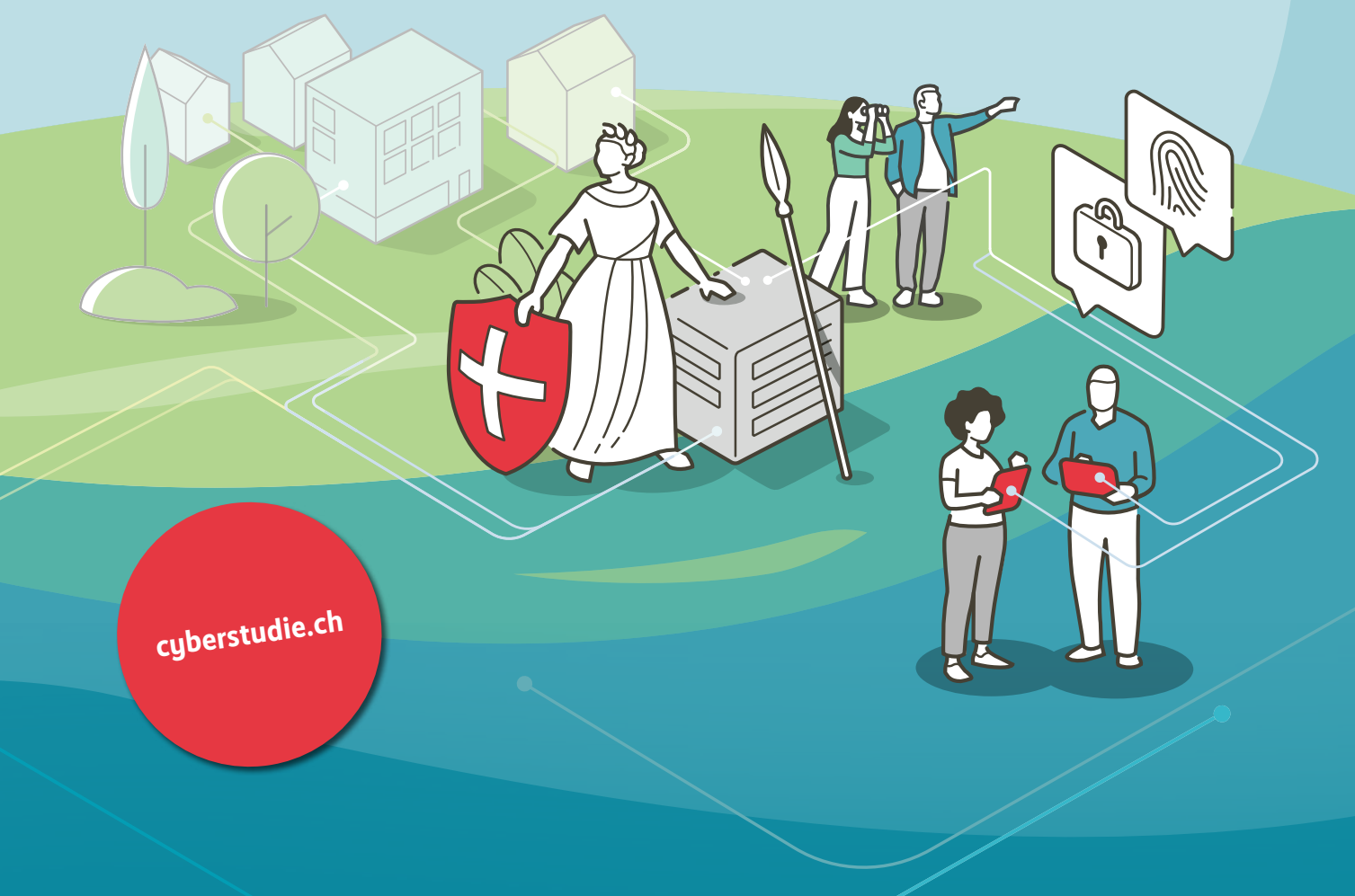


PMI Cyber sicurezza 2026

Uno studio della Mobiliare in collaborazione con UFCS, digitalswitzerland, HES-SO, HWZ e SATW

Marc K. Peter, Romain Geiser, Anu Anthamatten, Léonard Marbe, Anna V. Rozumowski, Tobias Schlegel e Karin Mändli Lerch



Sommario

Introduzione	3
01 PMI svizzere: a che punto sono nell'era digitale?	4
02 Sovranità digitale: un nuovo ambito tematico dell'attuale politica mondiale	6
03 Cyber criminalità: un problema da prendere sul serio, con nuovi pericoli legati all'IA	8
04 Cyber criminalità nelle PMI: più di 35 000 persone colpite, spesso con conseguenze gravi	10
05 Conoscenza delle cyber minacce e supporto	12
06 La cyber sicurezza acquisisce nuovamente un'importanza maggiore	14
07 Responsabilità per i cyber rischi: sempre più PMI definiscono competenze chiare	16
08 Implementazione di misure tecniche per la cyber sicurezza	18
09 Implementazione di misure organizzative per la cyber sicurezza	20
10 Il futuro: cresce l'importanza della cyber resilienza, ma molte PMI restano caute	22
Check list per le PMI svizzere	24
Strumenti pratici e metodologia di ricerca	26
Contatti di autrici e autori	27

Introduzione

Negli ultimi anni la trasformazione digitale ha permesso alle PMI svizzere di conseguire progressi significativi. Molte aziende investono in processi digitali, utilizzano servizi cloud, puntano sempre più su strategie digitali e si occupano di nuove tecnologie come l'intelligenza artificiale (AI). Cresce però la dipendenza da sistemi digitali, dati e fornitori di servizi esterni, e quindi aumentano anche i rischi. La cyber criminalità rappresenta oggi una delle principali sfide strategiche per le PMI svizzere. La maggior parte delle aziende prevede inoltre che, in futuro, le minacce legate all'intelligenza artificiale continueranno ad aumentare.

Lo studio sulla cyber sicurezza nelle PMI viene svolto annualmente dal 2020. I risultati dell'attuale edizione 2026 delineano un quadro articolato della situazione in Svizzera: molte PMI dispongono di solide basi tecniche quali aggiornamenti software, firewall, backup dei dati e autenticazione a più fattori. Restano tuttavia importanti lacune nelle misure organizzative, come già emerso negli anni precedenti. Piani di emergenza, audit sulla sicurezza, valutazioni dei fornitori e corsi di formazione sistematici per il personale sono ancora poco diffusi, ma sarebbero decisivi per la resilienza di un'azienda in caso di crisi.

È positivo però che la cyber sicurezza stia tornando al centro dell'attenzione: sempre più aziende definiscono le responsabilità e investono con continuità in ulteriori misure di protezione. La cyber resilienza è migliorata rispetto al 2025, ma resta inferiore al livello del 2024. Lo studio evidenzia inoltre che molte PMI continuano a sottovalutare il rischio di un grave cyber evento.

La conclusione principale è quindi chiara: oggi la cyber sicurezza non è più un compito di competenza esclusiva del settore IT, ma una responsabilità della dirigenza. Le PMI solide non si limitano a proteggere sistemi e dati, ma si preparano anche a livello organizzativo ad affrontare situazioni di emergenza. Combinare misure tecniche, responsabilità chiare, personale formato, backup verificati e un piano di emergenza efficace consente di rafforzare in modo duraturo la cyber resilienza e, al contempo, la competitività aziendale.

Nei dieci capitoli seguenti presentiamo i principali risultati dell'ultima edizione dello studio «PMI Cyber sicurezza 2026» e proponiamo raccomandazioni per rafforzare sicurezza e resilienza nelle PMI. I risultati dettagliati dello studio si trovano su cyberstudie.ch.

Berna e Zurigo, ottobre 2026

La Mobiliare, UFCS, digitalswitzerland, HES-SO, HWZ e SATW

01 PMI svizzere: a che punto sono nell'era digitale?

L'attuale sondaggio evidenzia una trasformazione digitale eterogenea in Svizzera. Molte aziende hanno già avviato questo percorso, ma i progressi compiuti variano a seconda di settore, dimensioni aziendali e propensione all'innovazione.



Il dato positivo è che la maggioranza delle PMI considera il proprio sviluppo digitale almeno moderatamente avanzato. Circa una su dieci ritiene che la propria strategia digitale sia addirittura avanzata o molto avanzata. Resta tuttavia un ampio margine di miglioramento: ***quasi una PMI su cinque dichiara di non avere né una strategia digitale né progetti in corso.***

Particolarmente interessante è la correlazione tra innovazione e digitalizzazione. ***Le aziende che sperimentano e adottano presto nuove tecnologie***

che sperimentano e adottano tempestivamente nuove tecnologie dispongono di una maturità digitale nettamente superiore rispetto ai «late follower».

I progetti di digitalizzazione in corso si concentrano soprattutto su aspetti pratici e benefici concreti. ***Le PMI investono principalmente per aumentare la soddisfazione dei clienti, sfruttare meglio i dati e digitalizzare e automatizzare i processi.*** Tali iniziative contribuiscono direttamente a migliorare l'efficienza e rafforzare la competitività. Sono invece meno diffusi i progetti dedicati allo sviluppo di nuovi modelli di business digitali, all'introduzione di nuove tecnologie o al miglioramento della propria attrattiva quale datore di lavoro.

