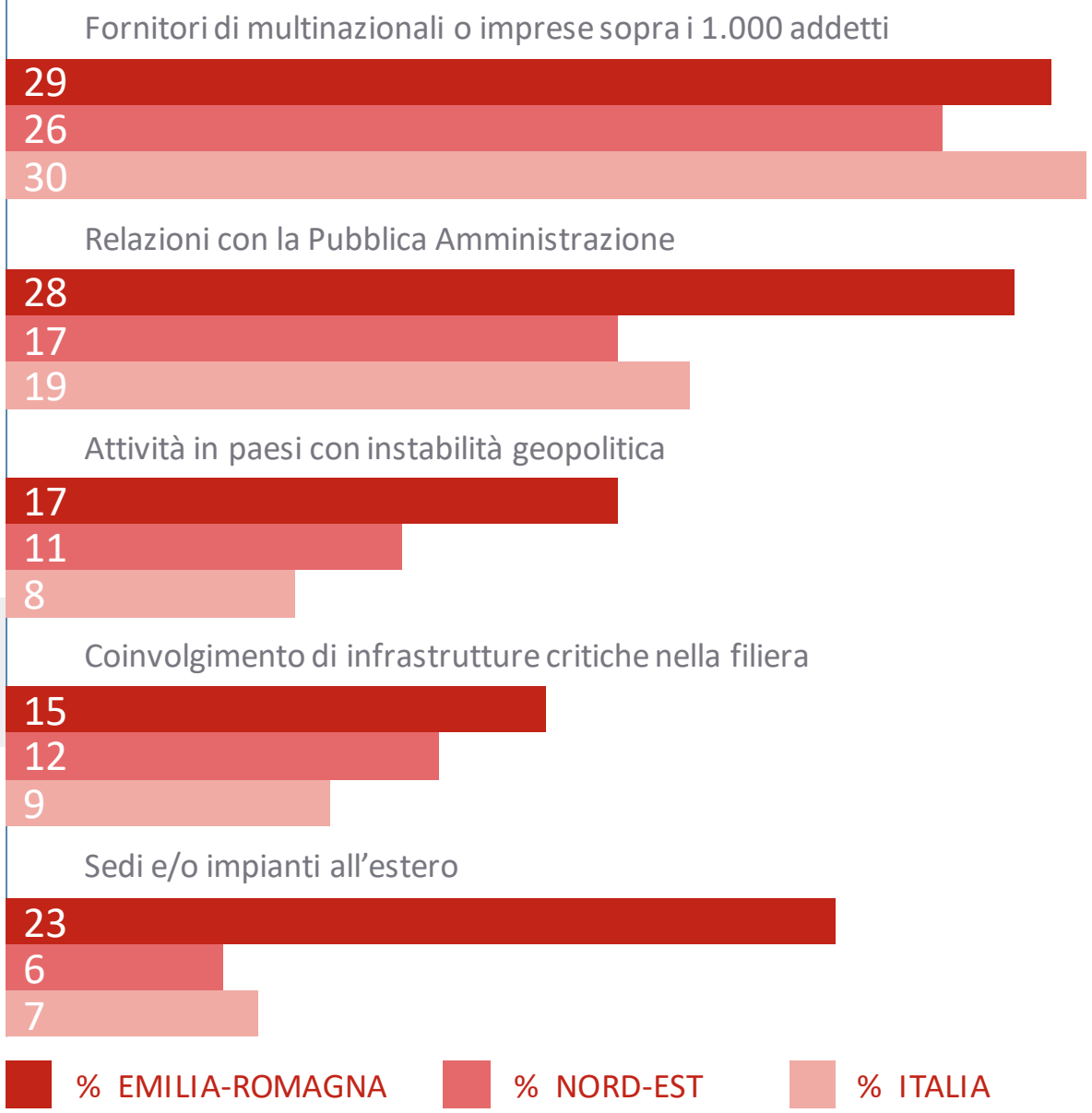
	NORD-EST	EMILIA -ROMAGNA
PMI che fanno ricorso a strumenti digitali per supportare l'attività aziendale	88%	91%
PMI operanti all'estero	66%	54%
PMI che dichiarano di aver subito una violazione negli ultimi 4 anni	13%	11%

ESPOSIZIONE AI RISCHI

// LE PMI EMILIANO-ROMAGNOLE RISULTANO MAGGIORMENTE ESPOSTE A RISCHI LEGATI ALLE TERZE PARTI RISPETTO ALLA MEDIA NAZIONALE

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**.



