Télétravail et cybersécurité dans les PME suisses

Stratégies et mesures des PME suisses de 4 à 49 collaboratrices et collaborateurs en 2023

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

La transformation des PME après le COVID-19

Étude n° 4

la Mobilière
satw
digitalswitzerland
ALLIANCE SÉCURITÉ DIGITALE SUISSE
n|w Fachhochschule Nordwestschweiz Hochschule für Wirtschaft
gfs-zürich MARKT- & SOZIALFORSCHUNG

Impressum

Marc K. Peter, Kristof A. Hertig, Andreas W. Kaelin,
Karin Mändli Lerch, Patric Vifian et Nicole Wettstein:
Télétravail et cybersécurité dans les PME suisses:
Stratégies et mesures des PME suisses
de 4 à 49 collaboratrices et collaborateurs en 2023
La Mobilière, digitalswitzerland, Hochschule für Wirtschaft FHNW,
Académie suisse des sciences techniques SATW,
Alliance Sécurité Digitale Suisse ASDS, gfs-zürich
Berne, septembre 2023

Coordination: Marc K. Peter, professeur à la Hochschule für Wirtschaft FHNW (www.fhnw.ch/wirtschaft)
Avec la collaboration de Mara Huber et Joël Grosjean (gfs-zh), ainsi que de Johan Lindeque (Hochschule für Wirtschaft FHNW).

Conception graphique: Polarstern SA, Soleure et Lucerne (www.polarstern.ch)

Les diapositives et le rapport final détaillé sont disponibles sur les sites Internet des partenaires de l'étude.

Sommaire

Introduction et principaux enseignements

Les dernières mesures anti-COVID ont été abolies au printemps 2022 et la Suisse est lentement revenue à la normale. Alors que la situation se détendait enfin, la guerre qui éclatait en Europe allait déclencher une nouvelle menace: celle de la pénurie d'énergie. Les entreprises ont alors de nouveau envisagé la possibilité du télétravail, cette fois pour cause de bureaux non chauffés.

Il n'a cependant pas été nécessaire de recourir une nouvelle fois au home office. En revanche, le thème de la cybercriminalité a pris une nouvelle dimension, sous l'effet de la guerre et des attaques lancées par les pirates informatiques russes contre certaines infrastructures occidentales, qui faisaient la une des médias. Après l'allocution vidéo de Volodymyr Zelensky au Palais fédéral le 15 juin 2023, les attaques ont également commencé à cibler la Suisse. À cette date, la recherche de terrain en vue de la présente étude venait toutefois de se terminer et la fuite majeure de données touchant une société informatique bernoise, au cours de laquelle la Confédération a perdu des données sensibles, n'a donc pas influé sur les présents résultats.

C'est dans ce contexte que la quatrième étude sur l'impact de la crise du COVID-19 sur la numérisation et la cybersécurité au sein des PME suisses a été réalisée. Un total de 502 dirigeantes et dirigeants de PME employant de 4 à 49 collaboratrices et collaborateurs a été interrogé par téléphone.

Les principaux résultats de l'étude sont résumés en douze chapitres, illustrés par douze graphiques. Le rapport de projet complet peut être consulté sur les sites web des partenaires du projet (voir encadré).

1. **Combien de membres de votre personnel pourraient théoriquement travailler depuis la maison?**
Depuis 2020, le nombre de postes adaptés au télétravail a diminué d'année en année. Le nombre de PME dans lesquelles une partie ou la totalité du personnel peut travailler à domicile est passé de 67% (en 2020) à 56% (en 2023).

2. **Combien de membres de votre personnel font du télétravail?**
Dans les entreprises où le télétravail existe, environ deux cinquièmes (42%) du personnel travaillent partiellement ou principalement depuis la maison. Comme dans les études précédentes, Genève et Zurich se distinguent en se montrant particulièrement favorables au télétravail.

3. **Quelle sera l'évolution du télétravail dans votre entreprise?**
En 2023, après la levée de toutes les mesures liées à la pandémie, près de trois quarts des personnes interrogées (73%) s'attendent à ce que la part du télétravail reste inchangée à long terme. Le recours à cette forme de travail semble s'être établie au niveau actuel dans la plupart des PME.

4. **Quels moyens numériques de communication votre entreprise utilise-t-elle?**
L'utilisation de l'ensemble des technologies de communication a été jugée plus faible en 2023 qu'en 2022. Selon les dirigeants interrogés, les outils de téléconférence sont moins utilisés (45%) qu'en 2022 (62%) et qu'en 2021 (64%).

5. **Faites-vous appel à un prestataire de services informatiques?**
La grande majorité des PME (79%) fait appel aux services de prestataires informatiques externes. Les PME qui disposent d'au moins un prestataire externe externalisent environ un tiers (36%) de leurs tâches informatiques. Parmi les prestataires informatiques, la moitié dispose déjà d'une certification en matière de sécurité informatique.

6. **Dans quelle mesure êtes-vous satisfait-e de votre prestataire informatique?**
Environ une PME sur sept (14%) a changé de prestataire de services informatiques au cours de l'année écoulée ou des deux dernières années. Neuf PME sur dix (91%) qui n'ont pas changé de prestataire de services se déclarent (très) satisfaites de celui-ci. Les prestataires informatiques ont reçu les meilleures notes pour leur bonne joignabilité et leur grande réactivité.

7. **Avez-vous déjà subi une cyberattaque?**
Une PME sur dix (11%) a déjà été victime d'une cyberattaque ayant nécessité un travail considérable pour réparer les dommages. Plus de la moitié (55%) des personnes interrogées ayant déjà fait l'objet d'une attaque a subi des dommages financiers. Près d'un huitième (13%) admet avoir subi des pertes de données clients et/ou des atteintes à la réputation.

8. Que pensez-vous de la cybercriminalité?
Les personnes interrogées envisagent la cybercriminalité comme un problème qu'il faut prendre au sérieux (valeur moyenne de 4,7 sur une échelle de 5). Elles reconnaissent également l'importance des mesures contre les cyberattaques (4,5). Plus les PME sont ouvertes aux technologies, plus elles jugent importants les risques et la nécessité de mesures de protection.

9. Êtes-vous bien informé-e sur les questions de cybersécurité?
Plus de la moitié (56%) des dirigeantes et dirigeants interrogés s'estime plutôt bien, voire très bien informée (valeurs de 4 à 5 sur une échelle de 5), tandis que tout juste deux tiers (65%) jugent la cybersécurité plutôt, voire très importante. Près d'un septième (14%) pense en revanche que la cybersécurité est un thème plutôt peu, voire très peu important.

10. Quelles mesures techniques avez-vous mises en place dans votre entreprise?
Les degrés de mise en œuvre des différentes mesures étudiées se situent entre 3,8 et 4,5 (sur une échelle de 5), et s'établissent donc globalement à un niveau quasiment inchangé par rapport aux deux dernières années. Les pionniers ont mis en place davantage de mesures que les early followers, et ceux-ci davantage que les late followers.

11. Quelles mesures organisationnelles avez-vous mises en place dans votre entreprise?
Comme lors des études précédentes, on constate que les entreprises appliquent toujours nettement moins de mesures organisationnelles que de mesures techniques. Les deux mesures organisationnelles les plus rarement implémentées sont la formation régulière du personnel (2,9 sur une échelle de 5) et la réalisation d'un audit de sécurité (2,8).

12. Comment voyez-vous la cybersécurité à l'avenir au sein de votre entreprise?
Près d'un tiers (52%) des personnes interrogées pense probablement renforcer les mesures de sécurité contre la cybercriminalité dans l'année à venir ou au cours des trois prochaines années. Les personnes les mieux informées en matière de cybersécurité prévoient davantage de mesures contre la cybercriminalité (3,6 sur 5) que les personnes moins informées (3,0).

Avec cette étude, nous accompagnons les PME depuis quatre ans. Le télétravail, la cybersécurité et la collaboration avec des prestataires informatiques constituent à la fois des défis et des facteurs de succès. Les PME qui anticipent la planification et la mise en place de mesures dans ces domaines seront à même d'appliquer leur stratégie numérique avec plus de succès et s'exposeront parallèlement à moins de risques.

Nous espérons que ce rapport et les résultats détaillés qui l'accompagnent vous aideront à faire le point sur votre situation personnelle, à mieux comprendre et à renforcer votre PME.

Berne, septembre 2023

Marc K. Peter
Responsable du centre de compétences Transformation numérique
Hochschule für Wirtschaft FHNW, Olten

Kristof A. Hertig
Programme Lead Infrastructure & Cybersecurity
digitalswitzerland, Zurich

Andreas W. Kaelin
Directeur d'Alliance Sécurité Digitale Suisse ASDS, Zoug
Senior Advisor digitalswitzerland, Zurich

Karin Mändli Lerch
Responsable de projet
gfs-zürich, Zurich

Patric Vifian
Marketing Manager PME
La Mobilière, Berne

Nicole Wettstein
Responsable du programme prioritaire Cybersécurité
Académie suisse des sciences
techniques SATW, Zurich

Le rapport d'étude complet, accompagné de l'ensemble des données et des tableaux, peut être consulté gratuitement au format PDF sur les sites web des partenaires de recherche:

www.cyberstudie.ch
www.digitalswitzerland.com
www.kmu-transformation.ch
www.satw.ch
www.mobiliere.ch/etude-pme

1. «Combien de membres de votre personnel pourraient théoriquement travailler depuis la maison?»

Question pratique aux PME:

Le télétravail est-il souhaité par votre personnel? Si oui, avez-vous défini un concept en matière d'environnement de travail afin de définir les règles du jeu?

