CYBER INDEX PMI

LA CULTURA DIGITALE PROTEGGE LA TUA IMPRESA

Promosso da

GENERALI

CONFINDUSTRIA

Partner scientifico

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT

osservatori.net digital innovation

Partner istituzionale

ACN

INDICE

CYBER INDEX PMI
LA CULTURA DIGITALE PROTEGGE LA TUA IMPRESA

RAPPORTO CYBER INDEX PMI 2023

INTRODUZIONE

Le piccole e medie imprese, il 99% del tessuto imprenditoriale del nostro Paese, sono un vero e proprio motore dell'Azienda Italia: vettori di creatività, eccellenza, capacità competitiva, innovazione e cultura. Accompagnano e segnano, da sempre, l'evoluzione e la geografia economica del nostro Paese concorrendo a determinare, spesso anticipando, le grandi trasformazioni sociali, economiche e ambientali.

Continuare a promuoverne l'innovazione e favorirne la trasformazione digitale è una delle principali sfide del Paese. In questo scenario, e anche in considerazione del complesso contesto macro- economico e geopolitico che abbiamo di fronte, la sicurezza informatica riveste un ruolo sempre più centrale nella visione strategica di trasformazione tecnologica.

Nonostante le loro dimensioni ridotte, o forse soprattutto per questo, anche le PMI sono soggette a minacce cibernetiche e a rischi informatici che possono avere conseguenze rilevanti sulle attività e sulla continuità di business, specialmente in un contesto di filiera. Se da un lato è d'obbligo cogliere le opportunità della trasformazione digitale per sostenere la competitività dell'impresa, dall'altro è fondamentale garantirne la sicurezza e preservarne il patrimonio informativo.

È in questo contesto che nasce Cyber Index PMI, il primo rapporto che misura lo stato di consapevolezza e capacità di gestione in materia di rischi cyber delle piccole medie imprese italiane. Lo fa grazie a una partnership di valore in cui crediamo molto che integra il pubblico e il privato per un beneficio comune, a servizio del Paese.

Il Rapporto evidenzia come vi sia ancora una ridotta consapevolezza e comprensione del tema dei rischi cyber da parte delle piccole e medie imprese italiane, a fronte di una crescente attenzione in materia da parte di un significativo campione di PMI intervistate.

Proprio per questo il nostro obiettivo è promuovere la cultura della cyber sicurezza e sostenere così la digitalizzazione delle organizzazioni aziendali, grazie ad azioni concrete sul territorio per sensibilizzare le PMI italiane.

Il Rapporto Cyber Index PMI 2023 è il primo passo di un percorso culturale in cui crediamo fortemente: un impegno che, evolvendosi nel tempo, auspichiamo possa fornire uno strumento utile alla conoscenza, alla consapevolezza e alla costruzione di nuove competenze nelle PMI italiane su un tema così cruciale e sfidante.

Un impegno per il futuro del nostro Paese, della nostra economia e della nostra società.

L'iniziativa è promossa da Generali e Confindustria, con il supporto scientifico degli Osservatori Digital Innovation della School of Management del Politecnico di Milano e con la partnership istituzionale con l'Agenzia per la Cybersicurezza Nazionale.

Di: ***Giancarlo Fancel,*** Country Manager Italy & CEO Generali Italia
Bruno Frattasi, Direttore dell'Agenzia per la Cybersicurezza Nazionale
Remo Marini, Group Chief Security Officer Generali
Agostino Santoni, Vice Presidente Confindustria con Delega al Digitale

Lo scenario in cui si muovono le imprese è caratterizzato da una crescita incessante delle minacce cyber. In un contesto di trasformazione digitale sempre più spinta, gli attacchi informatici aumentano senza sosta, prendendo di mira piccole e grandi organizzazioni. Di conseguenza, negli ultimi anni si è registrata una crescente attenzione al tema cybersecurity, diventato la prima priorità di investimento nel digitale per PMI e grandi imprese.
Da questa esigenza nasce la promozione dell'iniziativa "**Cyber Index PMI**" sviluppata da **Generali** e **Confindustria**, con il supporto scientifico dell'**Osservatorio Cybersecurity & Data Protection** della School of Management del Politecnico di Milano e con la partecipazione dell'**Agenzia per la Cybersicurezza Nazionale**.

L'iniziativa si struttura con una **ricerca triennale**, con l'obiettivo di **misurare il livello di cultura e consapevolezza del rischio cyber nelle piccole e medie imprese italiane**. In particolare, Cyber Index PMI evidenzia e monitora nel tempo il livello di conoscenza dei rischi cyber all'interno delle organizzazioni aziendali e le modalità di approccio adottate dalle stesse per la gestione di tali rischi.

Lo scopo principale del Rapporto Cyber Index PMI è quello di rispondere al bisogno delle aziende italiane di **conoscere**, **comprendere** ed **affrontare** al meglio la propria **esposizione al rischio cyber**, supportando le organizzazioni nella **scelta delle tutele più opportune**, rendendole consapevoli dell'**importanza del monitoraggio e del controllo delle attività** e mostrando loro le **tecniche** e le **tecnologie adottabili** a supporto della gestione del cyber risk.

A tal fine, a tutti coloro che hanno contribuito alla Ricerca e manifestato esplicito interesse, verranno successivamente condivisi i risultati dell'indagine e un **report personalizzato sul proprio posizionamento** rispetto al campione complessivo. Nello specifico, a conclusione dell'analisi viene attribuito ad ogni impresa un livello di maturità in materia di cyber sicurezza sulla scala "Principiante – Informata – Consapevole – Matura", in base al valore dell'indice ottenuto e quindi al grado di consapevolezza e di capacità di mitigazione del rischio.

Il report personalizzato rappresenta un **primo strumento di valutazione e di mappatura individuale per ciascuna azienda**. Sarà possibile affiancare successivamente un'**analisi approfondita** da effettuarsi con soluzioni specialistiche, utili per accrescere il livello di protezione rispetto ai rischi cyber: attività di consulenza, strumenti tecnologici e prodotti assicurativi, personalizzati in base alla cultura cyber e digitale d'impresa.

Con la partecipazione a questa indagine, le piccole e medie imprese italiane non solo supportano i partner dell'iniziativa dando un contributo nella creazione e nella diffusione della cultura cyber e digitale, ma ne traggono benefici anche in termini di acquisizione di consapevolezza, che possono portare ad un'innovazione tecnologica più sicura ed efficiente.

CYBER INDEX PMI
LA CULTURA DIGITALE PROTEGGE LA TUA IMPRESA

RAPPORTO CYBER INDEX PMI 2023

EXECUTIVE SUMMARY

Il panorama di riferimento per il rischio cyber sta vivendo un momento di grande turbolenza. Nella "nuova normalità" che è seguita al periodo di emergenza sanitaria, **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].
I fattori che contribuiscono ad aumentare l'esposizione al rischio cyber delle organizzazioni sono molteplici. Da un lato, c'è la **proliferazione di nuove tecnologie digitali sia in ambito business** sia in ambito consumer, fortemente accelerata dalla pandemia, che ha portato a **un'espansione della superficie d'attacco**. Dall'altro lato c'è **l'instabilità geopolitica**, che, con lo scoppio del conflitto russo-ucraino, ha evidenziato nell'**information warfare** un nuovo potenziale fronte. Anche la **gestione della supply chain** ha assunto una crescente rilevanza per le organizzazioni dal punto di vista della sicurezza. Gli attori lungo la filiera sono sempre più interconnessi su scala globale, tanto che spesso risulta più semplice per un aggressore **accedere alla rete di un'azienda tramite un attacco a terze parti**.
Negli ultimi anni, anche grazie a una forte visibilità mediatica, si è assistito a una **progressiva presa di consapevolezza** da parte delle aziende, con un aumento dell'attenzione nei confronti della sicurezza informatica, considerata la principale priorità di investimento in digitale per PMI e grandi imprese[2].

Il rischio cyber, nella sua concezione tradizionale di minaccia ai sistemi informativi, non ha mutato solo nella manifestazione, ma anche nella **frequenza** con cui colpisce e nella **gravità** degli effetti prodotti. La nuova immagine che le imprese hanno del rischio cyber, come rischio operativo a tutti gli effetti, è legata all'evidenza che tali rischi hanno un **impatto concreto sulla performance e sulla reputazione aziendale**. Il rischio cyber non è più percepito come una minaccia che si manifesta come mero problema tecnico dell'infrastruttura aziendale, quanto come **un pericolo che può avere impatto sugli azionisti e sugli investitori, sui partner commerciali e sui fornitori, sui dipendenti e sui clienti**.

1. Fonte: Rapporto Clusit, marzo 2023
2. Fonte: Osservatorio Digital Transformation Academy, School of Management Politecnico di Milano

Questa presa di coscienza viene concretamente evidenziata sia dalla **crescita del mercato italiano della cybersecurity**, che ha raggiunto nel 2022 il livello record di **1.86 miliardi di euro** (**+18%** rispetto al 2021[3]), sia dagli **investimenti previsti dal Piano Nazionale di Ripresa e Resilienza (PNRR)** che hanno portato alla nascita dell'**Agenzia per la Cybersicurezza Nazionale**.

3. Fonte: Osservatorio Cybersecurity & Data Protection, School of Management Politecnico di Milano

Nonostante la progressiva presa di coscienza rispetto all'importanza della materia, il **cyber index** evidenza **un quadro di generale ritardo** nelle PMI italiane. **Il valore medio dell'indice è 51** su un punteggio massimo di 100. Il cyber index è derivato da una valutazione su diverse dimensioni: approccio strategico, capacità di comprendere il fenomeno e le minacce (identificazione), introduzione di leve per mitigare il rischio (attuazione)[4].

Dal Rapporto si evince che **la crescente attenzione sul tema stenta a tradursi in un vero e proprio approccio strategico** (punteggio medio *approccio strategico*: 54) che preveda la definizione di investimenti e la formalizzazione di responsabilità. Sebbene le leve di attuazione siano maggiormente sviluppate (punteggio medio *attuazione*: 56), **le PMI faticano a stabilire priorità**, perché spesso mancano le azioni di identificazione corrette che permettano di approcciare il tema in maniera più oculata e consapevole (punteggio medio *identificazione*: 43).

I rispondenti, rappresentativi dell'intera popolazione di PMI italiane, possono essere raggruppati in 4 livelli di maturità:

- **Alcune PMI (14%) possono essere considerate "mature"**, con un approccio strategico alla tematica, pienamente consapevoli dei rischi e in grado di mettere in campo le corrette leve di attuazione con iniziative che riguardano persone, processi e tecnologie.
- Un ulteriore **31%** è composto da **aziende che si possono definire "consapevoli"**, in grado di comprendere le implicazioni dei rischi cyber, ma con una capacità operativa spesso ridotta per poter mettere in campo le corrette azioni.
- Seguono poi le "**informate**", categoria a cui afferisce il **35%** delle PMI. Non pienamente consapevoli del rischio cyber e degli strumenti da mettere in atto, si approcciano al rischio cyber in modo «artigianale».
- Si segnala ancora **un 20% di imprese che si possono definire "principianti"**, poco consapevoli dei rischi cyber e con un basso livello di adozione di misure di sicurezza.
- **Il livello di maturità delle imprese è correlato con la dimensione aziendale**. Sebbene sia il questionario sia l'impostazione dell'indice tengano in considerazione questo aspetto, il cyber index sintetico passa da un valore medio di **43 per le micro-imprese**, a **53 per le piccole** e fino a **61 per le medie**.

4. Per maggiori dettagli sulla costruzione dell'indice, è possibile consultare la sezione Nota Metodologica

Non si evidenziano invece rilevanti differenze territoriali. La cybersecurity si conferma una tema critico in tutta la penisola, indipendentemente dalla provenienza geografica dell'azienda.
Analizzando alcune aree verticali che compongono la gestione della cybersecurity aziendale, si dimostra il messaggio di sostanziale ritardo, sebbene alcune viste lascino ben sperare nel percorso di progressiva maturazione delle PMI. Nel **51%** dei casi, infatti, il tema della cybersecurity **è percepito come strategico**, con un **commitment da parte dei vertici aziendali** che può portare anche in un loro coinvolgimento diretto. Le principali iniziative di alto livello sono legate alla formalizzazione di una figura o una responsabilità di presidio della materia e alla definizione di un budget destinabile alla sicurezza informatica. Rispetto al primo punto, si evidenzia una tendenza ad esternalizzare le competenze (**35%** delle PMI preferisce **affidarsi a fornitori esterni per la gestione della cybersecurity**) dovuta alle risorse spesso limitate e alle difficoltà di reperimento sul mercato e inserimento in organico di figure con competenze specialistiche. Solo il **17%** delle PMI **ha inserito una figura interna ad-hoc**, mentre permane una quota di PMI **(22%)** che **non presidia la sicurezza informatica**.

Per quanto riguarda gli investimenti, il 58% delle PMI manifesta un'**attenzione concreta**, stanziando un **budget per la sicurezza informatica**. Nella maggior parte dei casi i fondi attingono a un più ampio budget IT, mentre nel restante 17% se ne prevede uno dedicato.
Per quanto riguarda le azioni di mitigazione, le principali evidenze sono relative ai temi tecnologici, alla gestione del fattore umano e al trasferimento del rischio:

- la maggior parte delle PMI **(57%)** ha introdotto una **dotazione tecnologica** per il monitoraggio delle anomalie e per la protezione dei dati aziendali;
- il **41%** prevede **contromisure per limitare l'esposizione degli utenti aziendali a rischi informatici**, agendo sul «fattore umano» tramite l'introduzione di policy comportamentali o iniziative di formazione degli utenti;
- il trasferimento del rischio cyber residuo è una possibilità ancora poco esplorata e conosciuta dalle PMI. Una quota pari al **17% ha già stipulato polizze assicurative**, mentre il **30% non è a conoscenza** delle possibilità di copertura del rischio cyber.

La prima edizione del Cyber Index PMI rilascia messaggi agrodolci. **Parte delle PMI italiane ha recepito la rilevanza del tema** e si sta attrezzando per affrontare uno scenario in evoluzione, caratterizzato dall'inasprimento del rischio cyber. La ridotta dimensione delle Piccole e Medie Imprese, però, rende il **percorso di maturazione arduo. Permane una quota significativa di aziende che faticano a gestire il rischio** in maniera oculata e che ne sottovalutano i potenziali impatti. La strada da fare è ancora lunga: la notevole complessità del contesto rende necessaria una trasformazione culturale, **interpretando la cybersecurity come un fattore abilitante della trasformazione digitale**.

Considerando la **centralità assunta dalla materia nel contesto sociale globale** e con l'obiettivo di rendere resiliente il sistema economico, **si avverte l'opportunità di un approccio di sistema** in cui, accanto alle organizzazioni, vi sia un ruolo crescente delle istituzioni per sensibilizzare e definire opportunità di investimento comuni, in aggiunta al rafforzamento infrastrutturale.

La **durata pluriennale del Cyber Index PMI**, iniziativa nata già con orizzonte triennale, consentirà di monitorare **l'evoluzione della maturità delle PMI italiane, con l'auspicio di rilevare significative evoluzioni nell'approccio ai temi cyber**.

CYBER INDEX PMI
LA CULTURA DIGITALE PROTEGGE LA TUA IMPRESA

RAPPORTO CYBER INDEX PMI 2023

GESTIONE DEL RISCHIO CYBER NELLE PMI

INDICE

In un mondo sempre più interconnesso e tecnologicamente avanzato, le **PMI** devono **sfruttare i vantaggi derivanti dalla trasformazione digitale** per poter far **crescere e fiorire i loro business**. Le nuove tecnologie, però, **presentano anche nuovi rischi e difficoltà da affrontare**. Uno dei **pericoli maggiori** deriva dalla possibile **compromissione di sistemi informativi e dati aziendali riservati** da parte di attori malevoli. Per poter proteggere al meglio i sistemi informativi aziendali bisogna implementare i concetti della cosiddetta Information Security.

Per **INFORMATION SECURITY** si intende l'insieme delle misure e degli strumenti finalizzati a garantire e preservare confidenzialità, integrità e disponibilità delle informazioni. Information Security è un concetto ampio che abbraccia **la sicurezza del patrimonio informativo nel suo complesso,** includendo anche aspetti organizzativi e di sicurezza fisica.
La **CYBERSECURITY** rientra nell'Information Security e **si pone l'obiettivo di difendere il sistema informatico.**

CONFIDENZIALITÀ

Offrire confidenzialità significa **garantire che i dati e le risorse siano preservati dal possibile utilizzo o accesso da parte di soggetti non autorizzati**. La confidenzialità deve essere assicurata lungo tutte le fasi di vita del dato: dall'immagazzinamento, alle fasi di utilizzo e transito lungo una rete di connessione.

INTEGRITÀ

L'integrità è la **capacità di mantenere la veridicità dei dati e delle risorse e garantire che non siano in alcun modo modificate o cancellate**, se non ad opera di soggetti autorizzati.

DISPONIBILITÀ

La disponibilità fa riferimento alla possibilità, per i **soggetti autorizzati**, di **poter accedere alle risorse per un tempo stabilito ed in modo ininterrotto**. Ciò significa impedire che avvengano interruzioni di servizio e garantire che le risorse infrastrutturali siano pronte per la corretta erogazione di quanto richiesto.

GESTIRE LA SICUREZZA INFORMATICA IN AZIENDA VUOL DIRE GARANTIRE LA **PROTEZIONE DEL SISTEMA INFORMATICO E DEL PATRIMONIO INFORMATIVO**

Nota: *all'interno del RAPPORTO CYBER INDEX PMI i termini information security e cybersecurity saranno utilizzati in maniera intercambiabile.*

L'Information Security si pone quindi l'obiettivo di mitigare il **RISCHIO CYBER**, ovvero qualsiasi **rischio di perdita finanziaria, interruzione di attività o danno alla reputazione di un'organizzazione derivante da violazioni ai dati o ai sistemi informatici aziendali**.
Negli ultimi anni, gli **attacchi alla sicurezza informatica stanno aumentano in maniera significativa**, utilizzando tecniche e modalità sempre più sofisticate. Anche le **tipologie di vittime sono sempre più diversificate:** non solo grandi aziende **multinazionali o fortemente esposte**, ma anche **piccole e medie imprese**. Questi attacchi indiscriminati **colpiscono tutti i settori**: dalla manifattura ai trasporti, dalle pubbliche amministrazioni alla sanità, esponendo ingenti quantità di dati personali e aziendali o bloccando l'operatività delle imprese. **Diventa**, quindi, **fondamentale proteggere il patrimonio informativo** attraverso una combinazione **di soluzioni tecnologiche e competenze professionali per monitorare e mitigare il rischio cyber.**

Il 2022 ha messo in luce un **elevato livello di aggressività da parte degli attori malevoli nei confronti delle imprese italiane**. Dalla ricerca dell'Osservatorio Cybersecurity & Data Protection emerge che il **67% delle grandi organizzazioni italiane** ha rilevato un effettivo **aumento degli attacchi cyber.** Il **14%** di esse, inoltre, ha confermato di aver **subito attacchi che hanno generato conseguenze concrete, come interruzione dell'operatività aziendale, costi di ripristino e risarcimento oltre a danni d'immagine.**

SI DEFINISCE **GESTIONE DEL RISCHIO CYBER** L'INSIEME DI ATTIVITÀ IMPLEMENTATE COL FINE DI RIDURRE LA **PROBABILITÀ E L'IMPATTO** DEL RISCHIO CYBER

2.489
Attacchi informatici gravi di pubblico dominio rilevati nel 2022 a livello globale

+60%
Crescita degli attacchi informatici dal 2018 al 2022

67%
Grandi aziende italiane che hanno rilevato un aumento degli attacchi cyber

14%
Grandi aziende italiane che hanno subito attacchi cyber con conseguenze tangibili

Fonte: *Rapporto Clusit, marzo 2023; Osservatorio Cybersecurity & Data Protection, School of Management, Politecnico di Milano, 2022*

Principali tipologie di attacco

I **sistemi informativi aziendali** vengono in genere **compromessi** utilizzando **strumenti e tecniche di attacco comuni**, come attacchi malware, ransomware, DoS/DDoS o phishing. I criminali possono inoltre sfruttare modalità di attacco più avanzate e mirate, come per esempio ATP (Advanced PersistentThreat) o Spear Phishing. Esploriamo nel dettaglio alcune delle tecniche di attacco più diffuse:

MALWARE

Il termine "malware" identifica generalmente **applicazioni dannose finalizzate ad arrecare danno informatico alla vittima.**

RANSOMWARE

Un "ransomware" è un **particolare tipo di malware** che, dopo aver limitato o impedito del tutto l'accesso al sistema infettato, in genere criptando i file presenti su un dispositivo, **richiede una somma di denaro da pagare per la sua rimozione** e relativa decodificazione dei file.

PHISHING

Per "phishing" si intendono i **tentativi di frode informatica volti a carpire i dati sensibili degli utenti**. Generalmente un attacco di phishing si traduce nell'invio di e-mail, contenenti indicazioni e loghi "familiari", con cui si invita la vittima a fornire informazioni riservate (ad esempio password, codici di accesso o dati della carta di credito). Questa pratica rientra nella più ampia famiglia del **social engineering**, tecnica di cybercrime basata sulla manipolazione delle persone per carpirne informazioni confidenziali e dati sensibili.

ATTACCHI DOS/DDOS

Gli attacchi di tipo DoS (**Denial of Service**) o DDoS (**Distributed Denial of Service**) sono **finalizzati ad interrompere la continuità di servizio, rendendo,** di fatto, **inaccessibili i servizi presi di mira**. Possono essere messi in atto generando un numero eccessivo di richieste al server o un volume di traffico maggiore rispetto alla banda disponibile, saturando le risorse a disposizione.

Principali vettori di attacco

Per portare a compimento con successo i loro attacchi malevoli, gli **attori criminali sfruttano numerosi vettori e modalità di attacco**, dalle più comuni e immediate alle più sofisticate e di lungo termine. I vettori di attacco più diffusi sono:

Attacchi basati sulla rete

Questi attacchi mirano alle **vulnerabilità dell'infrastruttura e dei protocolli di rete**.

Attacchi basati sul web

Le **applicazioni Web** presentano spesso **vulnerabilità** che gli aggressori sfruttano per ottenere un **accesso non autorizzato o compromettere i dati degli utenti.**

Attacchi di Social Engineering

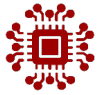
L'ingegneria sociale si rivolge alla **psicologia umana** e manipola le persone affinché **divulghino informazioni sensibili o eseguano azioni che compromettono la sicurezza**.

Attacchi basati su software

L'utilizzo di **software dannosi**, es. Malware, per **compromettere la sicurezza di sistemi e reti**.

Attacchi basati su connessioni wireless

Gli attacchi alle reti e ai dispositivi wireless sfruttano le **vulnerabilità dei protocolli di comunicazione wireless**.



Attacchi basati su infrastrutture fisiche

L'accesso fisico ai dispositivi o all'infrastruttura può essere sfruttato per **installare software malevoli o compiere azioni illegali**.

Attacco a terze parti

Merita un approfondimento, vista la diffusione, il vettore di attacco attraverso la filiera aziendale.

Un **attacco alla supply chain** è un tipo di attacco informatico che **prende di mira la catena di fornitura dell'impresa per compromettere la sicurezza di un sistema o di un'organizzazione**. Invece di attaccare direttamente i sistemi dell'organizzazione bersaglio, gli aggressori si concentrano sull'infiltrazione e sullo sfruttamento di componenti o processi affidabili all'interno della catena di fornitura per ottenere un accesso non autorizzato, rilasciare malware o manipolare il software.

I fattori di rischio

Gli attori malevoli hanno vari e diversificati motivi per portare a compimento le loro azioni criminali nei confronti delle organizzazioni. Proviamo a riassumere di seguito alcuni dei fattori di rischio più comuni:

Possesso di dati di clienti, fornitori, dipendenti

I dati riservati conservati dall'azienda possono rappresentare un obiettivo allettante per i criminali, che possono trafugarli per poi rivenderli ad altri malintenzionati oppure criptarli e chiedere un successivo riscatto per renderli nuovamente accessibili.

Proprietà di brevetti/segreti industriali

In maniera simile ai dati riservati, anche brevetti e segreti industriali di produzione possono essere un target appetibile per i malintenzionati. In questi casi molto spesso gli attori malevoli compiono queste azioni per conto di Stati nazionali, per azioni di spionaggio.

Partecipazione ad una filiera strategica

Essere membri di una filiera strategica aumenta la possibilità di essere vittima di attacchi, in quanto i malintenzionati cercano di sfruttare gli anelli deboli della filiera per riuscire ad entrare nei sistemi informativi collegati per colpire dall'interno vittime ben difese e prestigiose.

Esposizione nel contesto geopolitico

In situazioni di conflitto, si registra l'aumento della probabilità di subire un attacco, o campagne di attacchi mirati: in queste casistiche, l'attore malevolo si pone principalmente l'obiettivo di danneggiare e compromettere una determinata impresa, mettendo in secondo piano lo scopo estorsivo.

Le conseguenze degli attacchi

Purtroppo a volte gli **attacchi cyber** da parte di attori malevoli **possono andare a segno** e superare le difese aziendali violando i sistemi informativi ed informatici dell'impresa. Esaminiamo quindi quali sono le **conseguenze più comuni che le PMI italiane devono affrontare** in seguito ad un attacco hacker che va a buon fine:

Interruzione di servizio o ritardi nelle business operation

Un attacco hacker può portare al fermo delle macchine di produzione oppure al blocco dei sistemi informativi utilizzati in azienda, causando ingenti danni monetari legati all'interruzione delle attività.

Violazione o alterazione dei dati

I dati riservati dell'azienda possono essere criptati da ransomware, rendendoli inutilizzabili in mancanza di un corretto backup. Un'altra possibilità è che i dati vengano trafugati e poi diffusi sul web oppure venduti per ricavarne profitto.

Estorsione

L'obiettivo principale di molti criminali che usano ransomware è quello richiedere un riscatto, spingendo le vittime a pagare una somma di denaro per ottenere le chiavi con cui tornare in possesso dei dati riservati che sono stati criptati. È bene specificare che, avendo a che fare con organizzazioni criminali, il pagamento del riscatto non implica la garanzia di ottenere in cambio le chiavi per sbloccare i dati.