La situazione dell'intelligenza artificiale è particolarmente chiara: ***quasi la metà delle PMI intervistate non ha finora implementato progetti in questo ambito.*** Nonostante l'IA sia oggi un tema molto discusso, nelle PMI svizzere l'uso di queste tecnologie è ancora agli albori.

Le PMI individuano le ***principali opportunità strategiche*** nella cultura aziendale e dell'innovazione, nei partenariati nonché nella digitalizzazione e nell'automazione. Inoltre, il telelavoro è più diffuso

Quasi la metà delle PMI intervistate non ha ancora implementato progetti in ambito AI.

(i pionieri) valutano la propria maturità digitale molto più positivamente rispetto ai «late follower», tra i quali è anche più frequente l'assenza di una strategia digitale. Lo studio dimostra che ***le aziende***

nelle PMI rispetto all'anno precedente: ***il 61% delle aziende offre almeno in parte questa possibilità al proprio personale.***

Per le PMI la politica e l'economia globali rappresentano il rischio strategico maggiore.

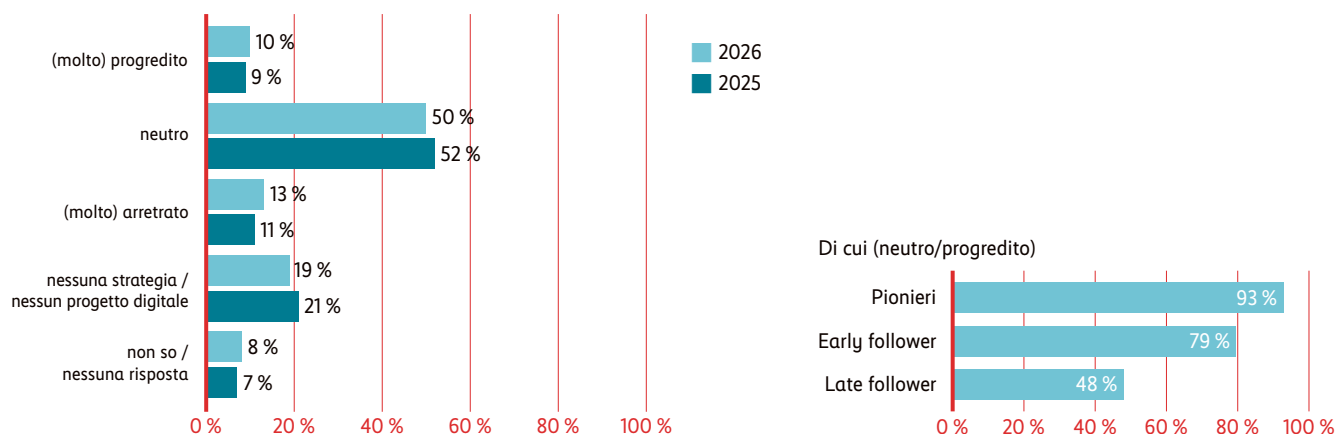
Circa un quinto o un quarto considera rischi strategici l'inflazione, la cyber criminalità e la mancanza di personale qualificato. Con l'aumentare delle dimensioni dell'azienda, assumono particolare rilevanza soprattutto la carenza di personale qualificato e la cyber criminalità.

I risultati mostrano che nel complesso le PMI svizzere stanno avanzando con costanza verso la digitalizzazione, ma l'attenzione è rivolta soprattutto all'ottimizzazione delle attività esistenti. Le opportunità davvero significative offerte dalla trasformazione digitale, ad esempio nuove offerte digitali, modelli di business innovativi o l'impiego mirato dell'IA, sono state finora sfruttate attivamente solo da una minoranza. Per molte aziende il potenziale maggiore per i prossimi anni potrebbe risiedere proprio in questi ambiti.

Progressi nella strategia digitale

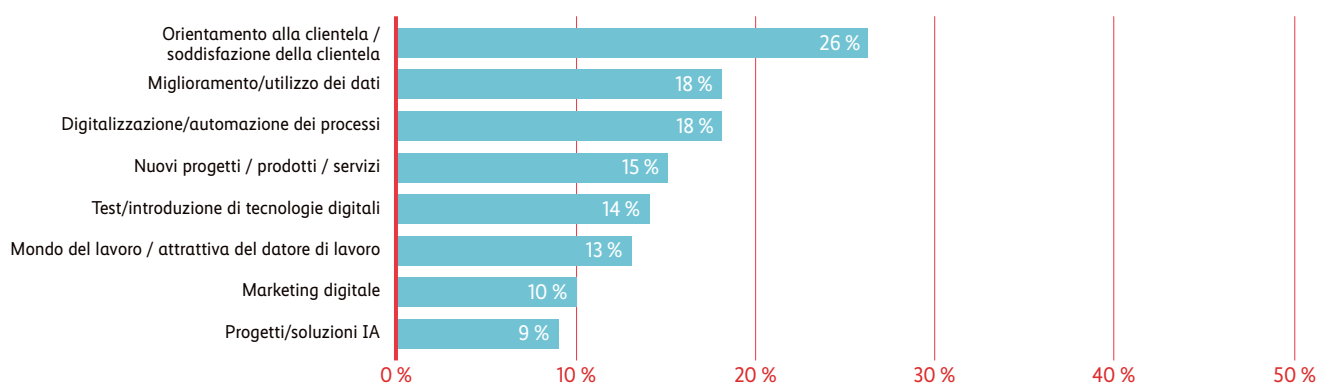
Domanda: come valuta lo stato di avanzamento della strategia digitale o della trasformazione digitale nella sua azienda?

Scala: 1–2: (molto) arretrato / 3–5: neutro / 6–7: (molto) progredito.



Misure strategiche digitali attuate

Domanda: Indichi su una scala da 1 a 7 il livello di implementazione di queste misure nella sua azienda negli ultimi tre anni. Scala: 1–2: (assolutamente) non implementate / 3–5: neutro / 6–7: (completamente) implementate. Risultati rappresentati: % di risposte 6–7 ((completamente) implementate)



02 Sovranità digitale: un nuovo ambito tematico dell'attuale politica mondiale

Gli sviluppi geopolitici degli ultimi anni hanno portato alla ribalta un nuovo tema: la sovranità digitale, con cui si intende **la capacità di un'azienda di poter decidere in modo il più possibile autonomo in merito a dati, tecnologie e dipendenze digitali**. Lo studio attuale rivela però che le PMI svizzere sono appena agli inizi.

I progressi maggiori riguardano le tematiche classiche: **protezione, proprietà e salvataggio dei dati**. Più di un terzo delle aziende intervistate ha già adottato misure concrete in questi ambiti. Anche la **protezione dai cyber rischi** è un'attività che le aziende praticano attivamente. Questi settori vengono probabilmente percepiti come direttamente rilevanti e critici dalle aziende.

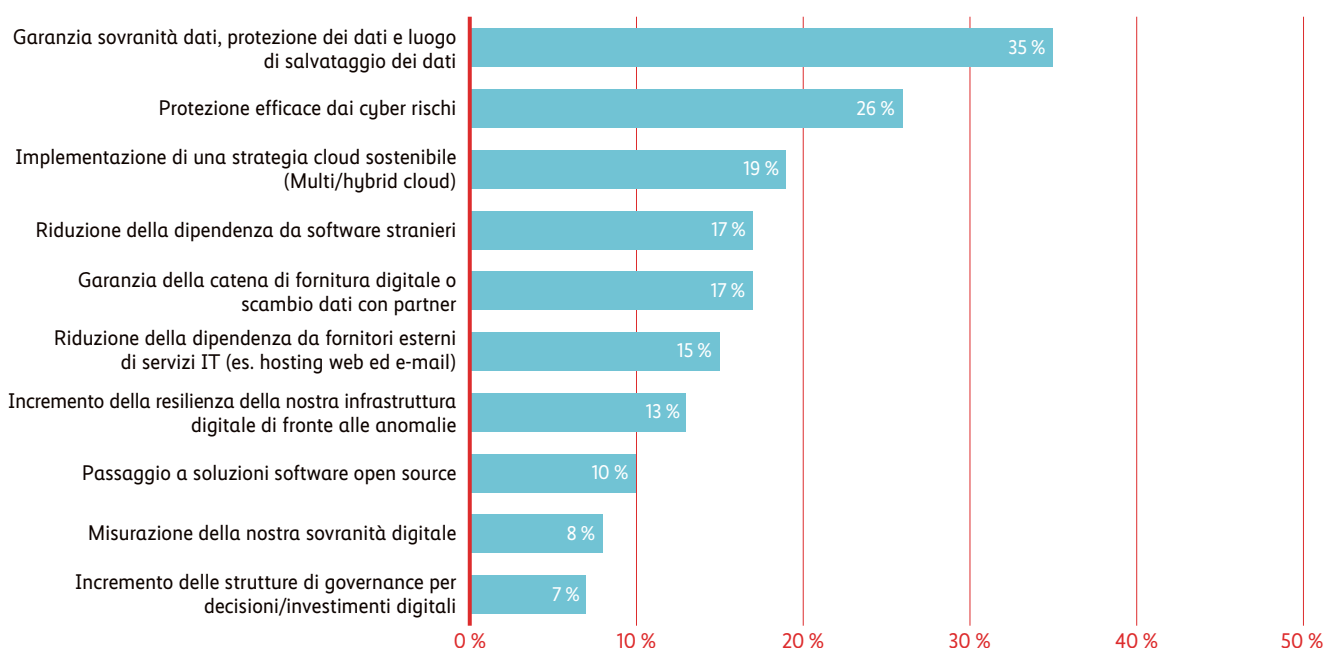
Molto meno diffuse sono invece le misure volte a ridurre la **dipendenza da alcune tecnologie o fornitori**. Ad esempio solo una minoranza delle PMI ha già adottato misure per ridurre la dipendenza da software stranieri, fornitori esterni di servizi IT o cloud. Allo stesso modo, tematiche quali la protezione della catena di approvvigionamento digitale o il passaggio a soluzioni open source sono state finora implementate solo in casi sporadici.

