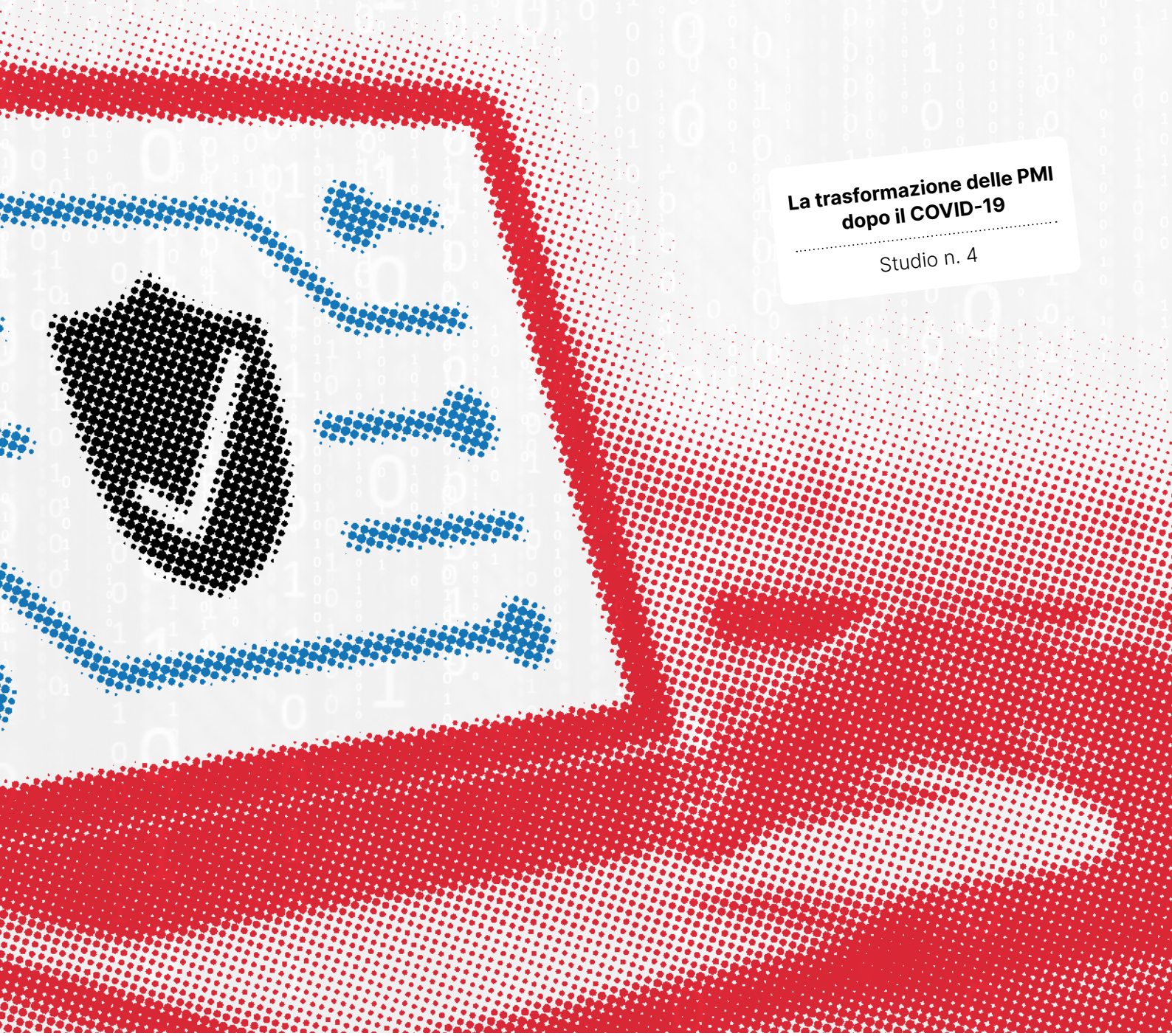
Home office e cyber sicurezza nelle PMI svizzere

Strategie e misure adottate dalle PMI svizzere con 4–49 collaboratori nel 2023

Marc K. Peter, Kristof A. Hertig, Andreas W. Kaelin,
Karin Mändli Lerch, Patric Vifian & Nicole Wettstein



La trasformazione delle PMI dopo il COVID-19

Studio n. 4

la Mobiliare
satw
digitalswitzerland
ALLIANZ DIGITALE SICHERHEIT SCHWEIZ
n|w Fachhochschule Nordwestschweiz Hochschule für Wirtschaft
gfs-zürich MARKT- & SOZIALFORSCHUNG

Colophon

Marc K. Peter, Kristof A. Hertig, Andreas W. Kaelin,
Karin Mändli Lerch, Patric Vifian et Nicole Wettstein:
Home office e cyber sicurezza nelle PMI svizzere:
strategie e misure adottate dalle PMI svizzere
con 4–49 collaboratori nel 2023
La Mobiliare, digitalswitzerland, Hochschule für Wirtschaft FHNW,
Accademia svizzera delle scienze tecniche SATW,
Alleanza Sicurezza Digitale Svizzera ASDS, gfs-zürich
Berna, settembre 2023

Coordinamento della pubblicazione: Prof. Dr. Marc K. Peter,
Hochschule für Wirtschaft FHNW (www.fhnw.ch/wirtschaft)
Con la collaborazione di Mara Huber e Joël Grosjean (gfs-zürich)
nonché di Johan Lindeque (Hochschule für Wirtschaft FHNW).

Layout: Polarstern SA, Soletta e Lucerna (www.polarstern.ch)

La serie di lucidi e il rapporto finale dettagliato sono disponibili sui siti web dei partner dello studio.

Sommario

Introduzione e informazioni importanti

Nella primavera del 2022 sono state revocate le ultime misure legate al COVID-19 e la Svizzera è lentamente tornata alla normalità. Ma proprio mentre sopraggiungeva finalmente una certa distensione, ecco che è scoppiata una guerra in Europa, che ha prospettato la possibilità di una penuria di energia. È stata nuovamente ventilata l'ipotesi di un ritorno all'home office, stavolta però per timori di uffici senza riscaldamenti.

Alla fine, questo nuovo ritorno in home office non si è reso necessario. Ad assumere una rilevanza del tutto nuova a causa della guerra è stato invece il tema del «cyber crimine»: gli attacchi di hacker russi alle infrastrutture occidentali sono infatti finiti in prima pagina. E dopo il videodiscorso di Zelensky alle Camere federali del 15 giugno 2023, anche la Svizzera è stata presa di mira. A quel punto la ricerca sul campo del presente studio era però già terminata. Anche il grave data breach presso una società di software bernese, in seguito al quale la Confederazione ha perso dati sensibili, non ha inciso in alcun modo sui risultati qui riportati.

Il quarto studio relativo agli effetti della crisi legata al COVID-19 su digitalizzazione e cyber sicurezza delle PMI svizzere è stato eseguito in questo contesto. Sono stati intervistati telefonicamente 502 dirigenti di PMI (da 4 a 49 collaboratori).

I principali risultati dello studio sono riassunti in dodici capitoli con altrettanti grafici. Il rapporto completo del progetto può essere ottenuto sui siti web dei partner dello studio (vedasi riquadro).

1. **Quanti dei suoi collaboratori potrebbero teoricamente lavorare in home office?**
Dal 2020 il numero dei posti compatibili con l'home office è diminuito di anno in anno. La percentuale delle PMI in cui una parte dei collaboratori o tutti i collaboratori possono lavorare da casa è scesa dal 67 % (nel 2020) al 56 % (nel 2023).

2. **Quanti dei suoi collaboratori lavorano in home office?**
Circa due quinti (42 %) dei collaboratori delle imprese in cui l'home office è possibile lavorano in parte o principalmente da casa. Come già emerso dagli studi preliminari, Ginevra e Zurigo si rivelano particolarmente favorevoli all'home office.

3. **Che ne sarà dell'home office nella sua impresa?**
Nel 2023, al termine di tutte le misure dovute alla pandemia, quasi tre quarti degli intervistati (73 %) si aspettano che la quota di collaboratori in modalità home office rimanga invariata a lungo termine. Sembra che il ricorso all'home office si sia affermato nella misura attuale nella maggior parte delle PMI.

4. **Quali mezzi di comunicazione digitali vengono impiegati nella sua impresa?**
L'utilizzo di tutte le tecnologie di comunicazione ha ricevuto una valutazione inferiore nel 2023 rispetto al 2022. Secondo i dirigenti intervistati, i tool di conferenza online vengono impiegati con una minore frequenza (45 %) rispetto al 2022 (62 %) e al 2021 (64 %).

5. **Si avvale di un fornitore di servizi IT?**
La maggior parte delle PMI (79 %) fa affidamento su fornitori esterni di servizi IT. Le PMI che dispongono almeno di un fornitore esterno di servizi IT delegano a questi circa un terzo (36 %) dei propri lavori IT. La metà dei fornitori di servizi IT vanta già una certificazione della sicurezza IT.

6. **Qual è il suo grado di soddisfazione in merito al suo fornitore di servizi IT?**
Circa una PMI su sette (14 %) ha sostituito il proprio fornitore di servizi IT negli ultimi uno-due anni. Nove PMI su dieci (91 %) che non hanno cambiato il proprio fornitore di servizi si ritengono (molto) soddisfatte. I fornitori di servizi IT hanno ricevuto le valutazioni migliori per la loro buona reperibilità e il rapido tempo di reazione.

7. **Ha già subito un attacco da parte di cyber criminali?**
Una PMI su dieci (11 %) ha già subito un attacco da parte di cyber criminali. Si è dunque reso necessario un notevole sforzo per rimediare ai danni subiti. Oltre la metà (55 %) degli intervistati che sono già stati oggetto di un attacco ha lamentato un danno economico. Circa un ottavo (13 %) ha dichiarato di aver subito perdite di dati dei clienti o danni alla reputazione.

8. Come valuta la cyber criminalità?
Secondo gli intervistati, la cyber criminalità è un problema da prendere sul serio (valore medio di 4,7 su una scala di 5 punti). Inoltre, ritengono importanti le misure contro i cyber attacchi (4,5). Più le PMI sono aperte e in sintonia con le tecnologie, maggiore è la valutazione sia dei rischi sia della necessità di adottare delle misure.

9. È informata/o sul tema della cyber sicurezza?
Un po' più della metà (56%) dei dirigenti intervistati si sente piuttosto oppure molto ben informato (valori 4–5 su una scala di 5 punti). Circa due terzi (65%) degli interpellati considerano il tema della cyber sicurezza piuttosto importante o molto importante. Pressoché un settimo (14%) degli intervistati considera invece la cyber sicurezza poco importante o per niente importante.