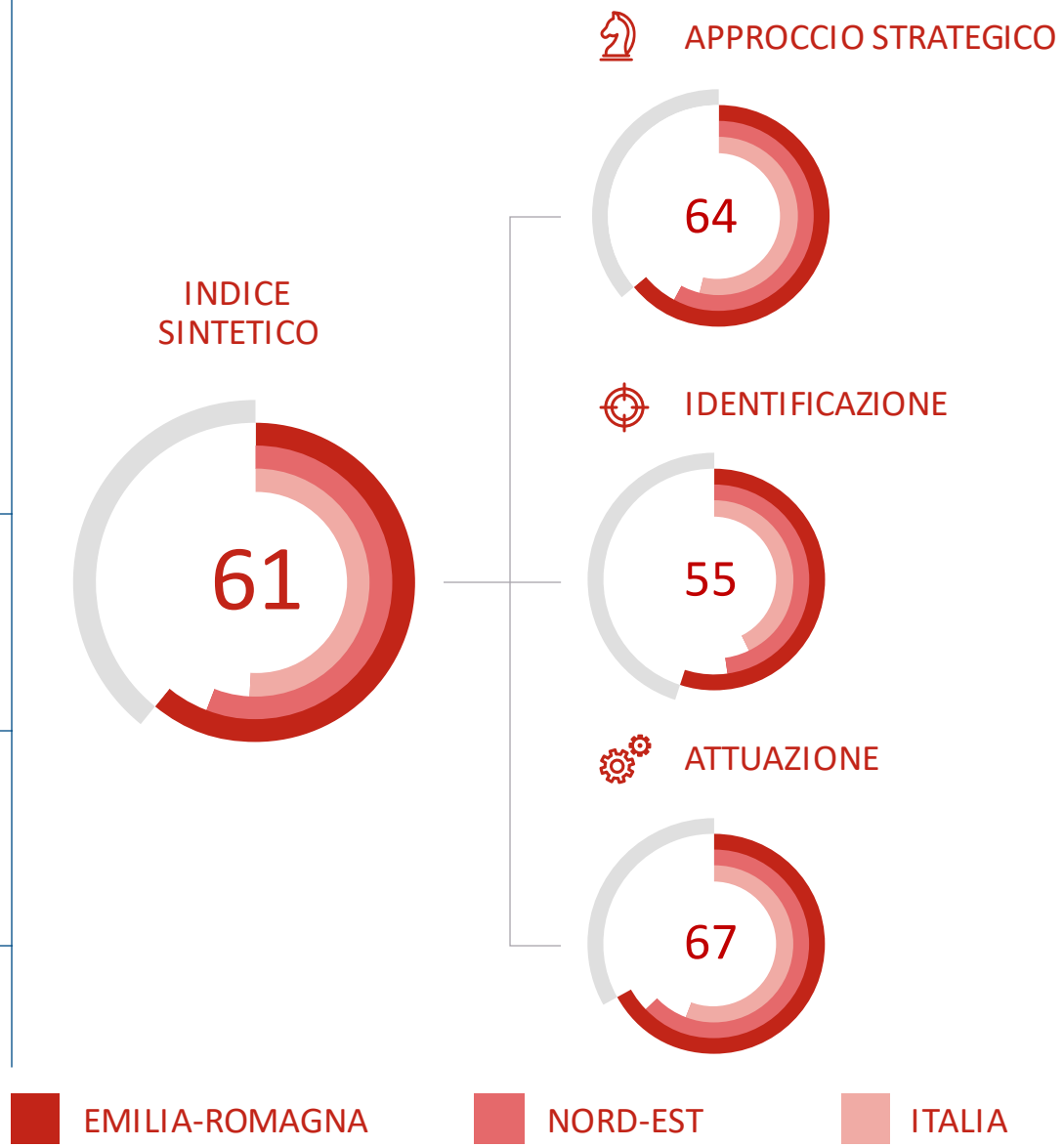
INDICE SINTETICO DELL'EMILIA-ROMAGNA

Le PMI dell'**Emilia-Romagna** dimostrano un **buon livello** di consapevolezza e preparazione

Si registra una lieve criticità nella dimensione dell'identificazione

La media dell'Emilia-Romagna è superiore sia alla media del Nord-Est **(56)**, sia alla media nazionale **(51)**

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.

78% degli imprenditori, o dei vertici aziendali, si interessa al tema della sicurezza informatica

76% delle PMI ha previsto fondi per l'acquisto di soluzioni e servizi per affrontare i rischi informatici

52% delle PMI ha definito un presidio interno, il **35%** ha affidato la responsabilità a un Partner esterno

LIVELLO APPROCCIO STRATEGICO

64	EMILIA-ROMAGNA
58	NORD-EST
54	ITALIA

AREE DI ANALISI

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

DIFFUSA MATURITÀ NELL'APPROCCIARSI IN MANIERA STRATEGICA ALLA SICUREZZA INFORMATICA, CON CRITICITÀ SULLE CERTIFICAZIONI ISO

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

55	EMILIA-ROMAGNA
48	NORD-EST
43	ITALIA

AREE DI ANALISI

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