È interessante notare **che molte aziende hanno sentito parlare solo in misura minima di alcuni aspetti della sovranità digitale**. Circa un quarto, infatti, non conosce strutture di governance per le decisioni digitali (solo il 7% dispone di una governance) e quasi un terzo non si è mai occupato di misurare la propria sovranità digitale. Tuttavia, sono proprio questi i temi che potrebbero acquisire

Sovranità digitale

Domanda: ha già pianificato o implementato misure relative alla «sovranità digitale»?

Scala: da 1 (non so cosa sia) a 4 (già implementate). Risultati rappresentati: % di risposte 4 (già implementate)



maggior rilevanza in futuro qualora le aziende intendessero gestire i propri rischi digitali in modo più sistematico.

Nel complesso, lo studio evidenzia che le PMI svizzere si occupano già attivamente della protezione dei dati e della cyber sicurezza, ma nella maggior parte dei casi considerano la sovranità digitale solo da questa prospettiva ristretta. ***La riflessione più ampia su come ridurre le dipendenze strategiche da tecnologie, piattaforme o singoli***



Molte aziende conoscono poco il tema della sovranità digitale.

fornitori rappresenta ancora un territorio inesplorato per molte aziende. Affrontare questi temi con anticipo permette di rafforzare la propria resilienza e operare in modo più indipendente in un mondo digitale sempre più incerto.

03 Cyber criminalità: un problema da prendere sul serio, con nuovi pericoli legati all'IA

La cyber criminalità è ormai da tempo all'ordine del giorno dei consigli di amministrazione delle PMI svizzere. Lo studio attuale traccia un quadro straordinariamente chiaro: quasi nove aziende su dieci (88%) considerano la cyber criminalità un problema serio. A prescindere da dimensioni, settori e tipologie aziendali, vi è ampio consenso sul fatto che *i cyber attacchi rappresentano oggi una minaccia reale per ogni PMI.*

molto esigua contraddice questa affermazione. L'IA viene quindi percepita da molte aziende non solo come un'opportunità, ma anche come un nuovo fattore di rischio.

È interessante notare che la percezione della minaccia non differisce quasi per nulla tra le PMI di piccole dimensioni e quelle più grandi. Indipendentemente dal fatto che un'azienda impieghi pochi

Le PMI ben preparate non vedono maggiori pericoli, ma più possibilità di agire.

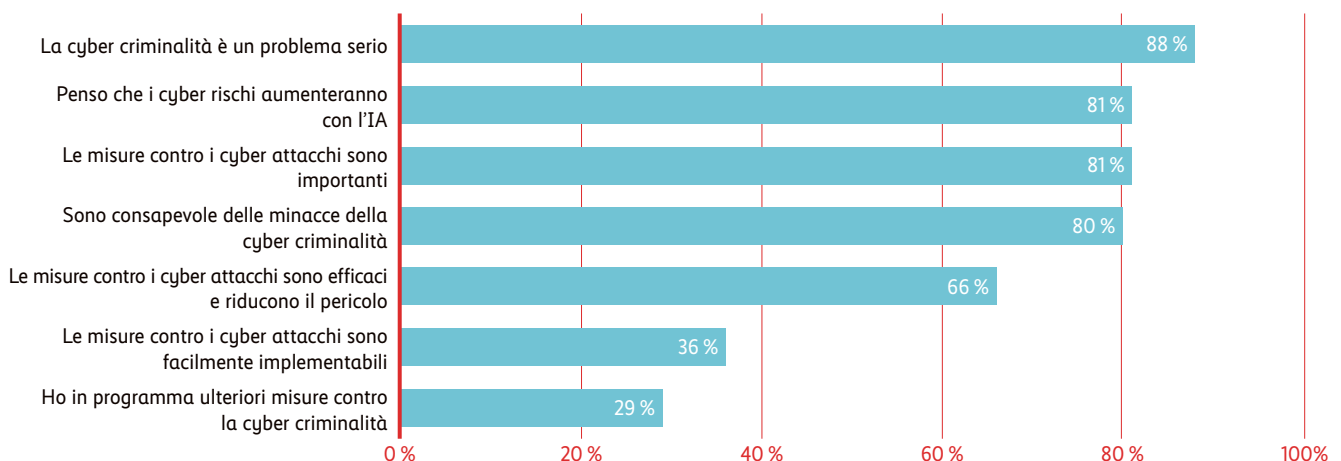
Lo studio evidenzia inoltre che la preoccupazione non riguarda solo i rischi attuali. *Quattro PMI su cinque (81%) ritengono che i pericoli aumenteranno ulteriormente a causa dell'IA.* Solo una minoranza

dipendenti o diverse decine, la valutazione del pericolo è pressoché identica. La cyber criminalità è oggi considerata una sfida per l'intero comparto delle PMI svizzere.

Opinioni sulla cyber criminalità

Domanda: in che misura è d'accordo con le seguenti affermazioni su cyber criminalità come malware, truffe online e hacking?

Scala: da 1 (non sono per niente d'accordo) a 5 (sono pienamente d'accordo). Risultati rappresentati: % di risposte 4-5 (pienamente d'accordo)



Lo studio evidenzia tuttavia anche un altro aspetto importante: la sola consapevolezza del problema non è sufficiente. Le aziende che si sentono meglio informate in materia di cyber sicurezza e che hanno già implementato misure di protezione tecniche o organizzative valutano i rischi a un livello simile a quello delle altre aziende. Sono tuttavia nettamente più convinte che i cyber rischi possano essere efficacemente ridotti. ***Le PMI ben preparate vedono quindi non solo maggiori pericoli, ma anche più possibilità di agire.***

In sintesi, si può affermare che le PMI svizzere riconoscono la minaccia della cyber criminalità in modo più consapevole che mai. Allo stesso tempo, a seguito dei rapidi progressi nel campo dell'IA, molte prevedono un ulteriore aggravarsi dei rischi. La sfida dei prossimi anni non sarà quindi quella di aumentare la consapevolezza del problema, bensì di tradurre tale presa di coscienza in misure di protezione concrete e in formazione continua.



04 Cyber criminalità nelle PMI: più di 35 000 persone colpite, spesso con conseguenze gravi



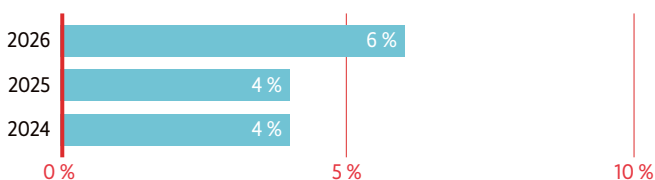
La buona notizia è che negli ultimi tre anni, la grande maggioranza delle PMI svizzere è stata risparmiata da gravi cyber attacchi (noti). Tuttavia, lo studio dimostra che la cyber criminalità può avere gravi ripercussioni sulle aziende colpite. Il 6 % delle PMI intervistate (ovvero, secondo un'extrapolazione, oltre 35 000 PMI in Svizzera) ha dichiarato di aver subito un cyber attacco negli ultimi tre anni (intervallo di variazione statistica: 35 200–36 700 PMI). Molte hanno riportato danni finanziari, problemi reputazionali, un ingente impiego di risorse o un elevato stress personale. Tra le aziende con almeno dieci dipendenti, la quota sale addirittura al 16 per cento.

È particolarmente rilevante la natura dei danni subiti. A differenza di quanto spesso si pensa, le perdite finanziarie non sono la principale preoccupazione. **Le aziende colpite indicano più di frequente l'enorme lavoro necessario per riparare i danni, seguito dallo stress emotivo.** Solo in seconda battuta emergono aspetti come i danni finanziari, la reputazione compromessa o la perdita dei dati dei clienti. I cyber attacchi, quindi, costano spesso soprattutto tempo ed energie e arrecano disagi.