10. Quali misure tecniche vengono adottate nella sua impresa?
Il grado di implementazione delle varie misure necessarie si attesta a 3,9 e a 4,5 (su una scala di 5 punti) ed è praticamente invariato rispetto ai due anni precedenti. I pionieri hanno attuato più misure degli Early Follower che, a loro volta, ne hanno implementate in quantità maggiore rispetto ai Late Follower.

11. Quali misure organizzative vengono adottate nella sua impresa?
Come già rilevato negli anni precedenti, le misure organizzative vengono ancora attuate in misura significativamente inferiore rispetto a quelle tecniche. Le due misure organizzative adottate più raramente sono la formazione periodica dei collaboratori (2,9 su una scala di 5 punti) e l'esecuzione di audit sulla sicurezza (2,8).

12. Come sarà il futuro della sua impresa per quanto riguarda il tema della cyber sicurezza?
Quasi la metà (52%) degli intervistati ritiene piuttosto probabile o molto probabile di aumentare le misure di sicurezza contro la cyber criminalità nei prossimi unotre anni. Le persone meglio informate sul tema della cyber sicurezza pianificano più misure contro la cyber criminalità (3,6 su una scala di 5 punti) rispetto a quelle meno informate (3,0).

Da quattro anni accompagniamo le PMI con questo studio. L'home office, la cyber sicurezza e la collaborazione con i fornitori di servizi IT sono sfide e, allo stesso tempo, fattori di successo. Le PMI che pianificano e attuano proattivamente queste tematiche potranno adottare con maggior successo le loro strategie digitali e correre rischi inferiori.

Con questo rapporto e i risultati dettagliati dello studio speriamo di fornire un contributo per analizzare la situazione attuale, comprendere i fenomeni e rafforzare le PMI.

Berna, settembre 2023

Marc K. Peter
Responsabile del centro di competenza Trasformazione digitale
Hochschule für Wirtschaft FHNW, Olten

Kristof A. Hertig
Program Lead Infrastructure & Cybersecurity
digitalswitzerland, Zurigo

Andreas W. Kaelin
Direttore Alleanza Sicurezza Digitale Svizzera ASDS, Zugo
Senior Advisor digitalswitzerland, Zurigo

Karin Mändli Lerch
Responsabile di progetto
gfs-zürich, Zurigo

Patric Vifian
Marketing Manager PMI
La Mobiliare, Berna

Nicole Wettstein
Responsabile del programma Cybersecurity
Accademia svizzera delle scienze tecniche
SATW, Zurigo

Il rapporto completo con tutti i dati e le tabelle può essere scaricato gratuitamente in formato PDF sui siti dei partner dello studio:

www.cyberstudie.ch
www.digitalswitzerland.com
www.kmu-transformation.ch
www.satw.ch
www.mobiliare.ch/studio-pmi

1. «Quanti dei suoi collaboratori potrebbero teoricamente lavorare in home office?»

Domanda pratica alla PMI:

I suoi collaboratori desiderano lavorare in home office? In caso affermativo, ha sviluppato un concetto di mondo del lavoro che definisca le regole del gioco?

Marc K. Peter, FHNW-HSW

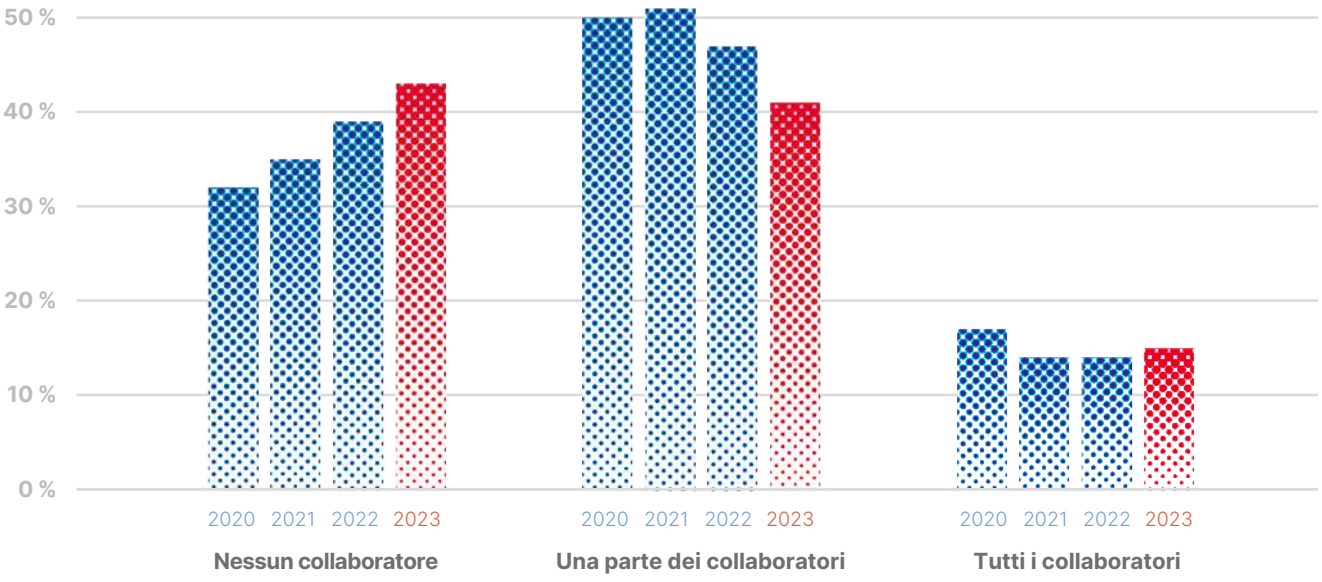
Nel 2020, quando questo studio è stato condotto per la prima volta, la prima fase obbligatoria dell'home office (COVID-19) si era già conclusa. Allora, circa un terzo (32%) dei dirigenti di PMI intervistati affermava che nessuno dei propri collaboratori poteva teoricamente lavorare in home office.

Dal 2020 il numero dei posti compatibili con l'home office è diminuito di anno in anno.

La metà (50%) dichiarava che una parte dei collaboratori poteva farlo. Circa un sesto (17%) sosteneva che tutti i collaboratori potevano teoricamente lavorare in home office.

Nel 2023 oltre due quinti (43%) degli intervistati hanno affermato che presso la propria impresa non fosse disponibile alcun impiego compatibile con l'home office. Altri due quinti all'incirca (41%) hanno indicato che una parte dei propri posti di lavoro fosse adatta per l'home office. Circa un settimo (15%) degli intervistati ha dichiarato che tutti i collaboratori potrebbero teoricamente lavorare in home office.

Il calo registrato dal 2020 al 2023 è significativo. Chi ha scritto questo studio parte dal presupposto che i datori di lavoro abbiano sempre più perso negli ultimi anni la loro opinione positiva riguardante l'home office, motivo per cui oggi ritengono che un numero inferiore dei loro posti di lavoro sia «teoricamente compatibile con l'home office». Ciò non significa però che in Svizzera il numero effettivo di attività compatibili con l'home office sia diminuito.



Numero di collaboratori dal 2020 al 2023 che potrebbero teoricamente lavorare da casa, poiché non devono ad esempio seguire i clienti in loco, guidare un veicolo o lavorare in un cantiere.

2. «Quanti dei suoi collaboratori lavorano in home office?»

Domanda pratica alla PMI:

Desidera che un numero sempre maggiore di collaboratori torni a lavorare in ufficio? In caso affermativo, che cosa offre loro affinché il lavoro in ufficio sia allettante?

Karin Mändli Lerch, gfs-zh

Vale ancora quanto affermato negli ultimi anni: la quota di collaboratori che lavorano in home office è più elevata per le PMI di minori dimensioni. Nelle PMI con 4–9 collaboratori, circa un quarto (24 % risp. 25 %) dei dipendenti lavora in parte o principalmente in home office. Nel complesso, dunque, circa la metà (49 %) dei collaboratori di questa classe di grandezza lavora almeno in parte in home office.

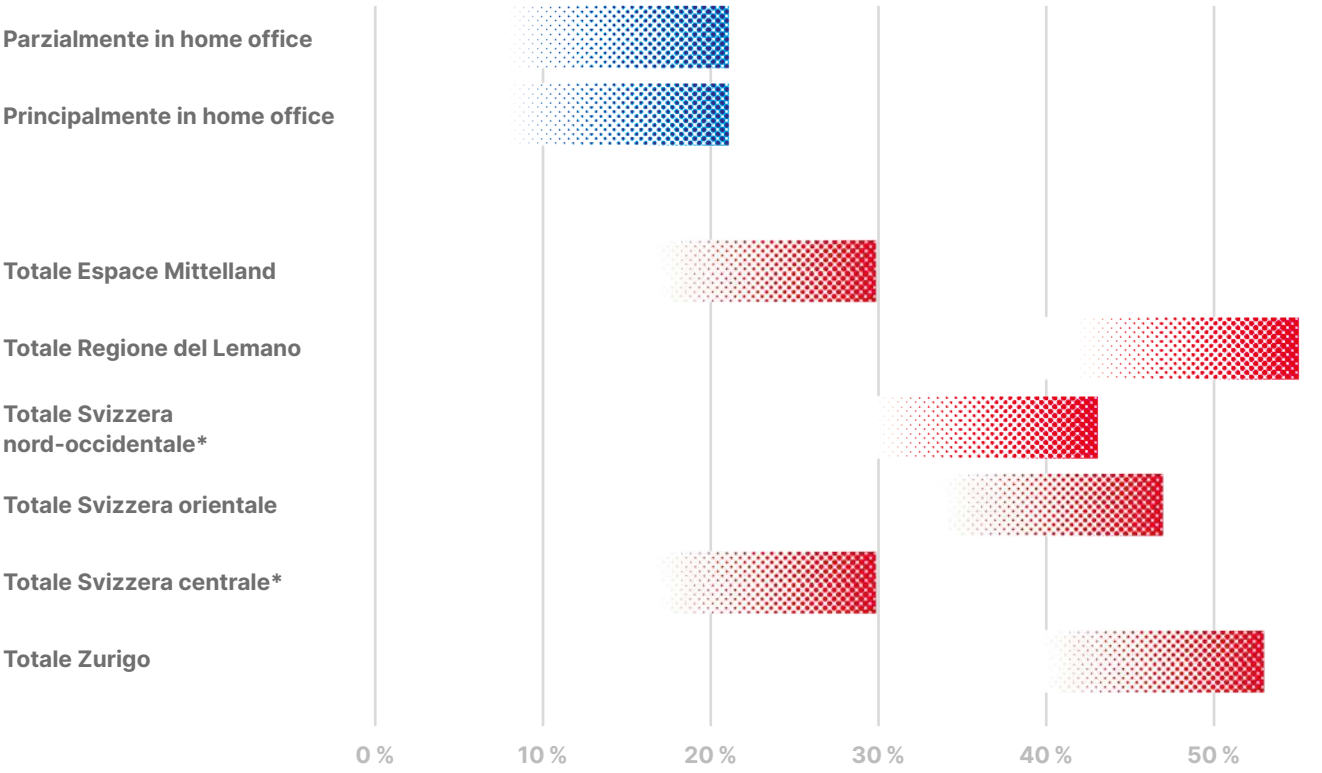
Circa due quinti (42 %) dei collaboratori lavorano in parte o principalmente in home office (in quelle aziende in cui almeno una persona può lavorare da casa).