89% delle PMI prevede un processo di mappatura degli asset informatici

49% delle PMI svolge attività di auditing sugli aspetti di sicurezza informatica

// BUON LIVELLO DI ATTENZIONE ALLE ATTIVITÀ DI BASE, A FRONTE DI DIFFICOLTÀ NELLA GESTIONE DELLE TERZE PARTI E NELLA MISURAZIONE DEL RISCHIO CYBER

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**.

74% delle PMI dispone di tecnologie di base per la protezione dei dati e dei dispositivi

56% delle PMI ha definito le corrette azioni per la gestione del fattore umano *(gestione degli accessi, policy comportamentali e iniziative di formazione)*

LIVELLO ATTUAZIONE

67	EMILIA-ROMAGNA
63	NORD-EST
56	ITALIA

AREE DI ANALISI

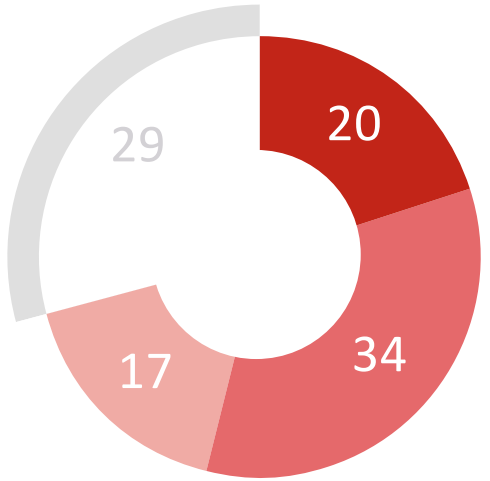
- Fattore umano
- Formazione
- Tecnologie
- Assicurazioni
- Gestione delle terze parti
- Programmi di info-sharing

// BUONA COGNIZIONE DELL'IMPIEGO DI LEVE PER LA GESTIONE DEL RISCHIO CYBER E DIFFUSA MATURITÀ IN TERMINI DI CAPACITÀ MITIGATORIA DEL RISCHIO CYBER

FOCUS PROTEZIONE EMILIA-ROMAGNA

Le PMI emiliano-romagnole sono comunque **consapevoli** dell'utilità delle polizze assicurative.