Un altro risultato importante è che non esiste un attacco tipico. **Un attacco che va a segno può passare tramite canali diversi: tra i più citati figurano phishing, hacking delle password, malware e attacchi a rete e server, ciascuno presente in circa un terzo degli incidenti.** Questo significa che le PMI non devono difendersi da una sola minaccia, ma da un ampio spettro di tecniche offensive.

Cyber attacchi che hanno causato danni

Domanda: la sua azienda negli ultimi 3 anni ha subito un cyber attacco che ha causato un danno finanziario o reputazionale, ha richiesto un notevole sforzo per la risoluzione del problema o ha causato un forte disagio emotivo? (Risposta: sì)



L'aspetto più citato dalle aziende colpite è l'enorme carico di lavoro necessario per la riparazione del danno.

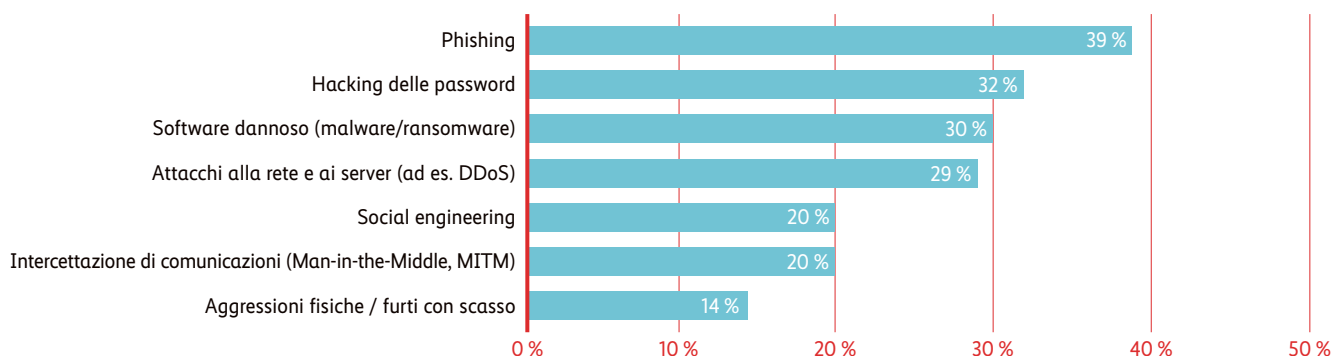
Anche il ricatto è un tema rilevante.

Circa il 7 % delle aziende intervistate (ovvero, secondo un'extrapolazione, circa 45 000 PMI in Svizzera) è già stato vittima di estorsioni da parte di criminali informatici (intervallo di variazione statistica: 43 300–45 380 PMI). Le realtà più colpite sono le aziende di maggiori dimensioni e quelle dei settori industriale ed edilizio. Alcune imprese hanno persino pagato il riscatto. Questo conferma che la cyber criminalità non è più solo un problema tecnico, ma una sfida gestionale e strategica.

I risultati mostrano chiaramente che, anche se solo una minoranza delle PMI viene colpita direttamente, le conseguenze di un attacco andato a segno possono essere rilevanti. L'importante, quindi, non è tanto la dimensione dell'azienda, quanto il suo livello di preparazione di fronte a diversi scenari di attacco e la sua capacità di proteggersi dai danni finanziari.

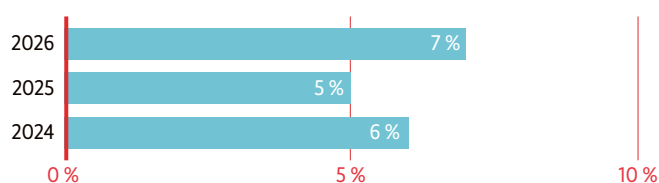
Tipo di attacco

Domanda: quale tipo di attacco ha subito? (Filtro: se ha subito un cyber attacco)



Estorsione

Domanda: La sua azienda è mai stata vittima di ricatti da parte di cyber criminali? (Risposta: sì)



05 Conoscenza delle cyber minacce e supporto

L'attuale sondaggio evidenzia che molte PMI svizzere si ritengono sostanzialmente ben preparate ad affrontare i cyber rischi. **Quasi la metà dichiara di essere sufficientemente informata sulle principali cyber minacce rilevanti per la propria attività.** Molte dichiarano di sapere dove poter ottenere informazioni, supporto o raccomandazioni concrete su come comportarsi in caso di emergenza.

È inoltre incoraggiante che **il 40 % delle imprese si dice disposto a segnalare spontaneamente gli incidenti rilevanti all'Ufficio federale della cibersicurezza (UFCS).** La consapevolezza dell'importanza dello scambio di informazioni e della collaborazione sembra quindi sostanzialmente diffusa.

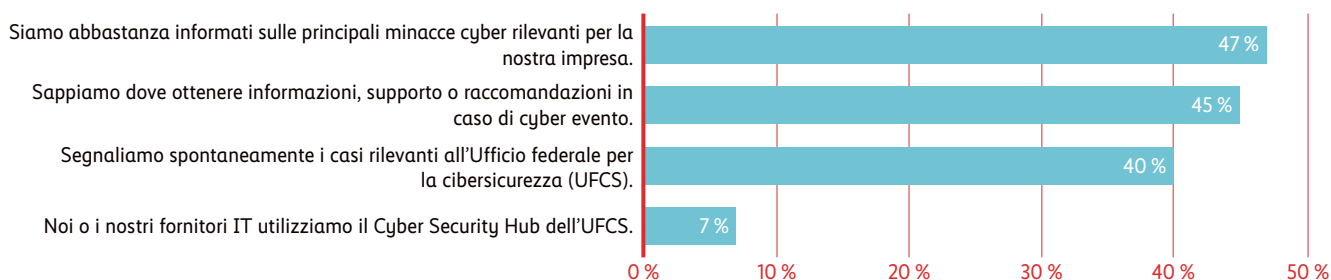
Lo studio evidenzia che l'utilizzo del Cybersecurity Hub da parte delle PMI ha ancora un potenziale di crescita, in particolare per le aziende di piccolissime dimensioni. Infatti, il Cybersecurity Hub dell'UFCS viene utilizzato solo da circa il 7 % delle aziende o dai loro fornitori di servizi informatici. Questo servizio si rivolge in primo luogo ai gestori di infrastrutture critiche e ai loro fornitori di servizi, ma anche le PMI possono registrarsi e usufruire dell'offerta.



Conoscenza delle cyber minacce e supporto

Domanda: Quanto è d'accordo con le seguenti affermazioni?

Scala: da 1 (per nulla) a 5 (del tutto). Risultati rappresentati: % di risposte 4-5 (del tutto d'accordo)



È inoltre evidente che le **PMI più grandi conoscono meglio le possibilità di supporto a loro disposizione rispetto alle aziende più piccole**. Quelle con un numero di dipendenti compreso tra 10 e 49 sanno molto più spesso chi contattare concretamente in caso di emergenza e utilizzano anche offerte come il Cybersecurity Hub con una frequenza significativamente più elevata. Le aziende più piccole si affidano probabilmente in misura maggiore alle proprie conoscenze generali o a partner esterni.

Le PMI più grandi conoscono meglio le proprie possibilità di supporto rispetto a quelle più piccole.

I risultati indicano che molte PMI tendono a valutare la propria cyber resilienza soprattutto dal punto di vista delle conoscenze personali. La preparazione organizzativa a un incidente è tuttavia, in alcuni casi, meno avanzata. **In questo ambito, però, i piani di emergenza, i processi definiti e il ricorso a offerte di supporto specializzate possono fare una differenza significativa qualora si verifichi effettivamente un incidente.**

Molte PMI si sentono informate e, secondo la propria valutazione, sanno a chi rivolgersi. Spesso però mancano strategie di sicurezza, piani di emergenza e audit. I risultati indicano quindi un divario tra la cyber resilienza percepita e quella effettivamente radicata a livello organizzativo.

06 La cyber sicurezza acquisisce nuovamente un'importanza maggiore

Dopo un calo registrato lo scorso anno, il tema della cyber sicurezza sta tornando ad essere una delle principali priorità per le PMI svizzere. Nel 2026, il 46 per cento delle aziende intervistate la considera importante o molto importante, mentre l'anno precedente questo valore era appena del 33 per cento. **Il tema torna così al livello degli anni precedenti.**

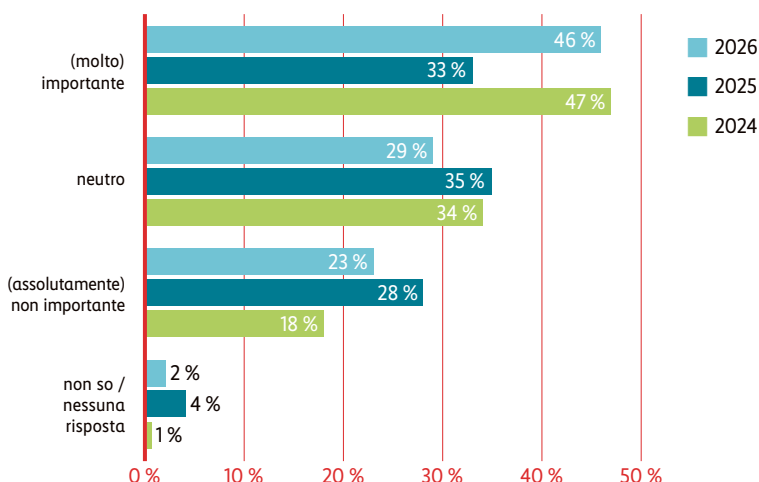
Tale tendenza è particolarmente marcata nelle aziende con almeno 10 dipendenti. **In questo gruppo, circa sei aziende su dieci attribuiscono un'elevata priorità alla cyber sicurezza.** Anche le aziende tecnologicamente avanzate, considerate pioniere o «early follower», attribuiscono alla cyber sicurezza un'importanza nettamente maggiore rispetto alle imprese meno innovative sul piano tecnologico («late follower»).