Costi di ripristino e risarcimento danni

In seguito ad un attacco hacker le aziende devono spendere ingenti quantità di denaro per ripristinare e rimettere in sicurezza i propri sistemi informativi. A volte, le aziende stesse possono anche essere oggetto di sanzioni da parte delle autorità per non aver protetto i dati personali dei propri clienti con le misure previste dalle normative vigenti.

Danno di immagine/reputazionale

Nelle fasi post attacco l'azienda deve anche ripristinare la propria immagine pubblica, danneggiata dall'incapacità di difendere con successo dati dei propri clienti o partner e/o da una inadeguata gestione dell'incidente.

Il ruolo della normativa nella gestione del rischio cyber

Come avviene per molti altri ambiti, la normativa contribuisce a definire standard e obblighi rivolti alle aziende per indirizzare le scelte operative e strategiche inerenti alla gestione del rischio cyber. La normativa può essere emanata sia da un Governo nazionale, sia da un'Istituzione sovranazionale, come l'Unione Europea. Ad esempio, l'UE ha approvato nel 2016 il Regolamento Generale sulla Protezione dei Dati, noto anche come GDPR, e dal 2018 è divenuto pienamente applicabile in tutti gli Stati Membri.

Indipendentemente dall'organo esecutivo, le **normative possono rivolgersi ad organizzazioni o settori specifici, promuovendo o imponendo un determinato comportamento, tra cui:**

1. l'attuazione di **misure di sicurezza adeguate per proteggere le informazioni considerate sensibili**. Tra le misure vengono inclusi l'implementazione di sistemi di autenticazione rafforzati, il controllo degli accessi, la crittografia dei dati e potenzialmente anche la designazione di un responsabile della sicurezza delle informazioni;
2. **la notifica di violazioni di sicurezza alle autorità competenti o agli individui interessati**. Ciò significa che se un'organizzazione subisce una violazione dei dati o la sua sicurezza è compromessa, potrebbe essere obbligata ad informare le parti interessate e adottare misure correttive;
3. **l'adeguamento a standard specifici**, come la norma ISO/IEC 27001, che fornisce un quadro per l'implementazione di un sistema di gestione della sicurezza delle informazioni.

Infine, le normative possono prevedere sanzioni di natura penale o amministrativa nel caso in cui non vengano recepite tempestivamente, soprattutto nel caso in cui dovessero verificarsi **violazioni di sicurezza informatica**.

Le normative giocano quindi un ruolo fondamentale nell'indirizzare le azioni delle aziende e garantire un adeguato livello di sicurezza informatica, anche all'interno di piccole e medie imprese; nelle pagine a seguire vengono quindi approfonditi il regolamento GDPR e la direttiva NIS 2, entrambi applicabili alle PMI italiane.

LE **NORMATIVE** SONO FONDAMENTALI PER **INDIRIZZARE LE AZIONI DELLE AZIENDE** E GARANTIRE UN ADEGUATO LIVELLO DI SICUREZZA INFORMATICA E PER AFFRONTARE LE SFIDE SEMPRE CRESCENTI NEL CAMPO

Il panorama normativo: GDPR

Tra le varie **disposizioni normative che possono interessare le PMI italiane**, sicuramente la più rilevante è quella contenuta all'interno del Regolamento generale sulla protezione dei dati (**GDPR**). Il GDPR è un regolamento emanato dall'Unione Europea (UE) che **stabilisce un quadro giuridico per la protezione dei dati personali e i diritti delle persone fisiche riguardo al trattamento di tali dati.**

Il Regolamento Generale è **entrato in vigore il 24 maggio 2016** ed è diventato applicabile **obbligatoriamente a partire dal 25 maggio 2018**, dopo un periodo di transizione di due anni, che ha permesso ai soggetti destinatari di implementare quanto necessario a mettersi in regola.

Il GDPR persegue **due obiettivi fondamentali**: da un lato, **adeguare la normativa**, ormai risalente al 1995, **alle nuove tecnologie**, dall'altro **armonizzare ed uniformare la normativa stessa a livello europeo**, creando un quadro normativo comune. Questi intenti vengono soddisfatti attraverso l'imposizione di una **serie di obblighi e principi fondamentali per garantire la protezione dei dati personali**. Tra questi, vi sono il principio di liceità, correttezza e trasparenza, che richiede che il trattamento dei dati abbia una base legale, sia trasparente per gli interessati e sia effettuato in modo lecito.

Inoltre, il principio di limitazione della finalità richiede che **i dati personali siano raccolti per scopi specifici, espliciti e legittimi e non siano trattati in modo incompatibile con tali scopi**.

Il GDPR impone anche **obblighi di sicurezza dei dati**. Le organizzazioni devono adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato al rischio, inclusi quelli di accesso non autorizzato, di perdita, di alterazione o di divulgazione dei dati personali.

Il Regolamento prevede inoltre l'obbligo di comunicazione alle autorità competenti entro 72 ore in caso di **violazione dei dati personali.**

In caso di mancato adempimento alle disposizioni, il Regolamento prevede sanzioni di diversa entità. Le autorità di controllo possono infliggere multe amministrative proporzionate all'entità della violazione: per esempio nel 2021 Amazon è stato multato per 746 milioni di Euro per non aver rispettato il consenso di profilazione per la pubblicità online.

IL **GDPR**, REGOLAMENTO IN VIGORE DAL 2016 IN **UNIONE EUROPEA**, IMPONE **OBBLIGHI E PRINCIPI** FONDAMENTALI PER LA **PROTEZIONE DEI DATI** E PREVEDE **SANZIONI** IN CASO DI VIOLAZIONE

Il panorama normativo: NIS 2

La nuova **direttiva Europea NIS 2** (Network and Information Security), entrata in vigore il 17 gennaio 2023 è una normativa sulla cybersecurity che riguarda le imprese che operano nel mercato comune Europeo. Si tratta di una **revisione della precedente direttiva NIS** del 2016, che introduceva obblighi di cyber sicurezza per gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali. La Direttiva NIS 2 **dovrà essere recepita entro 21 mesi dalla sua entrata in vigore** e per la **prima volta interesserà anche medie aziende, non solo quelle sopra i 250 dipendenti.**

Lo **scopo della direttiva è di garantire un elevato livello di sicurezza delle reti e dei sistemi informativi, prevenire e contrastare i cyberattacchi, e migliorare la cooperazione tra le autorità competenti**. La direttiva quindi **amplia il campo di applicazione** della precedente NIS, includendo **nuovi settori e attività** che sono considerati **critici per il funzionamento dell'economia e della società**, come amministrazioni pubbliche, servizi finanziari, servizi sanitari, servizi postali e di corriere, servizi di gestione dei rifiuti, servizi sociali, industrie chimiche, servizi alimentari e produzione industriale.

La direttiva NIS 2 stabilisce anche **requisiti più rigorosi per le misure di gestione dei rischi di cybersecurity che le entità soggette devono adottare**, nonché per la segnalazione degli incidenti di sicurezza informatica alle autorità competenti.

Inoltre, la direttiva NIS 2 prevede una **maggiore cooperazione** tra gli Stati membri e le istituzioni dell'UE per affrontare le sfide comuni in materia di cybersecurity, attraverso il **gruppo di cooperazione NIS**, i team di risposta agli incidenti di sicurezza informatica **(CSIRT)** e il centro europeo per la cybersecurity industriale, tecnologica e di ricerca **(ECCC)**.

IN VIGORE DA **GENNAIO 2023**, LA **DIRETTIVA NIS 2** HA LO SCOPO DI GARANTIRE UN ELEVATO LIVELLO DI SICUREZZA INFORMATICA, PREVENIRE E CONTRASTARE I CYBER ATTACCHI E MIGLIORARE LA COOPERAZIONE TRA LE AUTORITÀ COMPETENTI PER **MEDIE E GRANDI AZIENDE EUROPEE**

La cybersecurity nel PNRR

Il **PNRR** (Piano Nazionale di Ripresa e Resilienza), progetto strategico italiano ed europeo per il rilancio dell'economia italiana post emergenza Covid-19, **istituisce dei fondi per il rafforzamento della cybersecurity**. Gli investimenti sono **concentrati in due filoni**: la **trasformazione digitale della Pubblica Amministrazione** e l'**istruzione**. Potenziare PA ed istruzione permetterà di avere ricadute positive indirette anche sulle PMI italiane, ad esempio, con l'immissione di personale con nuove competenze nel settore.

In ambito PA, sono previsti **623 milioni di euro a favore di quattro pilastri principali.**

1. Rafforzamento dei **presidi di front-line** per la gestione degli alert e degli eventi a rischio sia per la PA che per il settore privato, migliorando in questo modo la prima linea di difesa contro possibili minacce.
2. **Miglioramento delle capacità di revisione dei componenti** utilizzati per la difesa da cyberattacchi.
3. **Immissione di nuove figure professionali nel corpo della Polizia di Stato** dedicate alla prevenzione e all'investigazione del crimine informatico.
4. **Rafforzamento delle unità cyber per la protezione della sicurezza nazionale e per la risposta alle minacce cyber**, focalizzando soprattutto l'attenzione verso le infrastrutture strategiche del Paese.

L'investimento nella PA permetterà di avere un **settore pubblico più forte e resiliente** contro le minacce cyber, capace di **trasmettere e diffondere questa conoscenza anche al settore privato**. Nella stessa ottica, il **rafforzamento delle unità cyber anti crimine** nel corpo della Polizia e della difesa **aiuterà il sistema paese a contrastare le crescenti minacce criminali**.

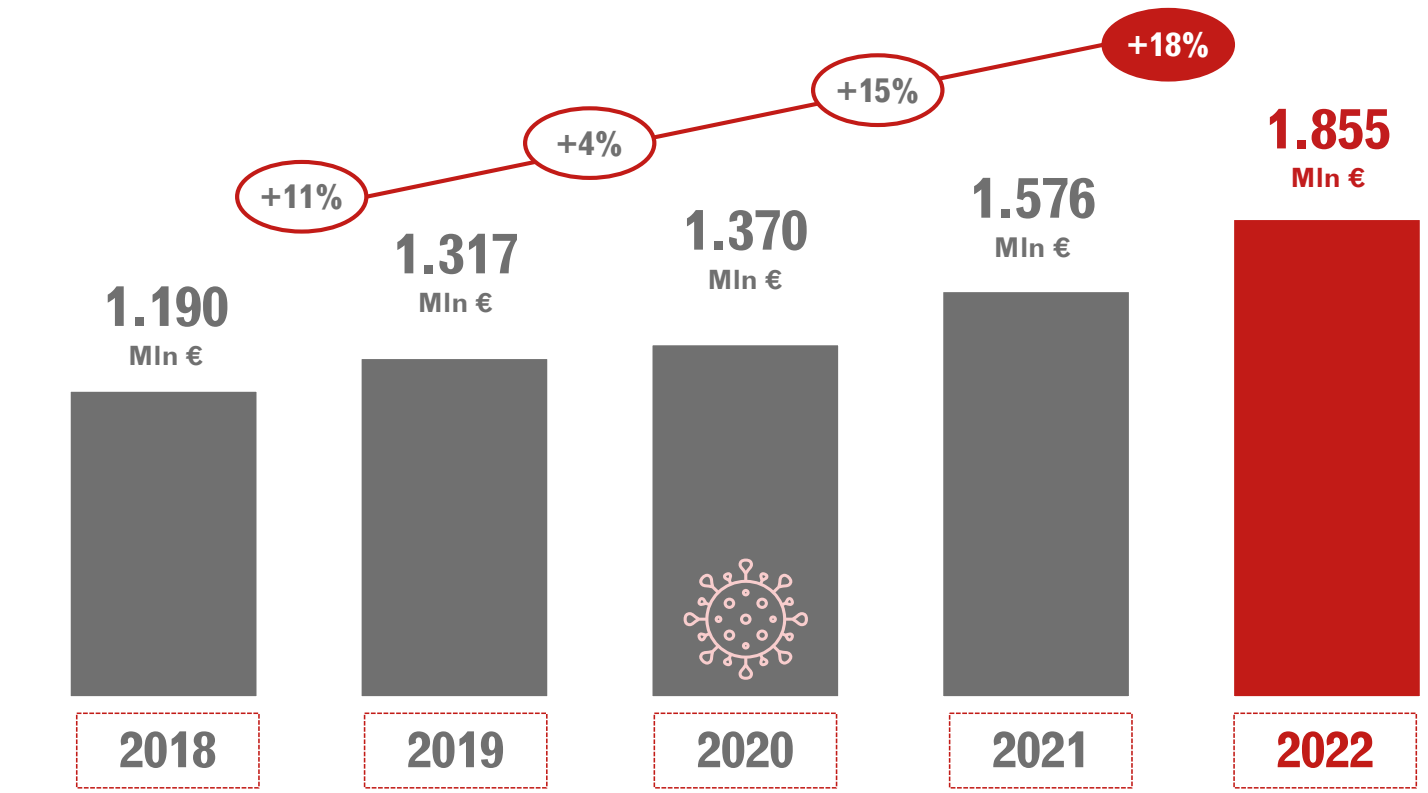
Il **secondo** importante **filone** di investimento riguarda gli **aspetti di istruzione, ricerca e sviluppo,** con la creazione di **partenariati estesi composti da reti diffuse di università, centri di ricerca e aziende private, al fine di sviluppare temi di ricerca con un approccio interdisciplinare**. Il focus sulla cybersecurity si concentra da un lato sullo studio e sullo sviluppo di soluzioni e tecnologie innovative, quali software di analisi dati basati su intelligenza artificiale, nuove tecnologie di cifratura dei dati e gestione delle chiavi attraverso l'uso della blockchain, e dall'altro sulla ricerca in ambito di soluzioni normative e di policy, combinando quindi aspetti tecnologici e normativi.

Anche in questo caso i **vantaggi** per le **PMI** saranno **principalmente indiretti, ma per questo non meno importanti e utili**. Nuovo personale con **alte competenze cyber e manageriali** è **fondamentale per poter gestire al meglio le nuove minacce che si affacciano nel cyberspace italiano**.

I FONDI DEL **PNRR** DESTINATI ALLA CYBER SECURITY SI CONCENTRANO SULLA **TRASFORMAZIONE DIGITALE DELLA PA E SULLA RICERCA**

Il mercato italiano della cybersecurity

GRAFICO 1



Il mercato della cybersecurity in Italia nel **2022 è cresciuto del 18%,** raggiungendo un valore complessivo di **1,86 miliardi di euro.**

È stata una crescita record, dettata anche da una progressiva presa di **consapevolezza del Top Management** che appare più sensibile alla materia.

La dinamica più interessante riguarda le **organizzazioni di medie dimensioni**, che conferiscono una **forte spinta al mercato**. Il **61% delle organizzazioni indica un aumento del budget** dedicato alla cybersecurity, leggermente più alto rispetto all'anno precedente e in **aumento di ben 10 punti percentuali rispetto ai valori pre-pandemia**. Al contrario, solo il 3% delle imprese dichiara una diminuzione della spesa.

Fonte: *Osservatorio Cybersecurity & Data Protection, School of Management, Politecnico di Milano*

Trend digitali e impatto sulla sicurezza informatica

I **TREND DIGITALI** hanno avuto un enorme impatto sul rischio cyber negli ultimi anni, influenzando direttamente i modelli di gestione, e conseguentemente il **mercato della cybersecurity**. L'avanzamento delle tecnologie digitali ha portato a una maggiore disponibilità di dati e a un miglior accesso alle informazioni, ma ha anche creato nuove sfide sul fronte della sicurezza. Tra le innovazioni digitali che generano nuove opportunità o minacce alla sicurezza aziendale si citano il **Cloud, l'Intelligenza Artificiale (AI) e i Big Data, l'IoT** (Internet of Things), con applicazioni anche in ambito industriale (**OT**), e la **Digital Identity**. La continua ricerca di nuove soluzioni tecnologiche e applicazioni sta facendo emergere nuovi trend di frontiera come il **Quantum Computing e la Blockchain**, che tuttavia ancora faticano a tradursi in sperimentazioni concrete in ambito cybersecurity. Di seguito una breve spiegazione dei trend che hanno generato un maggiore impatto negli ultimi anni:

CLOUD

In un contesto in cui le imprese adottano un numero sempre maggiore di servizi «della nuvola», rendendo i sistemi informativi sempre più distribuiti, bisogna prestare massima attenzione verso la sicurezza degli ambienti Cloud soprattutto in ottica prospettica, vista la veloce diffusione della tecnologia.

DIGITAL IDENTITY

In ambienti sempre più esposti a rischi ed intromissioni esterne è di fondamentale importanza certificare con precisione ed efficienza l'identità dei propri utenti interni ed esterni, definendo privilegi e modalità di accesso ai dati critici.

IOT-OT

La sempre maggiore interconnessione di dispositivi e sistemi, legata alla proliferazione di device e sensori IoT (Internet of Things) con applicazioni anche nel mondo industriale (OT - Operational Technology) porta inevitabilmente all'ampliamento della potenziale superficie di attacco. È fondamentale quindi proteggere correttamente i dispositivi connessi, così come i dati che vengono raccolti e scambiati da queste nuove fonti.

AI & BIG DATA

Le componenti di Artificial Intelligence & Big Data Analytics, vedono, da un lato, la crescente diffusione di algoritmi di AI sia nelle tecniche di attacco che di difesa, e dall'altro, la necessità di definire caratteristiche di integrità, confidenzialità e disponibilità di grandi moli di dati.

CYBER INDEX PMI
LA CULTURA DIGITALE PROTEGGE LA TUA IMPRESA

RAPPORTO CYBER INDEX PMI 2023

EVIDENZE DELLA RICERCA 2023

INDICE

Introduzione al Rapporto e impostazione metodologica

Il **Rapporto Cyber Index PMI 2023** ha l'obiettivo di fotografare il livello di conoscenza dei rischi cyber all'interno delle imprese di piccole e medie dimensioni e le modalità di approccio adottate dalle stesse nella gestione di tali rischi. Il rapporto si apre con un'**analisi dell'esposizione al rischio cyber** delle PMI, prosegue con una panoramica delle **evidenze del Rapporto** e si conclude con una serie di **approfondimenti condotti su alcune specifiche aree di analisi**. Ulteriori dettagli sull'impostazione del Rapporto sono presentati nelle pagine seguenti.

Il Rapporto è costruito sull'indagine di un campione composto da **708 Piccole e Medie Imprese italiane**, operanti principalmente nel comparto manifatturiero e industriale. Per la produzione degli output sono state escluse le imprese afferenti all'industria dell'ICT, nonostante ricoprano un ruolo strategico nell'implementazione di soluzioni e servizi di sicurezza informatica. Questa scelta è volta a limitare possibili distorsioni sui risultati dell'indagine, poiché le aziende operanti nel settore ICT sono per loro stessa natura più avanzate nell'approccio alle tecnologie.

ANALISI DELL'ESPOSIZIONE E PERCEZIONE DEL RISCHIO: la prima parte del rapporto presenta una mappatura delle PMI in relazione alla dotazione tecnologica, all'appartenenza a filiere critiche, all'attività verso l'estero e alle violazioni subite negli ultimi 4 anni. A seguire, viene illustrata la percezione circa le minacce cyber, i fattori di rischio, le conseguenze e il livello di preparazione.

Questo contributo aiuta sia a contestualizzare il ruolo di piccole e medie imprese all'interno del sistema economico, sia a comprendere il livello di conoscenza e consapevolezza delle PMI.

EVIDENZE DEL RAPPORTO: la seconda parte e la terza parte costituiscono il cuore del report e propongono una serie di viste sulla maturità complessiva delle PMI italiane, partendo dal Cyber Index PMI, come metrica sintetica della maturità, fino alle dimensioni che lo compongono - approccio strategico, identificazione, attuazione.
All'interno di queste sezioni sono presenti ulteriori spunti di confronto sui quattro livelli di maturità ottenuti e alcune viste sulle dimensioni d'impresa.

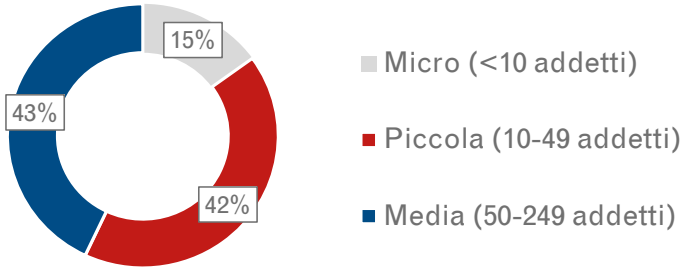
APPROFONDIMENTI: la quarta parte si compone di ulteriori evidenze verticali sulle 20 aree di analisi che confluiscono all'interno delle dimensioni approccio strategico, identificazione e attuazione e che contribuiscono quindi alla produzione dell'indice sintetico.

Struttura dell'indice e campione di analisi

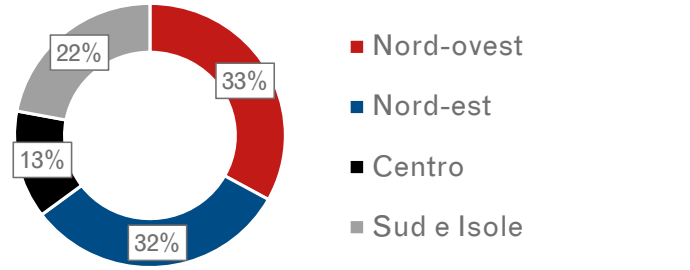
Le imprese sono valutate su alcune o tutte le aree di analisi, in relazione al livello di esposizione al rischio. I punteggi ottenuti da ciascun rispondente nelle aree di analisi contribuiscono a costituire la valutazione sulla singola dimensione, su base 100. Ciascuna delle tre dimensioni concorre poi in maniera eguale (33%) all'ottenimento del punteggio complessivo della singola impresa, anch'essa indicata in centesimi.
Le viste aggregate sulle aree, sulle dimensioni e sull'indice sintetico sono state ottenute come medie ponderate a seguito di un'attività di stratificazione sulle variabili dimensionali e territoriali, rendendo i risultati **rappresentativi dell'intera popolazione aziendale italiana**.

La ricerca ha coinvolto **708 PMI italiane**. Tra quelle considerate, il 65% proviene dal Nord, il 13% dal Centro e il 22% dal Sud e Isole. A livello dimensionale, il campione è composto per l'8% da micro imprese, il 50% da piccole imprese e il 42% da medie imprese. I comparti maggiormente rappresentati sono il manifatturiero (51% del campione), i servizi (34%) e l'ICT (7%). Per evitare effetti distorsivi sui risultati, le imprese fornitrici di soluzioni e servizi ICT non concorrono nella produzione del Cyber Index PMI. Il campione definitivo considerato è quindi pari a **658 PMI italiane.**

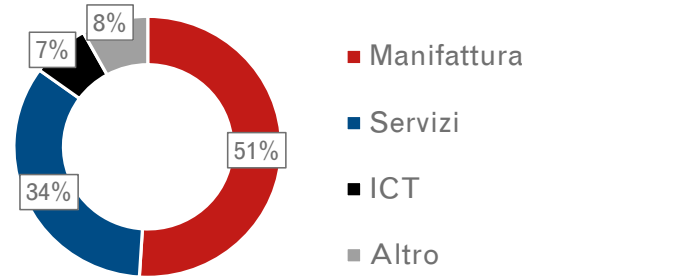
Dimensione aziendale



Collocazione territoriale



Settore



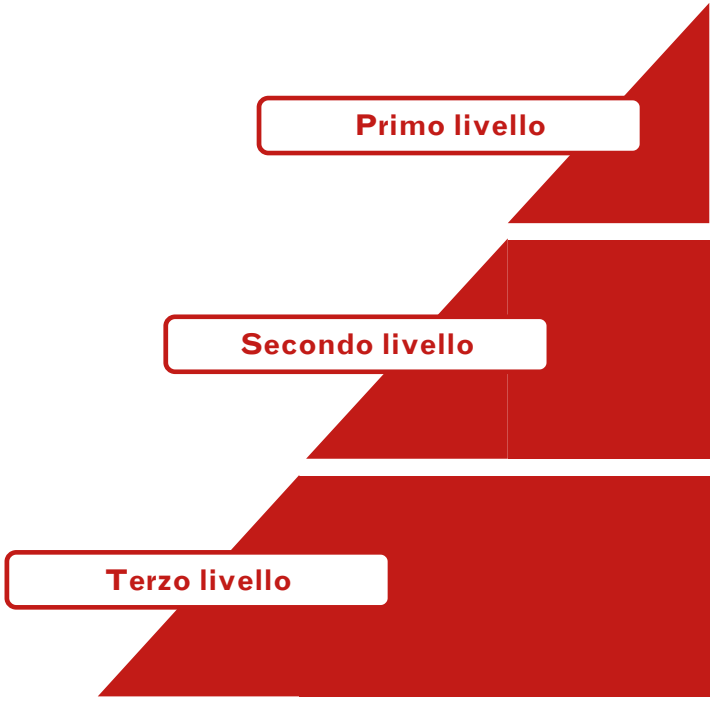
***Nota**: la categoria «altro» rappresenta aziende afferenti al comparto utility, logistica e commercio; i grafici sulla dimensione aziendale e la provenienza territoriale non tengono in considerazione le aziende ICT.*

La struttura dell'indice

Il **CYBER INDEX PMI** si articola in tre livelli di aggregazione:

1. un indice sintetico su scala da 1 a 100 che offre una fotografia complessiva della maturità delle PMI;
2. 3 dimensioni - approccio strategico, identificazione, attuazione – che aggregano le aree di analisi
3. 18 aree di analisi che raggruppano le singole domande del questionario.

Le pagine a seguire illustrano in dettaglio la metodologia di analisi e la relazione tra i 3 livelli che compongono l'indice.



Il **CYBER INDEX PMI**, ovvero l'indice generale, rappresenta in maniera sintetica la capacità delle piccole e medie imprese italiane di comprendere e mitigare il rischio cyber. L'indice è stato sviluppato su una scala da 0 a 100, come media dei risultati ottenuti dalle imprese su ciascuna delle tre dimensioni.