Marc K. Peter, FHNW-HSW

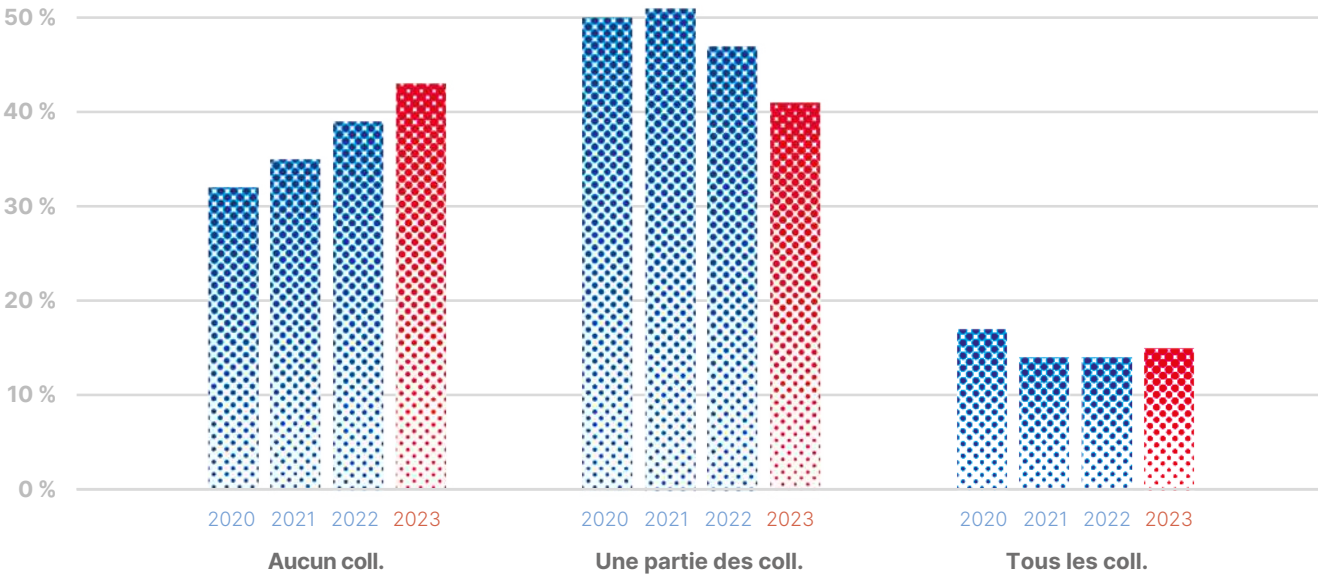
Lors de la première édition de cette étude en 2020, nous venions d'achever la première phase de l'obligation de télétravail (COVID-19). À cette époque, près d'un tiers (32%) des dirigeantes et dirigeants de PME interrogés affirmait que personne, parmi les collaboratrices et collaborateurs, ne pouvait en théorie travailler depuis la maison.

Depuis 2020, le nombre de postes adaptés au télétravail a diminué d'année en année.

La moitié (50%) reconnaissait qu'une partie du personnel pouvait être en télétravail. Environ un sixième (17%) déclarait que la totalité du personnel pouvait théoriquement travailler depuis la maison.

En 2023, plus de deux cinquièmes (43%) des personnes interrogées affirment qu'aucun poste n'est compatible avec le télétravail dans leur entreprise. Deux autres cinquièmes environ (41%) estiment qu'une partie de leurs postes est compatible avec le télétravail. Enfin, près d'un septième (15%) indique que l'ensemble du personnel peut théoriquement travailler depuis la maison.

Le recul entre 2020 et 2023 est marqué. Les auteurs supposent que l'attitude positive à l'égard du télétravail est en recul constant chez les employeurs et que, par conséquent, ceux-ci qualifient de moins en moins leurs emplois de «théoriquement compatibles avec le télétravail». Cette évolution ne signifie pas pour autant que le volume effectif de l'activité en télétravail a diminué en Suisse.



Nombre de collaboratrices et collaborateurs de 2020 à 2023 qui pourraient théoriquement travailler depuis la maison (p. ex. parce qu'ils ne doivent pas être en contact avec la clientèle sur place, conduire un véhicule ou travailler sur un chantier).

2. «Combien de membres de votre personnel font du télétravail?»

Question pratique aux PME:

Aimeriez-vous que votre personnel soit à nouveau plus présent au bureau? Si oui, que proposez-vous pour rendre le travail au bureau plus attrayant?

Karin Mändli Lerch, gfs-zh

Tout comme ces dernières années, la part de personnes télétravaillant est la plus élevée dans les PME les plus petites. Dans les entreprises qui emploient de quatre à neuf personnes, près d'un quart de celles-ci (24 % à 25 %) travaillent partiellement depuis la maison, voire principalement. C'est donc près de la moitié (49 %) du personnel de cette catégorie d'entreprises qui travaille, en partie du moins, depuis la maison.

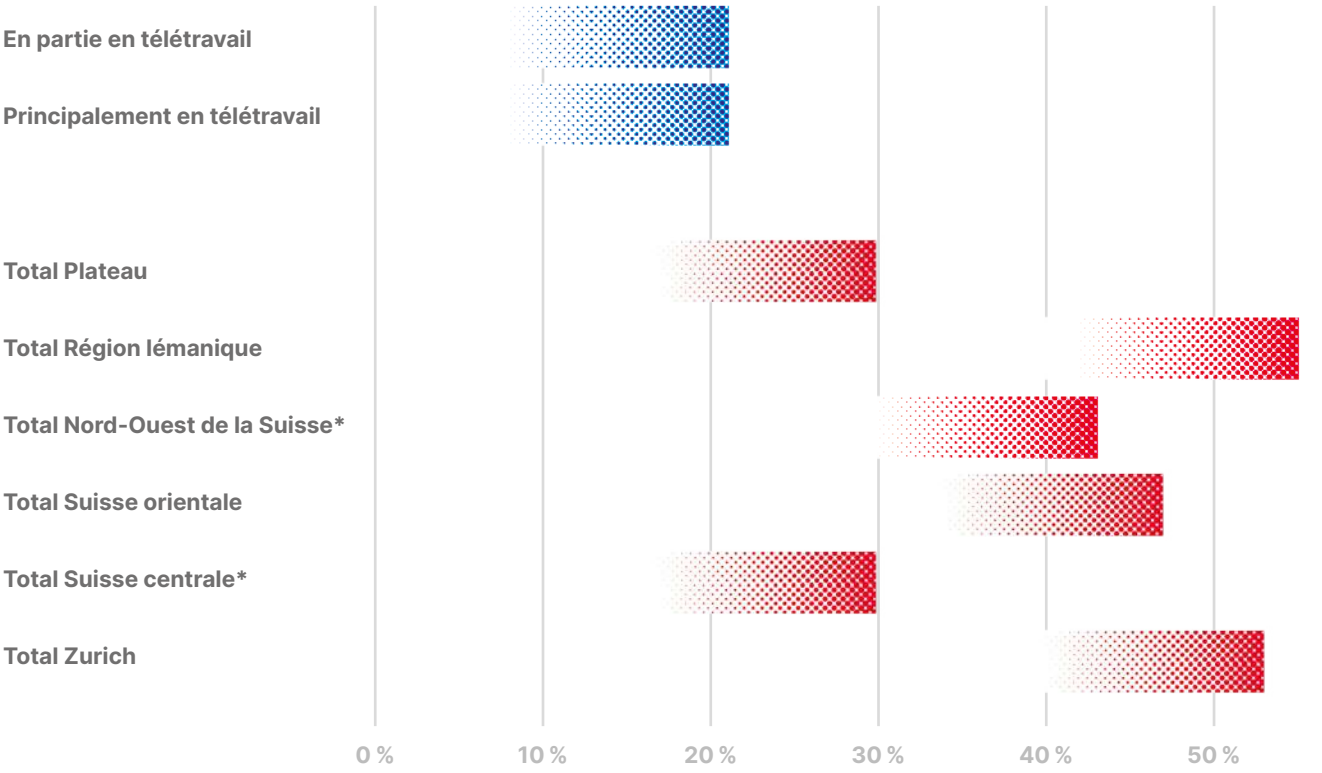
Près de deux cinquièmes (42 %) des collaboratrices et collaborateurs travaillent partiellement ou principalement depuis la maison (dans les entreprises dans lesquelles au moins une personne peut faire du télétravail).

Dans les PME employant dix à dix-neuf personnes, environ un septième (14 %) du personnel travaille partiellement ou principalement depuis la maison. Dans les PME de 20 à 49 collaboratrices et collaborateurs, c'est un peu plus d'un sixième (18 % et 17 %) de l'effectif qui travaille partiellement ou principalement depuis la maison.

Dans la dernière enquête, les possibilités de réponse ont été sous-divisées en «partiellement» et «principalement», ce qui pourrait avoir abouti à une autre appréciation et, partant, à des réponses différentes.

Après le confinement en 2020, 16 % des personnes employées par les PME interrogées étaient encore principalement en télétravail. Après la phase de télétravail obligatoire de 2021, cette proportion s'établissait encore à 20 %, puis, après celle de 2022, à 12 % seulement. En 2023, la part du télétravail est remontée à 21 %, et a donc presque doublé par rapport au creux de 2022, retrouvant quasiment le niveau de 2021. Les auteurs supposent que l'interprétation du terme «principalement» a évolué au cours des trois dernières années.

Comme dans les études précédentes, Genève et Zurich se distinguent en se montrant particulièrement favorables au télétravail.



Nombre de collaboratrices et collaborateurs (en pourcentage de l'effectif total) qui travaillent partiellement et principalement depuis leur domicile (dans les PME dans lesquelles au minimum une personne peut travailler depuis son domicile) (comportant moins de vingt participants à l'étude, le Tessin, en tant que sous-groupe, n'est pas représenté ici).

3. «Quelle sera l'évolution du télétravail dans votre entreprise?»