Nelle PMI con 10–19 collaboratori, circa un settimo (14 %) dei dipendenti lavora in parte o principalmente in home office. Per le PMI con 20–49 collaboratori, questa quota è pari a poco più di un sesto (18 % risp. 17 %).

Nel sondaggio più recente, le possibilità di risposta sono state suddivise in «In parte» e «Principalmente», il che avrebbe potuto comportare una valutazione diversa e quindi un atteggiamento differente degli intervistati per quanto riguarda le risposte.

Dopo il lockdown del 2020, il 16 % dei collaboratori dei dirigenti intervistati lavorava principalmente in home office. In seguito all'obbligo di lavoro in home office del 2021, questa percentuale ammontava ancora al 20 %, mentre nel 2022 solo al 12 %. Nel 2023 è salita nuovamente al 21 %, attestandosi quasi al doppio rispetto al minimo del 2022, raggiungendo pressoché la stessa quota del 2021. Gli autori suppongono che negli ultimi tre anni si sia sviluppata una nuova interpretazione del termine «principalmente».

Come già emerso dagli studi preliminari, Ginevra e Zurigo si rivelano particolarmente favorevoli all'home office.



Numero di collaboratori (in percentuale del totale dei collaboratori) che lavorano in parte e principalmente in home office (nelle PMI in cui almeno una persona può lavorare da casa; il Ticino, in quanto sottogruppo con meno di 20 partecipanti allo studio, non compare sul grafico).

3. «Che ne sarà dell'home office nella sua impresa?»

Domanda pratica alla PMI:

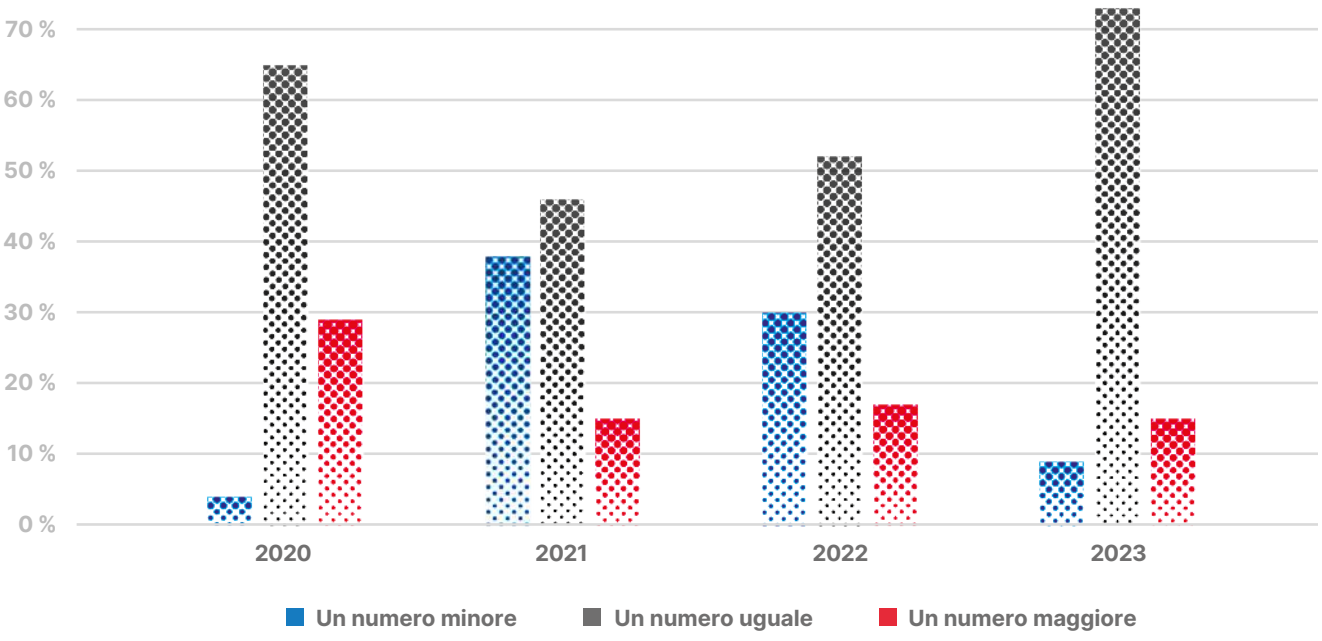
In che misura pianifica di ricorrere all'home office nella sua PMI? Parte dal presupposto che la situazione si sia nuovamente stabilizzata dopo il COVID-19?

Andreas W. Kaelin, ASDS

La valutazione della possibile variazione a lungo termine della quota di collaboratori che lavorano in home office è costantemente cambiata dal 2020. Subito dopo la prima fase obbligatoria dell'home office, che è andata di pari passo con il lockdown generale, quasi un terzo (29%) dei dirigenti intervistati si aspettava un aumento a lungo termine della quota di home office. Dopo la seconda fase obbligatoria dell'home office nel 2021, invece, oltre un terzo (38%) degli intervistati presupponeva che a lungo termine meno collaboratori avrebbero lavorato in home office e solo circa un intervistato su sette (15%) si attendeva un aumento. Nel 2022 quasi un terzo (30%) ha messo in conto una riduzione della quota di home office, mentre poco più di un sesto (17%) si aspettava un incremento.

Solo circa una persona su dieci (9%) prevede una riduzione e una su sette un aumento. Sembra dunque che la situazione si sia leggermente stabilizzata, in misura simile in tutti i sottogruppi.

Nel 2023, al termine di tutte le misure legate alla pandemia, quasi tre quarti degli intervistati (73 %) si aspettano che la quota di home office rimanga invariata a lungo termine.



Valutazione del numero di collaboratori che in futuro lavoreranno da casa: di più, uguale o di meno (nelle PMI in cui almeno una persona può lavorare da casa).

4. «Quali mezzi di comunicazione digitali vengono impiegati nella sua impresa?»

Domanda pratica alla PMI:

Come impiega le tecnologie di comunicazione? Esiste un piano per una comunicazione più efficiente? Inoltre, prende in considerazione il tema della cyber sicurezza?

Nicole Wettstein, SATW

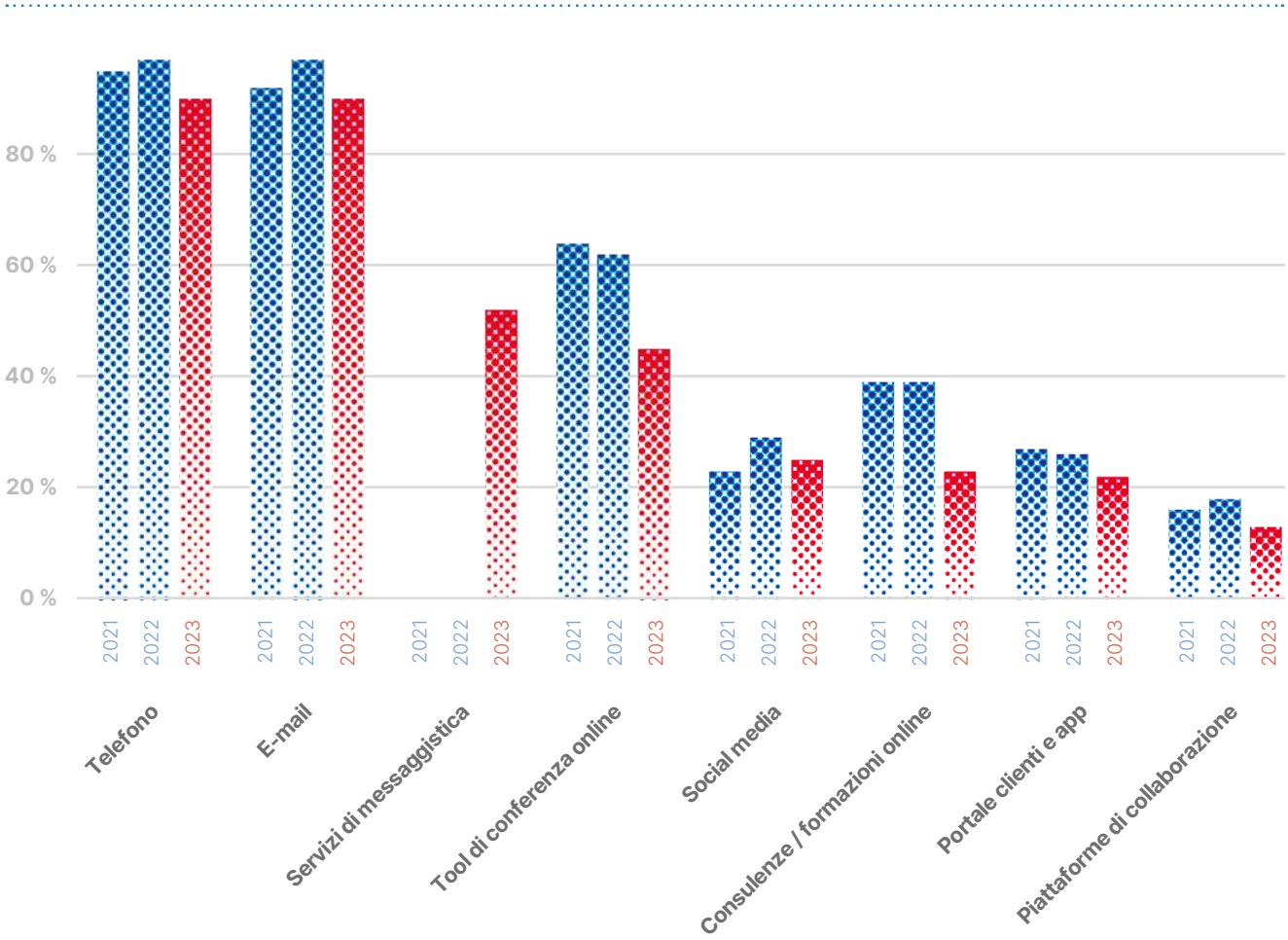
Anche nel 2023, come già accadeva negli studi precedenti, telefono ed e-mail (rispettivamente al 90%) sono i mezzi di comunicazione più utilizzati dalle PMI intervistate. Rispetto agli studi precedenti ci sono solo variazioni marginali.