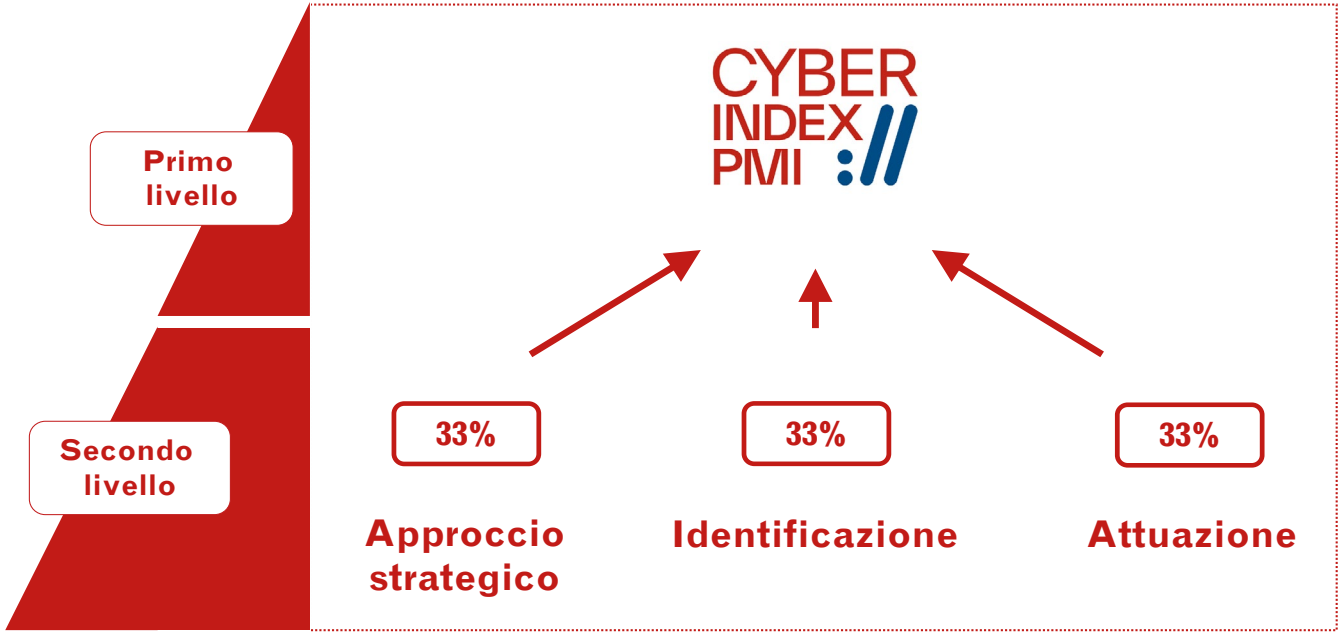
Le **3 DIMENSIONI** rappresentano le direzioni di sviluppo della sicurezza informatica all'interno dell'organizzazione aziendale e costituiscono l'aggregazione delle aree di analisi. Sebbene vengano considerate in maniera indipendente, con un approfondimento verticale, mantengono comunque un certo grado di relazione tra di loro, poiché concorrono alla creazione dell'indice generale.

Le **18 AREE DI ANALISI** aggregano le scelte strategiche e operative implementate internamente alle organizzazioni aziendali, valutando la strutturazione di processi e l'introduzione di tecnologie e competenze. Tali aree sono state indagate direttamente nelle domande del questionario sottoposto alle PMI e sono descritte all'interno della **PARTE 4**.

Primo livello: Cyber Index PMI

1L

Il **CYBER INDEX PMI,** ovvero l'indice generale, rappresenta in maniera sintetica la capacità delle piccole e medie imprese italiane di comprendere e mitigare il rischio cyber. L'indice è stato sviluppato su una scala da 0 a 100, come media dei risultati ottenuti dalle imprese su ciascuna delle tre dimensioni.



Il Cyber Index è costituito dalla media di tre dimensioni, che, come si può vedere dall'illustrazione, concorrono equamente alla produzione di una vista sintetica.

Partendo dal Cyber Index è possibile comprendere come le piccole e medie imprese si distribuiscono in relazione al punteggio ottenuto e generare quattro livelli di maturità.

Questi output sono disponibili all'interno della **PARTE 2** del rapporto.

Secondo livello: dimensioni dell'Indice

2L

Le **DIMENSIONI** – approccio strategico, identificazione e attuazione – rappresentano le direzioni di sviluppo della sicurezza informatica all'interno dell'organizzazione aziendale e costituiscono l'aggregazione delle aree di analisi. Sebbene vengano considerate in maniera indipendente, con un approfondimento verticale, mantengono comunque un certo grado di relazione tra di loro, poiché concorrono alla creazione dell'indice generale.

Approccio strategico

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

Aree di analisi

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**

Aree di analisi

Attuazione

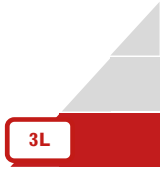
Capacità di selezionare il corretto **mix di competenze e modelli organizzativi** e di implementare **iniziative concrete** in termini di **persone**, **processi** e **tecnologie**

Aree di analisi

All'interno del modello di ricerca, le tre dimensioni rappresentate concorrono alla produzione della vista sintetica (ovvero l'indice generale Cyber Index PMI). Le dimensioni fungono da livello intermedio e sono a loro volta composte da aree di analisi che dettagliano le diverse scelte aziendali. Questa vista è utile per comprendere se esistono dimensioni su cui le PMI riscontrano maggiori criticità e individuare le priorità di azione all'interno di un percorso di maturità.

Questi output sono disponibili nella **PARTE 3** del rapporto.

Terzo livello: aree di analisi



Le **AREE DI ANALISI** rappresentano le scelte strategiche e operative implementate internamente alle organizzazioni aziendali, valutando strutturazione di processi e introduzione di tecnologie e competenze.

Le aree di analisi rappresentano la disaggregazione massima del modello di ricerca. Ciascuna di esse concorre alla costruzione di una dimensione (approccio strategico, identificazione o attuazione) e di conseguenza alla produzione del Cyber Index PMI.

Nella tabella di destra vengono rappresentate le 20 aree in relazione alla loro collocazione nella singola dimensione. Il colore assegnato a ciascuna area rappresenta il grado di complessità della scelta:

- il colore più chiaro identifica scelte strategiche e/o operative di **sicurezza informatica di livello base;**
- il colore mediano rappresenta scelte strategiche e/o operative di **sicurezza informatica di livello intermedio;**
- il colore più scuro indica scelte strategiche e/o operative di **sicurezza informatica di livello più sofisticato**.

Le 20 aree di analisi non si prefiggono di essere esaustive della materia ma di rappresentare con efficacia scelte strategiche e operative attuabili all'interno di piccole e medie imprese. Viste verticali sulle aree di analisi e ulteriori dettagli sui livelli di complessità sono disponibili all'interno della **PARTE 4** del rapporto.

**Nota: per ulteriori approfondimenti si rimanda alla PARTE 4 e alla nota metodologica*

Aree di analisi	
Approccio strategico	Commitment della proprietà
	Budgeting
	Presidio organizzativo
	Piano di sicurezza
	Certificazioni
Identificazione	Mappatura degli asset informatici
	Valutazione delle vulnerabilità
	Auditing della sicurezza informatica
	Misurazione del rischio cyber
	Valutazione del livello di sicurezza dei fornitori
	Cyber Risk Management
	Adeguamento alla compliance normativa
Attuazione	Gestione del fattore umano
	Formazione
	Polizze assicurative
	Tecnologie per la protezione dei dati
	Tecnologie per il monitoraggio di attività anomale
	Tecnologie per la protezione delle reti
	Linee guida dirette alle terze parti
	Programmi di info-sharing

Analisi dell'esposizione al rischio

La **PARTE 1** delle **EVIDENZE DAL RAPPORTO** si apre con una descrizione circa l'**ESPOSIZIONE AL RISCHIO*** delle piccole e medie imprese italiane. Sebbene la sicurezza informatica sia fondamentale per tutte le organizzazioni aziendali, è utile focalizzarsi su alcune variabili che contribuiscono a inasprire l'esposizione al rischio cyber. Al verificarsi di queste condizioni, iniziative di sicurezza di livello base sono necessarie ma non sufficienti a garantire una protezione adeguata, richiedendo quindi l'implementazione di specifiche scelte strategiche e/o operative più sofisticate. L'**ANALISI DELL'ESPOSIZIONE AL RISCHIO** mira quindi a mappare le PMI italiane in relazione ai fattori che generano un incremento della probabilità o dell'impatto di un attacco cyber. Di seguito le variabili prese in considerazione:

Strumenti digitali: l'introduzione di hardware e software, nonché l'incremento del bacino di utenti che li utilizza, contribuisce a definire la superficie attaccabile. Il processo di digitalizzazione supporta il business nella generazione di valore, ma allo stesso tempo è importante monitorare le vulnerabilità generate dalle nuove tecnologie, implementando opportune misure di protezione. L'analisi della dotazione tecnologica permette di definire la quota di imprese dotate di tecnologie di base, come sistemi ERP e CRM, o avanzate, come l'IoT e il Cloud.

Appartenenza a filiera critica: la condivisione di sistemi informativi con terze parti, fornitori o partner di un'azienda, implica punti di contatto tra due perimetri estranei. Questa situazione è un'occasione per i cyber criminali, che possono sfruttare le vulnerabilità di un'azienda per violarne un'altra, innescando un meccanismo a cascata. Operare in filiere che coinvolgono infrastrutture critiche, multinazionali o Pubblica Amministrazione espone le PMI a maggiori rischi, poiché potrebbero risultare l'anello debole per penetrare un obiettivo più strategico.

Attività estera: la vendita di prodotti e servizi in territori esteri e/o la dislocazione geografica di alcune sedi implicano un'estensione logica e tecnologica del dominio aziendale. Tale situazione genera un allargamento del perimetro di azione e conseguentemente incrementa l'esposizione dell'organizzazione a nuovi rischi. Questo rischio è estremizzato nel caso in cui l'attività produttiva venga condotta all'interno di paesi instabili dal punto di vista geopolitico, poiché l'azienda può essere target di attacchi mirati da parte di gruppi di criminali parastatali.

Violazioni subite negli ultimi 4 anni: un'azienda già vittima di attacchi cibernetici è maggiormente a rischio, in quanto possono essere state condivise ed esposte pubblicamente le informazioni relative al suo sistema informativo e alle sue vulnerabilità, che risultano quindi facilmente disponibili per i cybercriminali. Per queste aziende è quindi importante implementare strategie e strumenti di protezione del rischio cyber sempre aggiornati. L'analisi mira a stimare la quota di imprese che hanno subito una violazione, sebbene questa percentuale (basata su dati auto-dichiarati) possa risultare sottostimata rispetto alla realtà.

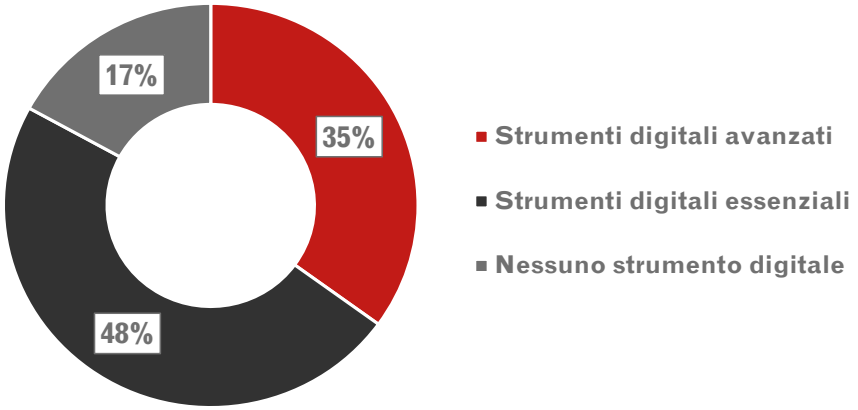
A seguire, vengono inserite 4 ulteriori viste circa la **PERCEZIONE DEL RISCHIO CYBER** misurata all'interno delle PMI italiane.

**Nota*: *per ulteriori approfondimenti si rimanda al glossario*

Strumenti digitali

Le aziende stanno investendo massivamente in strumenti digitali per sfruttare le opportunità emergenti dall'evoluzione tecnologica. Introdurre nuove tecnologie significa ampliare la potenziale **SUPERFICIE D'ATTACCO***, perciò se queste non vengono correttamente accompagnate da soluzioni di sicurezza, possono introdurre nuove vulnerabilità latenti nel perimetro aziendale, aumentando la probabilità di una violazione.
Dall'indagine condotta, emerge che il 35% delle PMI ha introdotto strumenti digitali avanzati, ovvero soluzioni in Cloud o dispositivi IoT. In particolare quest'ultima tecnologia, particolarmente diffusa nell'ambito industriale tanto da costituire un'area di sicurezza a sé stante (OT Security), richiede un elevato livello di attenzione. A seguire, il 48% delle PMI afferma di aver già introdotto strumenti digitali essenziali con l'obiettivo di supportare i processi aziendali, quali software per la gestione e la pianificazione operativa delle risorse e applicativi a supporto della gestione che digitalizzano le parti di front-end e di back-end aziendali. Completa la vista il 17% di imprese che invece dichiara di non aver ancora introdotto strumenti digitali.

GRAFICO 3



L'**83%** DELLE PMI ITALIANE **RICORRE A STRUMENTI DIGITALI PER SUPPORTARE I PROPRI PROCESSI AZIENDALI**

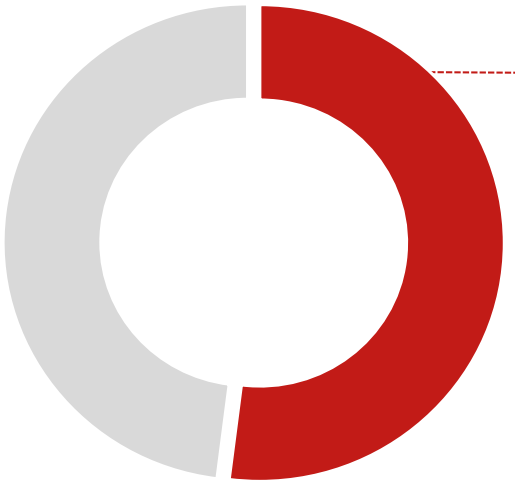
**Nota*: *per ulteriori approfondimenti si rimanda al glossario*

Appartenenza a filiera critica

Il secondo punto di attenzione presentato in questa sezione è relativo all'appartenenza a una filiera critica. Le aziende fanno affidamento a una vasta gamma di partner, sia in qualità di fornitori di input produttivi sia per esternalizzare processi a società specializzate. Spesso questa casistica comporta una relazione tra le parti, con un conseguente scambio di dati o la concessione di privilegi di accesso alle risorse, che richiede il massimo dell'attenzione. Un cyber criminale che riesce a violare i sistemi di un'azienda potrebbe infatti ottenere facilmente l'accesso anche ai sistemi dei partner.

Dal **RAPPORTO CYBER INDEX 2023** emerge come il 52% delle PMI italiane operi all'interno di una filiera potenzialmente critica. Tra le situazioni più comuni, si riscontrano la fornitura di prodotti e/o servizi a società multinazionali e l'attività in paesi politicamente instabili (30% delle PMI). Dai dati presentati emerge una forte esposizione ai rischi di filiera, che richiede un'attenta analisi sia nell'ottica di difendere i sistemi informativi sia di tutelare la partecipazione di piccole e medie organizzazioni a catene del valore strategiche.

GRAFICO 4

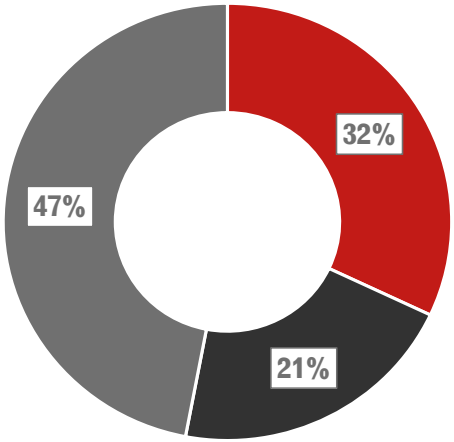


Il 52% delle PMI opera all'interno di filiere critiche

Mercati internazionali

La sicurezza informatica e la protezione dei dati sono elementi importanti da considerare per le aziende che operano a livello internazionale e che vendono i loro prodotti all'estero. Quando si considera la dimensione internazionale si aggiunge quindi un'ulteriore complessità, legata alle normative sulla privacy e alla sicurezza dei dati nei paesi in cui si opera. L'Unione Europea ha introdotto il Regolamento Generale sulla Protezione dei Dati (GDPR), paesi extra UE hanno adottato normative analoghe, ma che spesso richiedono alle aziende adeguamento a requisiti normativi eterogenei. Per vendere i propri prodotti all'estero in modo sicuro, è importante che le imprese familiarizzino con le normative di sicurezza informatica dei paesi esteri di interesse ed adottino le misure previste per proteggere dati e sistemi. Lo scopo finale dell'azienda rimane quello di proteggere sia il proprio business sia i propri clienti e partner dai rischi informatici, garantendo contemporaneamente la propria reputazione sul mercato internazionale. A tal fine, le aziende esposte che hanno una strategia di internazionalizzazione dovrebbero adottare misure di sicurezza avanzate e prestare la massima attenzione all'adeguamento normativo.

GRAFICO 5

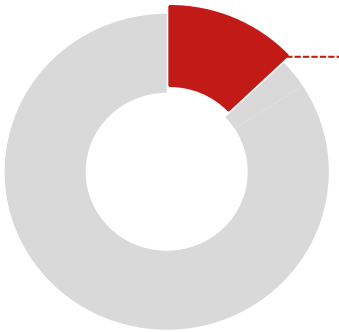


LE PMI ITALIANE SONO INCLINI A **OPERARE SU MERCATI INTERNAZIONALI**: IL **53%** HA VENDUTO PRODOTTI E/O SERVIZI ALL'ESTERO NEL 2021

Violazioni subite negli ultimi 4 anni

Le violazioni informatiche* possono causare ripercussioni negative su diversi fronti: dal furto di dati, fino all'interruzione dell'attività, passando dalle sanzioni nel caso in cui non fossero rispettate le misure di compliance previste dalle normative vigenti. Anche organizzazioni che non si reputano particolarmente esposte al rischio possono essere colpite da azioni malevole e la probabilità aumenta nell'eventualità che si verifichino i fattori visti in precedenza: nel caso in cui operino all'interno di una filiera strategica, abbiano relazioni internazionali o vulnerabilità di sicurezza legate a tecnologie non opportunamente mitigate. Inoltre, una conseguenza spesso sottovalutata è legata alla possibilità che un primo attacco possa favorire i criminali informatici nell'individuazione di punti vulnerabili del sistema, esponendo l'azienda a potenziali nuovi incidenti di sicurezza. Questo scenario è particolarmente comune e richiede un immediato intervento per la messa in sicurezza del sistema informativo.
Il messaggio che emerge, in relazione all'analisi sull'esposizione dei rischi, è che la piccola e media impresa risulta un bersaglio particolarmente appetibile per i criminali informatici.
Dall'indagine risulta che il 13% delle PMI ha subito almeno una violazione dei sistemi informativi aziendali.
A supporto di quanto affermato in questa sezione, emerge che le imprese all'interno di questa porzione del campione presentano in media una maggiore esposizione al rischio. Crescono infatti le percentuali di aziende che operano all'interno di una filiera critica e/o in contesti internazionali.

GRAFICO 6



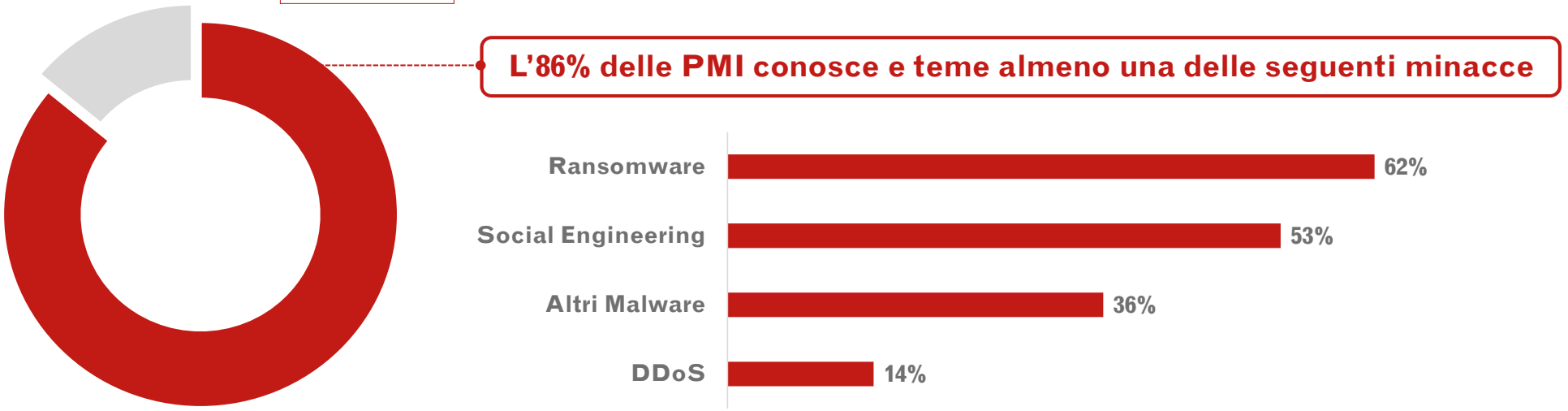
IL **13%** DELLE PMI ITALIANE AFFERMA DI AVER SUBITO **ALMENO UNA VIOLAZIONE DEI SISTEMI INFORMATIVI AZIENDALI NEGLI ULTIMI 4 ANNI**

**Nota*: *per ulteriori approfondimenti si rimanda al glossario*

Percezione delle minacce cyber

A completamento dell'**ANALISI DELL'ESPOSIZIONE AL RISCHIO** viene presentata una collezione di viste circa la **PERCEZIONE DEL RISCHIO CYBER di piccole e medie imprese italiane,** ovvero la **valutazione soggettiva** che le società fanno del grado di pericolosità delle minacce informatiche. Nonostante tale percezione dipenda da diverse variabili, come il livello di conoscenza della materia, la fiducia nei propri sistemi di sicurezza e l'importanza di dati e informazioni in azienda, contribuisce a **influenzare il comportamento** di individui ed organizzazioni **in materia di sicurezza informatica**. Ad esempio, se un'organizzazione percepisse di essere un potenziale obiettivo di attacchi cyber, potrebbe adottare soluzioni di sicurezza più avanzate e investire maggiormente in formazione e sensibilizzazione del personale. Viceversa, l'attenzione e l'adozione di soluzioni di sicurezza potrebbero essere carenti. Come si nota dal **GRAFICO 7** le PMI italiane si dichiarano particolarmente preoccupate circa minacce di attacchi **ransomware**, al primo posto e citato dal 62% delle PMI, seguito da attacchi basati sul **social engineering**, per il 53% delle piccole e medie imprese. Seguono al 36% i **malware** in generale e chiudono la classifica col 14% gli attacchi di tipo **DDoS. Il 14% residuo non conosce o non saprebbe giudicare le minacce.**

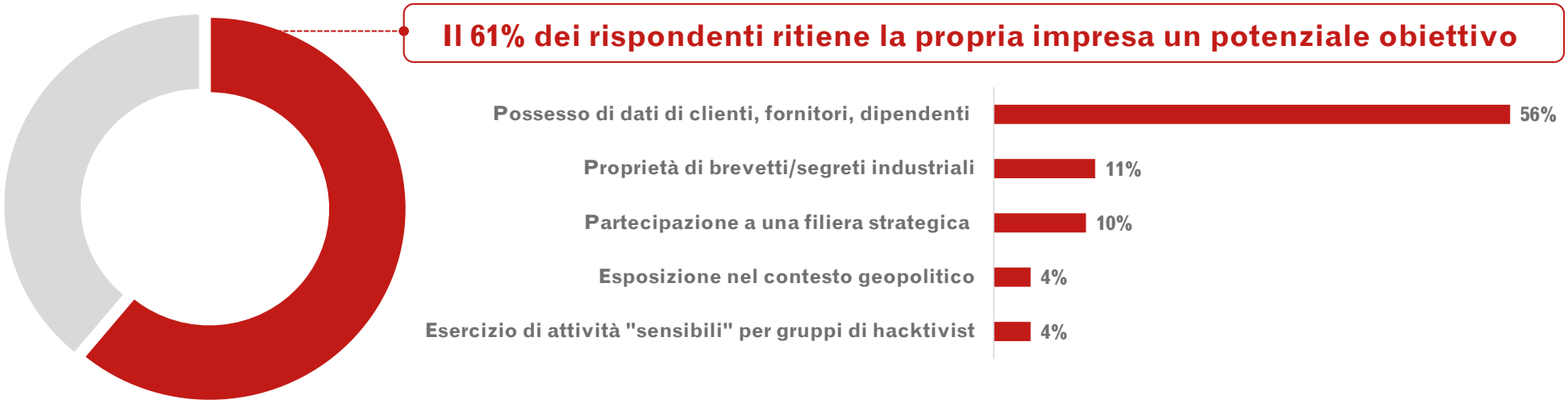
GRAFICO 7



Fattori di rischio interni all'azienda

Parallelamente alla minaccia, che rappresenta la tecnica utilizzata, è importante realizzare come le imprese percepiscono il rischio informatico e quali sono i fattori che rendono la propria organizzazione un potenziale obiettivo di attacchi cyber. **Dalle evidenze, il 61% delle PMI ritiene di poter essere un bersaglio di attacchi informatici e individua almeno un fattore di rischio all'interno del proprio perimetro**, **mentre il restante 39% non ritiene di poter essere l'oggetto di attacchi informatici**. Le PMI italiane temono particolarmente per il possesso di ingenti moli di dati relativi a diversi attori, tra cui clienti, fornitori e dipendenti (nel 56% dei casi), anche in virtù della normativa sulla protezione dati e le conseguenze sia sanzionatorie, sia risarcitorie. Sorprende come l'appartenenza a filiere strategiche venga considerato un fattore di rischio solo dal 10% delle PMI, sebbene molte si dichiarino fornitori di multinazionali. Infine, l'esposizione al contesto geopolitico preoccupa solo il 4% dei rispondenti, a fronte di un 9% che invece opera attivamente in paesi instabili.