Question pratique aux PME:

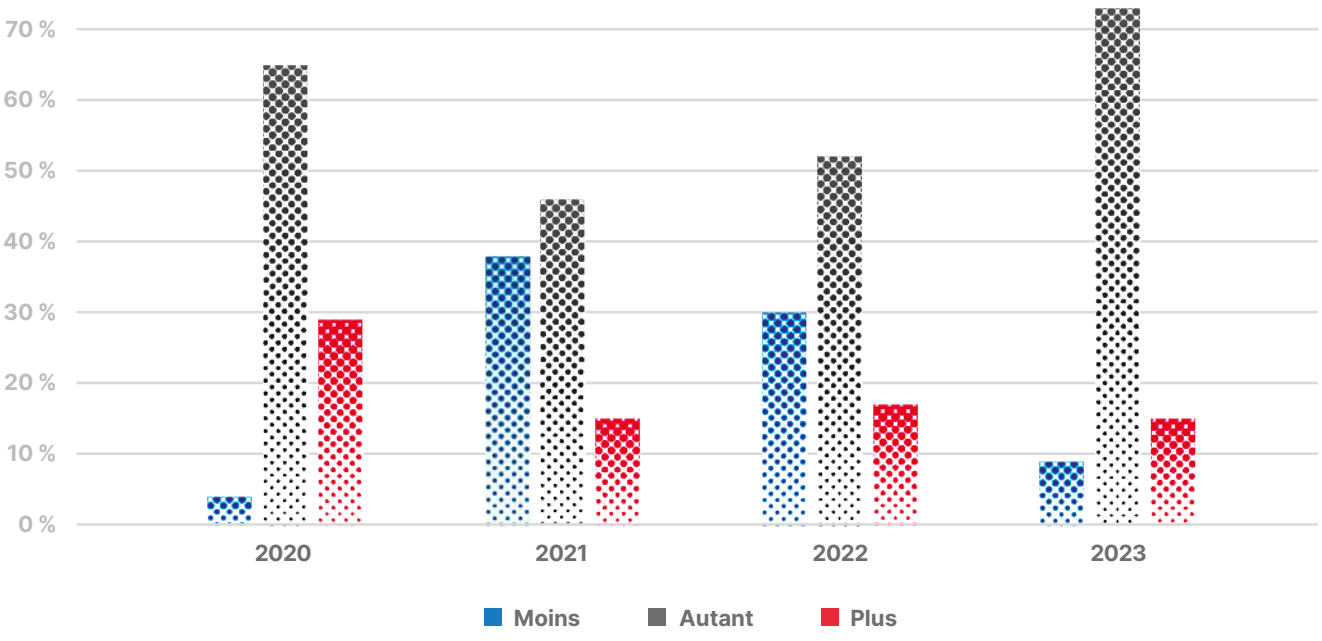
Dans quelle mesure prévoyez-vous un recours au télétravail dans votre PME? Estimez-vous que la situation s'est normalisée après le COVID-19?

Andreas W. Kaelin, ADSS

L'estimation de l'évolution à long terme de la part de personnes en télétravail n'a cessé de varier depuis 2020. Peu après la première phase de télétravail obligatoire dans le cadre du confinement général, près d'un tiers (29%) des dirigeants interrogés s'attendait à une augmentation à long terme de la proportion du télétravail. Après la deuxième phase de télétravail obligatoire en 2021, plus d'un tiers (38%) des personnes sondées en revanche pensait que la part du télétravail allait reculer à long terme, tandis que seul un septième (15%) tablait encore sur une progression. En 2022, un petit tiers (30%) s'attendait à un recul de la proportion du télétravail, alors que près d'un sixième (17%) escomptait une hausse.

Seule une personne sur dix (9%) a affirmé s'attendre à une diminution et une sur sept tablait sur une hausse. La situation semble donc s'être stabilisée, et ceci dans une mesure similaire dans l'ensemble des sous-groupes.

En 2023, après la levée de toutes les mesures liées à la pandémie, près de trois quarts des personnes interrogées (73 %) s'attendaient à un maintien à long terme de la part du télétravail à un niveau identique.



Estimation de l'évolution du nombre de personnes en télétravail dans les PME (augmentation, stabilité ou recul) (dans les PME dans lesquelles au moins une personne peut travailler depuis la maison).

4. «Quels moyens numériques de communication votre entreprise utilise-t-elle?»

Question pratique aux PME:

Comment utilisez-vous les technologies de communication? Existe-t-il un concept pour une communication plus efficace? Et tenez-vous compte à cet égard de la thématique de la cybersécurité?

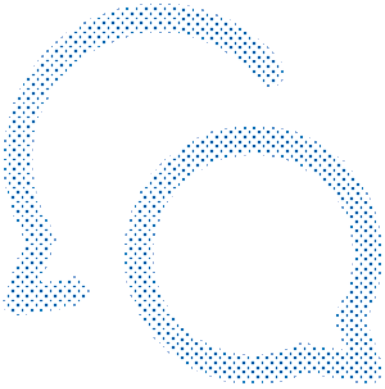
Nicole Wettstein, SATW

Avec 90% chacun, le téléphone et l'e-mail restent, en 2023, les moyens de communication les plus utilisés par les PME interrogées. La variation par rapport aux études précédentes est marginale.

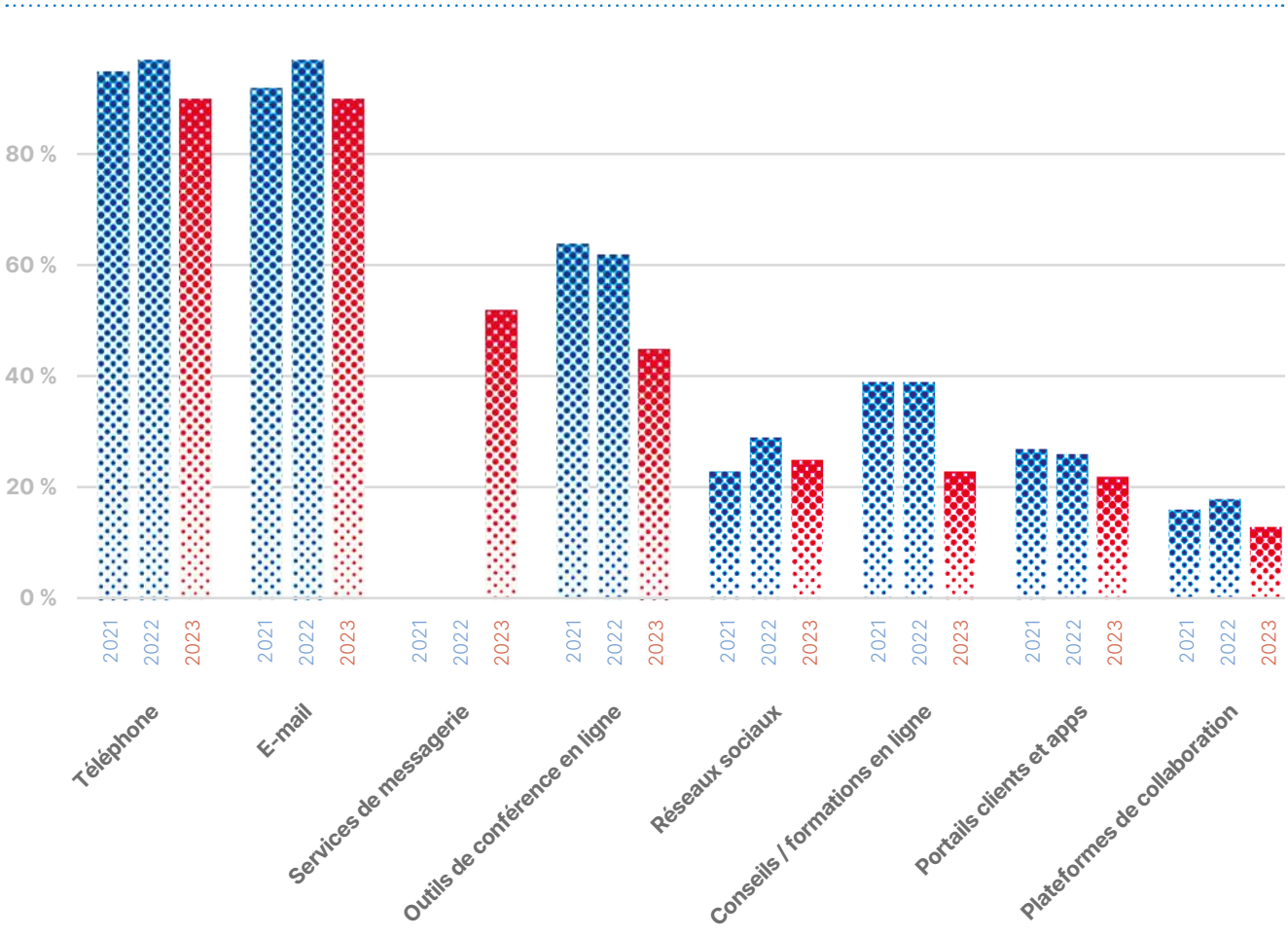
L'utilisation de l'ensemble des technologies de communication a été jugée plus faible en 2023 qu'en 2022. Cette diminution est particulièrement frappante en ce qui concerne les services de messagerie, tels que WhatsApp, Signal, Threema, Wire etc., lesquels faisaient encore l'objet de questions distinctes les années passées: l'app WhatsApp à elle seule était citée par près de deux tiers des personnes sondées dans les études précédentes (60% en 2022 et 62% en 2021). Dans la présente enquête, WhatsApp, avec Signal, Threema, Wire, etc., n'a été mentionné que par la moitié environ (52%) des personnes interrogées.

L'utilisation de conseils ou de formations en ligne a également fortement reculé (2021: 39%, 2022: 39%, 2023: 23%), tout comme l'utilisation de plateformes de collaboration telles que Slack, Confluence ou SharePoint. En moyenne, 3,6 moyens de communication différents ont été mentionnés.

Les outils de conférence en ligne tels que Skype, Teams, Zoom ou Google Meet sont également plus rarement utilisés (45 %) qu'en 2022 (62 %) et qu'en 2021 (64 %).



Plus les collaboratrices et collaborateurs peuvent en théorie travailler depuis chez eux, plus les moyens de communication sont utilisés dans les PME interrogées.



Utilisation des moyens numériques de communication dans les PME suisses de 2021 à 2023.

5. «Faites-vous appel à un prestataire de services informatiques?»

Question pratique aux PME:

Votre prestataire informatique dispose-t-il d'une certification en matière de sécurité? À défaut, comment vérifiez-vous ses compétences en cybersécurité?