L'utilizzo di tutte le tecnologie di comunicazione ha ricevuto una valutazione inferiore nel 2023 rispetto al 2022. Ciò è evidente in particolare per i servizi di messaggistica come WhatsApp, Signal, Threema, Wire ecc. che in passato erano oggetto di domande separate: negli studi precedenti il solo WhatsApp veniva menzionato già da quasi due terzi degli intervistati (60% nel 2022 e 62% nel 2021). Nel presente sondaggio, invece, è stato citato insieme a Signal, Threema, Wire ecc. solo da circa la metà (52%) degli interpellati.

Pure l'impiego di consulenze o formazioni online è decisamente diminuito (2021: 39%, 2022: 39%, 2023: 23%) così come il ricorso alle piattaforme di collaborazione quali Slack, Confluence o SharePoint. In media sono stati indicati 3,6 mezzi di comunicazione diversi.

Secondo i dirigenti intervistati, anche i tool di conferenza online come Skype, Teams, Zoom o Google Meet vengono utilizzati più raramente (45 %) rispetto al 2022 (62 %) e al 2021 (64 %).

Maggiore è il numero dei collaboratori che possono teoricamente lavorare in home office, più sono i mezzi di comunicazione utilizzati nelle PMI intervistate.



Impiego dei mezzi di comunicazione digitali nelle PMI svizzere dal 2021 al 2023.

5. «Si avvale di un fornitore di servizi IT?»

Domanda pratica alla PMI:

Il suo fornitore di servizi IT dispone di una certificazione della sicurezza? In caso negativo, come verifica le relative competenze in fatto di cyber sicurezza?

Andreas W. Kaelin, ASDS

Quest'anno abbiamo chiesto per la prima volta alle PMI se collaborano con un fornitore di servizi IT. La maggior parte di esse fa affidamento su un singolo fornitore di servizi IT (44%). Circa un terzo viene assistito da più fornitori di servizi IT (35%). Circa un dirigente su cinque ha affermato di non disporre di alcun fornitore di servizi IT (21%).

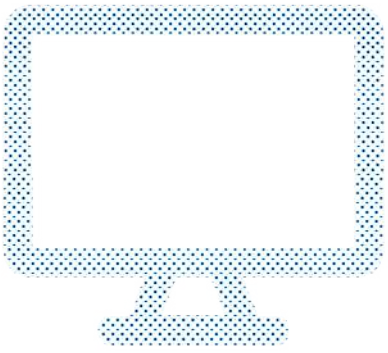
Le PMI che dispongono di almeno un fornitore esterno di servizi IT delegano a questi circa un terzo (36%) dei lavori IT. La maggior parte (84%) delle PMI che hanno affermato di collaborare con almeno un fornitore esterno di servizi IT viene da questi consigliata e assistita anche in fatto di cyber sicurezza.

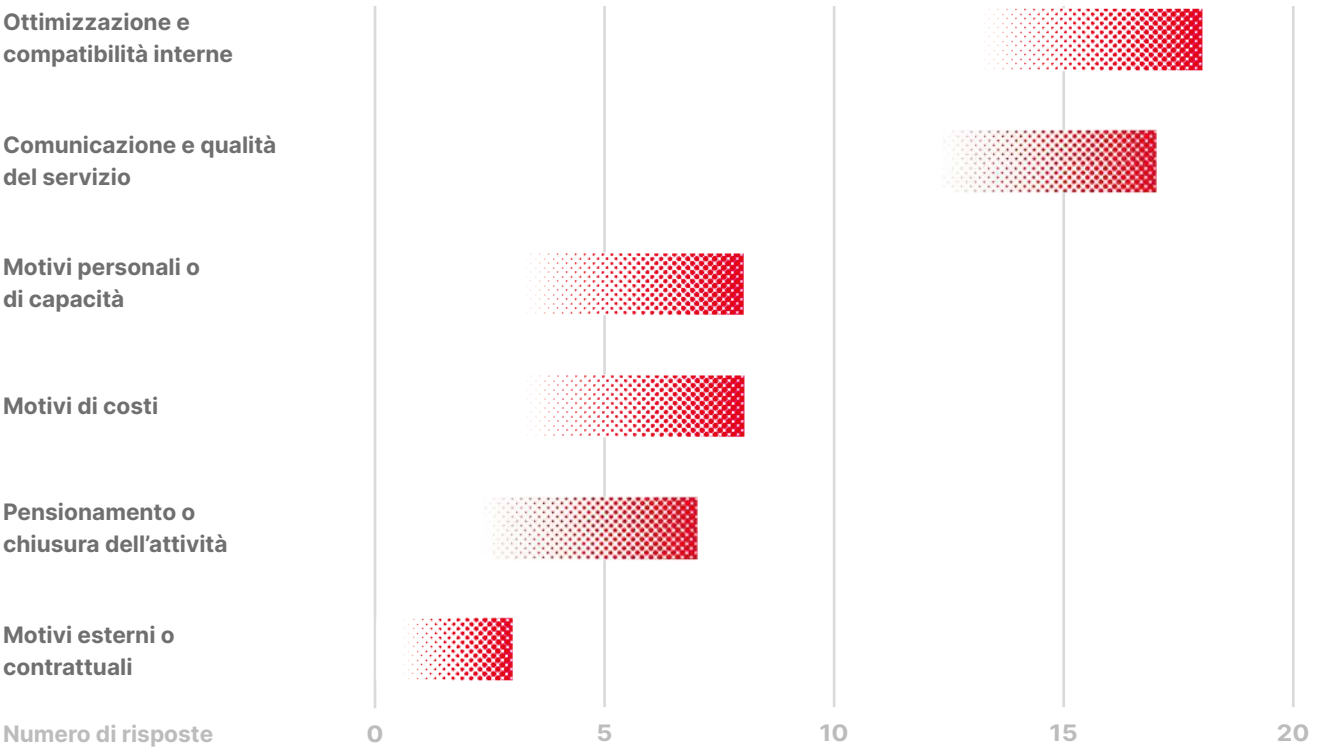
La quota dei fornitori di servizi IT con certificazione della sicurezza è dunque rimasta pressoché invariata rispetto al 2022. Colpisce a tal proposito l'elevata percentuale di intervistati (34%) che non hanno voluto o potuto rispondere alla rispettiva domanda.

Le PMI che negli ultimi uno-due anni hanno sostituito il proprio fornitore di servizi IT hanno proceduto a tale cambiamento soprattutto per motivi interni di ottimizzazione e compatibilità (ad esempio a causa dell'acquisto di un nuovo software o di un nuovo server) nonché in seguito a un certo grado di insoddisfazione per quanto riguarda comunicazione e qualità del servizio. Sono stati citati anche motivi personali, di capacità o di costi. Per la maggior parte delle PMI (64%) questo cambiamento sembra essere stato (molto) semplice.

La metà (53 %) dei fornitori di servizi IT dispone di una certificazione della sicurezza informatica come, ad esempio, ISO 27001.

Circa una PMI su sette (14 %) ha sostituito il proprio fornitore di servizi IT negli ultimi uno-due anni.



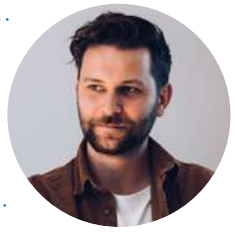


Motivi nel 2023 (numero di risposte) per cui i dirigenti hanno sostituito il proprio fornitore di servizi IT negli ultimi uno-due anni (nelle PMI che negli ultimi uno-due anni hanno sostituito il proprio fornitore di servizi IT; più risposte possibili).

6. «Qual è il suo grado di soddisfazione in merito al suo fornitore di servizi IT?»

Domanda pratica alla PMI:

I fornitori di servizi IT, in quanto partner strategici, possono fornire molto valore aggiunto. Ha già riflettuto sul modo in cui potrebbe diventare più efficiente grazie al suo fornitore di servizi IT?



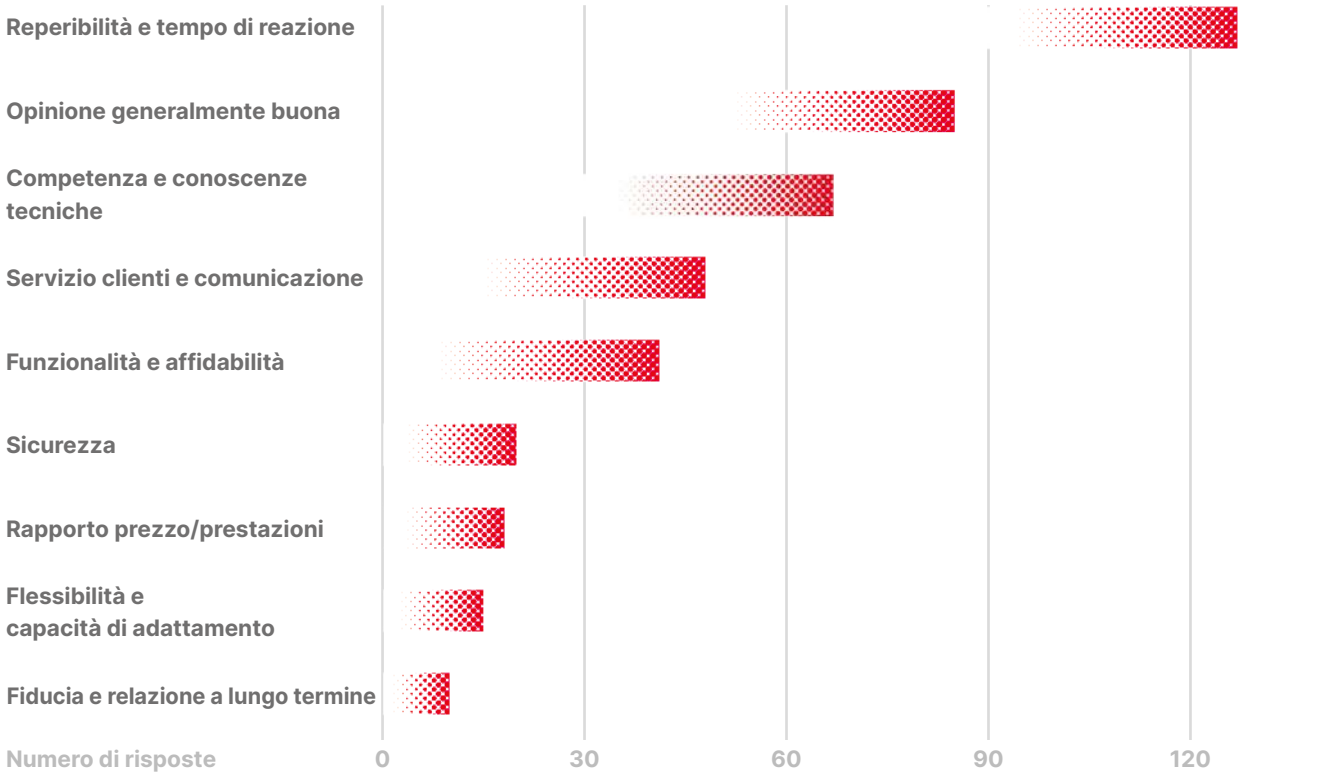
Kristof A. Hertig, digitalswitzerland

Le PMI che non hanno sostituito il proprio fornitore di servizi IT esibiscono un grado di soddisfazione molto elevato.