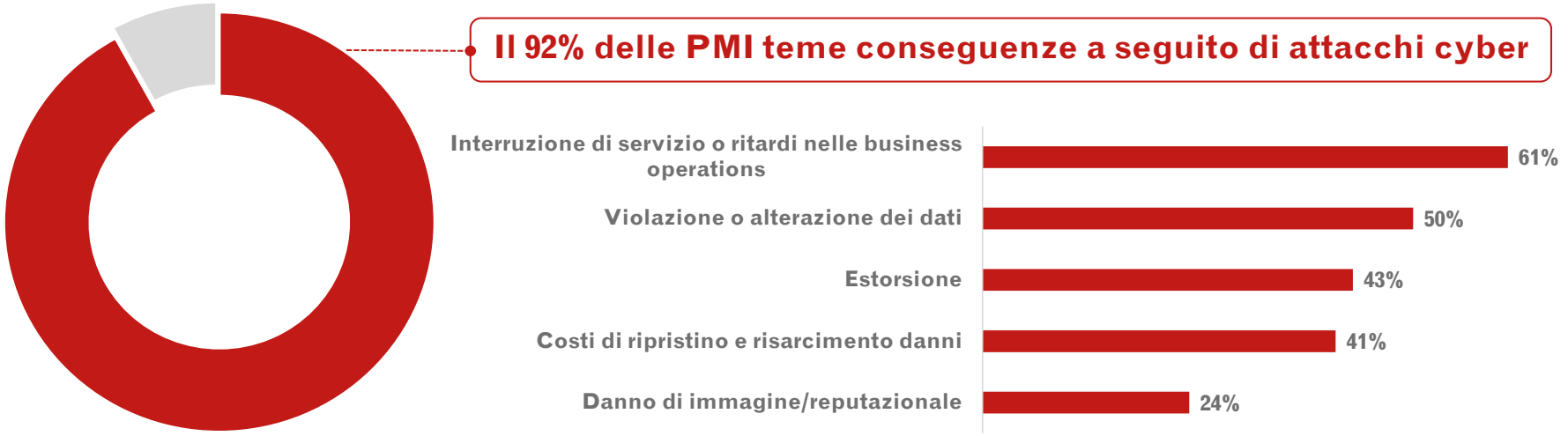
GRAFICO 8



Percezione delle conseguenze sull'impresa

Gli attacchi informatici possono avere conseguenze significative per le piccole e medie imprese tanto quanto per quelle delle grandi organizzazioni. Il **61% delle PMI teme l'interruzione o il ritardo delle operazioni aziendali**, il che può portare a una significativa perdita di produttività e a un rallentamento dell'attività di vendita. Il 50% teme la violazione o l'alterazione dei dati aziendali, sia proprie che di terzi. Come anticipato, se i dati dei clienti vengono compromessi a seguito di un attacco informatico, l'azienda può violare le normative sulla privacy dei dati, comportando serie conseguenze finanziarie, legali e reputazionali. **Proteggere i dati è importante anche per non dare adito ad attività estorsive, conseguenza che preoccupa il 43% delle PMI**. Una conseguenza che viene spesso sottovalutata sono i **costi di ripristino**; dopo un attacco informatico, le PMI devono investire risorse significative per ripristinare i sistemi e i dati, migliorare la sicurezza informatica e implementare misure preventive per evitare futuri attacchi. Questi costi possono essere onerosi per le PMI con risorse limitate, soprattutto se all'attacco fanno seguito azioni legali da parte dei clienti, dei partner commerciali o delle autorità di regolamentazione. Infine, **solo il 24%** fa rientrare tra le tre principali preoccupazioni i **danni d'immagine**.

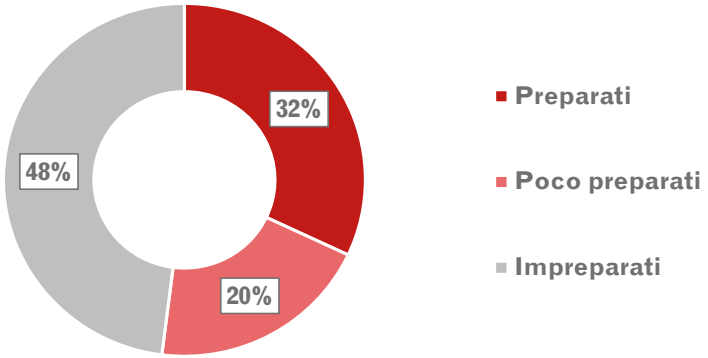
GRAFICO 9



Preparazione di fronte a un attacco cyber

L'ultimo aspetto percettivo esaminato riguarda la preparazione agli attacchi informatici. **Il rischio informatico**, in relazione al crescente numero di attacchi registrato negli ultimi anni, **è di difficile quantificazione**, così come è difficile comprendere se l'organizzazione sia preparata ad affrontarlo. L'obiettivo è sempre quello di introdurre sistemi di protezione e mitigazione del rischio, in relazione alle minacce maggiormente probabili e con un impatto maggiore sul business. Tuttavia, è sempre bene ricordare che **la capacità di rispondere alle minacce cyber difficilmente raggiunge la piena maturità, anche in organizzazioni con elevate risorse**. Secondo l'indagine condotta, il 32% delle PMI si sente preparato ad affrontare un attacco informatico, contro un **48% che non si ritiene pronto** e un 20% che si dichiara poco preparato.

GRAFICO 10



SOLO IL **32%** DELLE PMI ITALIANE SI SENTE **PRONTO AD AFFRONTARE E RISOLVERE EFFICACEMENTE UN ATTACCO CYBER**

Il Cyber Index PMI

CYBER INDEX PMI

IL CYBER INDEX EVIDENZIA UN QUADRO DI **GENERALE RITARDO** NELLE PMI ITALIANE. IL **VALORE MEDIO DELL'INDICE È 51** SU UN PUNTEGGIO MASSIMO DI 100

La seconda parte del **RAPPORTO CYBER INDEX 2023** si prefigge l'obiettivo di condividere con il lettore una fotografia sintetica del livello di sicurezza di piccole e medie imprese italiane. Il primo contributo fornito in questa sezione riguarda il **CYBER INDEX PMI**. A seguito dell'analisi di 658 PMI, **si constata un punteggio di maturità medio di 51**, su un totale ottenibile di 100. Il messaggio chiave che emerge da questa prima vista è di **sostanziale ritardo.**

È importante però sottolineare che la cybersecurity è un elemento abilitante per la trasformazione digitale in tutte le aziende, indipendentemente dalle loro dimensioni. Nonostante la consapevolezza dimostrata dalle PMI – **il 51% ritiene la sicurezza informatica rilevante*** – è evidente come questo tema continui ad essere posto in secondo piano rispetto al più ampio processo di trasformazione digitale, su cui si stanno già registrando buoni progressi.

Come anticipato nella **PARTE 1**, le piccole e medie imprese non solo concorrono in maniera rilevante all'economia del Paese, ma spesso operano come fornitori all'interno di filiere che coinvolgono grandi imprese, enti della Pubblica Amministrazione e infrastrutture critiche. Considerando il tessuto economico italiano, composto per oltre il 90% da piccole e medie imprese, la criticità rilevata appare particolarmente grave. In un periodo storico complesso, in cui le imprese hanno affrontato difficoltà legate alla crisi sanitaria e si ritrovano a dover fare i conti con l'inflazione e il conflitto russo-ucraino, è necessario supportare il loro processo di digitalizzazione sottolineando come la cybersecurity sia un fattore imprescindibile.

***Nota**: L'indice utilizza valori tra 0 e 100*
Nota: rimando alla parte 4 dell'Evidenze del Rapporto, commitment della proprietà*

Il Cyber Index PMI

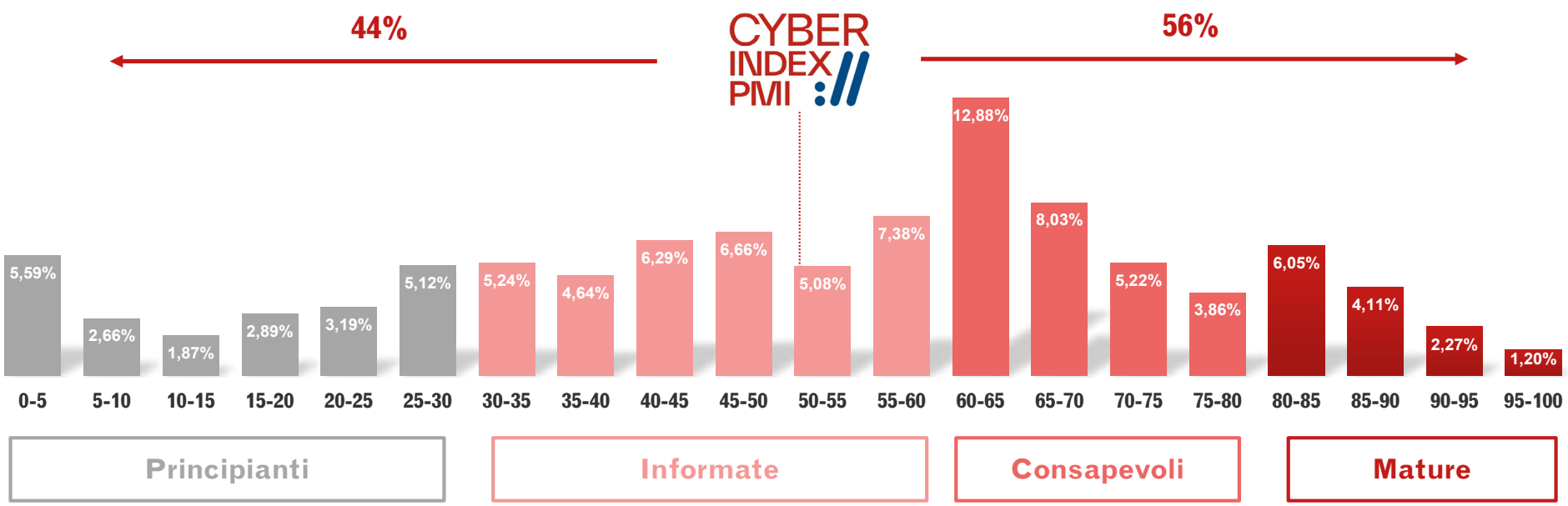
Il **CYBER INDEX PMI** si fonda su tre dimensioni: approccio strategico, identificazione e attuazione.
I punteggi ottenuti nelle singole dimensioni non si discostano significativamente dal Cyber Index sintetico, ribadendo una carenza diffusa in ambito cybersecurity. Dal risultato medio ottenuto nella dimensione approccio strategico (punteggio 54/100), che considera aree di primaria rilevanza come il budget e il presidio organizzativo, si denota come **le PMI italiane fatichino ad approcciarsi alla sicurezza informatica in maniera strategica.** Questa difficoltà si ritrova ulteriormente amplificata nell'identificazione (punteggio 43/100), ovvero nelle attività di monitoraggio dei rischi aziendali. Le piccole organizzazioni manifestano **grosse difficoltà nell'identificare e comprendere il rischio cyber**, a causa sia della lenta trasformazione culturale sia delle limitate competenze digitali presenti. Infine, dall'elaborazione dei dati risulta che piccole e medie imprese hanno già intrapreso attività di mitigazione dei rischi informatici (Attuazione 56/100), ma spesso con **scarsa cognizione del corretto impiego delle leve.** Questo messaggio conferma che **la sicurezza informatica è vista troppo spesso come una responsabilità esclusiva di IT Manager e sistemisti, nonostante il rischio cyber abbia un forte impatto anche sul business.**

***Nota**: l'Indice e le dimensioni utilizzano valori tra 0 e 100*
Nota: rimando alla parte 4 delle evidenze della Ricerca, commitment della proprietà*

Il Cyber Index PMI e i livelli di maturità

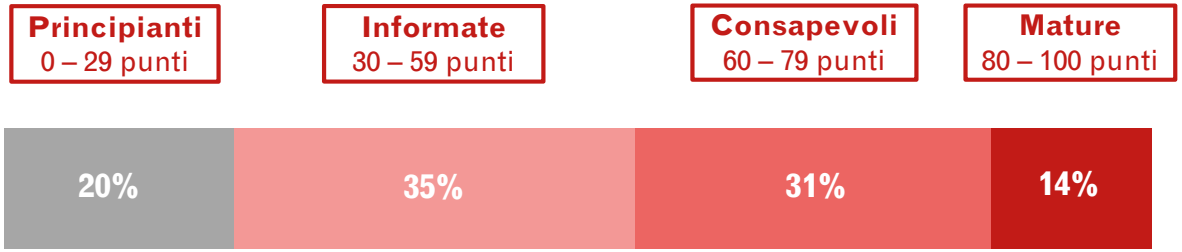
Partendo dalla distribuzione, attraverso un'aggregazione di aziende che hanno ottenuto punteggi simili è possibile identificare **4 livelli di maturità**. Raggruppare le imprese in quattro classi – denominate **principianti, informate, consapevoli e mature** – contribuisce non solo ad una miglior comprensione dello stato generale di salute delle PMI italiane, ma anche a delineare profili aziendali ricorrenti. Da questa attività si può intraprendere un **processo di monitoraggio pluriennale**, con l'obiettivo di rilevare l'evoluzione della maturità delle PMI italiane in ambito cybersecurity. L'auspicio è che negli anni a venire si possa testimoniare una crescita generale di tutte le imprese, sia quelle che si stanno approcciando alla security sia quelle il cui journey di maturità è già stato avviato. È importante infatti rimarcare che anche le imprese mature si troveranno continuamente di fronte a nuove sfide e minacce di sicurezza, che si trasformano con l'evoluzione delle tecnologie e del contesto.

GRAFICO 12



I 4 livelli di maturità

GRAFICO 13



È INDISPENSABILE CHE **TUTTE LE IMPRESE PROSEGUANO NEL LORO PERCORSO DI MATURITÀ** NELLA GESTIONE DEI RISCHI CYBER. **ANCHE LE IMPRESE MATURE SI TROVERANNO CONTINUAMENTE DI FRONTE A NUOVE SFIDE E MINACCE DI SICUREZZA**, CHE SI TRASFORMANO CON L'EVOLUZIONE DELLE TECNOLOGIE E DEL CONTESTO

Il 20% delle PMI si colloca al livello di partenza, ovvero tra i «principianti». Il 35% delle imprese, connotate da un livello di preparazione ancora limitato, può invece definirsi «informata». A seguire, il 31% dimostra particolare consapevolezza della materia, ricadendo nella categoria «consapevoli». Infine, solo il 14% rientra nella classe di maturità più alta («mature»).

Nelle pagine seguenti sarà dedicata una **vista verticale a ciascuno dei livelli di maturità, per descrivere meglio il profilo delle imprese** che vi rientrano.

***Fonte**: Rapporto Cyber Index PMI 2023, campione di 658 piccole e medie imprese italiane; risultati ottenuti a seguito di una rielaborazione statistica*

I 4 livelli di maturità

20%

Principianti
0 - 29

Le piccole e medie imprese «principianti» si caratterizzano per i **bassi valori ottenuti nelle tre dimensioni** che compongono l'indice. Nel 29% delle PMI, i **vertici aziendali** appartenenti a questo livello **non ritengono prioritario il tema** e nel 54% vi si stanno avvicinando recentemente. In entrambi i casi la definizione di una strategia di protezione è ancora agli albori e non sono generalmente previsti fondi dedicati (solo nel 3% delle PMI parte del budget IT è destinabile specificatamente alla sicurezza informatica). La mancanza di un approccio strategico comporta una **scarsa maturità generale anche sulle altre due dimensioni**.
In particolare, una criticità che caratterizza le aziende che rientrano in questo livello è legata alla **percezione del rischio**. Il 56% delle imprese «principianti» **non ritiene di essere un potenziale target** di attacchi cyber e il 39% addirittura **non ritiene gli attacchi cyber un rischio per la propria organizzazione**. Nonostante le realtà che ricadono in questo livello siano principalmente micro e piccole imprese, equamente distribuite territorialmente, il 18% è comunque fornitore di imprese sopra i 1.000 addetti. Questa statistica porta a considerazioni legate all'intera filiera, in cui l'attaccante sfrutta l'anello debole per colpire in seconda battuta un'azienda più grande. Per questa ragione, realtà poco mature dal punto di vista della gestione della sicurezza potrebbero rischiare di vedersi escluse da filiere strategiche con l'inasprirsi delle minacce e delle normative.

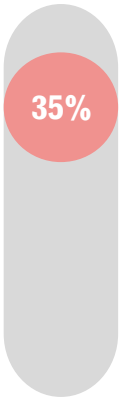
DIMENSIONI DI ANALISI

Approccio strategico	Identificazione	Attuazione
21	9	27

LE PMI «PRINCIPIANTI» HANNO **SCARSA PERCEZIONE DEL RISCHIO CYBER** E **STENTANO AD AVVIARE UN PERCORSO DI GESTIONE DELLA SICUREZZA**

***Nota**: le dimensioni utilizzano valori tra 0 e 100*

I 4 livelli di maturità



Informate
30 - 59

Le PMI "informate" dimostrano un **livello accettabile di comprensione del tema.** Nonostante i vertici di un'impresa su tre non ritengano la gestione del rischio cyber particolarmente rilevante, il punteggio medio ottenuto nell'approccio strategico (50/100) dimostra come i primi passi siano già stati compiuti. **In una PMI su due vengono destinati fondi per investimenti** e nell'**80% dei casi è previsto un presidio organizzativo**, tipicamente esterno. L'approccio strategico adottato **non è tuttavia sufficiente** a garantire una buona attività di monitoraggio del rischio; nel 35% dei casi **non è previsto un processo di mappatura degli asset informatici** e nel 58% dei casi **non vengono svolte attività di auditing**. Solo il 15% di PMI effettua test di misurazione del rischio cyber, attività che il più delle volte viene condotta in maniera non continuativa. La prospettiva adottata comporta l'introduzione di **leve attuative spesso scoordinate o poco efficaci**. Inoltre, difficilmente sono previste attività per la gestione del fattore umano e la presenza di strumenti tecnologici è scarsa o limitata a soluzioni di base. Compongono questo livello imprese di piccole e medie dimensioni con un business tradizionale, i cui investimenti sono tipicamente destinati alla continuità operativa. Tuttavia, tali realtà hanno un posizionamento in filiere che coinvolgono la Pubblica Amministrazione e imprese multinazionali, nonché un'ampia dotazione tecnologica e quindi un'ampia superficie di attacco potenziale.

DIMENSIONI DI ANALISI

LE PMI «INFORMATE» HANNO INTRAPRESO UN PROCESSO DI MATURAZIONE **COMPIENDO I PRIMI PASSI**

***Nota**: le dimensioni presentano valori tra 0 e 100*

I 4 livelli di maturità

31%

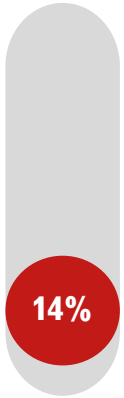
Consapevoli
60 - 79

Le piccole e medie imprese «consapevoli» dimostrano di aver sviluppato un **buon livello di approccio strategico**, soprattutto in relazione all'interesse dei vertici aziendali sulle implicazioni cyber. Nel **91% dei casi la direzione viene coinvolta**, e nel **69% ha un ruolo attivo** nell'indirizzamento delle strategie di sicurezza. Il 46% delle imprese ha responsabilizzato una figura di presidio della materia, tipicamente interna all'IT, mentre persiste la tendenza a trasferire parte delle responsabilità ad un partner esterno (31% dei casi). Per far fronte alla scelta di sourcing esterne, nell'**86%** dei casi sono presenti **fondi destinabili alla sicurezza informatica**, di solito direttamente collegati al budget IT. Rispetto alle PMI «informate», le **attività di identificazione vengono svolte con maggior continuità**. Oltre a condurre auditing sugli aspetti di sicurezza informatica, il 47% monitora il rischio cyber con cadenza almeno saltuaria. La capacità di introdurre processi e tecnologie per mitigare il rischio cyber, inoltre, è soddisfacente. Per migliorare la propria postura*, è necessario che le imprese consapevoli intensifichino le attività di identificazione e introducano soluzioni avanzate di mitigazione del rischio.
Rientrano in questo livello sia aziende di piccole sia di medie dimensioni, la cui attenzione è spesso legata a precedenti violazioni del sistema informatico ed informativo.

IL **31%** DELLE PMI DIMOSTRA **CONSAPEVOLEZZA DEI RISCHI CYBER**, ANCHE SE NON SEMPRE RIESCE A IDENTIFICARE CORRETTAMENTE LE PRIORITÀ D'AZIONE

**Nota: per ulteriori approfondimenti si rimanda al glossario*

I 4 livelli di maturità



Mature
80 - 100

Il livello più alto è composto da imprese considerate più mature rispetto alle altre e che quindi si approcciano in maniera strategica alla tematica, pienamente **consapevoli dell'importanza che la gestione del rischio cyber ricopre all'interno del proprio business**. Nel **91% dei casi il top management richiede una relazione periodica** e il **presidio organizzativo è tipicamente internalizzato** (83% dei casi). La totalità di queste imprese ha poi previsto **fondi destinabili alla sicurezza informatica**, grazie ai quali riesce a monitorare e interpretare i rischi. Nel 52% dei casi, l'**attività di auditing**, sia sulla sicurezza informatica sia sulla compliance, viene **estesa anche ai partner della filiera**. Un'ulteriore scelta degna di nota è legata al ricorso a un processo di **gestione del rischio cyber integrato al processo di risk management aziendale**, con una visione olistica. Il forte commitment del top management e la ben sviluppata capacità di identificazione dei rischi consentono di mettere in campo le **corrette leve di attuazione, con iniziative che riguardando persone, processi e tecnologie**. Circa il 54% delle imprese di questo livello ha infine attivato coperture assicurative per trasferire il rischio cyber residuo. Rientrano in questo livello imprese di medie dimensioni collocate principalmente nel nord Italia, ovvero fornitrici di multinazionali o con più di 1.000 addetti.

DIMENSIONI DI ANALISI

NEL **14%** DELLE PMI LA SICUREZZA INFORMATICA **È PERCEPITA COME UNA PRIORITÀ**, GARANTENDO IL GIUSTO SOSTEGNO A TUTTE LE INIZIATIVE DI MONITORAGGIO E MITIGAZIONE DEL RISCHIO CYBER

***Nota**: le dimensioni utilizzano valori tra 0 e 100*

Il Cyber Index PMI nelle micro, piccole e medie imprese

La sicurezza informatica è importante per tutte le aziende, indipendentemente dalle loro dimensioni. Tuttavia, aziende di diverse entità possono avere esigenze e rischi di sicurezza informatica altrettanto diversi. Tendenzialmente, **maggiore è la dimensione aziendale, maggiore sarà l'esposizione ai rischi**, in quanto si parla di una maggiore quantità di dati, un sistema IT più complesso e una maggiore tendenza ad introdurre strumenti digitali, sebbene ci siano fattori che possono incidere sull'esposizione al rischio anche delle imprese di dimensioni minori.

La dimensione aziendale incide in maniera significativa anche sulla **disponibilità di risorse finanziarie**, necessarie per investire in soluzioni e servizi di sicurezza informatica avanzati o assumere esperti in-house. Le piccole e medie imprese dovrebbero iniziare a considerare la sicurezza informatica come un investimento necessario e ad adattare le soluzioni in base alle loro esigenze e risorse. Per **mitigare i costi**, le PMI potrebbero optare per l'esternalizzazione delle competenze, ricorrendo a **managed e/o professional services**.

Con l'obiettivo di investigare più in profondità come la dimensione aziendale impatti la strategia di gestione del rischio cyber delle PMI italiane, le prossime pagine illustreranno degli **spaccati distinti per micro, piccole e medie imprese**. Il commento d'analisi iniziale del **RAPPORTO CYBER INDEX 2023** specifico per ogni categoria sarà seguito da un'osservazione più centrata sulle tre dimensioni - approccio strategico, identificazione ed attuazione.

LA SICUREZZA INFORMATICA È IMPORTANTE PER TUTTE LE AZIENDE, INDIPENDENTEMENTE DALLE LORO DIMENSIONI.

FATTORI CHE POSSONO INCIDERE SULL'ESPOSIZIONE AL RISCHIO:

- CONCENTRAZIONE DI **DATI SENSIBILI**
- **RELAZIONI** CON AZIENDE STRATEGICHE
- PROPENSIONE A INTRODURRE **TECNOLOGIE**
- **DISPONIBILITÀ DI RISORSE FINANZIARIE** PER L'ACQUISTO DI SOLUZIONI, SERVIZI E COMPETENZE DI SICUREZZA INFORMATICA

Il Cyber Index PMI nelle micro, piccole e medie imprese

Dalla **TABELLA 1** si evidenzia una **correlazione positiva tra maturità delle imprese e dimensione aziendale.** Sebbene fosse un risultato intuibile, rappresenta una conferma di come **le realtà più piccole necessitino di un supporto nel processo di presa di consapevolezza dei rischi e messa in sicurezza dell'azienda.**

TABELLA 1

	Approccio strategico	Identificazione	Attuazione	Media ponderata
Micro imprese (<10 addetti)	47	36	47	**43**
Piccole imprese (10-49 addetti)	57	44	59	**53**
Medie imprese (50-249 addetti)	60	58	67	**61**
CYBER INDEX	**54**	**43**	**56**	**51**

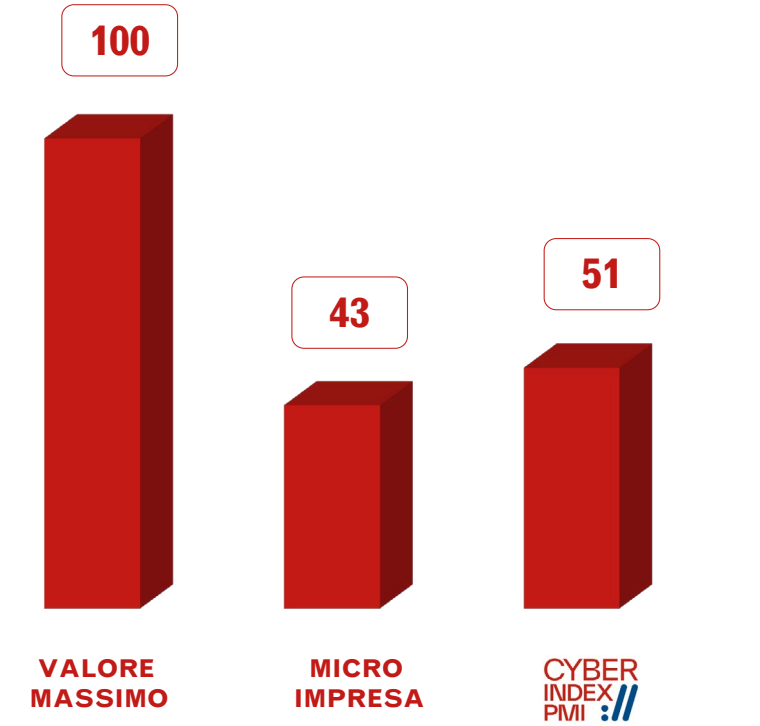
Cyber Index PMI nelle micro imprese

Aziende con un numero di addetti **inferiore a 10**, il cui volume d'affari fatturato in un anno **non supera i 2 milioni di euro**.