Andreas W. Kaelin, ADSS

Cette année, nous avons demandé pour la première fois aux PME si elles collaboraient avec un prestataire informatique. La plupart d'entre elles (44%) travaillent avec un seul prestataire informatique. Près d'un tiers (35%) fait appel à plusieurs prestataires informatiques. Un peu plus d'un cinquième (21%) des dirigeants interrogés affirme ne travailler avec aucun prestataire informatique.

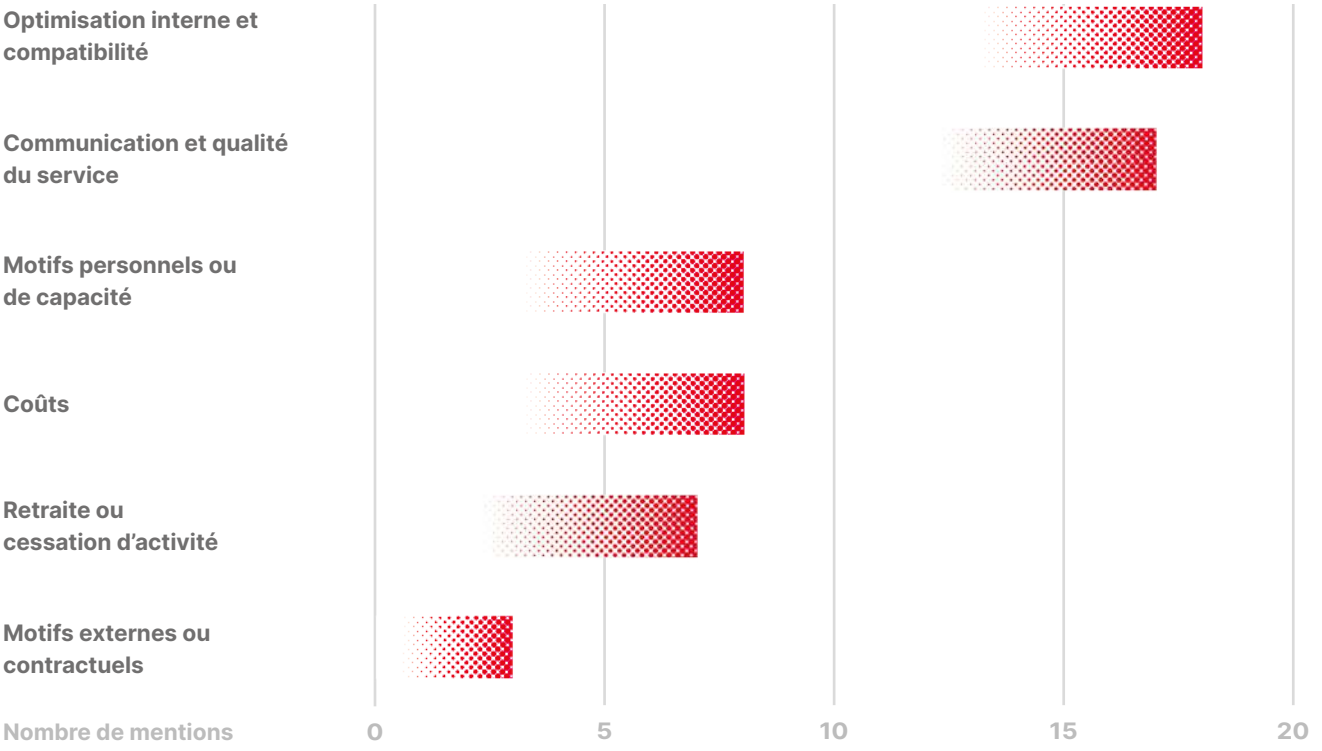
Les PME qui disposent d'au moins un prestataire informatique externe externalisent plus d'un tiers (36%) de leurs tâches informatiques. La majorité (84%) des PME qui indiquent collaborer avec au moins un prestataire informatique externe se fait également conseiller et assister par ce dernier dans le domaine de la cybersécurité.

La proportion de prestataires informatiques certifiés en sécurité n'a donc guère évolué par rapport à 2022. À cet égard, il est frappant de constater qu'une part élevée de personnes interrogées (34%) n'a pas voulu ou pu répondre à la question.

Les PME qui ont changé de prestataire informatique au cours de la dernière ou des deux dernières années l'ont fait avant tout pour des raisons d'optimisation interne et de compatibilité (p. ex. en raison de l'achat d'un nouveau logiciel ou d'un nouveau serveur), ainsi que par mécontentement par rapport à la communication et à la qualité des services. Les autres motifs évoqués sont d'ordre personnel ou liés aux capacités et aux coûts. Ce changement semble s'être effectué (très) simplement pour la plupart des PME (64%).

La moitié (53 %) des prestataires informatiques dispose d'une certification en matière de sécurité informatique, telle que la norme ISO 27001.

Environ une PME sur sept (14 %) a changé de prestataire de services informatiques au cours de l'année écoulée ou des deux dernières années.

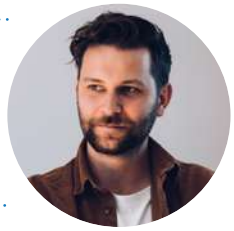


Motifs en 2023 (nombre de mentions) pour lesquels les dirigeants ont changé de prestataire informatique au cours de la dernière ou des deux dernières années (dans les PME qui ont changé de prestataire informatique au cours de l'année écoulée ou des deux dernières années; plusieurs réponses possibles).

6. «Dans quelle mesure êtes-vous satisfait-e de votre prestataire informatique?»

Question pratique aux PME:

En tant que partenaires stratégiques, les prestataires informatiques peuvent apporter une grande valeur ajoutée. Comment pourriez-vous gagner en efficacité grâce à votre prestataire informatique?



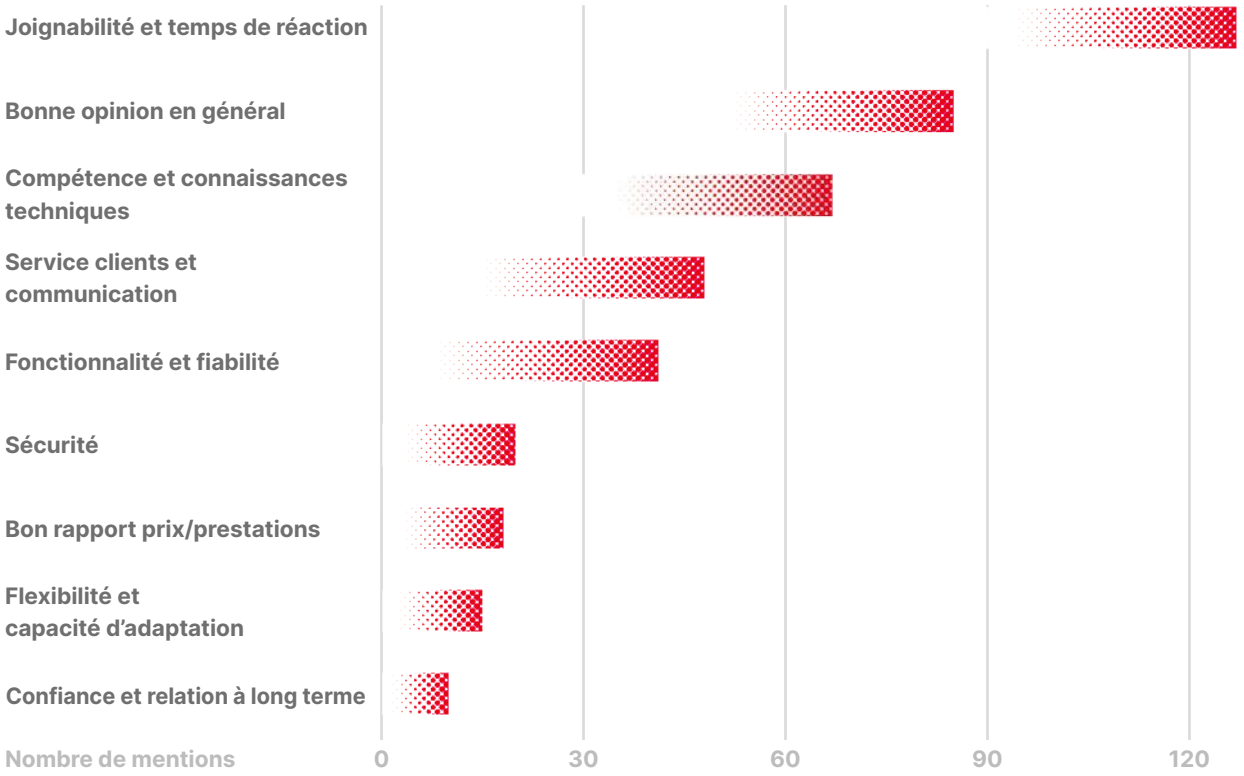
Kristof A. Hertig, digitalswitzerland

Les PME qui n'ont pas changé de prestataire informatique se déclarent très satisfaites de ce dernier.

Neuf PME sur dix (91 %) se déclarent (très) satisfaites de leur prestataire informatique.

La valeur moyenne s'établit donc à 4,5 (sur une échelle de 5; 1 = très insatisfait; 5 = très satisfait). Détail révélateur: les PME ayant un degré élevé de mise en œuvre de mesures techniques et organisationnelles visant à accroître la cybersécurité sont sensiblement plus souvent satisfaites de leur prestataire informatique que les PME ayant un degré de mise en œuvre plus faible.

Les motifs les plus fréquents pour lesquels les PME sont satisfaites de leur prestataire informatique sont la joignabilité et la réactivité, la bonne réputation («bonne opinion en général») ainsi que la compétence et l'expertise du prestataire informatique.



Motifs pour lesquels les dirigeants sont satisfaits de leur prestataire informatique en 2023
(dans les PME qui n'ont pas changé de prestataire informatique au cours de la dernière année ou des deux dernières années).

7. «Avez-vous déjà subi une cyberattaque?»

Question pratique aux PME:

Une PME sur dix a déjà été victime d'une attaque menée avec succès. Disposez-vous d'un concept d'urgence en cas de cyberattaque?