Nove PMI su dieci (91 %) hanno affermato di essere (molto) soddisfatte del proprio fornitore di servizi IT.

Il valore medio si attesta dunque a 4,5 su una scala da 1 (molto insoddisfatta/o) a 5 (molto soddisfatta/o). Dettaglio interessante: le PMI con un elevato grado di attuazione delle misure tecniche e organizzative per l'incremento della cyber sicurezza sono significativamente più spesso soddisfatte del loro fornitore di servizi IT rispetto alle PMI con un grado di attuazione inferiore.

I motivi più frequenti per cui le PMI sono soddisfatte del proprio fornitore di servizi IT sono la reperibilità e il tempo di reazione, la buona reputazione («Opinione generalmente buona») nonché la competenza e le conoscenze tecniche del fornitore di servizi IT.



Motivi nel 2023 per cui i dirigenti sono soddisfatti del proprio fornitore di servizi IT (nelle PMI che negli ultimi uno-due anni non hanno sostituito il proprio fornitore di servizi IT).

7. «Ha già subito un attacco da parte di cyber criminali?»

Domanda pratica alla PMI:

Una PMI su dieci ha già subito un attacco andato a buon fine. Dispone di un piano d'emergenza nel caso di un cyber attacco?

Karin Mändli Lerch, gfs-zh

Circa una persona intervistata su dieci (11%) ha dichiarato che la propria PMI ha già subito un attacco da parte di cyber criminali che ha richiesto un notevole sforzo per rimediare ai danni.

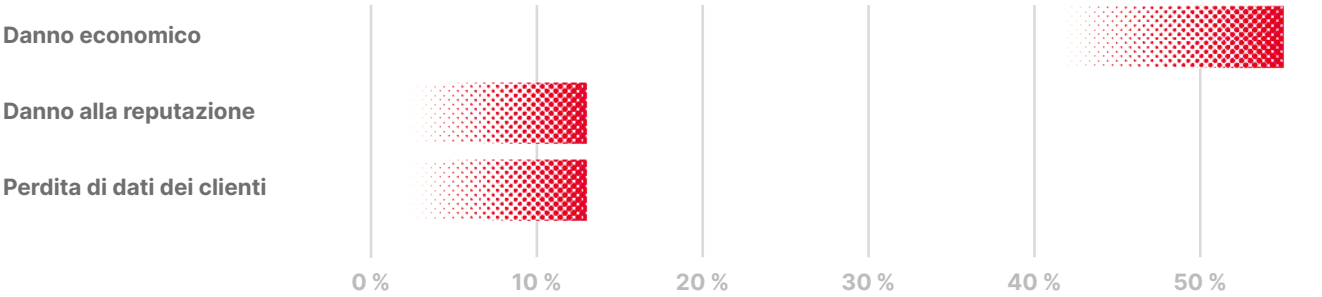
Non si registrano differenze tra i settori: i cyber attacchi possono colpire qualsiasi PMI.

Oltre la metà (55%) degli intervistati che sono già stati oggetto di un attacco ha lamentato un danno economico. Ciò corrisponde a circa il 6% del campione totale e significherebbe che il 6% delle PMI svizzere con 4–49 collaboratori ha già subito un danno economico in seguito a un cyber attacco.

Circa un ottavo (13%) degli intervistati che è già stato colpito ha subito una perdita dei dati dei clienti o un danno alla reputazione.

Una su sette (14%) considera piuttosto alto o molto alto il rischio di essere messa «fuori combattimento» per almeno un giorno a causa di un cyber attacco.

Una persona intervistata su dieci (10 %) ha affermato che la propria PMI è stata oggetto già una volta di un'estorsione da parte di cyber criminali.



Danni causati da un cyber attacco riuscito (solo per le PMI che hanno già subito una volta un attacco da parte di cyber criminali).

8. «Come valuta la cyber criminalità?»

Domanda pratica alla PMI:

I rischi dovuti ai cyber criminali sono noti, ma l'attuazione delle misure è troppo esigua. Che cosa potrebbe spingerla a implementare ulteriori misure?

Marc K. Peter, FHNW-HSW

Le sette domande relative alla cyber criminalità hanno ricevuto nel 2023 quasi le stesse risposte degli anni precedenti. Un elevato consenso ottengono le affermazioni «La cyber criminalità è un problema da prendere sul serio» (4,7), «Le misure contro i cyber attacchi sono importanti» (4,5) e «Sono consapevole delle minacce della cyber criminalità».

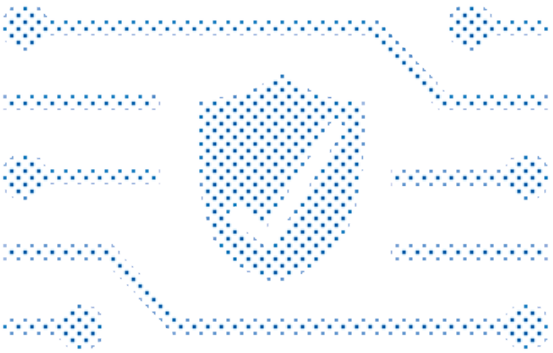
Gli intervistati sono meno d'accordo con le affermazioni «Le misure contro i cyber attacchi possono essere attuate in maniera semplice» (3,4) e «I miei colleghi pensano che la mia impresa debba proteggersi dai cyber attacchi» (3,2). Si può dunque affermare che la situazione è restata invariata rispetto ai due anni precedenti.

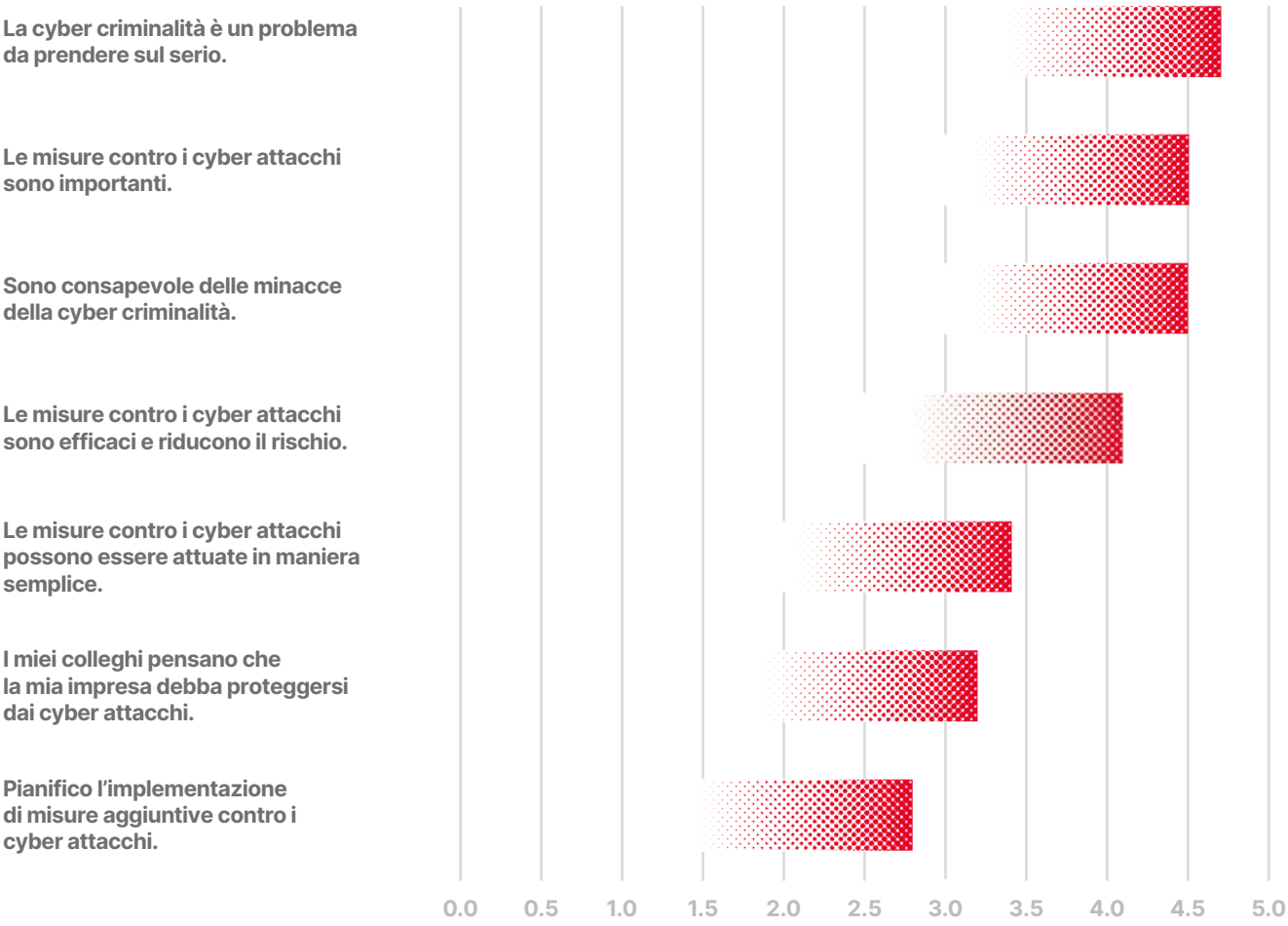
I motivi contrari alle misure possono risiedere nella rispettiva difficoltà di attuazione oppure nel fatto che gli intervistati non percepiscono la pressione sociale all'interno della PMI (ad esempio dei colleghi del comitato di direzione).

Inoltre, per tutte le affermazioni vale quanto segue: maggiore è l'attuazione tecnica od organizzativa delle misure di sicurezza, più elevato è anche il consenso in merito alle affermazioni.