La percezione dei cyber rischi aumenta con le dimensioni dell'azienda.

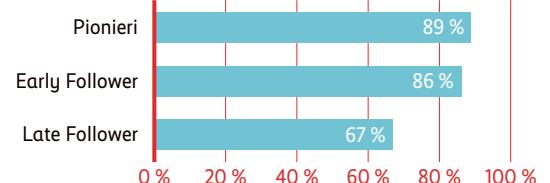
Priorità della cyber sicurezza

Domanda: qual è l'importanza del tema della cyber sicurezza nella sua azienda?

Scala: 1-2: (assolutamente) non importante / 3: neutro / 4-5: (molto) importante



Di cui (neutro / molto importante)



La crescente attenzione non è casuale. L'attuale studio dimostra che la cyber criminalità è oggi uno dei rischi strategici più importanti per le PMI svizzere. Con il 23% delle menzioni, si colloca praticamente alla pari di inflazione, aumento dei costi e carenza di personale qualificato. Solo le incertezze politiche ed economiche globali vengono citate con una frequenza leggermente superiore come rischio a lungo termine.

È interessante notare che la percezione dei cyber rischi aumenta con le dimensioni dell'azienda.

In quelle con un numero di dipendenti compreso tra 20 e 49, già più di un terzo considera la cyber criminalità uno dei maggiori rischi strategici.

In questo gruppo, il tema si colloca quindi ancora nettamente più in alto nella gerarchia dei rischi.

Nel complesso, i risultati mostrano che le PMI svizzere riconoscono sempre più che la cyber sicurezza non è solo una questione tecnica di competenza dell'IT, ma un tema strategico per l'azienda. Alla luce delle crescenti dipendenze digitali, delle nuove minacce e dei cyber criminali professionisti, la protezione dei dati, dei processi e dei rapporti commerciali torna ad assumere un ruolo centrale nella gestione aziendale.



07 Responsabilità per i cyber rischi: sempre più PMI definiscono competenze chiare

Lo studio attuale evidenzia una tendenza positiva: **le PMI svizzere stanno definendo con maggiore chiarezza le responsabilità legate alla cyber sicurezza**. Se in passato i cyber rischi erano spesso considerati marginali, oggi più di frequente viene individuato all'interno dell'azienda chi se ne occupa.

È cresciuta soprattutto la percentuale di aziende che affidano la responsabilità della cyber sicurezza a una persona **come incarico parziale**: nel giro di un anno è passata dal 15 al 21 per cento. **Quasi una PMI su dieci dispone inoltre di una figura dedicata, con competenze chiaramente definite in questo ambito.**

Molte aziende ricorrono a supporti esterni: più di un quarto delle PMI intervistate collabora con un partner esterno specializzato in cyber rischi. Soprattutto per quelle di piccole dimensioni, questa soluzione può aiutare a compensare la mancanza di risorse interne o di competenze specialistiche.

Il cambiamento più significativo riguarda però le aziende che finora avevano dato poca attenzione al tema. Rispetto all'anno precedente la percentuale di PMI per le quali i cyber rischi non rappresentano una priorità è scesa dal 42 al 36 per cento. Il calo si osserva anche tra le microimprese con uno fino a tre dipendenti, **segno che la consapevolezza dei cyber rischi sta crescendo anche nelle realtà più piccole.**

Molte aziende puntano su un supporto esterno.

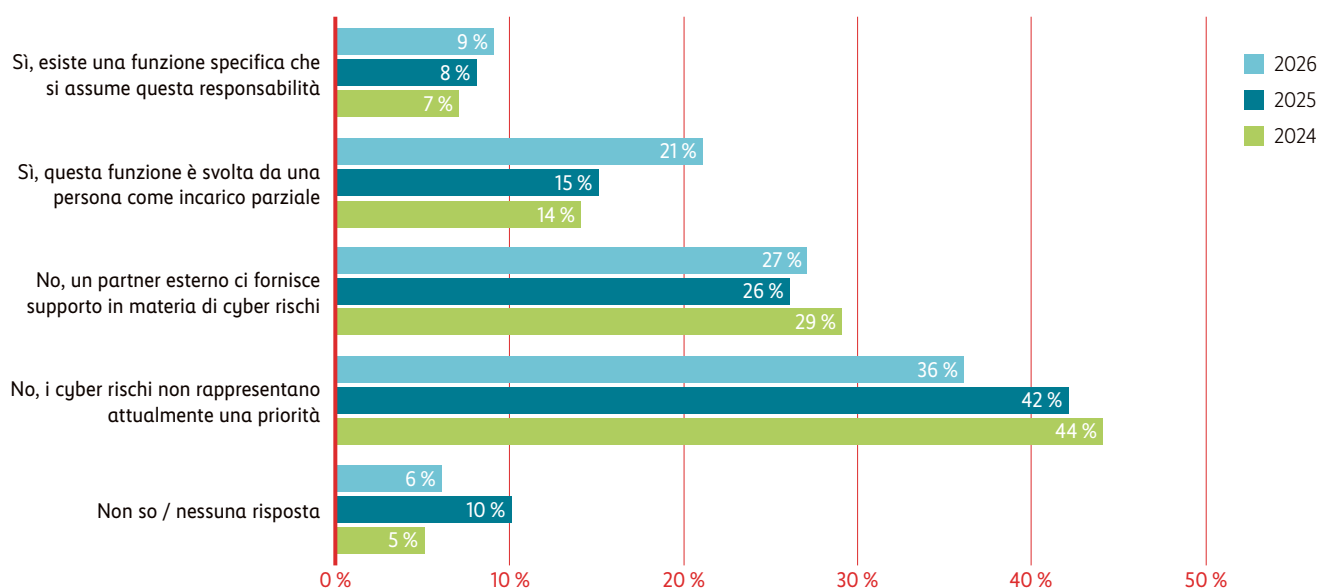


In base alle dimensioni delle aziende si profilano differenze marcate: in quelle con almeno dieci dipendenti, le responsabilità sono disciplinate con maggiore frequenza, sia internamente che con il supporto di specialisti esterni. Inoltre, queste aziende tendono a considerare i cyber rischi molto meno spesso come un «tema non prioritario».

Nel complesso, i risultati indicano che la cyber sicurezza nelle PMI svizzere sta diventando sempre più una responsabilità gestionale, non solo tecnica. La conclusione più importante è che non tutte le PMI necessitano di un responsabile dedicato per la cyber sicurezza, ma tutte devono stabilire con chiarezza chi è responsabile internamente e chi interviene in caso di emergenza.

Responsabilità per i cyber rischi

Domanda: la sua azienda ha una o più persone responsabili della cyber sicurezza?



08 Implementazione di misure tecniche per la cyber sicurezza

Le PMI svizzere continuano a investire soprattutto in misure di protezione tecniche consolidate. Quelle largamente più diffuse consistono negli aggiornamenti periodici del software: più dell'80 per cento delle aziende li implementa. Sono inoltre molto utilizzati i firewall, i backup dei dati e l'autenticazione a due o più fattori (MFA). Queste misure costituiscono oggi il fondamento della cyber sicurezza nella maggior parte delle PMI.

Sono invece decisamente meno diffusi i meccanismi di protezione avanzati, tra cui, ad esempio, il monitoraggio del traffico dati, la segmentazione delle reti o l'impiego dell'IA per la protezione dagli attacchi informatici. Sono proprio questi i temi che mettono in luce un ampio divario tra pionieri tecnologici e «late follower». Mentre le aziende

innovative ricorrono sempre più spesso a tali misure, molte PMI continuano ad affidarsi alle classiche misure di base.