Karin Mändli Lerch, gfs-zh

Environ une personne interrogée sur dix (11 %) a déclaré que sa PME avait déjà été victime d'une cyberattaque, qui l'a contrainte à engager des frais considérables pour la réparation du dommage.

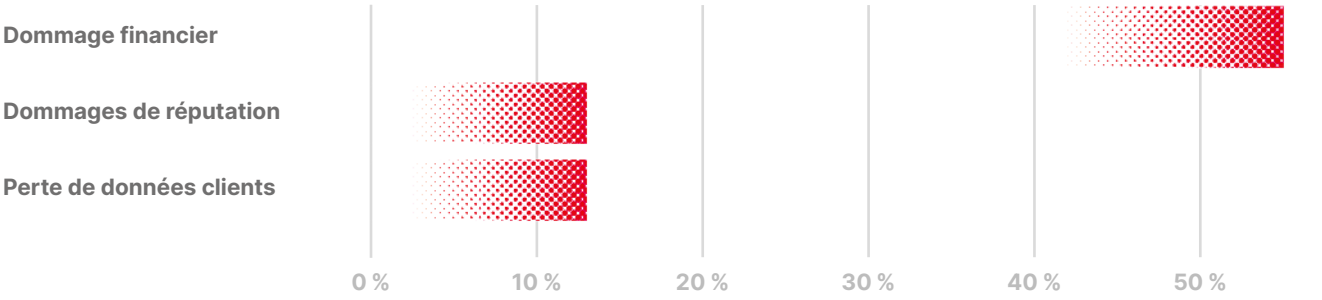
Il n'y a pas de différence entre les secteurs: les cyberattaques peuvent toucher toutes les PME.

Plus de la moitié (55 %) des personnes interrogées qui ont déjà fait l'objet d'une attaque a subi des dommages financiers. Ce qui correspond à quelque 6 % de l'échantillon global et signifierait que 6 % des PME suisses de 4 à 49 collaborateurs ont déjà subi un dommage financier du fait d'une cyberattaque.

Une PME interrogée sur huit (13 %) qui a déjà été victime d'une attaque a subi une perte de données clients ou une atteinte à la réputation.

Une PME sur sept (14 %) estime que le risque d'être paralysée durant au moins un jour à la suite d'une cyberattaque est plutôt élevé, voire très élevé.

Une PME interrogée sur dix (10 %) déclare avoir déjà subi une tentative de chantage de la part des cybercriminels.



Dommages causés par une cyberattaque réussie (uniquement parmi les PME qui ont déjà subi une cyberattaque).

8. «Comment évaluez-vous les risques liés à la cybercriminalité?»

Question pratique aux PME:

Si les risques de cyberattaque sont connus, la mise en œuvre de mesures demeure insuffisante. Qu'est-ce qui pourrait vous motiver à mettre en œuvre davantage de mesures?

Marc K. Peter, FHNW-HSW

En 2023, les réponses aux sept attitudes face à la cybercriminalité proposées sont presque identiques à celles des années précédentes. Les affirmations «La cybercriminalité est un problème à prendre au sérieux» (4,7), «Des mesures contre les cyberattaques sont importantes» (4,5) et «J'ai conscience des menaces liées à la cybercriminalité» (4,5) recueillent une forte approbation.

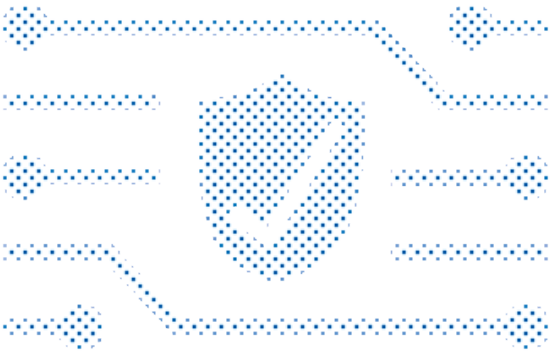
Les personnes interrogées sont moins d'accord avec les affirmations «Des mesures contre les cyberattaques sont faciles à mettre en place» (3,4) et «Mes collègues pensent que mon entreprise devrait se protéger contre les cyberattaques» (3,2). Comme ces deux dernières années, on peut ainsi affirmer ceci:

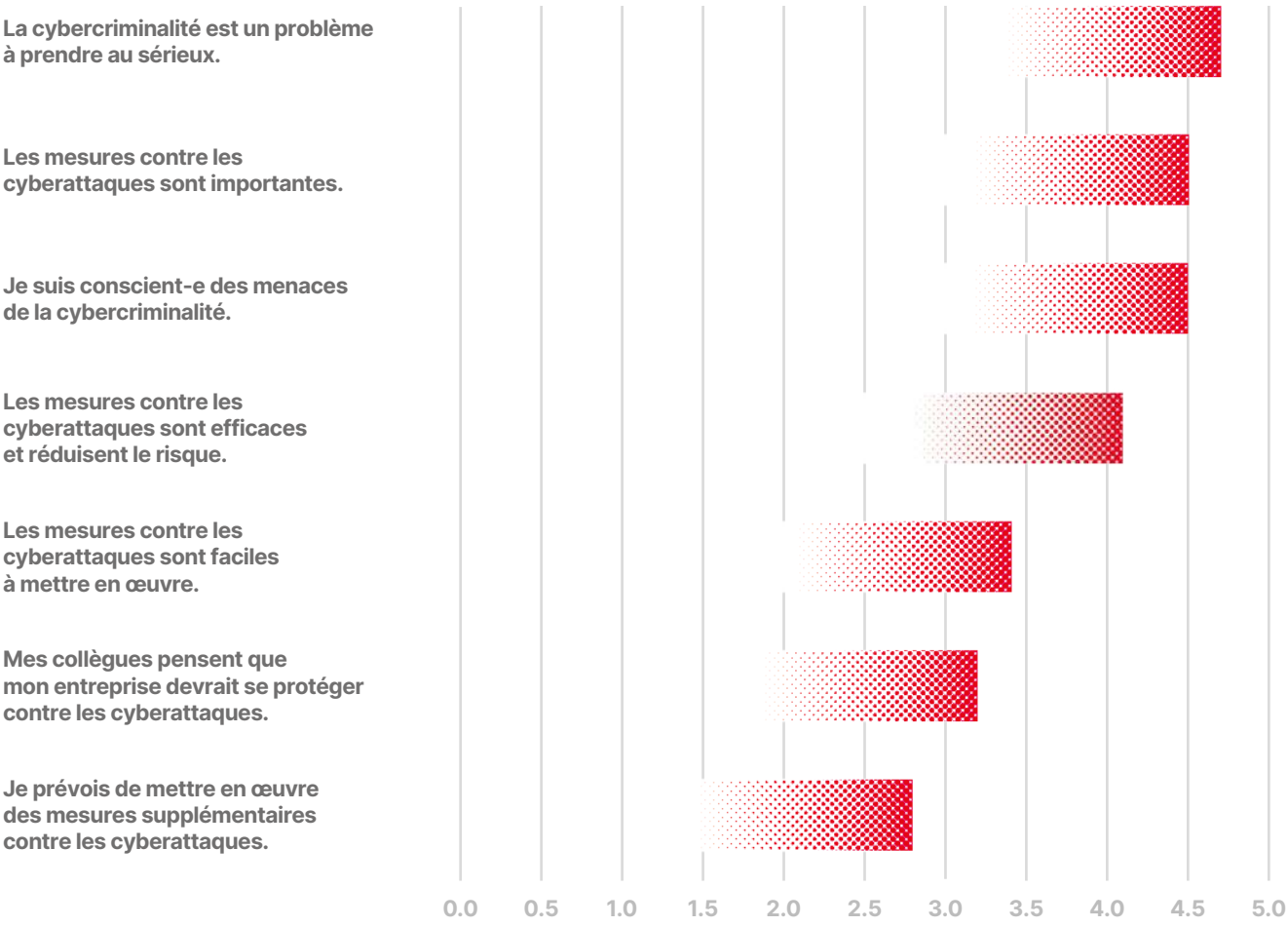
Le risque de la cybercriminalité est certes reconnu, mais seule une minorité des PME interrogées prévoit des mesures pour s'en prémunir.

Les raisons pour lesquelles ces mesures ne sont pas prises peuvent résider dans la difficulté de mise en œuvre ou dans le fait que les personnes interrogées ne ressentent pas de pression sociale au sein de leur PME (p. ex. de la part de leurs collègues de la direction).

En outre, plus la mise en œuvre technique ou organisationnelle des mesures de sécurité est élevée, plus l'approbation des affirmations l'est aussi. Ce constat vaut pour toutes les affirmations.

De même, plus les PME sont ouvertes aux technologies, plus elles approuvent les différentes affirmations.



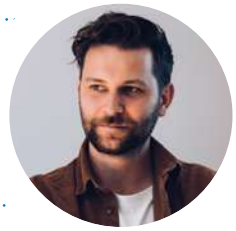


Approbation de ces affirmations par les dirigeants de PME suisses (sur une échelle de 5; 1 = pas du tout; 5 = pleinement).

9. «Êtes-vous bien informé-e sur les questions de cybersécurité?»

Question pratique aux PME:

La cybersécurité est une question omniprésente. Vous estimez-vous bien informé-e sur le sujet et comment vous informez-vous? Les conférences, formations continues et discussions avec votre prestataire informatique peuvent constituer une aide précieuse.



Kristof A. Hertig, digitalswitzerland

Plus de la moitié (56 %) des dirigeants d'entreprise interrogés se sentent plutôt informés, voire très bien informés en matière de cyberrisques (valeurs de 4 à 5 sur une échelle de 5). Ce résultat s'est lentement mais constamment amélioré ces dernières années (47 % en 2020).