Inoltre, più le PMI sono aperte e in sintonia con le tecnologie, maggiore è il loro consenso in merito alle varie affermazioni.

Il rischio della cyber criminalità è sì noto, ma le relative misure vengono pianificate solo da una minoranza degli intervistati.



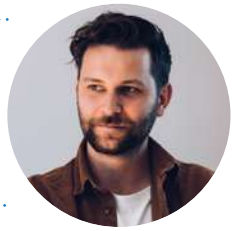


Consenso dei dirigenti delle PMI svizzere in merito alle affermazioni elencate (su una scala da 1 = per niente – a 5 = pienamente).

9. «È informata/o sul tema della cyber sicurezza?»

Domanda pratica alla PMI:

la cyber sicurezza è una costante ai giorni nostri. Quanto si sente informata/o sulla tematica e come si informa? Conferenze, formazioni continue e colloqui con il suo fornitore di servizi IT possono essere d'aiuto.



Kristof A. Hertig, digitalswitzerland

Poco più della metà (56%) dei dirigenti intervistati si sente piuttosto informata o molto bene informata sulla tematica dei cyber rischi (valori 4–5 su una scala di 5 punti). Questo valore è leggermente ma continuamente migliorato rispetto agli ultimi anni (2020: 47%).

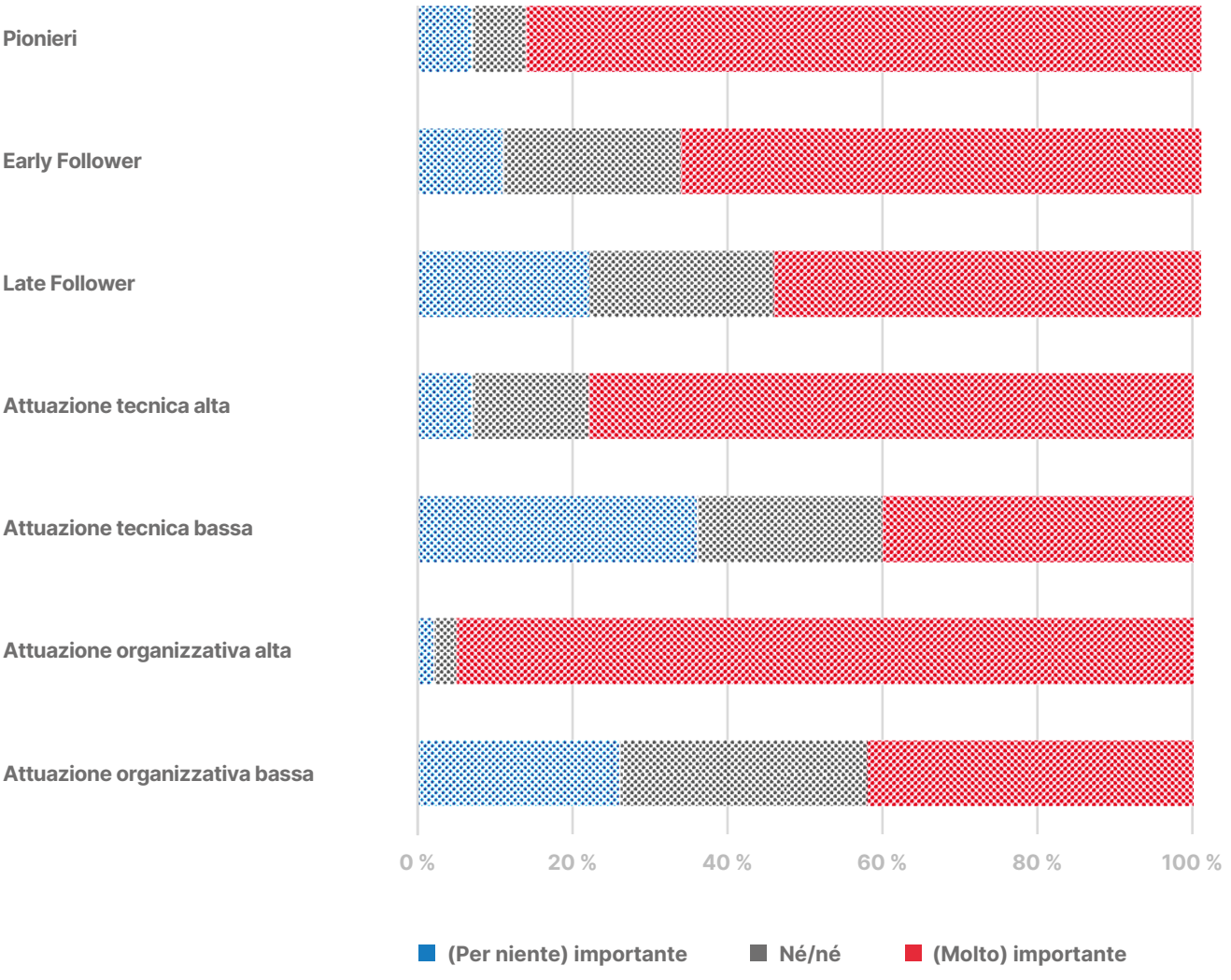
I pionieri che utilizzano precocemente le tecnologie digitali si sentono meglio informati.

I pionieri (4,2) si sentono significativamente meglio informati degli Early Follower (3,6) e questi, a loro volta, decisamente meglio informati dei Late Follower (3,3).

Particolarmente alte e significative sono le differenze tra le PMI che hanno attuato solo poche rispettivamente già molte misure di sicurezza tecniche e organizzative. Più di due terzi (69%) degli intervistati delle imprese con un elevata attuazione delle misure tecniche si sentono ben informati; tuttavia, per le PMI con un basso grado di implementazione delle misure tecniche questa quota scende a solo circa un quarto (26%).

Quasi due terzi (65%) degli intervistati ritengono che il tema della cyber sicurezza sia piuttosto importante o molto importante e circa un settimo (14%) lo considera piuttosto poco importante o per niente importante.

La cyber sicurezza viene considerata molto importante e la relativa valutazione è praticamente invariata dal 2020.



Valutazione del tema della cyber sicurezza nel 2023 nelle categorie
(su una scala da 1+2 = per niente importante/piuttosto poco importante, 3 = né/né fino a 4+5 = molto importante).

10. «Quali misure tecniche vengono adottate nella sua impresa?»

Domanda pratica alla PMI:

I pionieri che utilizzano precocemente le tecnologie digitali sono meglio protetti. Ha attuato nella sua PMI anche misure tecniche?

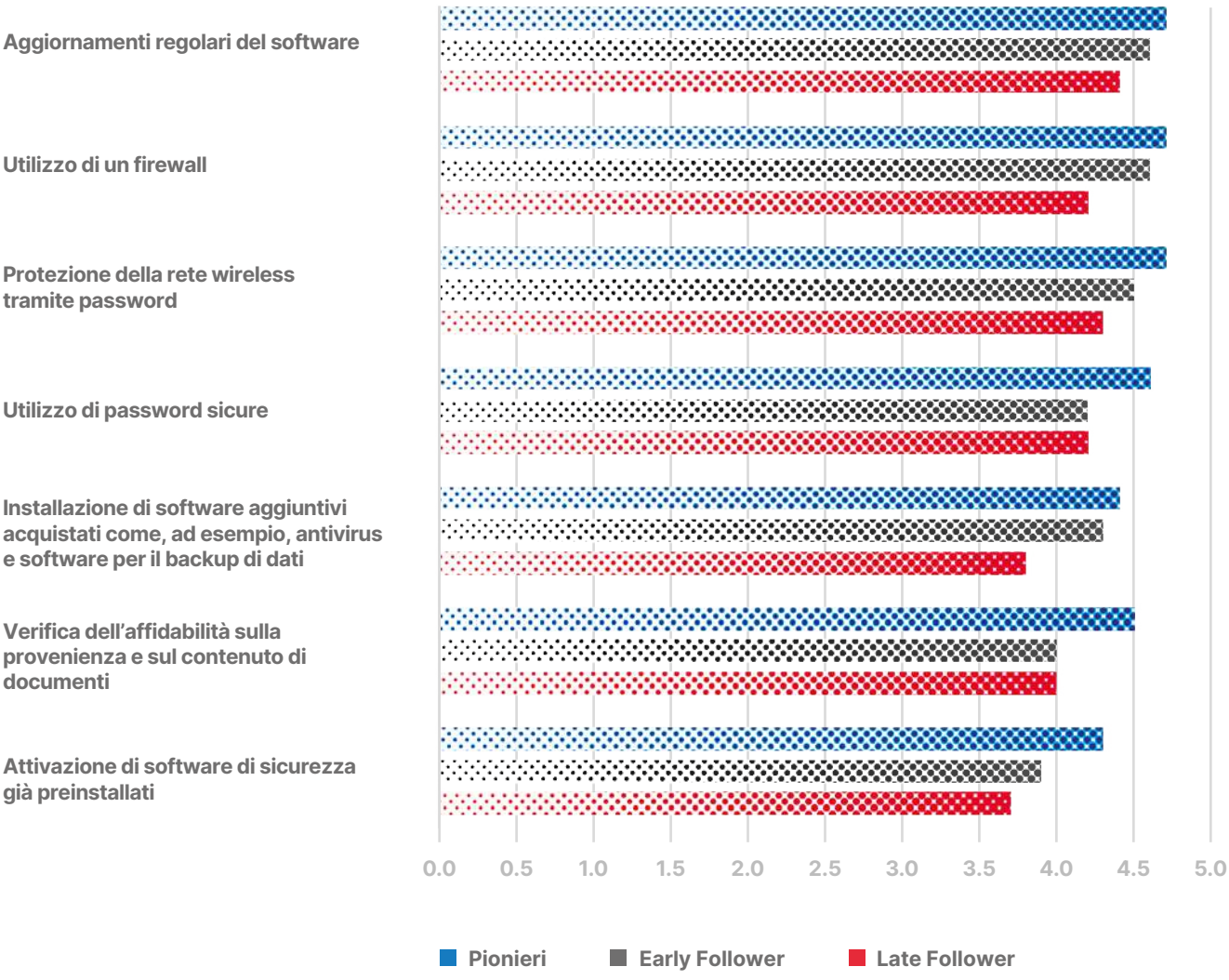
Patric Vifian, la Mobiliare

I gradi di implementazione delle diverse misure adottate si collocano tra 3,9 e 4,5 (su una scala di 5 punti), tutti su un livello praticamente invariato rispetto al 2022 e al 2021. Il maggiore grado di implementazione viene ottenuto dalle due misure «Aggiornamenti regolari del software» e «Utilizzo di un firewall» (entrambe 4,5).