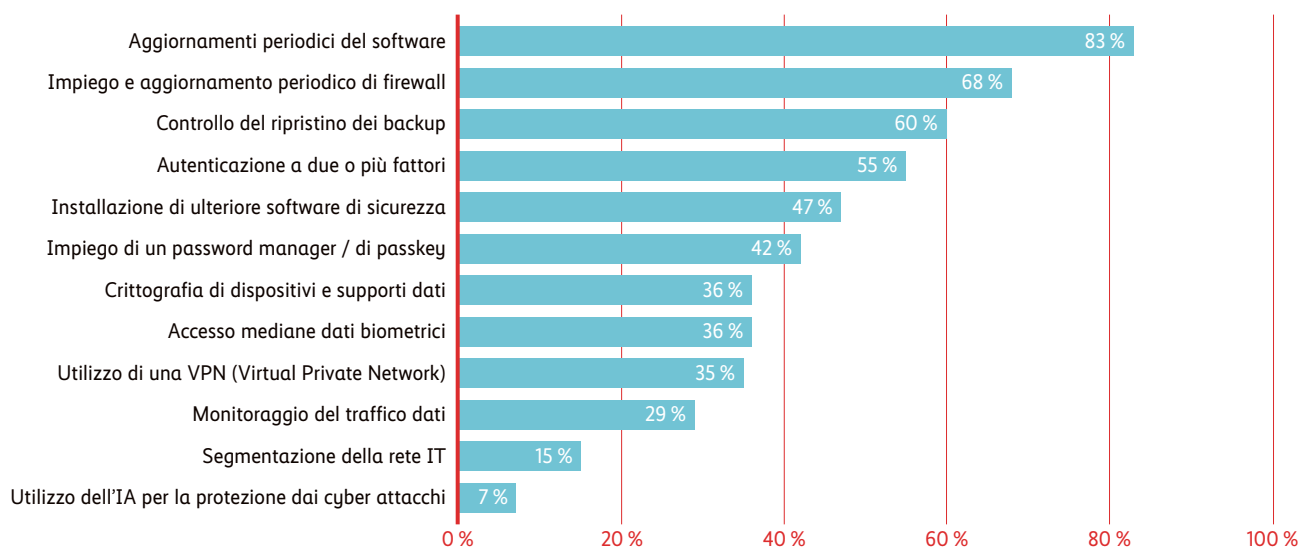
Un dato particolarmente incoraggiante riguarda il backup: **oggi nove PMI svizzere su dieci effettuano backup periodici dei dati**. La percentuale delle aziende che non li esegue è scesa ad appena il quattro per cento. Inoltre, sempre più aziende puntano su una combinazione di backup locale e backup su cloud. Questa soluzione aumenta l'affidabilità e riduce il rischio di una perdita totale dei dati.

Interessante è anche la sede di archiviazione dei dati: **circa tre quarti delle aziende che effettuano backup archiviano i propri dati in Svizzera**. Solo

Misure tecniche di cyber sicurezza

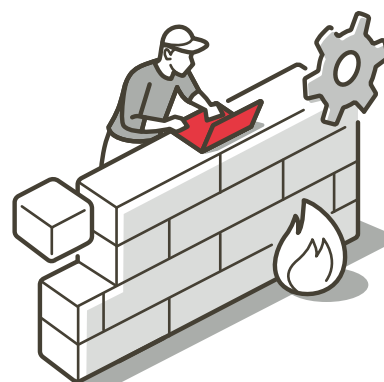
Domanda: In quale misura nella sua azienda sono implementate le seguenti misure organizzative per aumentare la cyber sicurezza?

Scala: 1-2: (assolutamente) non implementate / 3-5: neutro / 6-7: (pienamente) implementate. Risultati rappresentati: % di risposte 6-7 (pienamente implementate)



poche conservano le proprie copie di sicurezza al di fuori dell'Europa. Questo dimostra che la sovranità dei dati e il controllo sui dati aziendali sensibili rivestono un ruolo importante per molte PMI.

Il punto di maggiore vulnerabilità si evidenzia tuttavia in un altro ambito: un backup è utile solo se, in caso di emergenza, funziona correttamente. Sebbene oggi i backup periodici siano ormai la norma, **solo un quarto delle PMI verifica regolarmente il ripristino dei propri dati**. Di conseguenza, molte aziende non sanno se i propri dati possano effettivamente essere ripristinati a seguito di un cyber attacco, di un guasto tecnico o di un errore operativo.



Nove PMI svizzere su dieci effettuano oggi backup periodici dei dati.

I risultati mostrano che nel complesso molte PMI dispongono di misure tecniche di base. Tuttavia, permangono ancora lacune in materia di protezione degli accessi, monitoraggio, segmentazione e test del ripristino dei dati. Soprattutto per quanto riguarda il backup, negli ultimi anni sono stati compiuti importanti progressi. La prossima sfida consiste tuttavia non solo nel salvare i dati, ma anche nel testarne periodicamente il ripristino. Infatti, in caso di emergenza, ciò che conta non è solo la presenza di un backup, ma anche il suo effettivo funzionamento.

09 Implementazione di misure organizzative per la cyber sicurezza



Lo studio attuale mostra che le PMI svizzere in materia di cyber sicurezza puntano soprattutto su misure di protezione tecniche, **mentre quelle organizzative sono decisamente meno diffuse**. Le pratiche più comunemente adottate restano le regole di comportamento di base: gestione attenta dei dati personali, utilizzo di password sicure e verifica di documenti o e-mail sospetti. Si tratta di accorgimenti ormai consolidati nella maggior parte delle aziende.

Quando però si passa a processi e strutture più avanzati, il livello di implementazione cala sensibilmente. **Solo circa un terzo delle PMI realizza un inventario sistematico dei propri sistemi IT e**

servizi cloud oppure organizza periodicamente corsi di formazione per il personale. Ancora meno diffusi sono i piani di emergenza per la continuità operativa, la valutazione della sicurezza dei fornitori, i piani di sicurezza formali o la classificazione dei dati in base al livello di protezione richiesto. **Gli audit sulla sicurezza risultano la misura meno praticata.**

Le dimensioni aziendali incidono in modo significativo. Le regole di comportamento di base sono diffuse in misura simile tra piccole e grandi PMI, ma la professionalizzazione cresce con il numero di dipendenti. Le aziende che occupano da 10 a 49 dipendenti dispongono molto più spesso di piani di emergenza, supporto per la sicurezza informatica, linee guida dedicate e audit periodici rispetto alle microimprese.

Un'altra correlazione interessante riguarda la conoscenza della cyber sicurezza. Le aziende che si ritengono ben informate sui cyber rischi adottano misure organizzative di protezione significativamente più spesso rispetto a quelle meno ferrate. Questo vale per quasi tutti gli ambiti esaminati, dalla formazione del personale ai piani di emergenza e di sicurezza. Fanno eccezione soltanto

Solo circa un terzo delle PMI effettua un inventario sistematico dei propri sistemi IT e servizi cloud oppure organizza corsi di formazione periodici per il personale.

gli audit sulla sicurezza e la classificazione dei dati sensibili. In generale, un livello di informazione più elevato si associa quindi a una maggiore implementazione delle misure organizzative di protezione.

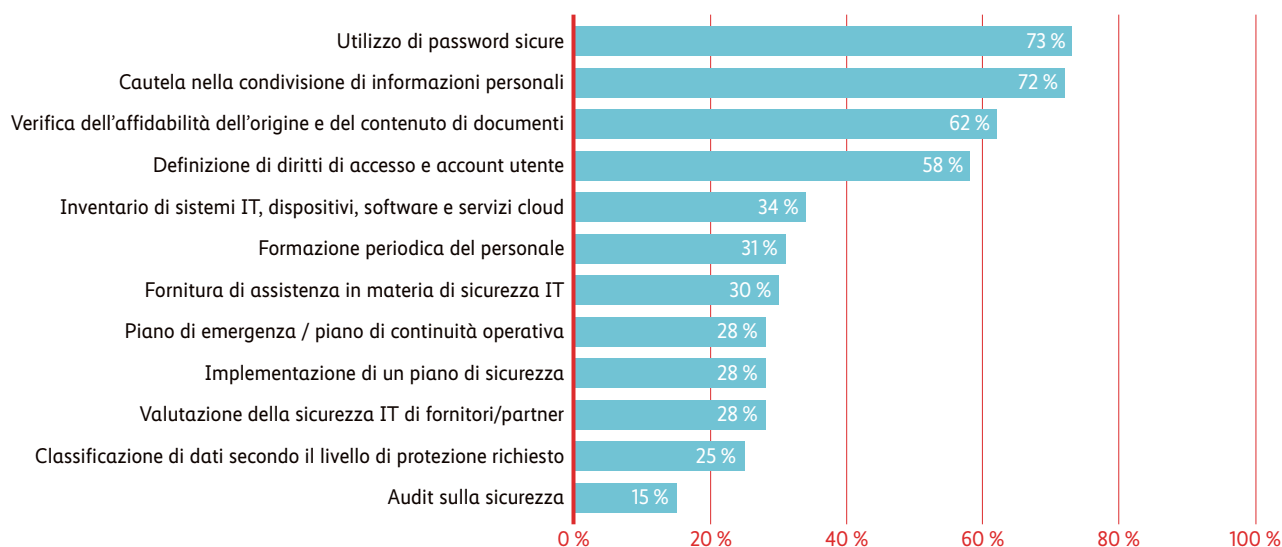
Anche la cultura dell'innovazione svolge un ruolo determinante. Le aziende aperte alle nuove tecnologie e i cosiddetti «early follower» presentano livelli di implementazione nettamente superiori rispetto ai «late follower». Questi ultimi dispongono molto più raramente di processi di sicurezza strutturati e registrano più spesso rispetto alla media valori bassi per quanto riguarda le misure organizzative.