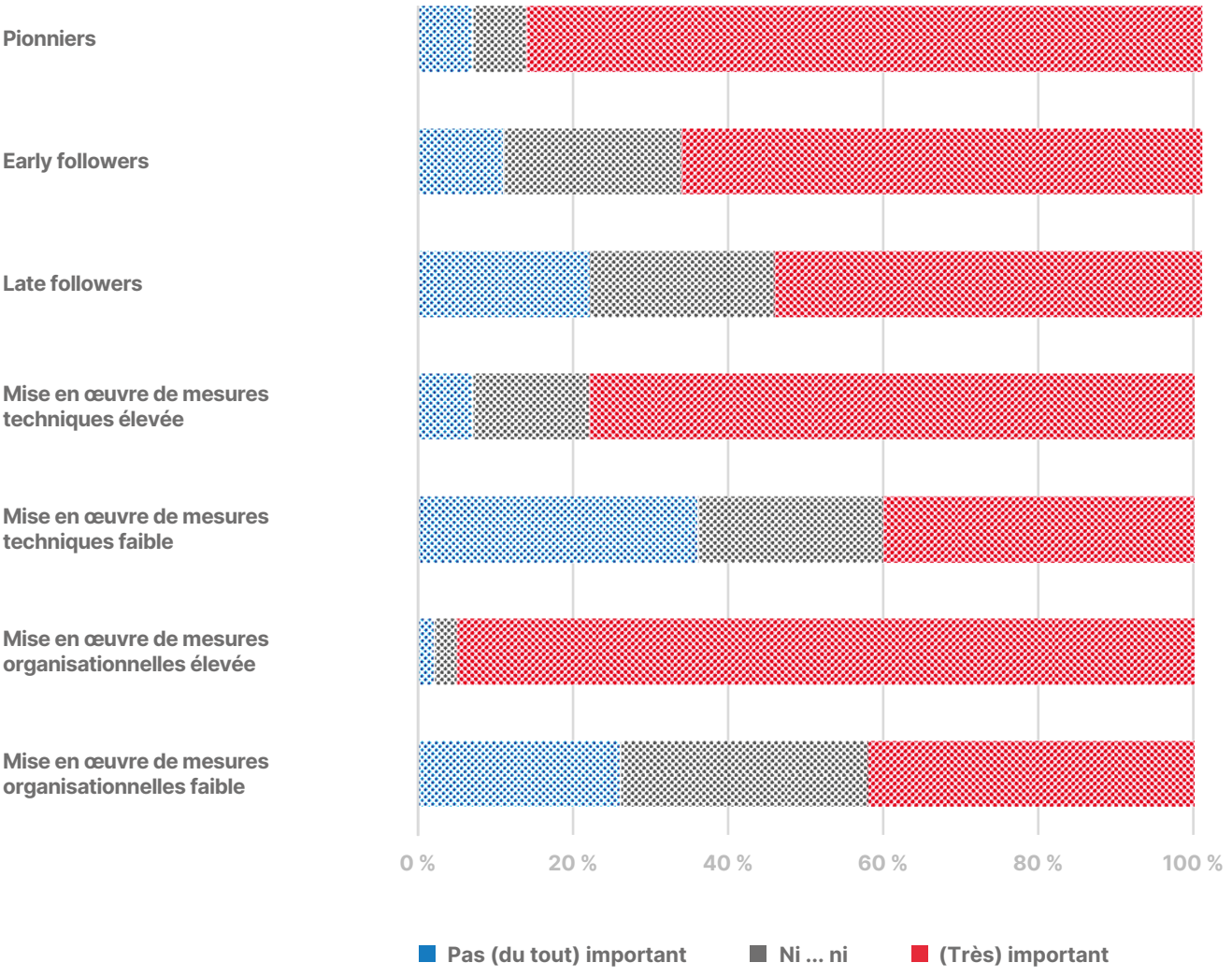
Les pionniers, qui appliquent les technologies numériques de façon précoce, se sentent mieux informés.

Les pionniers (4,2) se sentent sensiblement mieux informés que les early followers (3,6), lesquels se sentent sensiblement mieux informés que les late followers (3,3).

Les différences entre les PME qui n'ont mis en œuvre que peu de mesures de sécurité techniques et organisationnelles et celles qui en ont déjà implémenté beaucoup sont particulièrement marquées et significatives. Plus de deux tiers (69 %) des personnes interrogées dans les entreprises qui affichent un degré élevé de mise en œuvre des mesures techniques se sentent bien informées contre seul un quart (26 %) des personnes interrogées dans des PME à faible taux de réalisation de mesures techniques.

Près de deux tiers (65 %) des personnes sondées estiment que le thème de la cybersécurité est plutôt important, voire très, contre un septième (14 %) qui le juge peu important, voire pas du tout.

Les PME accordent pratiquement la même importance à la cybersécurité depuis 2020.



Évaluation du thème de la cybersécurité en 2023 dans les catégories sur une échelle de 5 (1+2 = pas [du tout] important); 3 = ni,...ni; 4+5 = [très] important).

10. «Quelles mesures techniques avez-vous mises en place dans votre entreprise?»

Question pratique aux PME:

Les pionniers, qui appliquent les technologies numériques de façon précoce, sont mieux protégés. Dans votre PME, avez-vous également mis en œuvre des mesures techniques?

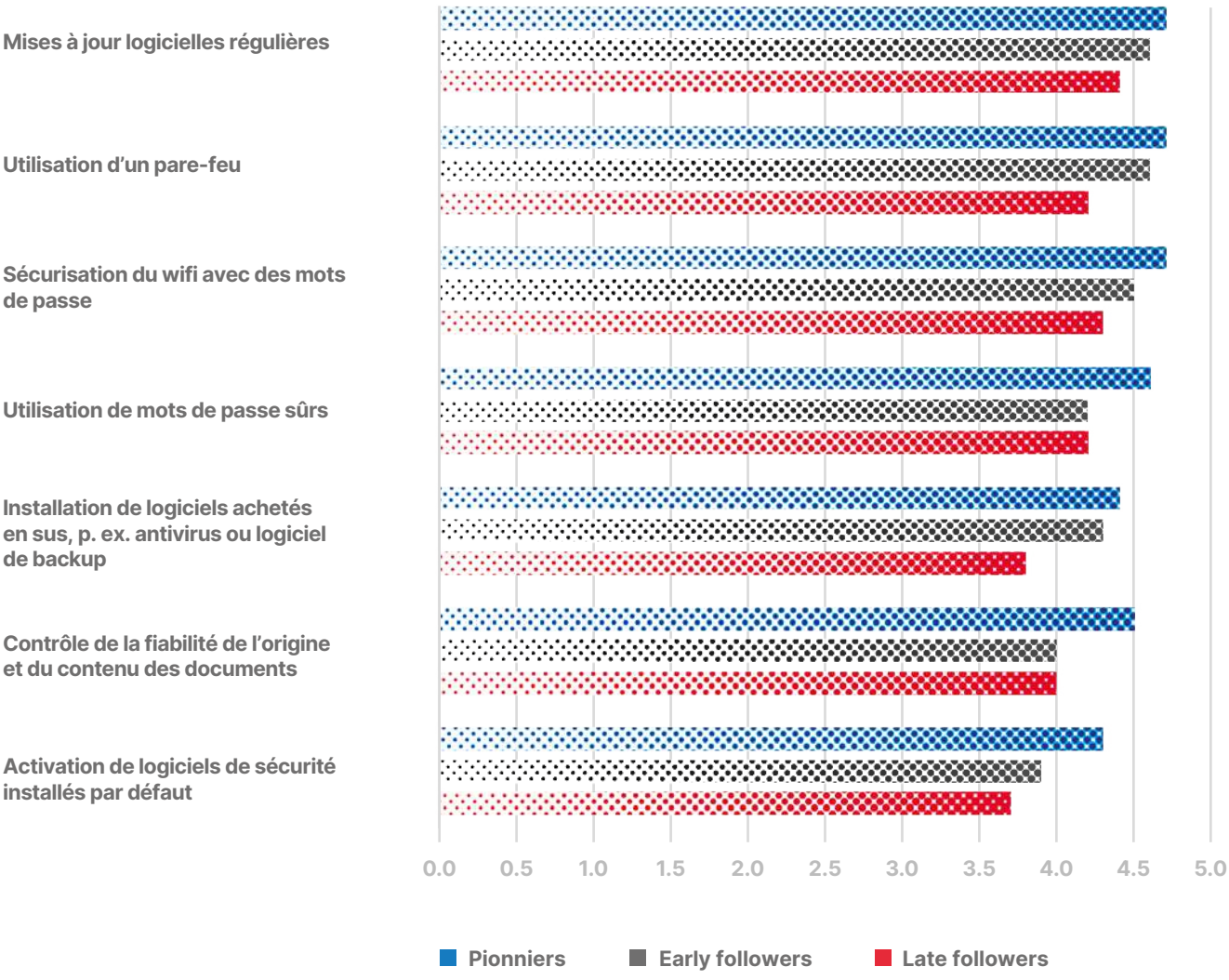
Patric Vifian, la Mobilière

Les degrés de mise en œuvre des différentes mesures proposées se situent entre 3,9 et 4,5 (sur une échelle de 5) et affichent tous un niveau pratiquement inchangé par rapport à 2022 et 2021. Les deux mesures «mises à jour régulières des logiciels» et «recours à un pare-feu» obtiennent le degré de mise en œuvre le plus élevé (toutes deux 4,5).

Comme les années précédentes, on constate pour toutes les mesures que plus les responsables se sentent informés en matière de cybersécurité, plus le niveau de réalisation des mesures l'est également.

L'ensemble des mesures a été plus fréquemment mis en œuvre dans les entreprises comptant de 20 à 49 collaboratrices et collaborateurs que dans celles de 4 à 9 et celles de 10 à 19 collaboratrices et collaborateurs.

Les pionniers ont implémenté davantage de mesures que les early followers, et ceux-ci davantage que les late followers.



Mise en œuvre des mesures techniques de cybersécurité dans les PME suisses en 2023
(sur une échelle de 5; 1 = pas du tout; 5 = pleinement).

11. «Quelles mesures organisationnelles avez-vous mises en place dans votre entreprise?»

Question pratique aux PME:

La cybersécurité est un facteur critique en matière de succès. Effectuez-vous régulièrement des formations pour votre personnel ainsi que des audits de votre sécurité informatique?