Le micro imprese sono particolarmente vulnerabili alle violazioni informatiche, poiché spesso non hanno le risorse o le competenze necessarie per implementare misure di sicurezza avanzate. Tuttavia, **le conseguenze di una violazione informatica possono essere altrettanto gravi** per le micro imprese rispetto a quanto lo sono per aziende di dimensioni maggiori (o addirittura più gravi, perché non si hanno gli strumenti per rispondere velocemente ed efficacemente).

Dal **RAPPORTO CYBER INDEX 2023** si nota come **il valore medio dell'indice sintetico ottenuto da queste imprese si fermi a 43** (su un valore massimo ottenibile pari a 100). Nonostante il basso punteggio ottenuto, l'esposizione al rischio di queste aziende non è sempre limitata: nel 53% dei casi l'impresa ha introdotto strumenti digitali almeno essenziali ed è quindi potenzialmente vittima di attacchi informatici; un 7% ha subito infatti almeno una violazione dei sistemi informativi aziendali tra il 2019 e il 2022. Inoltre, il 12% è fornitore di multinazionali o aziende sopra i 1.000 addetti, evidenziando una volta di più la centralità della sicurezza informatica anche nelle micro imprese e la necessità di supportarle nella messa in sicurezza. Fortunatamente il 45% delle proprietà si dichiara interessata al tema e nel 51% dei casi sono previsti fondi per l'acquisto di soluzioni.

GRAFICO 14



Cyber Index PMI nelle micro imprese

Aziende con un numero di addetti **inferiore a 10**, il cui volume d'affari fatturato in un anno **non supera i 2 milioni di euro**.

Approccio strategico

Nonostante il tema risulti rilevante all'interno delle micro imprese, l'approccio strategico soffre l'insufficiente disponibilità di risorse economiche e umane; **questa situazione critica si traduce in un punteggio di 47**, particolarmente limitato rispetto alla classe dimensionale superiore, che ottiene invece 57.

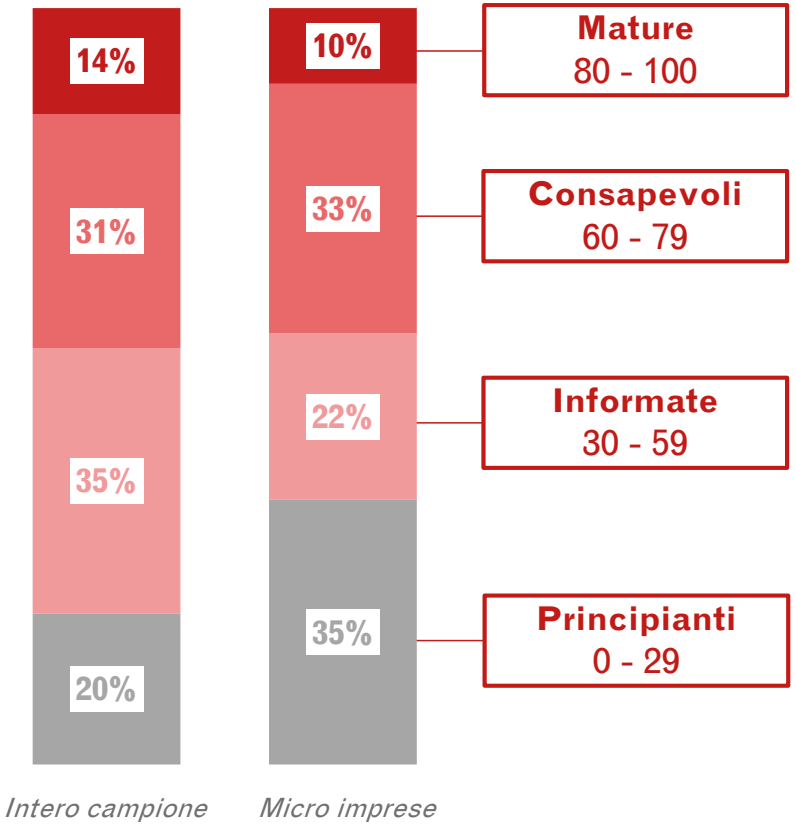
Identificazione

La capacità di comprendere e monitorare il rischio cyber è estremamente limitata all'interno delle micro imprese, che **spesso non intraprendono neppure attività base come la mappatura degli asset e l'auditing**. Ne consegue un punteggio fermo a 36.

Attuazione

Nel complesso le micro **imprese faticano nell'introdurre tecnologie di base** e talvolta sottovalutano anche attività a basso costo come la definizione degli accessi e i processi di backup. Il punteggio ottenuto per l'attuazione è pari a 47.

GRAFICO 15

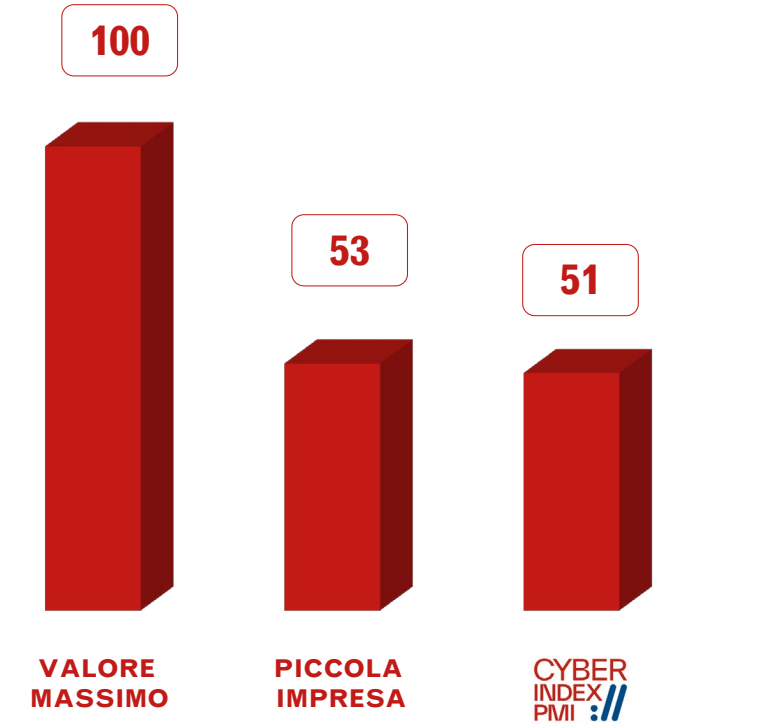


Cyber Index PMI nelle piccole imprese

Aziende con un numero di addetti **tra 10 e 49**, il cui fatturato in un anno **non supera i 10 milioni di euro**.

Con un **indice sintetico medio di 53** su un punteggio ottenibile di 100, le piccole imprese dimostrano una **postura in linea con la media**: questo gruppo di aziende è tuttavia il più colpito dalle violazioni informatiche, sfiorando le 15 imprese violate ogni 100 tra il 2019 e il 2022. Le imprese tra i 10 e i 49 addetti sono infatti spesso dotate di strumenti digitali avanzati (35%), hanno una fitta rete collaborativa con multinazionali e operano attivamente all'estero. Hanno quindi una **maggior esposizione al rischio delle micro imprese, che non sempre si accompagna a una adeguata preparazione rispetto alle minacce informatiche**. Nonostante ciò, **solo l'8% delle piccole imprese si ritiene impreparato** ad affrontare i rischi. Inoltre, il 42% delle proprietà non ritiene rilevante la sicurezza informatica, la cui gestione viene principalmente demandata a un partner esterno.

GRAFICO 16



Cyber Index PMI nelle piccole imprese

Aziende con un numero di addetti **tra 10 e 49**, il cui fatturato in un anno **non supera i 10 milioni di euro**.

Approccio strategico

Nonostante le criticità, l'approccio strategico delle piccole imprese italiane raggiunge un **punteggio di 57.** Una buona quota di esse dimostra quindi di essere in grado di destinare fondi e presidiare la materia con figure interne o esterne.

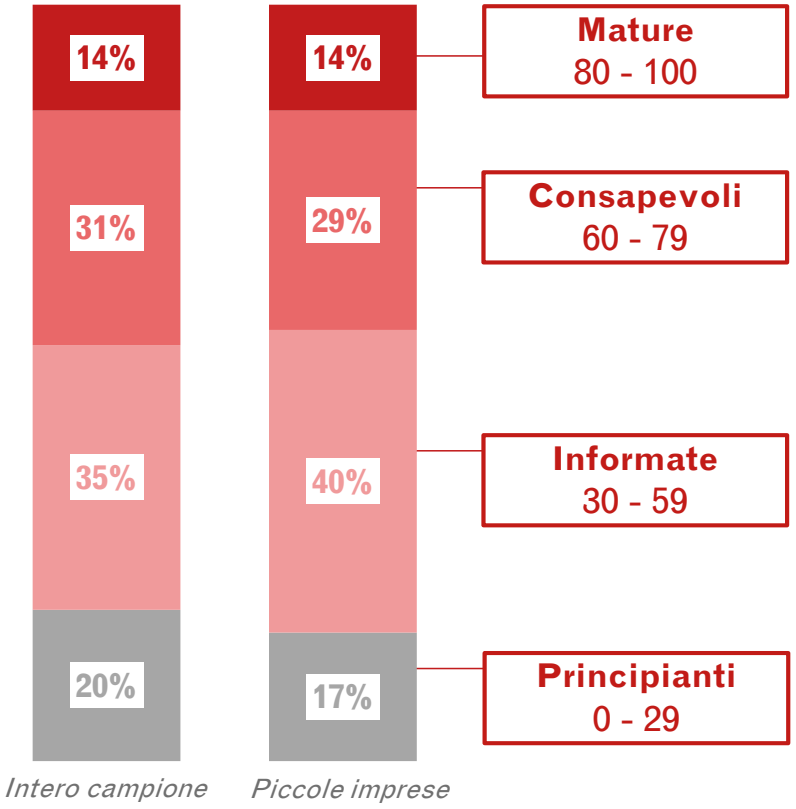
Identificazione

Anche per le piccole imprese la **difficoltà maggiore** è rappresentata dalla **fase di identificazione e comprensione del rischio cyber** (punteggio pari a **44**). Difficilmente le piccole imprese vanno oltre le attività di base, quali la mappatura degli asset informatici e l'auditing sugli aspetti della compliance.

Attuazione

Nella dimensione dell'attuazione emergono segnali positivi (punteggio pari a 59): **buona parte delle piccole imprese ha introdotto strumenti e processi** per il **monitoraggio e la protezione** del sistema informatico e dei dispositivi aziendali.

GRAFICO 17



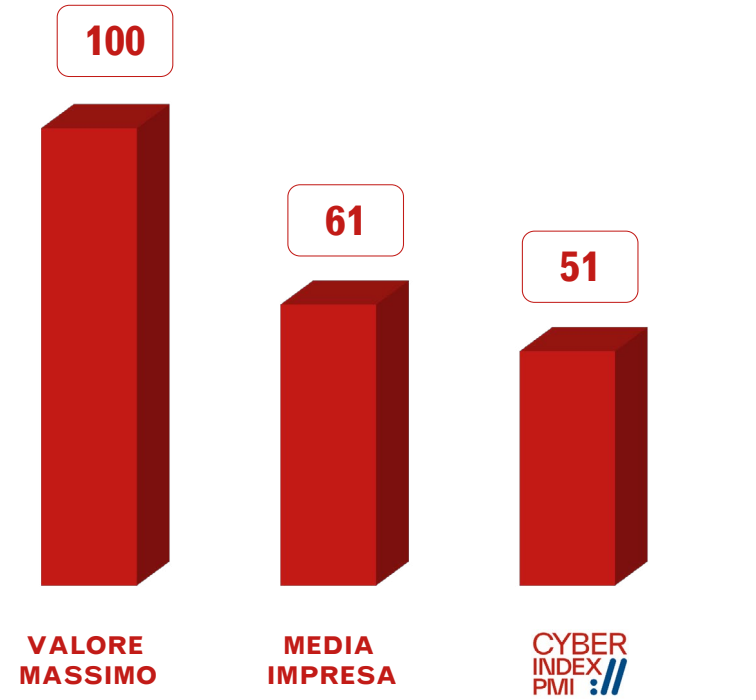
Cyber Index PMI nelle medie imprese

Aziende con un numero di addetti **tra 50 e 249**, e il cui fatturato in un anno **non supera i 50 milioni di euro**.

Le medie imprese hanno un approccio alla cybersecurity che, nel complesso, si può considerare adeguato. Dall'analisi dei dati, è emerso che **la dimensione dell'azienda incide sull'approccio adottato verso la sicurezza informatica**. Le ragioni chiave sono il **budget destinabile e le risorse umane specializzate disponibili**, tendenzialmente proporzionate alla capacità di spesa dell'impresa.

Le medie imprese che hanno **subito una violazione** ai sistemi informativi negli ultimi quattro anni sono il **18%, dato che risulta allarmante visto che il 78% di esse è parte di una filiera critica**. Secondo i risultati, il 29% ha sedi all'estero e il 15% opera in filiere estese in paesi instabili dal punto di vista geopolitico. Guardando entro i confini italiani, il 14% opera a contatto con infrastrutture critiche, mentre il 51% è fornitore di imprese oltre i 1.000 addetti. Queste statistiche rendono evidente come al crescere della dimensione emergano nuove criticità. **Nonostante queste realtà godano di una buona postura di sicurezza informatica (61/100), risultano comunque spesso impreparate ad affrontare uno scenario così complesso**.

GRAFICO 18



Cyber Index PMI nelle medie imprese

Aziende con un numero di addetti **tra 50 e 249**, e il cui fatturato in un anno **non supera i 50 milioni di euro**.

Approccio strategico

Nel **90%** delle medie imprese, i **vertici aziendali sono coinvolti** nella strategia in materia di sicurezza informatica e nell'**89% esiste un budget**. Il 90% ha poi definito un **presidio organizzativo**. Si registrano tuttavia risultati carenti per quanto riguarda le certificazioni e i piani di sicurezza. Il punteggio ottenuto per la dimensione è pari a 60.

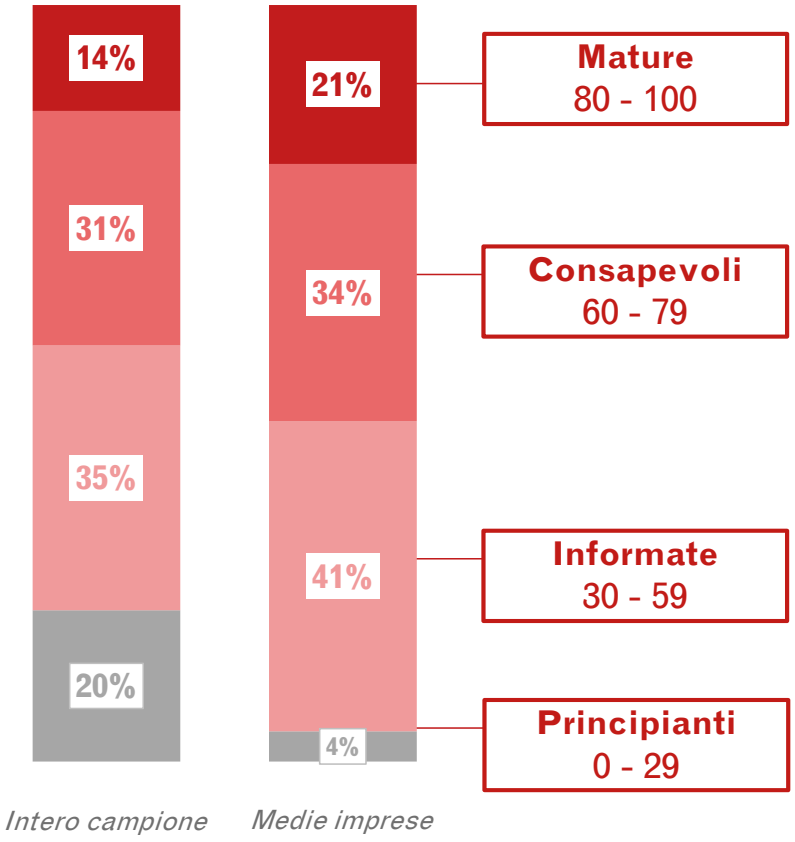
Identificazione

Nonostante il 31% delle medie imprese ancora non svolga attività di auditing, spesso vengono condotte analisi saltuarie per monitorare il rischio cyber. In relazione allo scenario descritto precedentemente, l'auspicio è che tali realtà migliorino le attività di gestione della sicurezza delle **terze parti**. Il punteggio ottenuto per la dimensione è pari a 58.

Attuazione

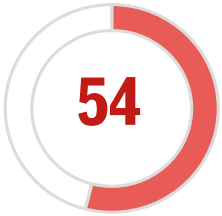
Complessivamente le medie imprese **sono in grado di adottare strumenti tecnologici, sono consapevoli delle iniziative necessarie per gestire il fattore umano** e si distinguono anche per una **buona conoscenza delle polizze assicurative** per trasferire il rischio. Il punteggio ottenuto per la dimensione è pari a 67.

GRAFICO 19



«Approccio strategico»

Approccio strategico



Identificazione

Attuazione

IL PUNTEGGIO DI **54/100** OTTENUTO NELL'**APPROCCIO STRATEGICO** DENOTA COME LE PMI ITALIANE GENERALMENTE **FATICHINO AD APPROCCIARSI IN MANIERA STRATEGICA ALLA CYBERSECURITY**

DIMENSIONE DI ANALISI

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.

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

***Nota**: L'indice utilizza valori tra 0 e 100*

«Approccio strategico»

La sola adozione di strumenti tecnologici non soddisfa appieno il concetto di corretta gestione della sicurezza. Infatti, è necessario abbinarvi una **visione organizzativa**, comprendente il coinvolgimento dei vertici aziendali, la definizione di un presidio organizzativo che indirizzi la materia e l'attivazione di un budget destinabile agli investimenti di lungo periodo.

Dal Rapporto si evidenzia come **chi ha già avviato un percorso di trasformazione digitale,** introducendo strumenti che spaziano da ERP e CRM fino a IoT e Cloud, **si approcci mediamente in maniera più strategica alla sicurezza informatica** (ottenendo un punteggio per la dimensione approccio strategico pari a 58/100) rispetto a chi ancora non ne ha introdotti (38/100).

Una nota positiva emersa dall'analisi spiega poi come le **imprese operanti all'interno di filiere strategiche o internazionali siano più attente al tema**. Infatti, le PMI che collaborano con infrastrutture critiche ottengono un punteggio di 62/100 (+8 p.ti rispetto alla media) e chi ha attive sedi e/o impianti all'estero si attesta su una media di 61/100 (+7 p.ti rispetto alla media).

Le **violazioni subite** sono un ulteriore **aspetto che spinge ad approcciarsi alla sicurezza informatica in maniera più strategica**. Restringendo il campione a coloro che hanno subito almeno una violazione negli ultimi 4 anni, si ottiene un valore di questa dimensione di 5 punti superiore, sintomo di come spesso le imprese prendano consapevolezza solo a posteriori di un incidente.

LE PMI CHE HANNO INTRAPRESO UN **PERCORSO DI TRASFORMAZIONE DIGITALE** OPERANO ALL'INTERNO DI UNA **FILIERA STRATEGICA** O HANNO SUBITO UNA **VIOLAZIONE DEI SISTEMI INFORMATIVI** SI APPROCCIANO IN MANIERA PIÙ STRATEGICA RISPETTO ALLA MEDIA COMPLESSIVA

«Identificazione»

Approccio strategico: 54

Identificazione: 43

Attuazione: 56

SI REGISTRA UNA **FORTE CRITICITÀ NELLA COMPRENSIONE DEL RISCHIO CYBER**, OVVERO NELLE ATTIVITÀ DI MONITORAGGIO DEI RISCHI AZIENDALI

DIMENSIONE DI ANALISI

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**.

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

L'**IDENTIFICAZIONE** È LA DIMENSIONE SULLA QUALE LE PMI APPAIONO IN GENERALE **MENO MATURE**

***Nota**: L'indice utilizza valori tra 0 e 100*

«Identificazione»

L'attività di identificazione, ovvero di comprensione dei rischi informatici e dei rischi sanzionatori derivanti da una possibile violazione, risulta essere quella **più complessa** e, di conseguenza, quella su cui piccole e medie imprese soffrono maggiormente. Tale attività è sempre più centrale all'interno dello scenario generale. Come anticipato, gli attacchi informatici sono sempre più frequenti e significativi, perciò **comprendere quali siano le vulnerabilità e le minacce è indispensabile per attuare le giuste azioni di mitigazione**. Identificare i rischi significa nel concreto affidarsi a profili e società esperti in vulnerability assessment, penetration testing, misurazione del rischio cyber e auditing*. Il Rapporto 2023 evidenzia un **dato allarmante** nella capacità di comprendere e monitorare il rischio: di fatto, il punteggio medio di identificazione si ferma a un 43/100, rappresentando quindi l'area più arretrata tra le tre considerate.

Come nella dimensione precedente, le imprese che monitorano i rischi con maggiore attenzione sono quelle che appartengono a filiere maggiormente complesse. In questo caso, spesso sono le società con cui le PMI si relazionano all'interno della catena del valore a imporre attività di monitoraggio come requisito necessario per instaurare una collaborazione commerciale. Allo stesso modo, le imprese che hanno subito un incidente in passato ottengono un punteggio superiore alla media.

È opportuno inoltre chiarire che le attività di identificazione sono utili e vantaggiose se **condotte in maniera periodica e ricorrente** durante l'attività d'impresa.

LE IMPRESE CHE MONITORANO I RISCHI SONO QUELLE CHE **APPARTENGONO A FILIERE MAGGIORMENTE COMPLESSE O CHE HANNO SUBITO UN INCIDENTE**

**Nota: rimando alla parte 4 dell'Evidenze della Ricerca, valutazione delle vulnerabilità, auditing della sicurezza informatica, misurazione del rischio cyber*

«Attuazione»

Approccio strategico

Identificazione

Attuazione

CON UN INDICE DI **56 SU 100**, L'ATTUAZIONE È LA DIMENSIONE IN CUI LE PMI ITALIANE OTTENGONO UN **PUNTEGGIO COMPLESSIVO PIÙ ALTO**

DIMENSIONE DI ANALISI

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.**

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

***Nota**: L'indice utilizza valori tra 0 e 100*

«Attuazione»

Con "attuazione" si fa riferimento all'**insieme di iniziative tecnologiche, umane e di processo poste in essere per proteggere il sistema informativo aziendale**. Tali attività, per risultare efficaci, richiedono anzitutto una **chiara percezione dei rischi**, quindi la relazione con la fase di identificazione è particolarmente rilevante. Dai risultati del Rapporto emerge una **discreta propensione ad introdurre iniziative di sicurezza**, quello che spesso **manca** è **l'indirizzamento delle priorità d'investimento.**

Complessivamente le piccole e medie imprese italiane hanno una buona preparazione su questa dimensione, che è anche quella in cui si registra il punteggio più alto, sebbene permangano importanti elementi di miglioramento.

Spesso si riconduce l'attività di attuazione ad un piano tecnologico. Questa scelta è riduttiva rispetto alla realtà, in cui **gli utenti rappresentano spesso la principale vulnerabilità** sfruttata dai criminali per sferrare attacchi informatici. Di conseguenze, la gestione del fattore umano è rilevante almeno al pari della sfera tecnologica.

Parallelamente agli interventi di mitigazione e protezione, un ulteriore strumento a cui si può ricorrere, spesso sottovalutato, è la **stipula di polizze** a copertura del rischio cyber residuo. Questa soluzione è particolarmente funzionale per quanto riguarda la riduzione dei costi occorsi per l'interruzione dell'attività aziendale o dei risarcimenti a terze parti a seguito di una violazione.

COMPLESSIVAMENTE LE **PMI ITALIANE HANNO UNA BUONA PREPARAZIONE IN TERMINI DI ATTUAZIONE**. MANCA INVECE LA CAPACITÀ DI INDIRIZZAMENTO DELLE PRIORITÀ D'INVESTIMENTO

Introduzione alle aree di analisi

Le aree di analisi, presentate anche nella sezione «Introduzione al rapporto e impostazione metodologica», afferiscono ad una o più domande del questionario. Al fine di condurre un'indagine il più possibile adeguata alle caratteristiche delle piccole e medie imprese, il questionario è stato sviluppato in maniera modulare su più livelli di approfondimento, legati alla dimensione e all'esposizione al rischio delle singole organizzazioni. I risultati delle 20 aree di analisi, riportate all'interno della tabella e di cui si darà visibilità nella **SEZIONE 4**, sono pertanto frutto dell'elaborazione delle risposte di 3 campioni diversi:

- Le aree di analisi rappresentate dal colore più chiaro e che indicano le scelte strategiche e/o operative di sicurezza informatica di **livello base** sono state sottoposte all'intero campione di **658 imprese**;
- Le aree di analisi rappresentate dal colore mediano e che indicano le scelte strategiche e/o operative di sicurezza informatica di **livello intermedio** sono state sottoposte a **322 imprese**, che hanno dimostrato una **MEDIA O ALTA ESPOSIZIONE** al rischio;
- Le aree di analisi rappresentate dal colore più scuro e che indicano le scelte strategiche e/o operative di sicurezza informatica di **livello avanzato** sono state sottoposte a **204 imprese**, che hanno dimostrato un'**ALTA ESPOSIZIONE** al rischio.