Nel complesso, i risultati mostrano che la maggior parte delle PMI sa adottare comportamenti prudenti nella gestione quotidiana. **La vera sfida consiste però nell'integrare la cyber sicurezza nei processi organizzativi.** Piani di emergenza, formazione, verifiche dei fornitori e audit sulla sicurezza periodici sono spesso meno visibili di strumenti come i firewall, ma possono essere decisivi per reagire rapidamente a un cyber incidente e mantenere la continuità operativa.

Misure organizzative per la cyber sicurezza

Domanda: In quale misura nella sua azienda sono attuate le seguenti misure organizzative per aumentare la cyber sicurezza?

Scala: 1-2: (assolutamente) non implementate / 3-5: neutro / 6-7: (pienamente) implementate. Risultati rappresentati: % di risposte 6-7 (pienamente implementate)



10 Il futuro: cresce l'importanza della cyber resilienza, ma molte PMI restano caute

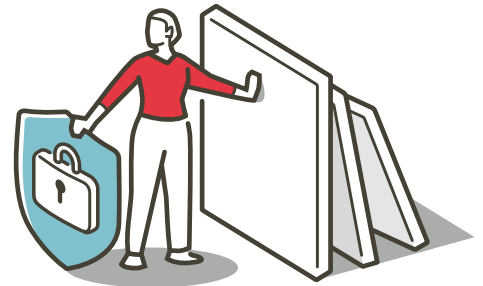
Lo studio attuale delinea un quadro sostanzialmente positivo della cyber resilienza nelle PMI svizzere. Un'azienda su due ritiene di essere ben o molto ben protetta dai cyber attacchi e pronta ad affrontarne uno; una percezione addirittura leggermente migliorata rispetto all'anno precedente. Sono particolarmente fiduciose le imprese più grandi e quelle tecnologicamente più avanzate.

I pionieri della digitalizzazione valutano la propria resilienza in modo nettamente più favorevole rispetto ai «late follower», che hanno invece un approccio molto più critico.

Allo stesso tempo, la cyber sicurezza torna ad rivestire una posizione strategica. Dopo il calo di priorità registrato lo scorso anno, oggi quasi una PMI su due la considera importante o molto importante. Il tema è tornato al centro dell'attenzione

soprattutto nelle aziende con più di dieci dipendenti. Anche le imprese innovative gli attribuiscono un'importanza superiore alla media.

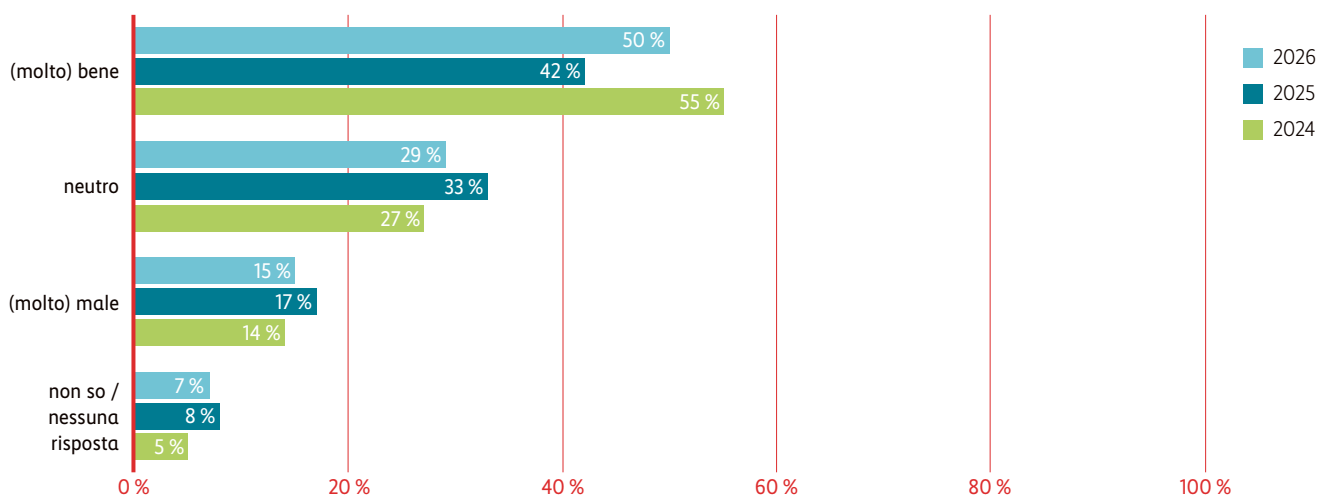
Guardano al futuro, circa due PMI su cinque ritengono (molto) probabile l'adozione di ulteriori misure di sicurezza nel futuro prossimo (uno-tre anni). La propensione a intervenire cresce con le



Cyber resilienza

Domanda: A suo avviso, in che misura la sua azienda è protetta dai cyber attacchi e preparata ad affrontarne uno?

Scala: 1-2: (molto) male / 3: neutro / 4-5: (molto) bene



Cyber resilienza non significa solo prevenire gli attacchi, ma anche ripristinare rapidamente l'operatività dopo un incidente.

dimensioni dell'azienda e con il livello di informazione. Le aziende che si sentono ben informate sulla cyber sicurezza pianificano nuovi investimenti molto più spesso rispetto a quelle meno informate.

Nonostante l'elevata consapevolezza del problema, emerge una certa contraddizione. Sebbene in altre parti del sondaggio la cyber criminalità sia chiaramente percepita come una minaccia concreta, la maggioranza delle PMI ritiene che, nei prossimi due o tre anni, un cyber attacco possa interrompere l'attività per almeno un giorno. Solo circa un'azienda su dieci prevede un rischio elevato, valutazione che aumenta in modo significativo soprattutto tra le PMI più grandi. I risulta-

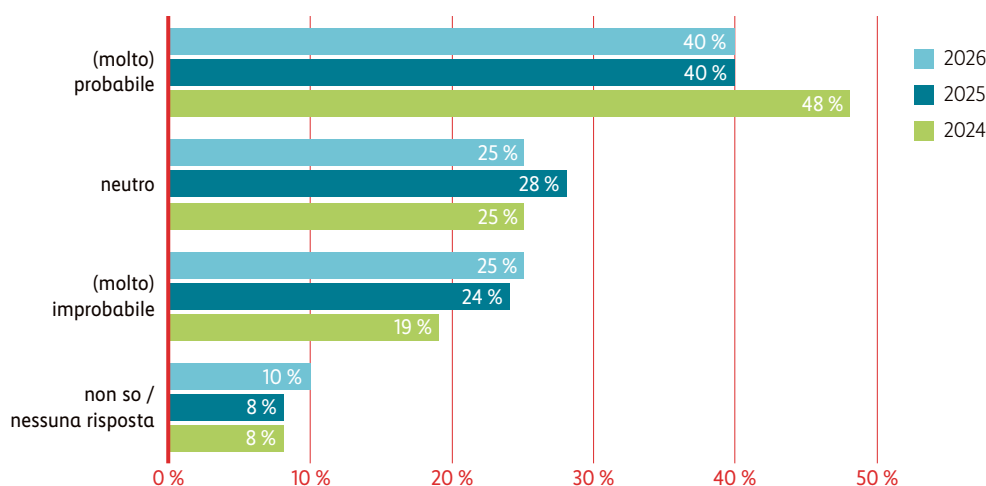
ti suggeriscono che, pur avendo oggi maggiore fiducia nella propria resilienza, molte aziende potrebbero in parte sottovalutare le conseguenze di un incidente.

La cyber resilienza non riguarda solo la prevenzione degli attacchi, ma anche la capacità di ripristinare rapidamente l'operatività. Per questo, nei prossimi anni saranno sempre più importanti il miglioramento continuo delle misure di protezione, la preparazione alle emergenze e le verifiche periodiche della sicurezza.

Incremento delle misure di cyber sicurezza

Domanda: con quale probabilità aumenterà le misure di sicurezza contro la cyber criminalità nel prossimo futuro (uno-tre anni)?

Scala: 1-2: (molto) improbabile / 3: neutro / 4-5: (molto) probabile



Implementazione

Check list su cyber sicurezza e cyber resilienza per le PMI svizzere

Secondo i risultati dello studio, molte PMI hanno una buona padronanza delle basi tecniche. Rimane ancora molto da fare sul fronte delle misure organizzative, nella preparazione alle emergenze e nella verifica periodica dell'efficacia delle misure di protezione esistenti. Questa check list aiuta a rafforzare la propria cyber resilienza.