Nicole Wettstein, SATW

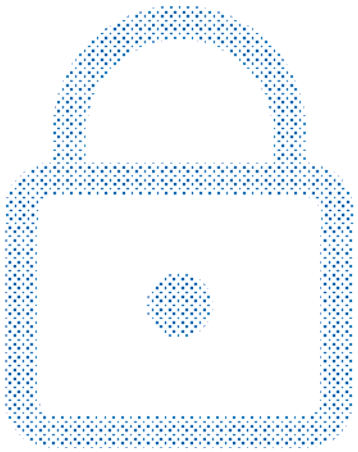
Comme dans les études précédentes, on constate que les entreprises appliquent toujours nettement moins de mesures organisationnelles que de mesures techniques. La mesure organisationnelle la plus fréquemment mise en œuvre est le contrôle de la restaurabilité de la sauvegarde des données (4,2), suivie de la prudence lors du partage d'informations personnelles (4,2) ainsi que de la sensibilisation des collaboratrices et collaborateurs aux e-mails de hameçonnage (4,0). Les deux mesures organisationnelles les plus rarement implémentées sont la formation régulière des collaboratrices et collaborateurs (2,9) et la réalisation d'un audit de sécurité (2,8).

Les différences sont toutes significatives (voir graphique sur Page 23).

Plus les personnes interrogées se sentent informées en matière de cyberrisques, plus le niveau de la mise en œuvre de mesures organisationnelles est élevé. Le degré de mise en œuvre de la mesure «formation régulière des collaboratrices et collaborateurs» est particulièrement faible (1,9) dans les PME des dirigeants qui s'estiment (plutôt) mal informés.

Les plus grandes PME ont davantage mis en œuvre la grande majorité des mesures organisationnelles que les plus petites.

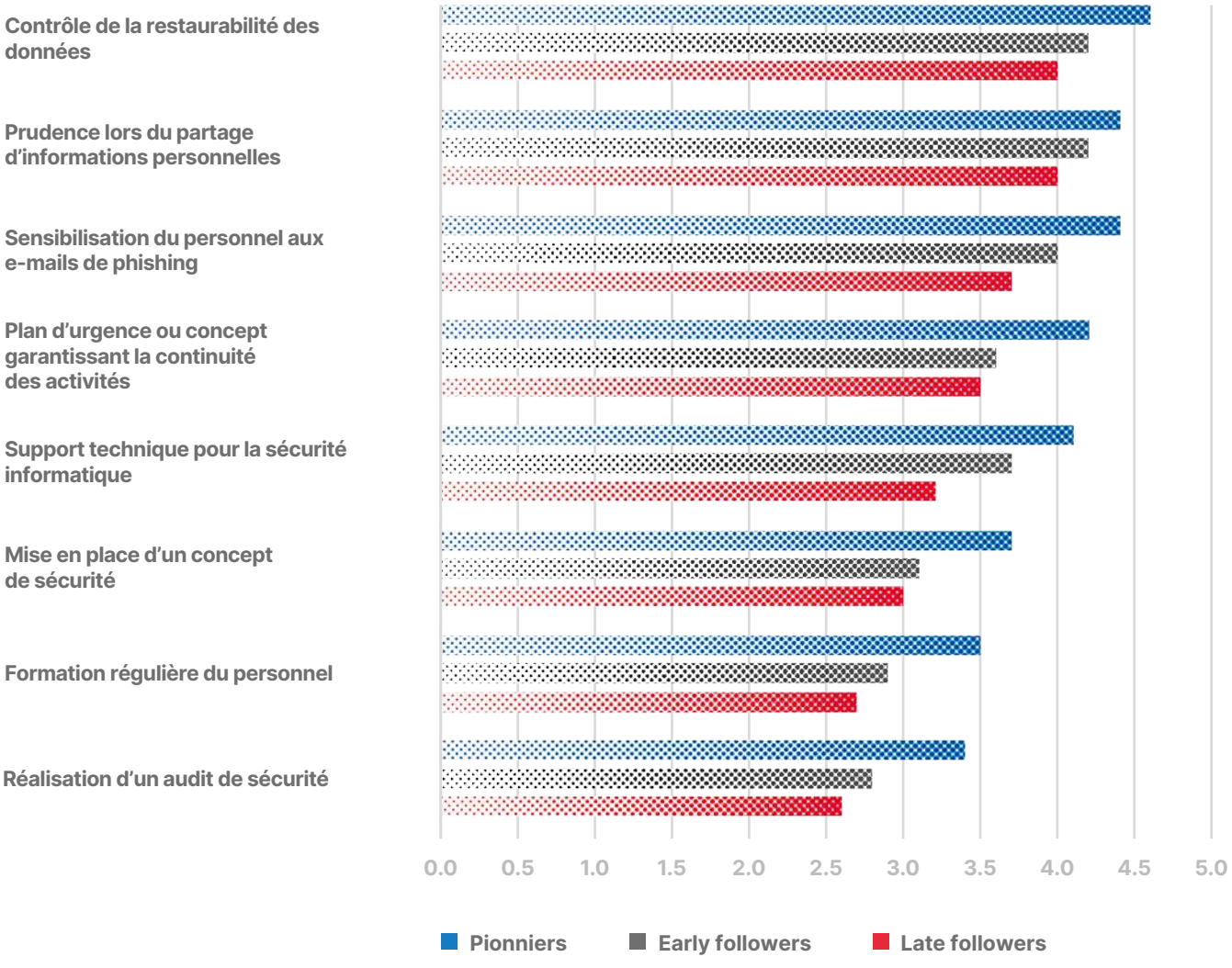
Les pionniers sont ceux qui ont appliqué le plus de mesures organisationnelles, les late followers le moins.



Bon à savoir: mots de passe

Près de neuf personnes interrogées sur dix (89 %) ont mis en place au minimum une disposition de sécurité en matière de mots de passe. Cela signifie également que pratiquement une entreprise sur dix (11 %) ne dispose d'aucune mesure en la matière. Il existe quelques mesures de sécurité en matière de mots de passe simples à mettre en œuvre:

- renouvellement régulier des mots de passe (60 %);
- authentification à deux facteurs (60 %);
- longueur du mot de passe d'au moins 12 signes (59 %);
- définition d'un mot de passe différent pour chaque service (58 %);
- programme de gestion des mots de passe (32 %).



Mise en œuvre des mesures organisationnelles de cybersécurité dans les PME suisses en 2023 (sur une échelle de 5; 1 = pas du tout à 5 = pleinement).

12. «À l'avenir, à quoi ressemblera la cybersécurité dans votre entreprise?»

Question pratique aux PME:

Comment envisagez-vous l'avenir de la cybersécurité dans votre PME? Celle-ci est-elle prête à affronter l'avenir ou devrait-elle mettre en place davantage de mesures pour renforcer la sécurité informatique?

Patric Vifian, la Mobilière

Près de la moitié (52%) des personnes interrogées estiment qu'il est plutôt, voire très vraisemblable qu'elles renforcent leurs mesures de sécurité contre la cybercriminalité dans l'année ou au plus dans les trois prochaines années. Cette valeur est presque identique à celle de l'année dernière (55%), mais sensiblement plus élevée qu'en 2021 (40%).

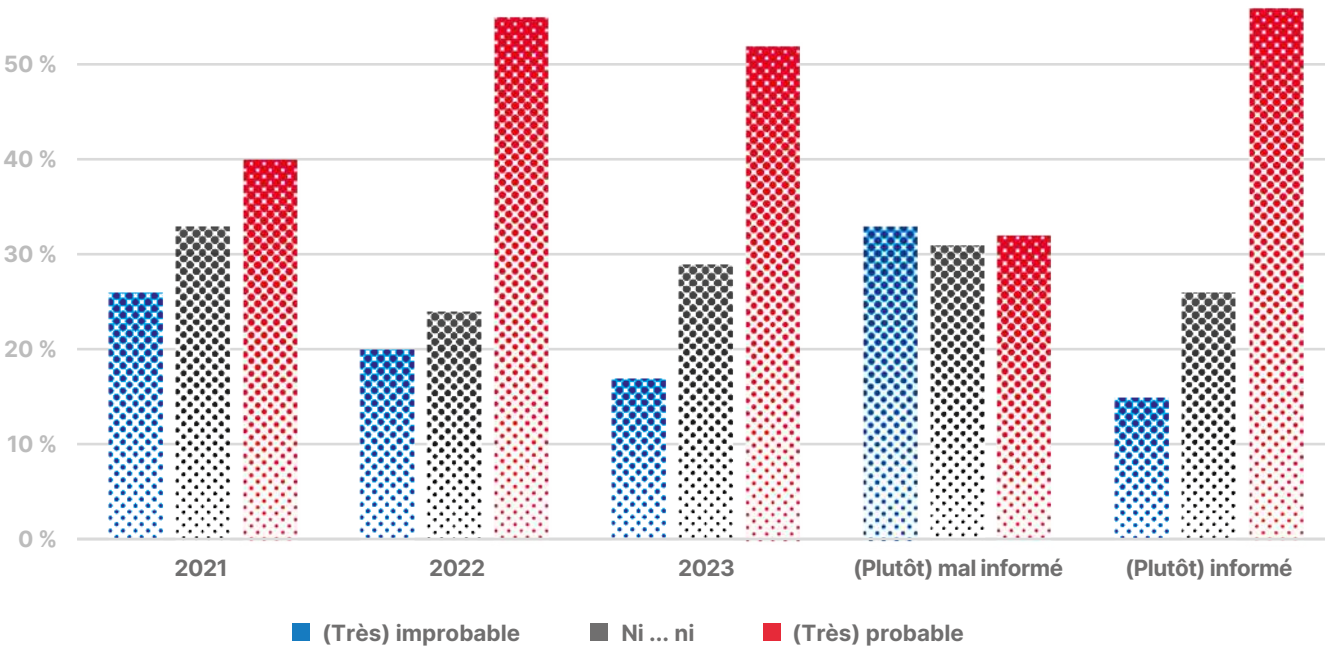
Plus la PME est grande, plus elle tend à prévoir des mesures à l'avenir.