Per garantire un'interpretazione dei risultati corretta, si suggerisce quindi di prestare attenzione al campione riportato sotto ciascuno dei grafici rappresentati. Per ulteriori dettagli si rimanda alla nota metodologica.

Dimensione	Aree di analisi	Campione
Approccio strategico	Commitment della proprietà	658
	Budgeting	658
	Presidio organizzativo	658
	Piano di sicurezza	322
	Certificazioni	204
Identificazione	Mappatura degli asset informatici	658
	Valutazione delle vulnerabilità	322
	Auditing della sicurezza informatica	658
	Misurazione del rischio cyber	322
	Valutazione del livello di sicurezza dei fornitori	322
	Cyber Risk Management	204
	Adeguamento alla compliance normativa	204
Attuazione	Gestione del fattore umano	658
	Formazione	658 - 204
	Polizze assicurative	658
	Tecnologie per la protezione dei dati	658
	Tecnologie per il monitoraggio di attività anomale	658
	Tecnologie per la protezione delle reti	322
	Linee guida dirette alle terze parti	204
	Programmi di info-sharing	204

Commitment della proprietà

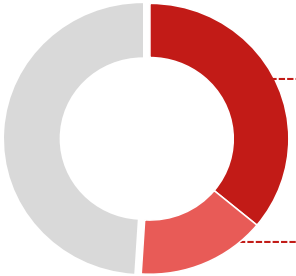
Il commitment della proprietà indica il livello di interesse e coinvolgimento dei vertici aziendali nelle scelte strategiche di gestione del rischio cyber ed è un buon indicatore per rappresentare la rilevanza assunta dalla materia all'interno di piccole e medie imprese.

Dalle evidenze del Rapporto emerge come il 51% delle proprietà – o delle direzioni aziendali – si interessi al tema, sebbene con intensità diversa. Nel **36%** dei casi, infatti, **il vertice aziendale viene coinvolto nell'indirizzamento del tema e richiede una relazione periodica**; questa situazione avviene principalmente nelle realtà di piccole dimensioni. Il **15%** delle imprese invece dichiara che l'imprenditore **ritiene rilevante il tema ma non è coinvolto attivamente** nei diversi processi di gestione.

A complemento della torta vi sono aziende che ancora non ritengono rilevante la sicurezza informatica. Il 7% dichiara che si sta avvicinando al tema in questo periodo, principalmente a seguito di una violazione dei sistemi informativi aziendali, mentre il 42% delle proprietà non risulta preoccupato del rischio cyber. Quest'ultima porzione è tipicamente costituita da micro imprese.

APPROCCIO STRATEGICO

COMMITMENT DELLA PROPRIETÀ: volontà dei proprietari o dei vertici aziendali ad impegnarsi a livello strategico per garantire una solida gestione della sicurezza informatica



36% L'imprenditore o i vertici aziendali indirizzano il tema e richiedono periodicamente una relazione

15% L'imprenditore o i vertici aziendali si interessano ma senza partecipare al processo decisionale

Campione: 658 piccole e medie imprese italiane

NEL **51%** DELLE PMI IL TEMA DELLA CYBERSECURITY **È PERCEPITO COME RILEVANTE**, CON UN **COMMITTMENT DIRETTO DA PARTE DELLA PROPRIETÀ**

Budget e fondi per la cybersecurity

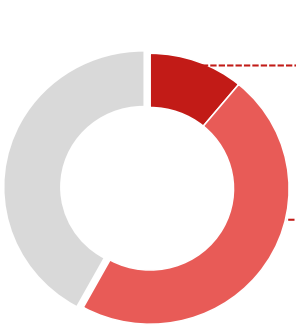
Stanziare risorse per la sicurezza informatica è una priorità d'azione a seguito della presa di consapevolezza della proprietà. Circa il **58%** delle PMI italiane **stanzia fondi per proteggere i sistemi informatici e i dati sensibili**, sebbene solo le imprese di maggiori dimensioni riescano a destinare un budget dedicato.

Nonostante spesso la proprietà non sia consapevole dell'importanza della sicurezza informatica, un 27% di imprese si dichiara intenzionato a stanziare fondi appositi in futuro. Persiste, infine, un 15% che invece non ritiene necessario stanziare fondi. Anche in questo caso, a soffrire maggiormente sono le micro imprese.

L'entità del budget per la sicurezza informatica di una piccola o media impresa può variare molto in base alle dimensioni dell'azienda. Tuttavia, è bene specificare che anche destinare ingenti somme di denaro non garantisce necessariamente una protezione efficace. È quindi importante avere una visione di lungo termine, misurando periodicamente i progressi compiuti e attuando le corrette azioni in accordo con le proprie esigenze e priorità.

APPROCCIO STRATEGICO

BUDGETING: allocazione di risorse economiche destinabili all'acquisto di servizi e soluzioni di sicurezza informatica, all'assunzione di personale specializzato e alla formazione dei dipendenti



11% Esiste un budget dedicato

47% Parte del budget IT è destinabile alla sicurezza informatica

Campione: 658 piccole e medie imprese italiane

IL **58%** DELLE PMI MANIFESTA **UN'ATTENZIONE CONCRETA** VERSO LE TEMATICHE DELLA SICUREZZA INFORMATICA, **STANZIANDO UN BUDGET** APPOSITO

Presidio organizzativo della cybersecurity

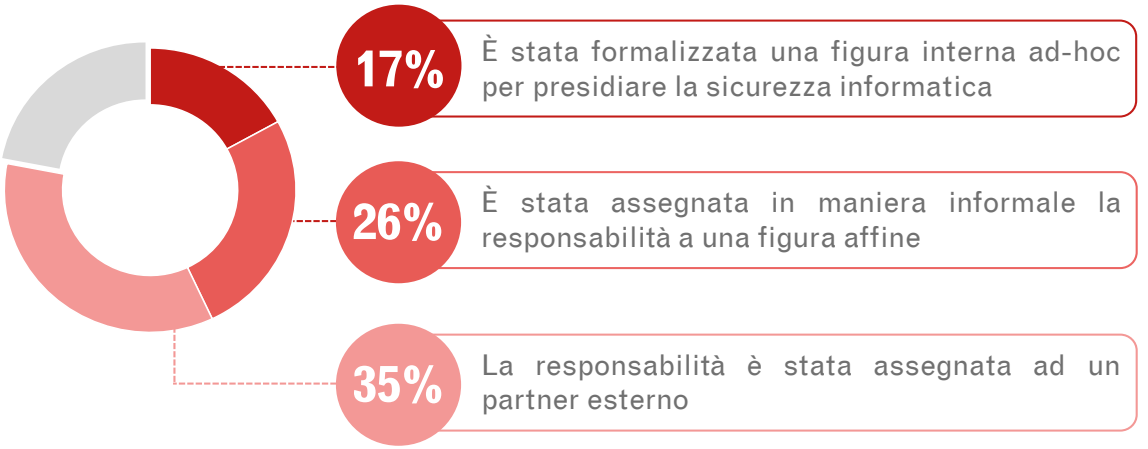
Implementare un presidio organizzativo comporta la chiara definizione dei ruoli e delle responsabilità all'interno dell'impresa per la gestione della sicurezza informatica, nonché la configurazione di relazioni con la proprietà, il team IT e il business.

La soluzione ideale è la formalizzazione di **una figura ad-hoc che presidi la sicurezza informatica**, scelta fatta dal **17%** delle PMI italiane. Tale figura si colloca nel 40% dei casi all'interno dell'IT, nel 36% dei casi riporta direttamente alla proprietà, mentre nel restante 24% è inserito in un'altra funzione.
Tuttavia, **l'azione più ricorrente è l'assegnazione del presidio organizzativo ad un partner esterno (35%)**, che spesso gestisce interamente la sicurezza informatica aziendale. Questa soluzione si rivela spesso la più percorribile non richiedendo particolari investimenti iniziali, ma la visibilità sul processo di gestione del rischio cyber risulta spesso limitato.
Il 26% delle PMI ha poi deciso di assegnare la responsabilità della sicurezza a una figura affine, tipicamente rappresentata dall'IT manager.

Preoccupa infine il 12% di PMI che non ritiene prioritario presidiare la sicurezza informatica, mentre il 10% sta valutando l'introduzione di un presidio.

APPROCCIO STRATEGICO

PRESIDIO ORGANIZZATIVO: definizione di ruoli e responsabilità, interni o esterni, inerenti alla gestione dell'intero processo di sicurezza informatica aziendale



Campione: 658 piccole e medie imprese italiane

IL 35% DELLE PMI SI AFFIDA A FORNITORI ESTERNI, EVIDENZIANDO UNA **TENDENZA AD ESTERNALIZZARE LE COMPETENZE.** SOLO IL **17%** DELLE PMI HA INSERITO UNA **FIGURA INTERNA AD-HOC**

Piano di sicurezza

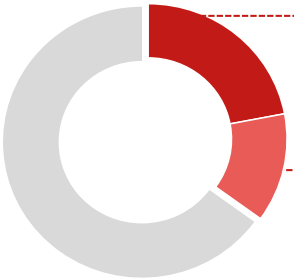
Lo sviluppo di un piano di sicurezza informatica richiede la definizione del perimetro da difendere, la valutazione dei rischi e l'organizzazione di leve di mitigazione (procedure, ruoli e strumenti). Il piano di sicurezza rappresenta quindi la formalizzazione di una strategia e coinvolge tutti gli elementi abilitanti la sicurezza informatica. Tale piano, tuttavia, richiede una costante revisione in relazione al cambiamento del contesto e dei fattori in gioco.

Lo sviluppo di un piano di sicurezza informatica è una scelta strategica di livello intermedio, che ha coinvolto un campione di imprese con un'esposizione al rischio considerata medio-alta.

Tra queste, **il 35% ha definito un piano di sicurezza** ma solo il 22% si impegna a rivederlo almeno annualmente. Il 45% invece non ha definito formalmente un piano ma si affida a prassi e linee guida informali. Nonostante la percentuale sul campione complessivo risulti bassa, si segnala comunque la presenza di piccole e medie imprese particolarmente avanzate.

APPROCCIO STRATEGICO

PIANO DI SICUREZZA: sviluppo di un documento strategico che definisce le politiche, le procedure e le misure di sicurezza da implementare per proteggere i dati, le risorse e le infrastrutture aziendali dalle minacce informatiche



22% È stato approvato un piano di sicurezza informatica rivisto almeno annualmente

13% È stato approvato un piano di sicurezza informatica rivisto saltuariamente

Campione: 322 piccole e medie imprese italiane

NEL **35%** DELLE PMI È STATO **APPROVATO UN PIANO DI SICUREZZA INFORMATICA** CHE VIENE RIVISTO ANNUALMENTE O OCCASIONALMENTE

Certificazioni aziendali di sicurezza informatica

Le **certificazioni ISO** (International Organization for Standardization) sono standard internazionali riconosciuti a livello globale che stabiliscono requisiti e linee guida per diverse aree di gestione aziendale. In relazione alla sicurezza informatica risultano particolarmente importanti:

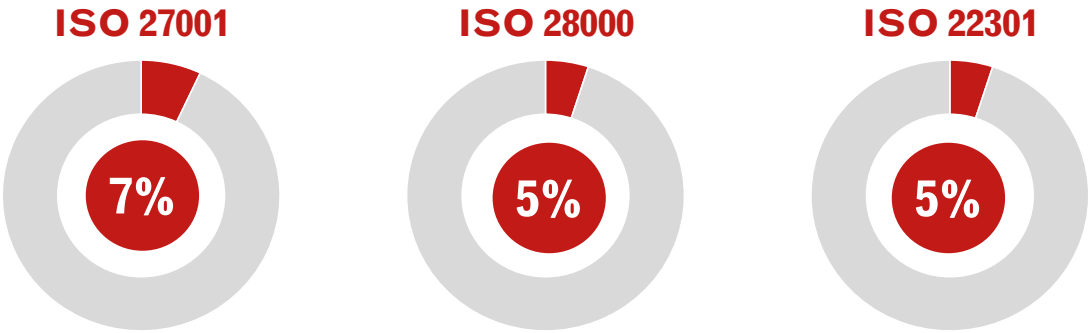
1. ISO 27001 – definizione dei requisiti per garantire la confidenzialità, l'integrità e la disponibilità delle informazioni dell'organizzazione;
2. ISO 28000 – definizione dei requisiti per la gestione della sicurezza nella filiera (supply chain security);
3. ISO 22301 – definizione dei requisiti per garantire la continuità delle operazioni, la ripresa delle attività in caso di interruzioni e il ripristino delle funzioni critiche dovute a violazioni informatiche.

Poiché il conseguimento e il mantenimento di una certificazione ISO sono considerati una scelta strategica di livello avanzato, è possibile considerare le certificazioni come elementi che contribuiscono attivamente allo sviluppo della sicurezza informatica all'interno delle imprese.

Tra le PMI che hanno una alto livello di esposizione al rischio (campione di 204 PMI) **questa buona pratica è ancora poco diffusa**, sebbene possa generare una miglior postura di sicurezza, maggior fiducia dei partner e un concreto sforzo di conformità alle normative.

APPROCCIO STRATEGICO

CERTIFICAZIONI: conseguimento di attestazioni circa la conformità dei sistemi informativi e dei processi aziendali ai requisiti di sicurezza e privacy previsti dalle certificazioni ISO 27001, ISO 28000 e ISO 22301



Campione: 204 piccole e medie imprese italiane

MENO DEL 10% DELLE PMI AD ALTA ESPOSIZIONE CONSEGUE LE **CERTIFICAZIONI** DISPONIBILI IN MATERIA DI SICUREZZA INFORMATICA E PROTEZIONE DEI DATI

Mappatura degli asset informatici

La mappatura degli asset informatici è un processo che consiste nell'identificazione, nella classificazione e nella documentazione di tutti gli asset informatici presenti all'interno di un'organizzazione e delle relative dipendenze. Gli asset informatici possono includere hardware, software, dati, reti, sistemi operativi, applicazioni, dispositivi mobili, device IoT e altri componenti IT rilevanti. Una mappatura degli asset informatici ben eseguita fornisce una panoramica chiara del perimetro aziendale da difendere e funge da analisi preliminare per le attività di vulnerability assessment.

Dai risultati del Rapporto 2023 emerge come **questo processo sia implementato su base continuativa nel 34% delle PMI,** che riconoscono l'importanza di mantenere un monitoraggio costante e una gestione efficace degli asset. Ciò può includere l'aggiornamento delle informazioni, la gestione delle licenze software, la pianificazione dei cicli di vita, la gestione delle patch di sicurezza e la gestione delle modifiche.

Il 33% invece svolge la mappatura una tantum o la limita a determinati asset rilevanti. Il 17% ne sta valutando l'introduzione mentre il 16% non prende in considerazione questa attività.

IDENTIFICAZIONE

MAPPATURA DEGLI ASSET INFORMATICI: strutturazione di un processo di identificazione e catalogazione di tutti i componenti tecnologici e delle risorse digitali di un'organizzazione

34% Esiste un processo strutturato di mappatura di tutti gli asset informatici su base continuativa

33% Esiste un processo di mappatura che riguarda alcuni asset informatici o viene condotta una mappatura una tantum

Campione: 658 piccole e medie imprese italiane

NEL **67%** DELLE PMI ESISTE **UN PROCESSO DI MAPPATURA** ALMENO SALTUARIA DI ALCUNI ASSET INFORMATICI

Valutazione delle vulnerabilità

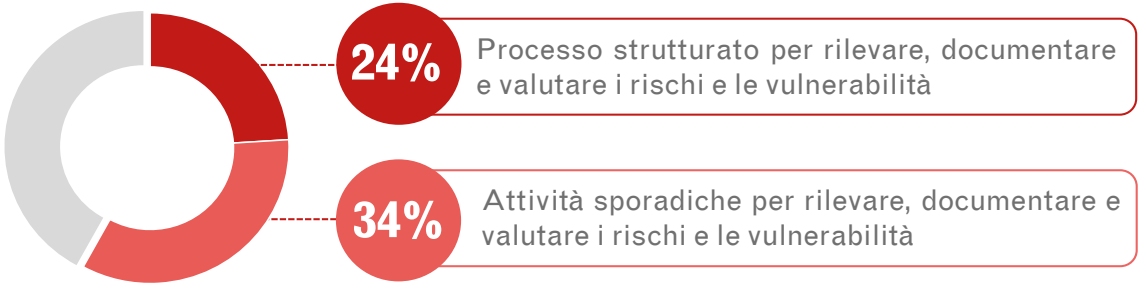
La valutazione delle vulnerabilità (o vulnerability assessment) è un processo che identifica, valuta e documenta le vulnerabilità presenti in un sistema informatico, una rete o un'applicazione, che potrebbero essere sfruttate da minacce esterne o interne per compromettere la sicurezza e l'integrità del sistema.

Basandosi sulle vulnerabilità identificate e sulla loro valutazione, l'organizzazione può integrare nel piano di sicurezza azioni da intraprendere per affrontarle, come l'applicazione di patch o altre misure appropriate.

La valutazione delle vulnerabilità è un'attività operativa di livello intermedio che richiede una buona maturità nell'Approccio Strategico e nelle precedenti attività di identificazione. Tra i 322 rispondenti, il **58% afferma di condurre la valutazione delle vulnerabilità**, ma solo il 24% ha un processo strutturato e continuativo. Anche in questo caso è importante monitorare costantemente il sistema e sottoporlo a periodiche valutazioni per identificare nuove minacce o potenziali vulnerabilità. Completano la vista un 35% di imprese interessate a introdurre questa attività nel prossimo futuro e un 7% che invece non manifesta questa volontà.

IDENTIFICAZIONE

VALUTAZIONE DELLE VULNERABILITÀ: conduzione di analisi mirate a identificare e valutare le vulnerabilità presenti nei sistemi informatici, nelle reti, nelle applicazioni e negli asset digitali di un'organizzazione



Campione: 322 piccole e medie imprese italiane

IL **58%** DELLE PMI CON MEDIA ESPOSIZIONE AL RISCHIO AFFERMA DI CONDURRE TEST PER **VALUTARE LE VULNERABILITÀ** DEL SISTEMA. DI QUESTE, SOLO IL **24%** HA UN PROCESSO STRUTTURATO E CONTINUATIVO

Auditing della sicurezza informatica

L'auditing della sicurezza informatica è un insieme di processi e attività che mira a valutare la presenza e l'efficacia di misure di sicurezza implementate da un'organizzazione per proteggere il perimetro da minacce e garantire la compliance alle normative.

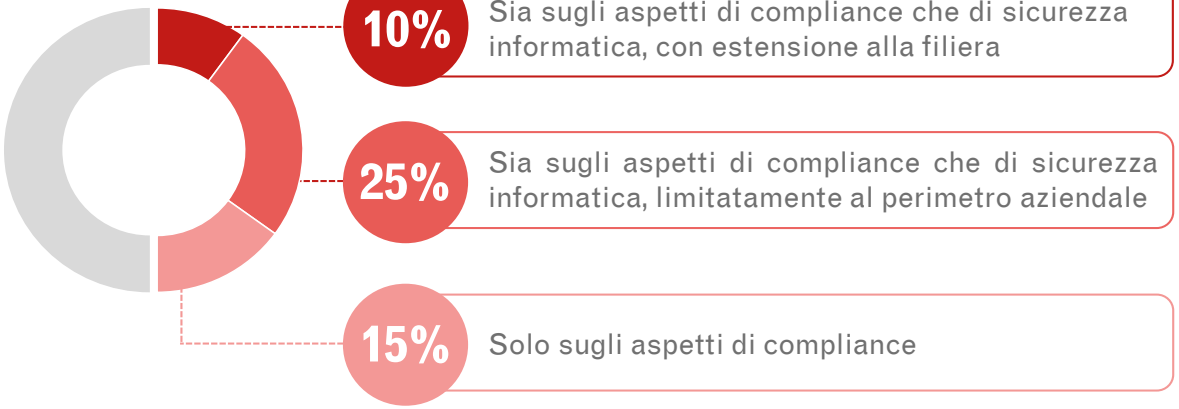
Queste attività risultano particolarmente utili in quanto contribuiscono ad identificare le lacune e forniscono raccomandazioni specifiche per migliorare la sicurezza informatica aziendale.

Il 35% delle PMI afferma di svolgere attività di auditing sia sugli aspetti di compliance che di sicurezza informatica, e circa il 10% di esse estende tale analisi anche alla filiera. Il 15% svolge invece attività di auditing limitatamente agli aspetti di compliance normativa, contribuendo comunque a migliorare la postura negli aspetti legati alla protezione dei dati.

Completa la vista il restante 50% delle PMI, rappresentato principalmente da imprese di piccole e micro dimensioni, che invece non svolge attività di auditing, anche a causa di una pressione normativa inferiore.

IDENTIFICAZIONE

AUDITING DELLA SICUREZZA INFORMATICA: conduzione di analisi sistematiche di valutazione e verifica delle misure di sicurezza informatica e della compliance normativa



Campione: 658 piccole e medie imprese italiane

LA METÀ DELLE PMI SVOLGE ATTIVITÀ DI **AUDITING**. DI QUESTE, IL **35%** VERIFICA SIA GLI ASPETTI DI COMPLIANCE SIA QUELLI DI SICUREZZA INFORMATICA E IL **10%** ESTENDE LE ATTIVITÀ **ANCHE ALLA FILIERA**

Misurazione del rischio cyber

La misurazione del rischio cyber è un processo che mira a valutare e quantificare il livello di rischio associato alle minacce informatiche e alla sicurezza delle informazioni all'interno di un'organizzazione, misurando probabilità di accadimento e potenziali impatti degli scenari identificati. Questo processo aiuta a rilevare le aree di maggiore esposizione al rischio e a prendere decisioni informate sulla gestione e l'allocazione delle risorse per mitigarlo.

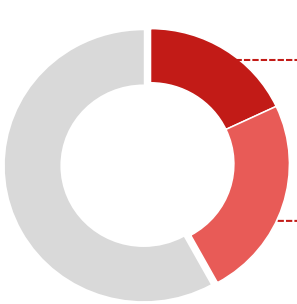
La misurazione del rischio cyber si pone a complemento di un processo iniziato con l'identificazione degli asset e la valutazione delle vulnerabilità. Tale area viene per tanto analizzata esclusivamente all'interno di imprese con un'esposizione al rischio superiore alla media (322 PMI).

Tra queste, **il 18% afferma di compiere la misurazione del rischio su base annuale o semestrale, mentre il 24% effettua test in maniera saltuaria**.

La misurazione del rischio cyber dovrebbe essere un processo periodico. Tuttavia, è indispensabile pianificarne la valutazione ogni volta che l'ambiente informatico subisce modifiche significative a seguito di violazioni o cambiamenti nell'operatività aziendale, come l'ingresso in nuovi mercati, l'espansione delle operazioni o il lancio di nuovi prodotti o servizi.

IDENTIFICAZIONE

MISURAZIONE DEL RISCHIO CYBER: conduzione di analisi mirate a valutare e quantificare periodicamente il rischio associato alle minacce informatiche e alle vulnerabilità all'interno di un'organizzazione



18% Test periodici di misurazione del rischio cyber, con cadenza almeno annuale

24% Test di misurazione del rischio cyber condotti saltuariamente

Campione: 322 piccole e medie imprese italiane

IL **42%** DELLE PMI CON MEDIA ESPOSIZIONE AL RISCHIO CONDUCE **TEST DI MISURAZIONE DEL RISCHIO CYBER**. DI QUESTE, IL **18%** LO FA PERIODICAMENTE

Valutazione del livello di sicurezza dei fornitori

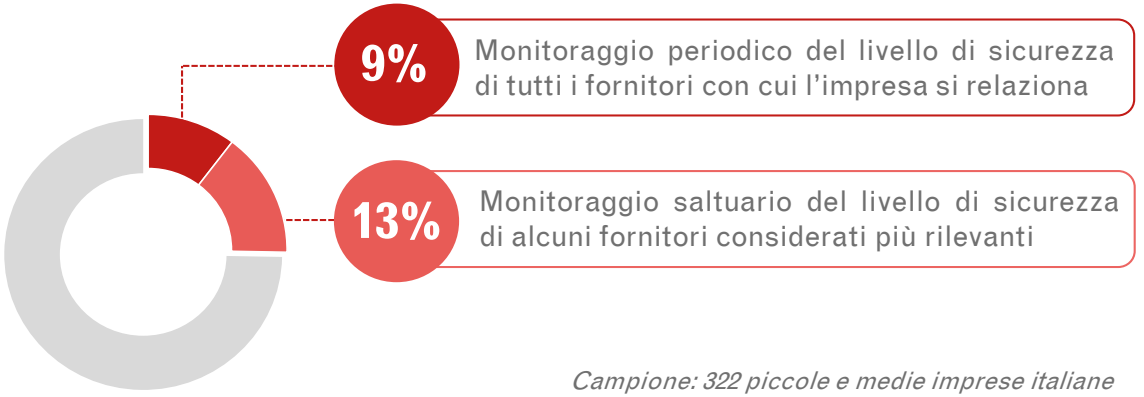
La valutazione del livello di sicurezza dei fornitori è un processo fondamentale per garantire reciproca fiducia nella sicurezza delle informazioni tra imprese e terze parti. La valutazione del livello di sicurezza dei fornitori consente di valutare l'adeguatezza delle misure di sicurezza implementate per proteggere dati e risorse aziendali. Nonostante la difesa del proprio dominio aziendale rimanga la priorità, è altresì importante considerare che le minacce possono sfruttare l'altrui vulnerabilità per diffondersi nella filiera. Tale area di analisi viene quindi valutata all'interno di organizzazioni altamente esposte al rischio, che collaborano con imprese di grosse dimensioni e multinazionali.