Per tutte le misure si applica in modo significativo quanto segue (come negli anni precedenti): più è elevato il grado di informazione in materia di cyber sicurezza, maggiore è l'attuazione delle misure.

Tutte le misure sono stata attuate più spesso dalle aziende con 20–49 collaboratori rispetto a quelle con 4–9 rispettivamente 10–19 collaboratori.

I pionieri hanno attuato più misure degli Early Follower che, a loro volta, ne hanno implementate in quantità maggiore rispetto ai Late Follower.



Attuazione delle misure tecniche di cyber sicurezza nelle PMI svizzere 2023 (su una scala da 1 = per niente a 5 = pienamente).

11. «Quali misure organizzative vengono adottate nella sua impresa?»

Domanda pratica alla PMI:

La cyber sicurezza è oggi un tema critico. Svolge una formazione regolare dei collaboratori e audit sulla sicurezza informatica?

Nicole Wettstein, SATW

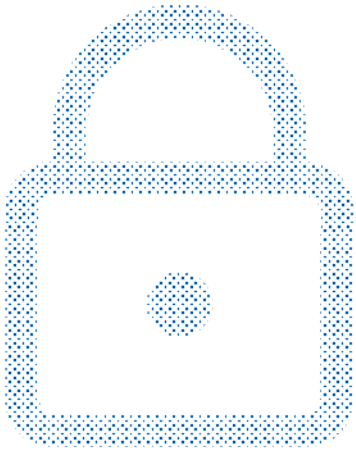
Come già rilevato negli anni precedenti, le misure organizzative vengono ancora attuate in misura significativamente inferiore rispetto a quelle tecniche. La misura organizzativa maggiormente implementata è il controllo del ripristino del backup (4,2), seguita dal comportamento prudente nella condivisione delle informazioni personali (4,2) e dalla sensibilizzazione dei collaboratori in merito alle e-mail di phishing (4,0). Le due misure organizzative attuate più raramente sono la formazione periodica dei collaboratori (2,9) e l'esecuzione di audit sulla sicurezza (2,8).

Le differenze sono tutte significative (vedasi grafico a Pagina 23).

Meglio gli intervistati si sentono informati in merito al tema dei cyber rischi, maggiore è la loro attuazione di misure organizzative. Particolarmente basso è il grado di implementazione della formazione periodica dei collaboratori tra le persone (piuttosto) disinformate (1,9).

Per quanto riguarda la maggior parte delle misure organizzative, queste vengono implementate dalle PMI più grandi piuttosto che da quelle più piccole.

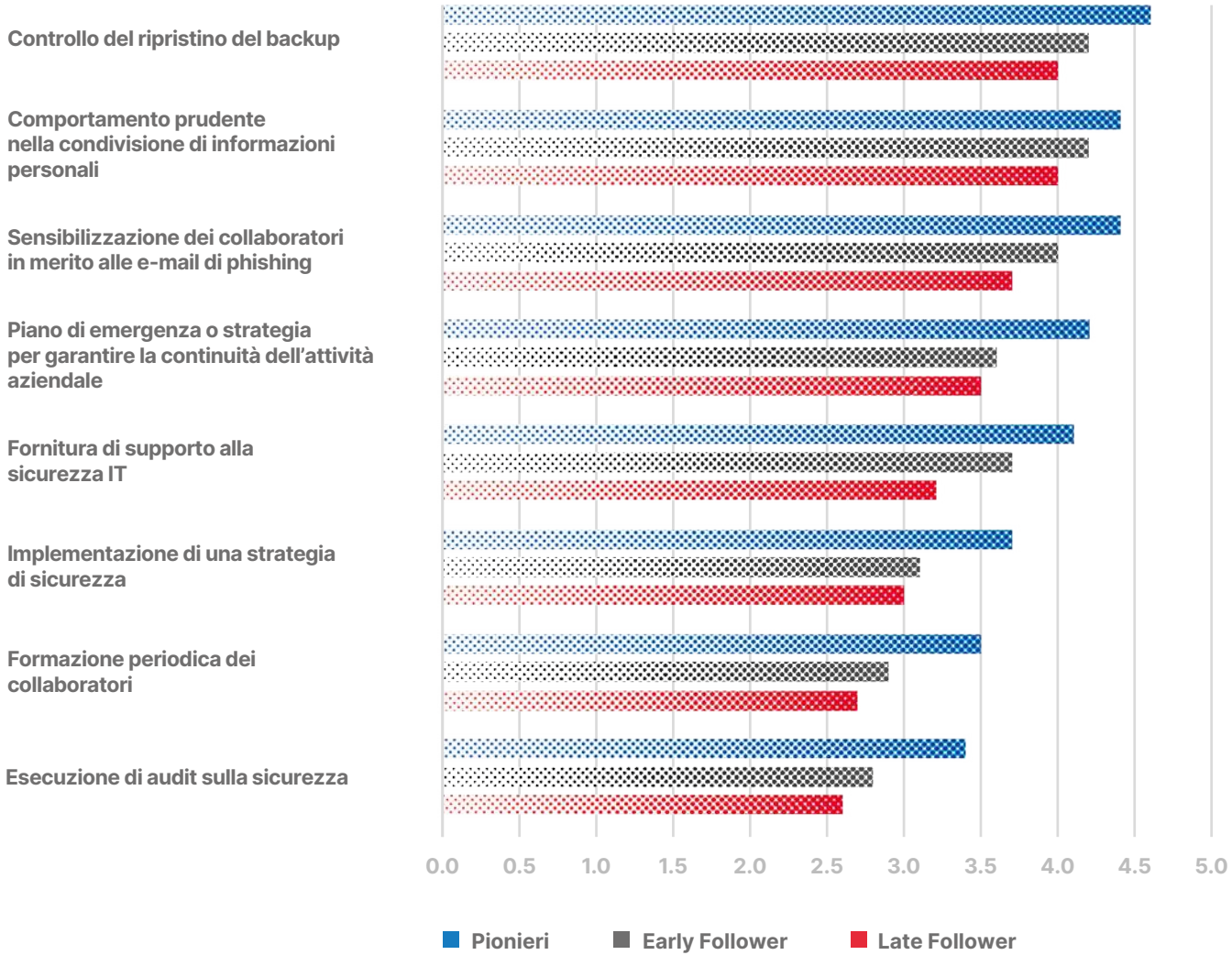
I pionieri hanno attuato la maggior parte delle misure organizzative, i Late Follower sono coloro che ne hanno implementate di meno.



Buono a sapersi: password

Quasi nove intervistati su dieci (89 %) hanno adottato almeno una misura di sicurezza riguardante la password. Tuttavia, ciò significa anche che circa una persona interpellata su dieci (11 %) non ha implementato alcuna misura corrispondente. Ecco come vengono attuate le misure di sicurezza riguardanti la password:

- cambiamento periodico delle password (60 %);
- autenticazione a due fattori (60 %);
- lunghezza minima della password di dodici caratteri (59 %);
- password diverse per ogni servizio (58 %);
- programma di gestione delle password (32 %).



Attuazione delle misure organizzative di cyber sicurezza nelle PMI svizzere 2023 (su una scala da 1 = per niente a 5 = pienamente).

12. «Come sarà il futuro della sua impresa per quanto riguarda il tema della cyber sicurezza?»

Domanda pratica alla PMI:

E come vede il suo futuro per quanto riguarda il tema della cyber sicurezza? È ben preparato per il futuro o necessiterebbe di ancora più misure per l'aumento della sicurezza informatica?

Patric Vifian, la Mobiliare

Circa la metà (52%) degli intervistati ritiene piuttosto probabile o molto probabile di aumentare le proprie misure di sicurezza contro la cyber criminalità nei prossimi uno-tre anni. La percentuale è pressoché invariata rispetto all'anno precedente (55%) e nettamente superiore a quella del 2021 (40%).

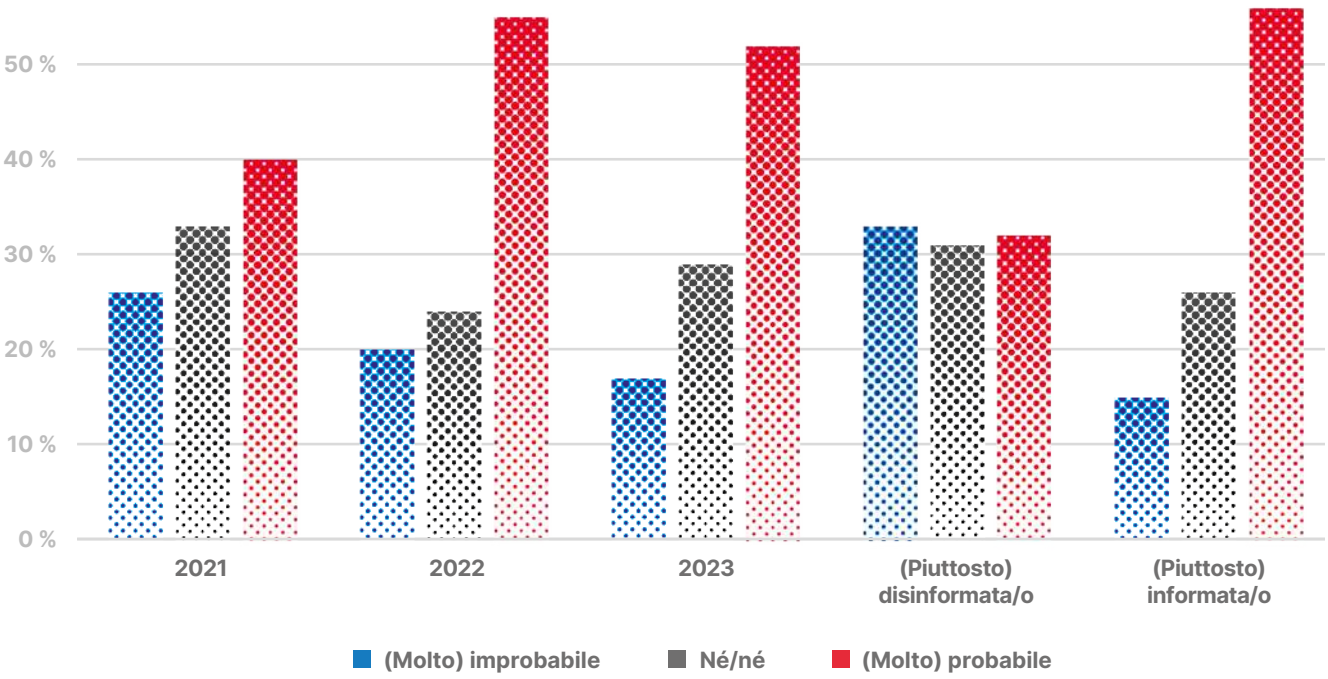
Più grande è la PMI, maggiore è la pianificazione delle misure future.