Misure tecniche per la cyber sicurezza

1. Consolidamento delle regole fondamentali

- ☐ Aggiornare periodicamente sistemi operativi, applicazioni e dispositivi.
- ☐ Utilizzare un firewall e aggiornarlo costantemente.
- ☐ Attivare l'autenticazione a più fattori (MFA) per la posta elettronica, i servizi cloud e i sistemi critici.
- ☐ Integrare software di sicurezza aggiuntivi (ERD / Endpoint Protection, antivirus).
- ☐ Adottare password manager o passkey.

2. Protezione dei dati

- ☐ Eseguire periodicamente backup dei dati.
- ☐ Conservare i backup sia localmente sia nel cloud.
- ☐ Per quanto possibile, conservare copie dei backup anche in Svizzera.
- ☐ Testare periodicamente il ripristino dei backup. Solo i backup funzionanti offrono protezione in caso di emergenza.
- ☐ Crittografare i dispositivi, i supporti dati e i dati sensibili.

3. Protezione dell'infrastruttura

- ☐ Implementare soluzioni VPN per gli accessi esterni.
- ☐ Utilizzare l'accesso biometrico quando opportuno.
- ☐ Monitorare il traffico dati e le attività sospette.
- ☐ Isolare i sistemi critici tramite segmentazione della rete.
- ☐ Valutare il potenziale delle soluzioni di protezione basate sull'IA.

Misure organizzative per la cyber sicurezza

1. Sensibilizzazione del personale

- ☐ Stabilire regole chiare per gestire le informazioni personali e riservate.
- ☐ Introdurre regole vincolanti per password sicure.
- ☐ Controllare l'attendibilità di e-mail, link e documenti.
- ☐ Formare periodicamente il personale sui cyber rischi.

2. Creazione di strutture e responsabilità

- ☐ Attribuire chiaramente le responsabilità in materia di cyber sicurezza.
- ☐ Gestire in modo sistematico diritti di accesso e account degli utenti.
- ☐ Effettuare un inventario di tutti i sistemi IT, dispositivi, pacchetti software e servizi cloud.
- ☐ Organizzare un supporto interno o esterno per la sicurezza IT.
- ☐ Documentare il piano di sicurezza aziendale.

3. Rafforzamento della resilienza

- ☐ Predisporre un piano di emergenza e una strategia per la continuità operativa.
- ☐ Stabilire le responsabilità in caso di crisi.
- ☐ Individuare in anticipo i punti di riferimento per il supporto in caso di emergenza come fornitori di servizi IT, assicuratori, Ufficio federale per la cibersicurezza (UFCS).
- ☐ Segnalare gli incidenti rilevanti all'Ufficio federale per la cibersicurezza (UFCS).

4. Revisione periodica dei rischi

- ☐ Valutare la sicurezza IT di fornitori e partner.
- ☐ Classificare i dati secondo il livello di protezione richiesto.
- ☐ Eseguire periodicamente audit sulla sicurezza.
- ☐ Verificare le dipendenze digitali da fornitori, piattaforme o servizi cloud specifici.

La cyber resilienza non si limita alla prevenzione degli attacchi. Le aziende di successo sanno riconoscere un attacco, contenerne i danni, ripristinare rapidamente l'operatività e trarne insegnamento.

Strumenti pratici per rafforzare la cyber resilienza

Cyber test per PMI

- Questo test di autovalutazione consente di scoprire cosa attrae gli hacker della propria organizzazione e di ricevere consigli personalizzati sulla cyber sicurezza.
<https://www.mobiliare.ch/campagna/cybertest>
- «IT Sec 4 KMU» permette di calcolare il proprio cyberscore e di individuare misure concrete per migliorare la propria cyber sicurezza.
<https://itsec4kmu.ch/>

Ufficio federale della cibersicurezza UFCS

- Informazioni per imprese e autorità sulla protezione e sulle procedure da seguire in caso di cyber incidenti nonché sull'obbligo di segnalazione.
<https://www.bacs.admin.ch/it/infos-imprese-e-autorita>
- Informazione sul Cybersecurity Hub (CSH)
<https://www.bacs.admin.ch/it/informazioni-csh>

Cybersecurity Map

- La Cybersecurity Map offre ai responsabili decisionali una panoramica concisa degli sviluppi tecnologici più rilevanti
<https://www.satw.ch/en/focus-topics/cybersecurity/satw-cybersecurity-map>

Metodologia di ricerca

Lo studio aveva lo scopo di analizzare l'atteggiamento delle PMI svizzere verso cyber criminalità, cyber sicurezza e digitalizzazione.

Tra il 24 giugno e il 10 luglio 2026 è stato somministrato un sondaggio online a cui hanno risposto 507 dirigenti di PMI con 1-49 dipendenti. La selezione si è basata sul panel Internet di YouGov, composto da circa 115 000 membri.

Il campione è stato definito con quote non proporzionali per dimensione aziendale e regione linguistica, quindi ponderato proporzionalmente.

La popolazione statistica rappresentata dal campione comprende circa 614 400 imprese con un organico da 4 a 49 dipendenti (UST STATENT, 2025) distribuite in tutte le regioni della Svizzera. L'intervallo di confidenza del campione totale si colloca al +/- 4,4 % con un livello di confidenza del 95 % (distribuzione 50/50).

Il campione ponderato rispecchia la struttura della popolazione per dimensione aziendale e regione linguistica; di conseguenza, i risultati sono trasferibili alla popolazione statistica entro i limiti dell'intervallo di confidenza.

Contatto YouGov:
Karin Mändli Lerch,
karin.maendlilerch@yougov.ch

Contatti di autrici e autori



Marc K. Peter
Professore di Digital Business
HES-SO Valais-Wallis School of Management
marckurt.peter@hes-so.ch



Romain Geiser
Program Manager NCS
Ufficio federale della cibersicurezza
ncs@ncsc.admin.ch



Anu Anthamatten
Senior Project Manager
digitalswitzerland, Zurigo
anu@digitalswitzerland.com



Léonard Marbe
Senior Marketing Manager
La Mobiliare
leonard.marbe@mobiliar.ch



Anna V. Rozumowski
Docente e responsabile di corso di laurea
HWZ Hochschule für Wirtschaft Zürich
anna.rozumowski@fh-hwz.ch



Tobias Schlegel
Responsabile Tech Intelligence
SATW Schweizerische Akademie
der Technischen Wissenschaften
tobias.schlegel@satw.ch



Karin Mändli Lerch
Senior Research Consultant
YouGov
karin.maendlilerch@yougov.ch

Marc K. Peter, Romain Geiser, Anu Anthamatten,
Léonard Marbe, Anna V. Rozumowski,
Tobias Schlegel e Karin Mändli Lerch:

PMI Cyber sicurezza 2026

Uno studio della Mobiliare in collaborazione
con UFCS, digitalswitzerland, HES-SO,
HWZ e SATW

- Ufficio federale della cibersicurezza UFCS
- La Mobiliare
- digitalswitzerland
- HES-SO Valais-Wallis School of Management
- HWZ Hochschule für Wirtschaft Zürich
- SATW Schweizerische Akademie
der Technischen Wissenschaften
- YouGov

cyberstudie.ch
Berna e Zurigo, ottobre 2026

Colophon

Marc K. Peter, Romain Geiser, Anu Anthamatten, Léonard Marbe, Anna V. Rozumowski, Tobias Schlegel e Karin Mändli Lerch

PMI Cyber sicurezza 2026:

Uno studio della Mobiliare in collaborazione con UFCS, digitalswitzerland, HES-SO, HWZ e SATW

Ufficio federale della cibersicurezza UFCS, la Mobiliare, digitalswitzerland, HES-SO Valais-Wallis School of Management, HWZ Hochschule für Wirtschaft Zürich, SATW Schweizerische Akademie der Technischen Wissenschaften, YouGov
Berna e Zurigo, ottobre 2026

Questo lavoro è stato preparato con cura. Tuttavia, in nessun caso e nemmeno nell'ambito del presente lavoro, autrici, autori e partner di ricerca partecipanti si assumono alcuna responsabilità per la correttezza delle informazioni, dei riferimenti e dei consigli o per eventuali errori di stampa.

Tutti i diritti, inclusi quelli della traduzione in altre lingue, sono riservati.

I diritti dei marchi citati sono di proprietà dei rispettivi titolari.

Senza l'autorizzazione scritta delle autrici e degli autori, nessuna parte di quest'opera può essere riprodotta in qualsiasi forma o trasmessa e/o tradotta in una lingua utilizzabile dalle macchine, in particolare dalle macchine per l'elaborazione dei dati.

Coordinamento della pubblicazione: Prof. Dr. Marc K. Peter,
HES-SO Valais-Wallis School of Management

Con la collaborazione di Thomas Burkhardt (YouGov), Michèle C. Kaufmann (YouGov), Kenza Leclerc (UFCS), Bettina Mavrommatis (UFCS) e David Torcasso (digitalswitzerland).

Layout: team Gestione media, la Mobiliare

Illustrazione: Livia Lüthi

Le diapositive contenenti tutti i risultati del sondaggio sono disponibili sui siti web dei partner dello studio o su cyberstudie.ch.