Prendendo in riferimento le 322 imprese interessate, emerge che **solo il 9% conduce attività di monitoraggio periodico su tutti i fornitori, mentre il 13% esegue valutazioni solo sui fornitori rilevanti**.

È evidente che la valutazione del livello di sicurezza dei fornitori non sempre sia agevole, soprattutto per le risorse destinabili alla security. È quindi consigliabile richiedere alle terze parti di possedere o conseguire certificazioni di sicurezza, come la ISO 27001 e la ISO 28000.

IDENTIFICAZIONE

VALUTAZIONE DEL LIVELLO DI SICUREZZA DEI FORNITORI: valutazione della sicurezza dei fornitori, ovvero verifica della conformità alle politiche di sicurezza dell'impresa



Campione: 322 piccole e medie imprese italiane

SOLO IL 9% DELLE PMI CON MEDIA ESPOSIZIONE AL RISCHIO **MONITORA PERIODICAMENTE IL LIVELLO DI SICUREZZA DI TUTTI I FORNITORI** CON CUI SI RELAZIONA. NEL **78%** DEI CASI, QUESTA ATTIVITÀ NON È ANCORA PREVISTA

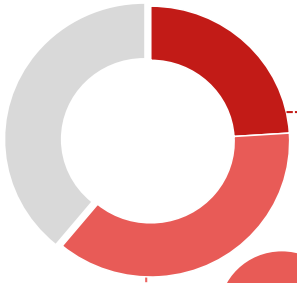
Cyber Risk Management

Il Cyber Risk Management è il processo di identificazione, valutazione e mitigazione dei rischi legati alla sicurezza informatica e alla protezione dei dati a 360°. Nonostante al suo interno si considerino diverse aree della dimensione **IDENTIFICAZIONE**, questa variabile è analizzata verticalmente al fine di capire se sia già stato sviluppato un processo formalizzato di gestione del rischio ed, eventualmente, se sia integrato all'interno di un processo di risk management aziendale. Integrare l'aspetto cyber nel processo di risk management aziendale più ampio consente di affrontare in modo olistico i rischi di sicurezza informatica all'interno dell'organizzazione. Questo approccio integrato aiuta a garantire che i rischi cibernetici vengano considerati alla stregua di altre tipologie di rischi aziendali e che quindi vengano adottate le misure adeguate per mitigarli.

Tale area è indagata internamente alle organizzazioni altamente esposte al rischio cyber. Tra le 204 prese in considerazione, **il 24% afferma di gestire il rischio cyber all'interno di un processo integrato di risk management aziendale**, mentre il 37% lo gestisce come un rischio a sé stante, all'interno della funzione IT o di un'altra funzione di controllo, garantendone quindi una visione solo parziale. Completa il campione un 39% che, nonostante conduca diverse delle attività presentate in precedenza, non ha ancora introdotto un processo formalizzato.

IDENTIFICAZIONE

CYBER RISK MANAGEMENT:
strutturazione di un processo di identificazione, valutazione, mitigazione e monitoraggio dei rischi legati alla sicurezza informatica all'interno di un'organizzazione



24% Gestione del rischio cyber integrato nel processo di Risk Management aziendale

37% Gestione rischio a sé stante all'interno della funzione IT o di un'altra singola funzione

Campione: 204 piccole e medie imprese italiane

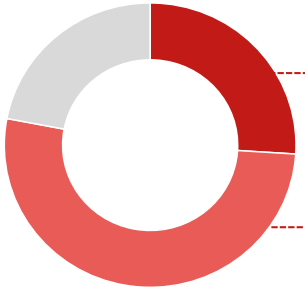
NONOSTANTE LA TRASVERSALITÀ DELLA SICUREZZA INFORMATICA, NEL **37%** DELLE PMI ALTAMENTE ESPOSTE AL **RISCHIO CYBER**, QUESTO VIENE ANCORA **GESTITO COME RISCHIO A SÈ STANTE**. NEL 39% IL PROCESSO DI CYBER RISK MANAGEMENT NON È INVECE DEFINITO

Adeguamento alla compliance normativa

L'adeguamento alla compliance normativa è un elemento fondamentale nella gestione del rischio cyber. Fa riferimento alla conformità a direttive, leggi e regolamenti in materia di sicurezza informatica e protezione dei dati. Essere conformi alle normative è essenziale per evitare sanzioni legali, danni reputazionali e perdite finanziarie. Nonostante le normative che impattano le PMI siano relativamente poche rispetto a quelle emanate per le grandi organizzazioni, un processo di adeguamento integrato genera sinergie, aumenta l'efficienza e riduce i rischi sanzionatori. L'adeguamento alla compliance normativa in maniera integrata implica un approccio olistico e coordinato all'adempimento dei requisiti normativi e delle leggi applicabili. Questo approccio integra gli sforzi di conformità normativa in tutti i processi aziendali con le politiche di sicurezza informatica, garantendo un'implementazione coerente e sistematica delle misure di sicurezza

Prendendo in considerazione le PMI maggiormente esposte ai rischi cyber e ai rischi sanzionatori, **il 25% dichiara di gestire il processo di adeguamento in maniera integrata**, a fronte di un 52% che invece gestisce separatamente i requisiti imposti dalle diverse normative. Il restante 23%, infine, non ha definito un processo consolidato di adeguamento alla compliance.

IDENTIFICAZIONE **ADEGUAMENTO ALLA COMPLIANCE NORMATIVA:** strutturazione di un processo integrato di adeguamento ai requisiti normativi



25% I progetti di adeguamento alle diverse normative vengono gestiti in maniera integrata

52% I progetti di adeguamento alle diverse normative vengono gestiti separatamente

Campione: 204 piccole e medie imprese italiane

NEL **25%** DELLE PMI AD ALTA ESPOSIZIONE AL RISCHIO I PROGETTI DI **ADEGUAMENTO NORMATIVO** IN MATERIA DI SICUREZZA INFORMATICA VENGONO **GESTITI IN MANIERA INTEGRATA,** GENERANDO SINERGIE, AUMENTANDO L'EFFICIENZA E RIDUCENDO I RISCHI SANZIONATORI

Gestione del fattore umano

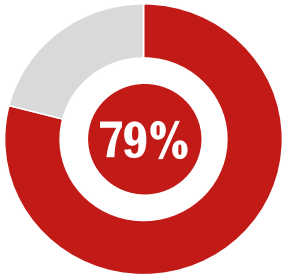
Come anticipato in precedenza, la vulnerabilità legata al comportamento umano rimane una delle principali cause di violazioni della sicurezza informatica. La gestione del fattore umano è un aspetto critico e, oltre alla tecnologia e alle attività di formazione, vi sono ulteriori soluzioni e buone pratiche che possono limitare l'esposizione al rischio. Si parla, ad esempio, di gestione delle password, gestione del personale in remoto e autentificazione multi-fattore.

Le **policy comportamentali, adottate dal 68% delle PMI**, comprendono linee guida mirate a indirizzare il comportamento degli utenti circa il corretto utilizzo di risorse e dispositivi aziendali così come l'adeguata gestione delle password. La **gestione degli accessi, implementata nel 79% delle imprese**, è invece un processo necessario per gestire al meglio i privilegi e le autorizzazioni per accedere a risorse e dati sensibili.
Affinché le policy comportamentali siano utili, è doveroso che vi sia un'attività di monitoraggio sulla loro effettiva comprensione ed attuazione da parte di tutti coloro che si relazionano con l'impresa, dalla proprietà ai dipendenti dei vari dipartimenti fino agli utenti esterni che si interfacciano saltuariamente con il sistema. La tecnologia risulta di grande supporto, in quanto spesso permette l'implementazione di alcune policy indipendentemente dal grado di consapevolezza dell'utente, come per esempio il cambio password obbligatorio o il rispetto di specifici requisiti di sicurezza per la costruzione delle chiavi di accesso.

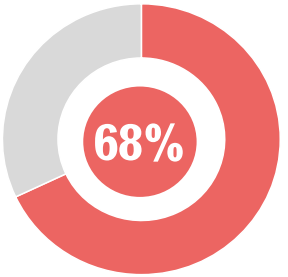
ATTUAZIONE

GESTIONE DEL FATTORE UMANO: introduzione di policy mirate a indirizzare il comportamento degli utenti e a limitarne le vulnerabilità

GESTIONE DEGLI ACCESSI



POLICY COMPORTAMENTALI



Campione: 658 piccole e medie imprese italiane

NEL **79%** DELLE PMI SONO STATI DEFINITI **DIRITTI E MODALITÀ DI ACCESSO** AI DATI AZIENDALI.
NEL **68%** ESISTONO **POLICY COMPORTAMENTALI PER I DIPENDENTI,** VOLTE A LIMITARE I COMPORTAMENTI CHE ESPONGONO L'ORGANIZZAZIONE AI RISCHI CYBER

Formazione

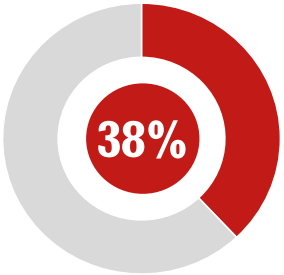
La maggior parte delle violazioni di sicurezza informatica avviene a causa di errori umani, quali negligenza o disattenzione. La formazione sulla sicurezza informatica in azienda è quindi fondamentale non solo per garantire che i dipendenti e gli utenti siano in grado di riconoscere le minacce informatiche, ma anche per assicurare che le best practices esistenti di protezione dei dati sensibili e degli asset aziendali siano effettivamente messe in pratica. Le attività di formazione, da programmare per tutti i dipendenti, solitamente comprendono corsi a cadenza regolare e simulazioni realistiche degli attacchi informatici più comuni, come il phishing.

Le iniziative di **formazione, poste in essere nel 38% delle PMI**, sono generalmente utili per migliorare la consapevolezza degli utenti. Sono molti i corsi disponibili, a pagamento o gratuiti, on-line o off-line, che garantiscono una buona preparazione. Un'alternativa è rappresentata da workshop interattivi e simulazioni, che vengono più efficacemente partecipati e recepiti. L'attività di simulazione è destinata in particolare ad organizzazioni con una esposizione al rischio medio-alta e la cui disponibilità economica ne garantisce la piena riuscita. Tra le 204 imprese di riferimento, **solo il 30% organizza simulazioni di phishing** per testare la preparazione dei dipendenti e allenarli a riconoscere le potenziali minacce.

ATTUAZIONE

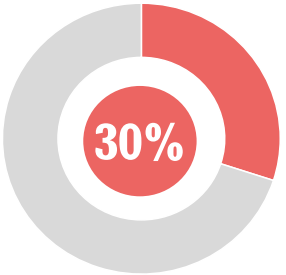
FORMAZIONE: pianificazione di attività di sensibilizzazione e formazione, frontali o interattive, verso gli utenti aziendali

FORMAZIONE



Campione: 658 piccole e medie imprese italiane

SIMULAZIONI DI PHISHING



Campione: 204 piccole e medie imprese italiane

IL **38%** DELLE PMI DEL CAMPIONE TOTALE PREVEDE **INIZIATIVE DI FORMAZIONE** PER I DIPENDENTI IN MATERIA DI RISCHIO CYBER. CONSIDERANDO LE **PMI AD ALTA ESPOSIZIONE AL RISCHIO**, IL **30%** CONDUCE **SIMULAZIONI DI PHISHING**

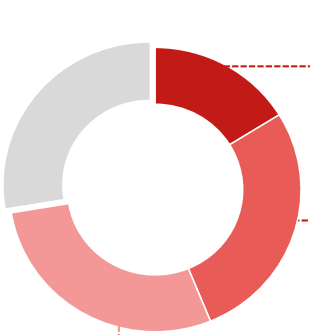
Polizze assicurative

Le polizze assicurative offrono un ulteriore livello di protezione, in particolare sul piano finanziario, alle organizzazioni contro gli incidenti informatici e le violazioni dei dati. Queste polizze sono progettate per coprire i costi associati alla gestione degli incidenti, alla riparazione dei danni, alla responsabilità legale e ad altre conseguenze finanziarie derivanti da violazioni dei dati o attacchi informatici. È importante sottolineare che le assicurazioni non sostituiscono la necessità di implementare azioni di mitigazione del rischio, bensì aggiungono la possibilità di trasferire a una terza parte la quota di rischio residuo, che permane a valle dell'introduzione di opportune misure di sicurezza informatica.

Il 17% delle PMI italiane ha già adottato polizze assicurative, mentre il 29% ne sta valutando l'introduzione. Il trasferimento del rischio cyber residuo rimane in ogni caso una possibilità ancora poco conosciuta dalle PMI: il 30%, infatti, non era a conoscenza delle opportunità di copertura del rischio cyber.

ATTUAZIONE

POLIZZE ASSICURATIVE: stipula di polizze assicurative per coprire e trasferire a una terza parte il rischio cyber residuo



17% Già attive coperture assicurative per trasferire il rischio cyber

29% In valutazione l'introduzione di coperture assicurative per trasferire il rischio cyber

29% Non a conoscenza della possibilità di stipulare polizze per trasferire il rischio cyber

Campione: 658 piccole e medie imprese italiane

IL TRASFERIMENTO DEL RISCHIO CYBER RESIDUO È UNA POSSIBILITÀ ANCORA POCO ESPLORATA E CONOSCIUTA DALLE PMI: SOLO IL **17% HA GIÀ INTRODOTTO POLIZZE ASSICURATIVE**, MENTRE IL **25% NON NE CONOSCEVA LA POSSIBILITÀ**

Tecnologie di protezione dei dati

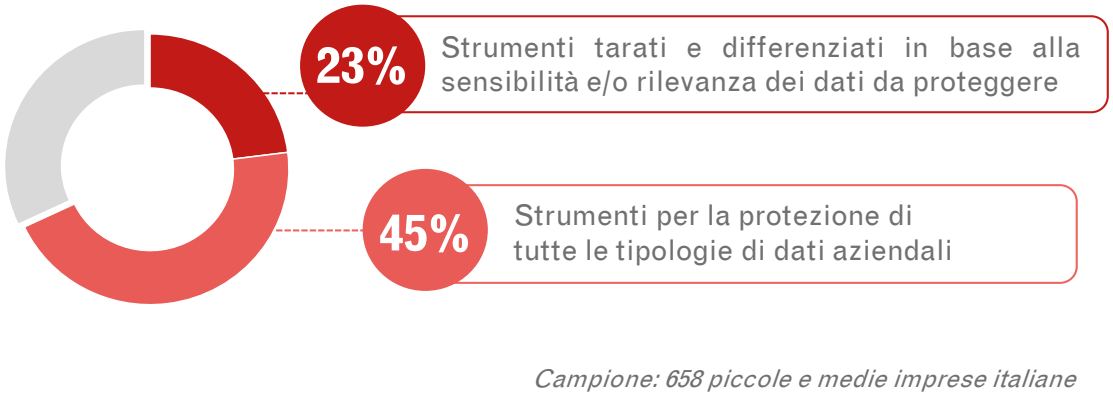
Come è stato illustrato nel capitolo 3 del rapporto, il principale obiettivo dell'Information Security è quello di garantire la Confidenzialità, l'Integrità e la Disponibilità del patrimonio informativo in caso di perdita o violazione dei dati. Le tecnologie di protezione dei dati sono quindi considerate la base per il raggiungimento di una buona postura di sicurezza.

Una delle più diffuse tecniche di protezione dei dati è la crittografia, ovvero la pratica che rende i dati illeggibili per gli utenti non autorizzati. Parallelamente è indispensabile introdurre soluzioni di backup e ripristino dei dati. La creazione regolare di backup delle informazioni critiche e la capacità di ripristinarle in caso di perdita, danneggiamento o attacco informatico sono componenti essenziali all'interno di una buona strategia di data protection. I backup dovrebbero essere crittografati e archiviati in luoghi sicuri, al fine di garantire un ripristino efficace e veloce dei dati in caso di necessità.

Il 68% delle piccole e medie imprese italiane dichiara la presenza in azienda di strumenti per la protezione dei dati. Di queste, il 23% afferma inoltre di tenere in considerazione la rilevanza dei dati da proteggere e di aver introdotto strumenti differenziati in base alla sensibilità.

ATTUAZIONE

TECNOLOGIE DI PROTEZIONE DEI DATI: introduzione di soluzioni di cifratura e autenticazione, nonché di gestione dei backup e dei ripristini, per garantire la riservatezza e l'integrità dei dati



Campione: 658 piccole e medie imprese italiane

LA PROTEZIONE DEI DATI RISULTA ESSERE UNA DELLE PRIORITÀ DI SICUREZZA INFORMATICA PER LE IMPRESE. NEL **68%** DELLE PMI ITALIANE SONO PRESENTI **STRUMENTI PER LA PROTEZIONE DEI DATI**; DI QUESTE UN 23% LI DIFFERENZIA IN BASE ALLA SENSIBILITÀ DEI DATI STESSI

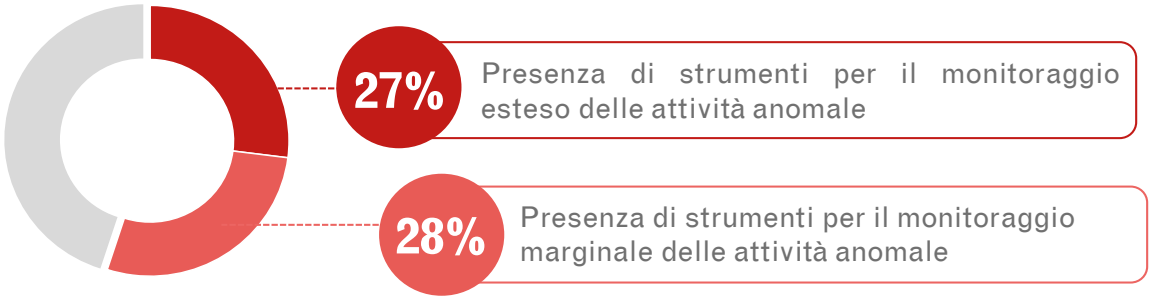
Tecnologie per il monitoraggio di attività anomale

Il monitoraggio delle attività anomale è il processo di sorveglianza e registrazione delle attività all'interno di un sistema aziendale (e dei dispositivi che lo compongono) al fine di identificare comportamenti o eventi insoliti o non conformi. L'obiettivo principale è rilevare e rispondere tempestivamente a potenziali minacce informatiche, intrusioni o violazioni dei dati. Questo risultato viene conseguito con soluzioni di natura prettamente tecnologica quali software anti-malware, sistemi di informazioni e gestione degli eventi di sicurezza (SIEM) e sistemi di analisi comportamentale.
La capacità di intercettare anomalie dipende tuttavia dalla tecnologia alla base della soluzione. Negli ultimi anni si sta assistendo ad un crescente utilizzo dell'intelligenza artificiale e del machine learning proprio perché garantiscono rapidità e maggiore efficacia.

Rispetto a tale necessità, **il 55% delle piccole e medie imprese dichiara di aver introdotto strumenti per il monitoraggio di attività anomale**. Tra queste, il 28% conduce tale attività marginalmente, ovvero non in maniera completa e approfondita.

ATTUAZIONE

TECNOLOGIE PER IL MONITORAGGIO DI ATTIVITÀ ANOMALE: introduzione di soluzioni di monitoraggio e analisi per individuare attività sospette o anomale all'interno del sistema informativo e informatico



Campione: 658 piccole e medie imprese italiane

DEL **55%** DI PMI CHE DICHIARA DI AVER INTRODOTTO **STRUMENTI PER IL MONITORAGGIO DI ATTIVITÀ ANOMALE**, IL 28% DI QUESTE LO FA ANCORA IN MANIERA MARGINALE

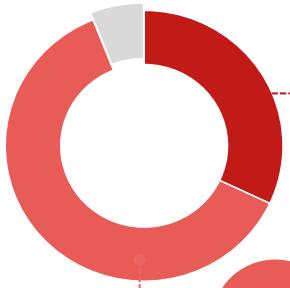
Tecnologie per la protezione delle reti

Le tecnologie per il monitoraggio del traffico di rete forniscono una visibilità approfondita sulle attività di rete, consentendo alle organizzazioni di prevenire, identificare e rispondere tempestivamente alle minacce informatiche e migliorare le prestazioni del sistema. La protezione della rete dovrebbe essere una priorità costante per le organizzazioni, diventando imprescindibile nel caso in cui il perimetro aziendale si estenda per il ricorso al cloud, al remote working e all'IoT. Esistono diverse tecnologie disponibili per la protezione delle reti e dei dati all'interno di un'organizzazione. Tra quelle di base si citano i firewall, ovvero elementi hardware o software che monitorano il flusso del traffico in entrata e in uscita, utilizzando regole di sicurezza per consentire o bloccare gli eventi, e le virtual private network (VPN), che danno la possibilità di stabilire connessioni cifrate e sicure tra dispositivi o reti remote e la rete aziendale.

Dalle evidenze del Rapporto, ottenute da un campione di imprese mediamente esposto, risulta che **le tecnologie di protezione delle reti almeno di base sono presenti nel 94% delle PMI**. **Solo il 32% di esse adotta strumenti avanzati**, come sistemi di rilevamento o prevenzione delle intrusioni (IDS – IPS) e sistemi di protezione dalle minacce avanzate (ATP). Completa la vista un 6% di piccole e medie imprese che attualmente non ricorre a tali soluzioni.

ATTUAZIONE

TECNOLOGIE PER LA PROTEZIONE DELLE RETI: strumenti per garantire la sicurezza dei sistemi di rete dell'organizzazione, attraverso attività di monitoraggio del traffico e rilevazione di comportamenti anomali



32% Presenza di strumenti avanzati per la protezione delle reti (es. IDS-IPS, ATP)

62% Presenza di strumenti di base per la protezione delle reti (es. VPN e firewall)

Campione: 322 piccole e medie imprese italiane

LA **PROTEZIONE DELLE RETI AZIENDALI** È CHIAVE NELLA PROTEZIONE DELLA SICUREZZA INFORMATICA DI UN'IMPRESA. TRA LE PMI CON MEDIA ESPOSIZIONE AL RISCHIO, IL **32% ADOTTA STRUMENTI AVANZATI** E IL **62% DISPOSITIVI DI SICUREZZA DI BASE**

Linee guida dirette alle terze parti

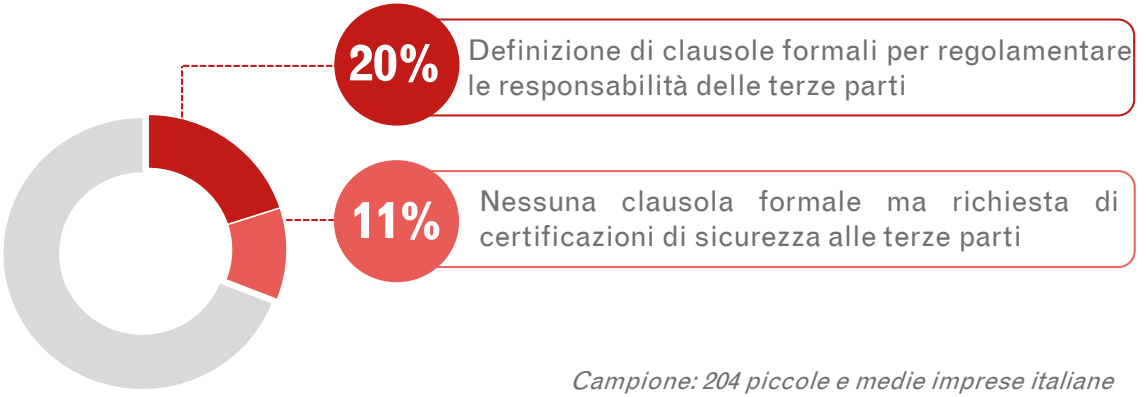
Più volte nel corso di questo report è stata esplicitata l'importanza di adottare soluzioni di sicurezza informatica che tengano conto anche dell'appartenenza a una filiera strategica o delle relazioni con altre organizzazioni. Al fianco di attività di valutazione, certamente indispensabili per orientare le scelte di fornitura, sono sempre più spesso adottate linee guida che disciplinino la responsabilità tra le parti. La definizione di policy comportamentali è una sfida sia per le grandi imprese, sia per le piccole imprese particolarmente esposte.

Dall'analisi di 204 imprese si realizza come questa pratica risulti spesso complessa: solo **il 21% di esse ha definito clausole formali al fine di regolamentare responsabilità e attività del fornitore o partner, mentre l'11% si limita a richiedere certificazioni**. Nel 34% dei casi si sta valutando l'introduzione di clausole formali mentre un ulteriore 34% di imprese non ritiene rilevante questa attività.

Va specificato che la gestione della sicurezza nei rapporti con le terze parti dovrebbe essere un tema di primaria attenzione anche per le PMI, che spesso si trovano ad interagire con realtà di grosse dimensioni. Questo aspetto, negli anni a venire, potrebbe risultare determinante nell'instaurazione di rapporti commerciali e nella partecipazione a filiere di rilevanza strategica.