Il valore medio delle imprese più piccole intervistate (4–9 collaboratori) si attesta a 3,5 (su una scala di 5 punti), per le medie imprese (10–19 collaboratori) a 3,6 e per quelle più grandi (20–49 collaboratori) a 3,7.

Non ci sono differenze significative tra le grandi regioni e i settori, anche se la probabilità di aumentare le misure di sicurezza tende a essere leggermente più elevata per i settori Servizi finanziari e Informazione e comunicazione (3,9) rispetto agli altri (3,4–3,6).

Significativa è la differenza tra gli intervistati (piuttosto) disinformati (3,0) e quelli (piuttosto) informati (3,6). Anche i pionieri (4,0) e gli Early Follower (3,7) programmano decisamente più spesso un aumento delle misure di sicurezza rispetto ai Late Follower (3,2).

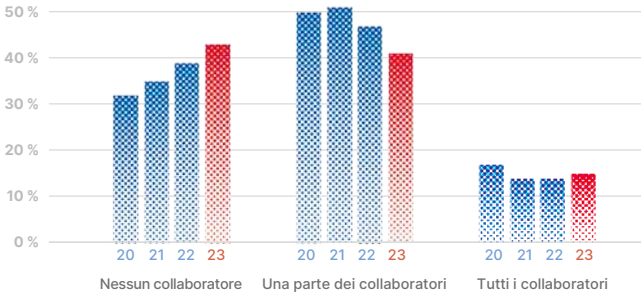
I dirigenti meglio informati sul tema della cyber sicurezza pianificano più misure.



Probabilità che le PMI aumentino le misure di sicurezza informatica contro la cyber criminalità nei prossimi uno-tre anni (su una scala da 1+2 = molto improbabile e improbabile, 3 = né/né fino a 4+5 = probabile e molto probabile).

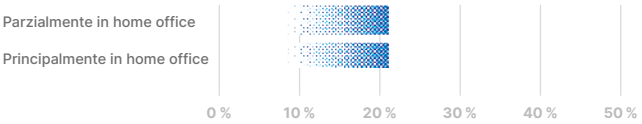
I grafici informativi principali su una pagina:

Collaboratori che teoricamente possono lavorare in home office



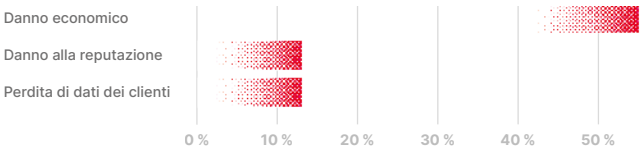
Numero di collaboratori dal 2020 al 2023 che potrebbero teoricamente lavorare da casa, poiché non devono ad esempio seguire i clienti in loco, guidare un veicolo o lavorare in un cantiere.

Collaboratori che attualmente lavorano in home office



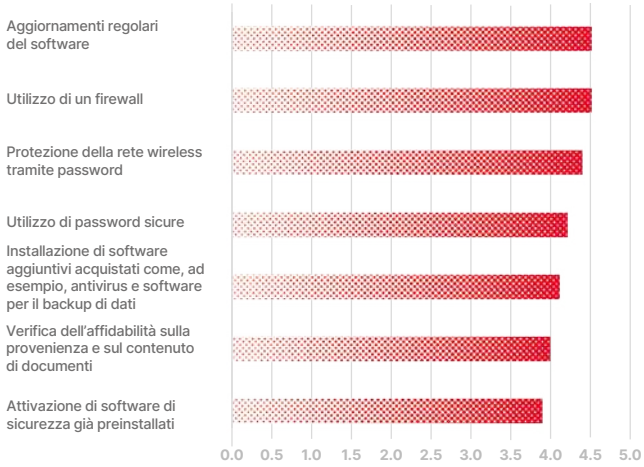
Numero di collaboratori (in percentuale del totale dei collaboratori) che lavorano in parte e principalmente in home office (nelle PMI in cui almeno una persona può lavorare da casa).

Danno dovuto a cyber attacchi



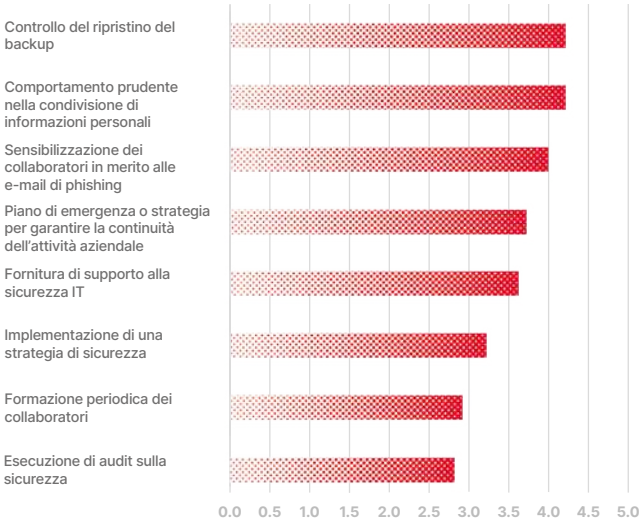
Danni causati da un cyber attacco riuscito (solo per le PMI che hanno già subito una volta un attacco da parte di cyber criminali).

Misure tecniche di cyber sicurezza implementate



Attuazione delle misure tecniche di cyber sicurezza nelle PMI svizzere 2023 (su una scala da 1 = per niente a 5 = pienamente).

Misure organizzative di cyber sicurezza attuate



Attuazione delle misure organizzative di cyber sicurezza nelle PMI svizzere 2023 (su una scala da 1 = per niente a 5 = pienamente).

Metodologia di ricerca

Il sondaggio telefonico mediante CATI (Computer Assisted Telephone Interviewing) è stato realizzato dal 18 aprile al 13 giugno 2023 presso i dirigenti di piccole imprese (da 4 a 49 collaboratori) nella Svizzera italiana, tedesca e francese.

La popolazione statistica rappresentata dal campione comprende circa 153 000 ditte con un organico da 4 a 49 collaboratori in tutte le regioni del Paese (UST/STATENT 2017). L'intervallo di confidenza del campione totale si colloca al +/– 4,4% con un livello di sicurezza del 95% (distribuzione 50/50). Il sondaggio mostra una rappresentazione strutturalmente identica della popolazione in riferimento alle dimensioni aziendali e alle regioni linguistiche. I risultati sono pertanto trasferibili alla popolazione statistica, tenendo conto dell'intervallo di confidenza.

Il campione è stato realizzato proporzionalmente alle dimensioni delle aziende. A tal fine, la ripartizione delle tre classi di grandezza (secondo il numero di collaboratori) è stata assicurata mediante il controllo delle quote. La ripartizione per grandi regioni è stata ottenuta mediante una prestratificazione degli indirizzi.

Il campione comprende 326 PMI con 4–9 collaboratori (campione: 65%/UST STATENT: 66%), 110 PMI con 10–19 collaboratori (22%/22%) e 66 PMI con 20–49 collaboratori (13%/12%). Gli indirizzi provengono da un broker di indirizzi svizzero con un potenziale di oltre 100 000 indirizzi (il che corrisponde a 2/3 della popolazione statistica).

I sottogruppi concernenti l'innovazione tecnica (pionieri, Early Follower e Late Follower) sono stati formati in base alle domande sull'adozione di nuove tecnologie:
- i pionieri sono sempre tra i primi che acquistano e utilizzano le nuove tecnologie e i nuovi apparecchi;
- gli Early Follower cominciano a utilizzare le nuove tecnologie e i nuovi apparecchi solo quando sono a conoscenza delle esperienze maturate dagli altri;
- i Late Follower acquisiscono le nuove tecnologie e i nuovi apparecchi solo quando sono per loro indispensabili.

Per i sottogruppi relativi alle attuazioni tecniche e organizzative di misure riguardanti la cyber sicurezza è stata calcolata la media di tutte le misure tecniche e organizzative (i valori medi da 1 a 3 sono sinonimo di bassa implementazione delle misure, il valore medio 4 di media implementazione delle misure e il valore medio 5 di alta implementazione delle misure).

Sono state contattate 37 376 PMI, di cui 21 636 non erano reperibili (ad esempio, rifiuto, nessuna risposta, telefono occupato o segreteria telefonica). Il tasso di risposta ammonta al 3,2% (a fronte di 502 interviste realizzate).

Indicazione generale sulla lettura dei grafici: i sottogruppi che comprendono meno di 30 interviste vengono contrassegnati per precauzione con un * al fine di evitare una sopravvalutazione. I sottogruppi con $n \geq 20$ vengono rappresentati, mentre quelli con $n < 20$ non più. Le percentuali sono arrotondate ai numeri interi, pertanto potrebbero sussistere piccole differenze di arrotondamento. L'opzione «Non so/nessuna risposta» non è stata indicata ai fini della leggibilità dei grafici, motivo per cui talvolta la somma di tutte le risposte non ammonta al 100%.

Contatto / Autori

Prof. Dr. Marc K. Peter
Responsabile del centro di competenza Trasformazione digitale
FHNW für Wirtschaft, Olten
marc.peter@fhnw.ch

Kristof A. Hertig
Program Lead Infrastructure & Cybersecurity
digitalswitzerland, Zurigo
kristof@digitalswitzerland.com

Andreas W. Kaelin
Direttore Alleanza Sicurezza Digitale Svizzera ASDS, Zug
Consigliere anziano, digitalswitzerland, Zurigo
andreas@digitalswitzerland.com

Karin Mändli Lerch
Responsabile di progetto
gfs-zürich, Zurigo
karin.maendlilerch@gfs-zh.ch

Patric Vifian
Marketing Manager PMI
La Mobiliare, Berna
patric.vifian@mobi.ch

Nicole Wettstein
Responsabile del programma Cybersecurity
Schweizerische Akademie der Technischen Wissenschaften SATW, Zurigo
nicole.wettstein@satw.ch

Marc K. Peter, Kristof A. Hertig, Andreas W. Kaelin,
Karin Mändli Lerch, Patric Vifian et Nicole Wettstein:

Home office e cyber sicurezza nelle PMI svizzere:
strategie e misure adottate dalle PMI svizzere
con 4–49 collaboratori nel 2023

– La Mobiliare
– digitalswitzerland
– Hochschule für Wirtschaft FHNW
– Accademia svizzera delle scienze tecniche SATW
– Alleanza Sicurezza Digitale Svizzera ASDS
– gfs-zürich

www.cyberstudie.ch
Berna, settembre 2023