// IL TRASFERIMENTO DEL RISCHIO CYBER RESIDUO È UNA POSSIBILITÀ ANCORA POCO ESPLORATA DALLE PMI. SOLO IL 20% 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

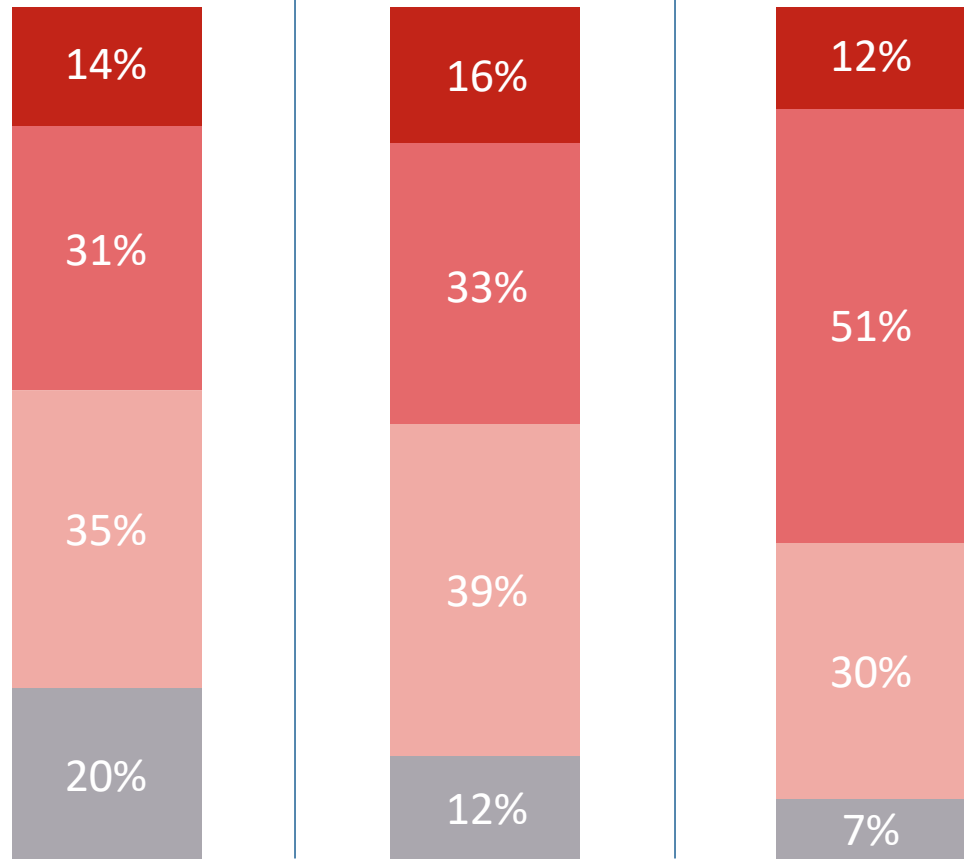
- Approccio strategico valido
- Coinvolgimento della direzione che talvolta ha anche un ruolo attivo nell'indirizzamento delle strategie di sicurezza
- Fondi destinabili alla sicurezza informatica, spesso direttamente collegati al budget IT
- Attività di identificazione dei rischi condotte in maniera 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 2023

Bit.ly/CIPMI2023

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

COMPILAZIONE SURVEY 2024

L'indagine è stata aggiornata nei contenuti:
sono stati integrati temi legati al Patch Management, Competenze e Disaster Recovery.

Compila la Survey 2024
inquadrando il seguente QR code
o al link:

Bit.ly/cyberindexpmi2024

CYBER INDEX PMI

Grazie

Promosso da:

GENERALI

CONFINDUSTRIA

Partner scientifico:

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT

osservatori.net digital innovation

Partner Istituzionale:

ACN