ATTUAZIONE

LINEE GUIDA DIRETTE ALLE TERZE PARTI: definizione di policy comportamentali e linee guida per fornitori e partner della filiera



Campione: 204 piccole e medie imprese italiane

IL RISCHIO LEGATO ALLE TERZE PARTI È SPESSO SOTTOVALUTATO DALLE PMI AD ALTA ESPOSIZIONE: SOLO IL **21%** DI QUESTE PMI HA DEFINITO **CLAUSOLE FORMALI E LINEE GUIDA PER FORNITORI E PARTNER**

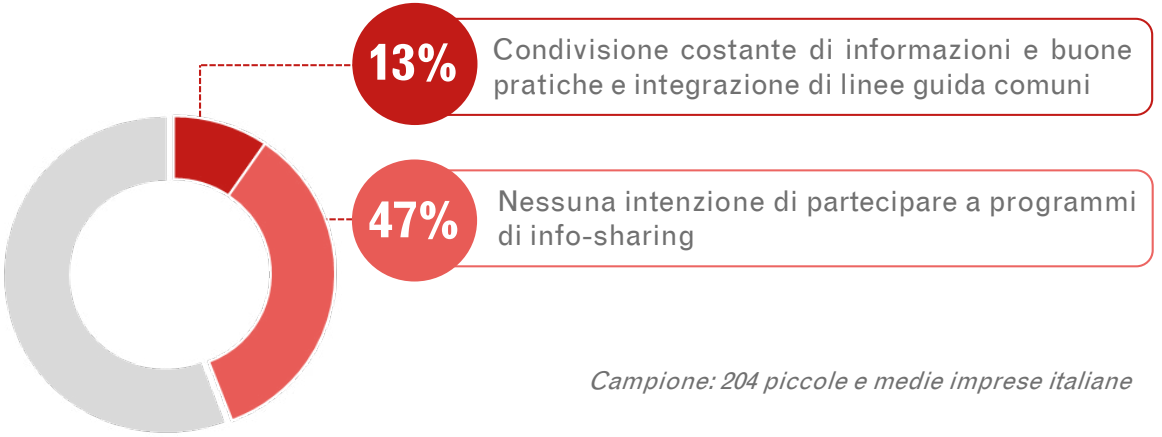
Programmi di info-sharing

La partecipazione ad una filiera è un fattore essenziale da considerare nella valutazione dell'esposizione al rischio informatico di un'azienda, indipendentemente dalle sue dimensioni. Oltre ad introdurre linee guida e policy per fornitori e partner, è importante e utile che venga posto in essere un programma continuativo di condivisione delle informazioni relative alla sicurezza informatica, il che comprende, ad esempio, la scoperta di vulnerabilità, la notifica di violazioni ai sistemi informativi, eventuali anomalie rilevate. Affinché si possa assicurare un buon livello di sicurezza, è opportuno che tutte le parti abbiano aperti canali di comunicazione, anche con altre aziende del mercato (competitor o imprese operanti in altri settori) e con le istituzioni.

Dalle evidenze del Rapporto emerge che **solo nel 13% delle PMI le informazioni e le buone pratiche sono condivise costantemente** e vi è un'integrazione di linee guida comuni. Per un 13%, invece, l'attività di info-sharing esiste, ma viene svolta in maniera saltuaria. Completano il campione un 29% di PMI che attualmente non partecipa a tali programmi ma vorrebbe valutarlo in futuro e un ulteriore 47% che non considera rilevante l'attività di condivisione delle informazioni.

ATTUAZIONE

PROGRAMMI DI INFO-SHARING: partecipazione ad iniziative che promuovono lo scambio di informazioni sulle minacce informatiche tra organizzazioni



Campione: 204 piccole e medie imprese italiane

IL **47%** DELLE PMI AD ALTA ESPOSIZIONE AL RISCHIO **NON CONSIDERA LA PARTECIPAZIONE A PROGRAMMI E ATTIVITÀ DI CONDIVISIONE DELLE INFORMAZIONI**. SOLO IL 13% SVOLGE L'ATTIVITÀ DI INFO-SHARING IN MANIERA COSTANTE

Uno dei principali fattori che rende le PMI vulnerabili agli attacchi dei cybercriminali è la tendenza a sottovalutare l'**impatto potenziale dei rischi cyber**. Tale percezione è legata anche alla diffusione limitata, tra le imprese italiane, di una più ampia cultura del rischio, indicata dalla letteratura scientifica e da altre ricerche (fonti secondarie).

Le evidenze del **RAPPORTO CYBER INDEX PMI** suggeriscono come una consapevolezza incompleta della propria vulnerabilità disincentivi l'adozione di un **approccio pienamente strategico** alla sicurezza informatica. A questo proposito, i gap più significativi riguardano la definizione di budget dedicati e la formalizzazione di responsabilità di presidio della materia, uniti alla carenza di investimenti in iniziative di sensibilizzazione e formazione del personale.

A livello operativo si riscontra una scarsa diffusione di processi strutturati di risk management, dall'identificazione delle priorità di azione fino alla copertura assicurativa del rischio residuo, passando per l'implementazione di opportune azioni di mitigazione. **Senza una chiara comprensione dei rischi specifici che possono influire sulle loro attività, in sintesi, le PMI possono trovarsi nella situazione di non sapere su quali aree focalizzare le proprie risorse (sempre limitate) e attenzioni**.

Nonostante una parte delle PMI italiane, specialmente di medie dimensioni, dimostri un buon livello di preparazione, **una quota significativa di imprese sembra collocarsi nella fase iniziale di un percorso di maturazione** nella gestione della sicurezza informatica. Le PMI necessitano pertanto di uno stimolo a integrare la gestione dei rischi cyber nella propria strategia aziendale, in modo da cogliere le opportunità e minimizzare gli impatti negativi derivanti da eventi imprevisti. In tale contesto, la **collaborazione tra istituzioni pubbliche, organizzazioni private e università** può svolgere un ruolo propulsivo nella diffusione della cultura del rischio e dell'approccio strategico alla sicurezza informatica.

Le **partnership pubblico-private** possono inoltre contribuire a sviluppare e consolidare soluzioni efficaci e innovative ai rischi cyber rivolte alle PMI: piattaforme per il monitoraggio dei rischi e degli episodi di attacco cyber, sistemi di alert, toolkit per la valutazione sistematica delle vulnerabilità o ancora servizi di business continuity e ripresa dagli incidenti. Un sistema di offerta nel quale i prodotti assicurativi intervengono a copertura dei danni finanziari e operativi derivanti dai rischi residui, favorendo la resilienza del sistema imprenditoriale.

Il **Cyber Index PMI rappresenta uno strumento prezioso per valutare l'evoluzione dell'approccio delle PMI italiane alla gestione dei rischi cyber ed accelerare la trasformazione culturale all'interno delle PMI, nonché indirizzare le misure messe in campo dai diversi attori coinvolti.** I partecipanti alla rilevazione che hanno manifestato l'interesse riceveranno infatti un report personalizzato contenente indicazioni sulla situazione corrente e linee guida per intraprendere un percorso di maturazione.

È importante sottolineare che la durata pluriennale dell'iniziativa consentirà di ottenere una visione più completa e accurata della postura di sicurezza delle PMI, considerando che la gestione dei rischi cyber è un processo in continua evoluzione e le minacce possono mutare nel tempo. Nonostante l'iniziativa abbia coinvolto ben 708 imprese sull'intero territorio italiano, l'auspicio è che il numero di organizzazioni coinvolte nell'indagine cresca negli anni e che si possano rilevare significative evoluzioni nell'approccio delle PMI italiane alla gestione dei rischi cyber

CYBER INDEX PMI
LA CULTURA DIGITALE PROTEGGE LA TUA IMPRESA

RAPPORTO CYBER INDEX PMI 2023

APPENDICI

GENERALI

Generali è l'assicuratore più conosciuto in Italia con oltre 28 miliardi di premi totali e una rete capillare di 40 mila distributori, oltre ai canali online e di bancassurance e 15 mila dipendenti. A Generali fanno capo Alleanza Assicurazioni, Das, Genertel e Genertellife, Generali Welion, Generali Jeniot, Leone Alato e le attività della Business Unit Cattolica.

La sostenibilità in Generali

Generali vuole contribuire alla creazione di una **società sana, resiliente e sostenibile**, dove le persone possano progredire e prosperare. Viene così interpretato il ruolo d'impresa responsabile che crea **valore durevole per i propri stakeholder** (dai collaboratori agli azionisti, dagli investitori ai clienti, dai fornitori alle istituzioni e comunità locali).

L'impegno e la responsabilità di Generali si concretizza in numerosi progetti in ambiti ad alto impatto sociale ed ambientale quali, ad esempio, la Cyber-sicurezza, il Terzo Settore, l'Educazione e la Formazione, l'Arte e la Cultura, il Welfare e molti altri ancora.

CONFINDUSTRIA

Confindustria è la principale associazione di rappresentanza delle imprese manifatturiere e di servizi in Italia.
La mission dell'associazione è favorire l'affermazione dell'impresa quale motore della crescita economica, sociale e civile del Paese.
In linea con questi principi, Confindustria definisce strategie e percorsi comuni, condividendo - nel rispetto degli ambiti di autonomia e influenza - obiettivi e iniziative con il mondo dell'economia e della finanza, delle Istituzioni nazionali, europee e internazionali, della PA, delle Parti Sociali, della cultura e della ricerca, della scienza e della tecnologia, della politica, dell'informazione e della società civile.
Confindustria sostiene e promuove la libertà di impresa e la concorrenza nel quadro di un'economia di mercato, svolgendo un ruolo strategico nel definire le priorità politiche per rafforzare il sistema industriale e stimolare la crescita economica e sociale dell'Italia, rendendola sempre più competitiva sui mercati globali.
Il valore aggiunto di Confindustria è la sua rete, che si dirama dalla sede centrale di Roma alla Delegazione di Bruxelles, punto di riferimento per l'intero Sistema Italia presso l'Unione Europea, e alle 222 Organizzazioni associate presenti sul territorio e nei settori.
Il sistema di valori di Confindustria si fonda sulla rappresentanza, unitaria, organica e strategica degli interessi delle imprese, sull'identità associativa, basata sul libero mercato, sulla centralità della imprenditorialità e dell'impresa, sulla responsabilità e sulla sostenibilità.
Nuove sfide tracciano costantemente le strade dello sviluppo e della crescita economica, sociale e culturale: la transizione digitale, quella energetica e quella ambientale sono tra le prioritarie.
Lo scopo di Confindustria è di affrontarle alla continua ricerca di soluzioni per lo sviluppo del sistema produttivo e per il benessere del Paese.

OSSERVATORI DIGITAL INNOVATION – POLITECNICO DI MILANO

Gli Osservatori Digital Innovation della School of Management del Politecnico di Milano nascono nel 1999 con l'obiettivo di **fare cultura in tutti i principali ambiti di Innovazione Digitale**. Oggi sono un punto di riferimento qualificato sull'Innovazione Digitale in Italia che integra attività di **Ricerca, Comunicazione e Aggiornamento continuo**. *La Vision che guida gli Osservatori è che l'Innovazione Digitale sia un fattore essenziale per lo sviluppo del Paese*. La mission è produrre e diffondere conoscenza sulle opportunità e gli impatti che le tecnologie digitali hanno su imprese, pubbliche amministrazioni e cittadini, tramite modelli interpretativi basati su solide evidenze empiriche e spazi di confronto indipendenti, pre-competitivi e duraturi nel tempo, che aggregano la domanda e l'offerta di Innovazione Digitale in Italia.

Le attività di ricerca sono svolte da un team di oltre 100 tra Professori, Ricercatori e Analisti impegnati su circa 50 differenti Osservatori che affrontano tutti i temi chiave dell'Innovazione Digitale nelle Imprese (anche PMI) e nella Pubblica Amministrazione. Sono classificabili in 3 macro categorie: Digital Transformation, Digital Solutions e Verticals.

L'**Osservatorio Cybersecurity & Data Protection** rientra tra le Digital Solution ed è alla sua nona edizione. Intende rispondere al bisogno delle aziende di conoscere, comprendere e affrontare le **nuove minacce alla sicurezza informatica** supportando le aziende stesse nella scelta delle tutele più opportune, rendendole consapevoli dell'importanza del monitoraggio e del controllo delle attività e mostrando loro le tecniche e le tecnologie a **supporto della cybersecurity** adottabili.

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

L'Agenzia per la cybersicurezza nazionale (ACN) è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della sicurezza e resilienza cibernetiche. Istituita nel 2021 (Decreto Legge n.82 del 14 giugno 2021), ha ridefinito l'architettura nazionale di cybersicurezza e promuove un quadro normativo coerente nel settore.

L'Agenzia ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico e si occupa di prevenire e mitigare il maggior numero di attacchi cibernetici e di favorire il raggiungimento dell'autonomia strategica nazionale ed europea nel settore del digitale, in sinergia con il sistema produttivo e con il mondo della ricerca.
Supporta i soggetti pubblici e privati nazionali, che esercitano funzioni ed erogano servizi essenziali, nella prevenzione e mitigazione degli incidenti, nonché ai fini del ripristino dei sistemi.
L'Agenzia, inoltre, esercita attività di certificazione e vigilanza, in particolare valuta prodotti e servizi informatici e conduce attività ispettive e di verifica per gli adempimenti normativi nel campo della cybersicurezza. Favorisce e promuove attività di conoscenza e consapevolezza in tema cyber, attraverso percorsi formativi per lo sviluppo della forza lavoro di settore e campagne di sensibilizzazione e diffusione della cultura della cybersicurezza.

Tra i suoi principali compiti, l'attuazione della Strategia Nazionale di Cybersicurezza, adottata dal Presidente del Consiglio che contiene gli obiettivi da perseguire entro il 2026 e l'attuazione dell'investimento PNRR 1.5 Cybersecurity, per rafforzare l'ecosistema digitale nazionale potenziando i servizi di gestione della minaccia cyber.

Alessandro Piva

Laureato in Ingegneria delle Telecomunicazioni e in Ingegneria Gestionale al Politecnico di Milano nel 2006, ha poi conseguito l'Executive Master in Business Administration (EMBA) presso il MIP Politecnico di Milano. Alla School of Management del Politecnico di Milano, dove lavora da oltre 15 anni, è Direttore di svariati Osservatori nel mondo della trasformazione digitale, quali Cybersecurity & Data Protection, Cloud Transformation, Artificial Intelligence, Quantum Computing & Communication e Responsabile della Ricerca dell'Osservatorio Big Data & Business Analytics. Accanto alle attività di ricerca si occupa di formazione executive e consulenza per imprese e pubbliche amministrazioni.

Giorgia Dragoni

Si è laureata nel 2014 in Ingegneria Gestionale al Politecnico di Milano, indirizzo Manufacturing & Management, e nello stesso anno ha iniziato a lavorare negli Osservatori Digital Innovation occupandosi di trasformazione digitale e cybersecurity. Ha conseguito l'Executive Master in Management presso il MIP nel 2022. Attualmente è ricercatrice senior sui temi Cybersecurity & Data Protection e Big Data Analytics e dal 2020 è Direttrice dell'Osservatorio Digital Identity.

Nicola Ciani

Laureato in Business & Administration presso l'Università di Bologna, sta frequentando il percorso Executive in Digital Transformation della School of Management del Politecnico di Milano. Dal 2021 è ricercatore degli Osservatori Cybersecurity & Data Protection e Big Data & Business Analytics.

Ivan Antozzi

Si è laureato in Computer Science and Engineering - Ingegneria Informatica presso il Politecnico di Milano nel 2018. Un anno più tardi ha iniziato a lavorare negli Osservatori Digital Innovation occupandosi di trasformazione digitale e Cloud. Attualmente è ricercatore sui temi Cloud, Data Center e Cybersecurity & Data Protection. Ha completato ad ottobre 2022 il Percorso Executive in Project Management presso la Polimi Graduate School of Management.

Jacopo Polverino

Laureato in European and International Studies presso l'Università degli Studi di Trento, dal 2021 è analista degli Osservatori Cybersecurity & Data Protection e Cloud Transformation.

INGRID SALVADORI

Laureata in International Relations presso l'Università di Bologna, dal 2023 è analista dell'Osservatorio Cybersecurity & Data Protection.

L'iniziativa Cyber Index PMI si è posta gli obiettivi di:

- **misurare il livello di cultura e di consapevolezza del rischio cyber nelle piccole e medie imprese italiane, nonché il livello di preparazione;**
- **renderle consapevoli dell'importanza del monitoraggio e del controllo delle attività;**
- **mostrare loro le tecniche e le tecnologie adottabili per la gestione del rischio cyber.**

Il Rapporto Cyber Index PMI si basa su un'**indagine rivolta a responsabili della sicurezza informatica**, responsabili IT, titolari, o altri responsabili di **piccole e medie imprese italiane** con un numero di lavoratori entro le 249 unità. Alle PMI è stato somministrato un questionario CAWI, progettato e veicolato in collaborazione con Generali e Confindustria.

Il **questionario** è stato sviluppato in **maniera modulare** su diversi **livelli di approfondimento** legati alla **dimensione** e all'**esposizione al rischio** – valutata in relazione all'adozione di strumenti digitali, all'appartenenza a filiere critiche, al livello di internazionalizzazione e a eventuali violazioni subite negli ultimi 4 anni – delle singole organizzazioni. La modularità del questionario ha l'obiettivo di garantire l'adeguatezza delle domande poste rispetto alle caratteristiche delle diverse aziende e alla necessità di dotarsi di processi, tecnologie e competenze.

All'aumentare dell'esposizione e della complessità **aumenta il numero di domande** su temi di particolare rilevanza in sicurezza informatica. Nella survey dedicata alle imprese con minore esposizione al rischio, il numero delle domande è pari a 13, aumentando a 20 nel caso l'esposizione sia di livello medio, fino ad un totale di 28 per le imprese con elevata esposizione al rischio cyber.

La somministrazione di un diverso numero di domande garantisce comunque una valutazione equa: la valutazione nella singola dimensione viene espresso in centesimi, ovvero il rapporto tra il punteggio ottenuto e quello ottenibile dalle domande cui è stata sottoposta la PMI.

Le domande sono rappresentative di **20 aree di analisi**, ovvero scelte strategiche e operative di particolare rilevanza all'interno di imprese di piccole e medie dimensioni. Tali aree sono afferenti a **3 dimensioni**:

- ***Approccio strategico***: formalizzazione della **responsabilità** della sicurezza informatica e definizione degli **investimenti** a lungo termine. Rientrano in questa dimensione le seguenti aree di analisi: commitment della proprietà, budgeting, presidio organizzativo, piani di sicurezza, certificazioni;

- ***Identificazione***: capacità di comprendere il rischio cyber in relazione al **dominio aziendale** e la **filiera**, nonché adeguarsi ai **requisiti normativi**. Rientrano in questa dimensione le seguenti aree di analisi: mappatura degli asset informatici, valutazione delle vulnerabilità, auditing della sicurezza informatica, misurazione del rischio cyber, valutazione del livello di sicurezza dei fornitori, cyber risk management, adeguamento alla compliance normativa;

- ***Attuazione***: capacità di selezionare il corretto **mix di competenze e modelli organizzativi** e di implementare **iniziative concrete** in termini di **persone, processi e tecnologie**. Rientrano in questa dimensione le seguenti aree di analisi: gestione del fattore umano, formazione, polizze assicurative, tecnologie per la protezione dei dati, tecnologie per il monitoraggio di attività anomale, tecnologie per la protezione delle reti, linee guida dirette alle terze parti, programmi di info-sharing.

1. Commitment della proprietà: volontà dei proprietari o dei vertici aziendali a impegnarsi a livello strategico per garantire una solida gestione della sicurezza informatica;
2. Budgeting: allocazione di risorse economiche destinabili all'acquisto di servizi e soluzioni di sicurezza informatica, all'assunzione di personale specializzato e alla formazione dei dipendenti;
3. Presidio organizzativo: definizione di ruoli e responsabilità, interni o esterni, inerenti la gestione dell'intero processo di gestione del rischio cyber;
4. Piano di sicurezza: sviluppo di un documento strategico che definisce le politiche, le procedure e le misure di sicurezza da implementare per proteggere i dati, le risorse e le infrastrutture aziendali dalle minacce informatiche;
5. Certificazioni: conseguimento di attestazioni circa la conformità dei sistemi informativi e dei processi aziendali ai requisiti di sicurezza e privacy previsti dalle certificazioni ISO 27001, ISO 28000 e ISO 22301;
6. Mappatura degli asset informatici: strutturazione di un processo di identificazione e catalogazione di tutti i componenti tecnologici e delle risorse digitali di un'organizzazione;
7. Valutazione delle vulnerabilità: conduzione di analisi mirate a identificare e valutare le vulnerabilità presenti nei sistemi informatici, nelle reti, nelle applicazioni e negli asset digitali di un'organizzazione;
8. Auditing della sicurezza informatica: conduzione di analisi sistematiche di valutazione e verifica delle misure di sicurezza informatica e della compliance normativa;
9. Misurazione del rischio cyber: conduzione di analisi mirate a valutare e quantificare periodicamente il rischio associato alle minacce informatiche e alle vulnerabilità all'interno di un'organizzazione;
10. Valutazione del livello di sicurezza dei fornitori: valutazione della sicurezza dei fornitori, ovvero verifica della conformità alle politiche di sicurezza dell'impresa;
11. Cyber risk management: strutturazione di un processo di identificazione, valutazione, mitigazione e monitoraggio dei rischi legati alla sicurezza informatica all'interno di un'organizzazione;
12. Adeguamento alla compliance normativa: strutturazione di un processo integrato di adeguamento ai requisiti normativi;
13. Gestione del fattore umano: introduzione di policy mirate a indirizzare il comportamento degli utenti e a limitarne le vulnerabilità;

14. Formazione: pianificazione di attività di sensibilizzazione e formazione, frontali o interattive, verso gli utenti aziendali;
15. Polizze assicurative: stipula di polizze assicurative per coprire e trasferire a una terza parte il rischio cyber residuo;
16. Tecnologie di protezione dei dati: introduzione di soluzioni di cifratura e autenticazione, nonché di gestione dei backup e dei ripristini, per garantire la riservatezza e l'integrità dei dati;
17. Tecnologie per il monitoraggio di attività anomale: introduzione di soluzioni di monitoraggio e analisi per individuare attività sospette o anomale all'interno del sistema informativo e informatico;
18. Tecnologie per la protezione delle reti: strumenti per garantire la sicurezza dei sistemi di rete dell'organizzazione, attraverso attività di monitoraggio del traffico e rilevazione di comportamenti anomali;
19. Linee guida dirette alle terze parti: definizione di policy comportamentali e linee guida per fornitori e partner della filiera;
20. Programmi di info-sharing: partecipazione ad iniziative che promuovono lo scambio di informazioni sulle minacce informatiche tra organizzazioni.

ASSET INFORMATICI: rientrano in questa categoria i dispositivi assegnati al personale (PC, smartphone e tablet), i dispositivi fisici e virtuali che costituiscono l'infrastruttura aziendale (server, sistemi di archiviazione, reti e relativi dispositivi), i software, i dati presenti all'interno del sistema informativo (database e repository di documenti), i sistemi di lavoro in mobilità, le soluzioni cloud e i dispositivi IoT

ESPOSIZIONE AL RISCHIO: misura in cui un individuo, un'azienda o un'entità è soggetto a eventi o circostanze che potrebbero comportare conseguenze negative o danni derivanti dal rischio cyber

INFRASTRUTTURE CRITICHE: organizzazioni, imprese o enti la cui interruzione o momentanea indisponibilità dei servizi provoca l'indebolimento in maniera significativa del funzionamento normale di un Paese

IoT: dispositivi fisici e sensori in grado di raccogliere, elaborare e scambiare dati e/o informazioni anche in tempo reale attraverso l'utilizzo di canali di comunicazione (es. reti internet)

MANAGED E/O PROFESSIONAL SERVICES: si intendono servizi offerti in maniera continuativa da provider esterni all'organizzazione per garantire il supporto e la manutenzione dei sistemi informativi aziendali

OT SECURITY: per OT (Operational Technology) security si intende la messa in sicurezza di componenti hardware e software dedicati al monitoraggio e al controllo di processi e asset fisici prevalentemente in ambito industriale o nei settori che gestiscono infrastrutture critiche (Oil&Gas, Energy, Utilities, Telco)

POSTURA: in inglese "security posture", indica lo stato di sicurezza delle reti, delle informazioni e dei sistemi di un'azienda, basato sulle risorse di sicurezza delle informazioni (ad esempio, persone, hardware, software, politiche) e sulle capacità in atto per gestire la difesa dell'azienda e reagire ai cambiamenti della situazione.

SUPERFICIE ATTACCABILE: insieme dei punti sul confine di un sistema, di un elemento del sistema o di un ambiente attraverso cui un aggressore può provare ad entrare per compromettere o estrarre dati da quel sistema. Esempi di superfici di attacco sono software, piattaforme, dispositivi fisici e utenti dei sistemi aziendali

SUPPLY CHAIN SECURITY: si fa riferimento a processi, tecnologie e competenze attraverso cui un'organizzazione gestisce e regola il rapporto con le terze parti (fornitori, partner, clienti), al fine di miti- gare i rischi e le minacce cyber derivanti dalla propria catena del valore

VIOLAZIONE INFORMATICA: violazione dei sistemi informativi, comunemente nota come "hacking", è un'attività illecita che prevede l'accesso non autorizzato a un sistema informatico al fine di ottenere informazioni sensibili o danneggiare il sistema stesso

Politecnico di Milano School of Management, Osservatorio Cybersecurity & Data Protection (2023), Ricerca 2022, IX ed., **Lo scenario della cybersecurity in Italia nel 2022** (osservatori.net)

Politecnico di Milano School of Management, Osservatorio Cybersecurity & Data Protection (2023), Ricerca 2022, IX ed., **Le competenze per la cybersecurity e la gestione del fattore umano** (osservatori.net)

Politecnico di Milano School of Management, Osservatorio Cybersecurity & Data Protection (2022), Ricerca 2021, VIII ed., **La gestione del rischio cyber in un contesto di filiera estesa** (osservatori.net)

Politecnico di Milano School of Management, Osservatorio Digital Transformation Academy (2022), Priorità dell'innovazione digitale per le imprese per il 2023: trend di investimento, XIV ed., **Priorità dell'Innovazione Digitale per le imprese per il 2023: trend di investimento** (osservatori.net)

Clusit (2023). Rapporto sulla sicurezza ICT in Italia.

Agenzia per la Cybersicurezza Nazionale (2022), **Manuale operativo implementazione misura #82. Piano di implementazione Strategia Nazionale di Cybersicurezza 2022-2026**

Alleanza Assicurazioni, Fondazione Mario Gasbarri, SDA Bocconi School of Management (2022), **Rapporto Edufin Index, I ed.**

RAPPORTO 2023

CYBER INDEX PMI

LA CULTURA DIGITALE PROTEGGE LA TUA IMPRESA

Promosso da

GENERALI

CONFINDUSTRIA

Partner scientifico

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT

osservatori.net digital innovation

Partner istituzionale

ACN