La valeur moyenne des plus petites entreprises interrogées (employant 4 à 9 personnes) est de 3,5 (sur une échelle de 5), celle des entreprises de taille moyenne (10 à 19 personnes) de 3,6 et celle des plus grandes entreprises (20 à 49 personnes) de 3,7.

Il n'y a pas de différences significatives ni entre les grandes régions, ni entre les branches, même si la probabilité de renforcer les mesures de sécurité a tendance à être légèrement plus élevée dans les secteurs des services financiers ainsi que de l'information et de la communication (3,9) que dans les autres secteurs (3,4 à 3,6).

La différence entre les répondants (plutôt) mal informés (3,0) et les répondants (plutôt) informés (3,6) est marquée. De même, les pionniers (4,0) et les early followers (3,7) sont sensiblement plus nombreux à prévoir un renforcement des mesures de sécurité que les late followers (3,2).

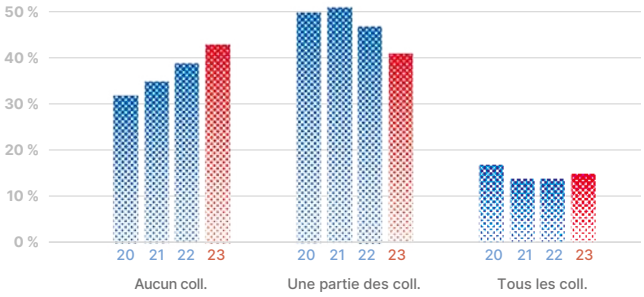
Les dirigeants les mieux informés en matière de cybersécurité planifient davantage de mesures.



Probabilité que les PME renforcent les mesures de sécurité informatique contre la cybercriminalité dans l'année ou dans les trois ans à venir (sur une échelle de 5; 1+2 = [très] improbable; 3 = ni, ni; 4+5 = [très] probable).

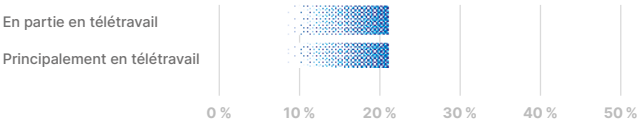
Les principales infographies en un coup d'œil:

Collaborateurs qui peuvent théoriquement télétravailler



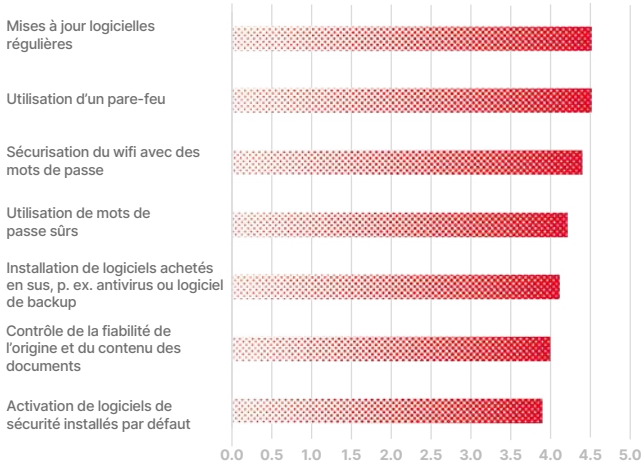
Nombre de collaboratrices et collaborateurs de 2020 à 2023 qui pourraient théoriquement travailler depuis la maison (p. ex. parce qu'ils ne doivent pas être en contact avec la clientèle sur place, conduire un véhicule ou travailler sur un chantier).

Collaborateurs qui font actuellement du télétravail



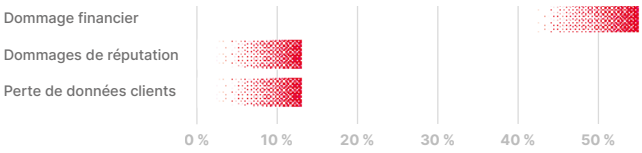
Nombre de collaboratrices et collaborateurs (en pourcentage de l'effectif total) qui travaillent partiellement et principalement depuis leur domicile (dans les PME dans lesquelles au minimum une personne peut travailler depuis son domicile).

Mesures techniques de cybersécurité mises en œuvre



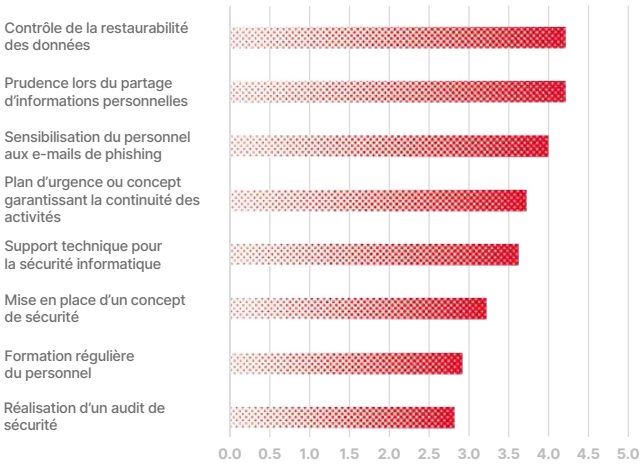
Mise en œuvre des mesures techniques de cybersécurité dans les PME suisses en 2023 (sur une échelle de 5; 1 = pas du tout; 5 = pleinement).

Dommages causés par une cyberattaque



Dommages causés par une cyberattaque réussie (uniquement parmi les PME qui ont déjà subi une cyberattaque).

Mesures organisationnelles de cybersécurité mises en œuvre



Mise en œuvre des mesures organisationnelles de cybersécurité dans les PME suisses en 2023 (sur une échelle de 5; 1 = pas du tout à 5 = pleinement).

Méthode de l'enquête

L'enquête téléphonique assistée par ordinateur (Computer Assisted Telephone Interview, CATI) a été réalisée du 18 avril au 13 juin 2023 auprès de dirigeantes et dirigeants de petites entreprises (de 4 à 49 collaboratrices et collaborateurs) en Suisse alémanique, en Suisse romande et au Tessin.

Le panel représenté par cet échantillon couvre environ 153 000 entreprises employant de 4 à 49 personnes dans toute la Suisse (OFS, STATENT 2017). L'intervalle de confiance de l'échantillon total est de 95%, avec une marge d'erreur de +/- 4,4% pour 50/50. Les données collectées reflétant une structure homogène du panel en termes de tailles d'entreprise et de régions linguistiques, les résultats peuvent être extrapolés à celui-ci en tenant compte de l'intervalle de confiance.

L'échantillon a été prélevé proportionnellement à la taille des entreprises, en veillant à garantir la répartition des trois catégories de taille (par nombre de collaboratrices et collaborateurs) au moyen de quotas. La répartition par taille de région a été réalisée à l'aide d'une stratification basée sur les adresses.

L'échantillon compte 326 PME employant de 4 à 9 personnes (échantillon: 65% / OFS, STATENT: 66%), 110 PME de 10 à 19 personnes (22% / 22%) et 66 PME de 20 à 49 personnes (13% / 12%). Les adresses sont fournies par un courtier d'adresses suisse, à partir de plus de 100 000 adresses potentielles (ce qui correspond à 2/3 du panel).

Les sous-groupes relatifs à l'innovation technique (pionniers, early followers et late followers) ont été constitués sur la base des questions concernant l'adaptation aux nouvelles technologies:

- Les pionniers font toujours partie des personnes ou entreprises qui achètent et utilisent en premier les nouveaux appareils et les nouvelles technologies.
- Les early followers (ou adopteurs précoces) ne commencent à utiliser les nouveaux appareils et technologies qu'après avoir eu connaissance d'expériences vécues par d'autres utilisateurs.
- Les late followers (ou adopteurs tardifs) ne recourant aux nouveaux appareils et technologies qu'à partir du moment où ceux-ci deviennent indispensables pour eux

Pour les sous-groupes relatifs aux mises en œuvre technique et organisationnelle des mesures de cybersécurité, nous avons calculé la moyenne de toutes les mesures techniques ou organisationnelles (les valeurs moyennes de 1 à 3 traduisent une faible mise en œuvre, la moyenne de 4 une mise en œuvre moyenne et la moyenne de 5 comme une mise en œuvre élevée des mesures).

Un total de 37 376 PME a été contacté, parmi lesquelles 21 636 n'étaient pas joignables (p. ex. refus, pas de réponse, ligne occupée ou répondeur automatique). Avec 502 entretiens réalisés, le taux de réponse atteint 3,2%.

Remarque générale en vue de la lecture des graphiques: les sous-groupes comportant moins de 30 entretiens sont signalés un moyen d'un astérisque «*» afin d'éviter une surinterprétation. Les sous-groupes de vingt entretiens ou plus sont représentés, tandis que ceux qui en comptent moins de 20 ne le sont pas. Les pourcentages sont arrondis à des chiffres entiers, raison pour laquelle il peut exister de petits écarts d'arrondi. L'option de réponse «ne sais pas / pas de réponse» n'a pas été indiquée afin de préserver la lisibilité des graphiques. Dès lors, la somme de toutes les réponses n'atteint pas toujours 100%.

Contact / autrices/auteurs

Prof. Dr. Marc K. Peter
Responsable du centre de compétences Transformation numérique
FHNW Hochschule für Wirtschaft, Olten
marc.peter@fhnw.ch

Kristof A. Hertig
Programme Lead Infrastructure & Cybersecurity
digitalswitzerland, Zurich
kristof@digitalswitzerland.com

Andreas W. Kaelin
Directeur Alliance Sécurité Digitale Suisse ASDS, Zug
Conseiller principal, digitalswitzerland, Zurich
andreas@digitalswitzerland.com

Karin Mändli Lerch
Responsable de projet
gfs-zürich, Zurich
karin.maendlilerch@gfs-zh.ch

Patric Vifian
Marketing Manager PME
La Mobilière, Berne
patric.vifian@mobi.ch

Nicole Wettstein
Responsable du programme prioritaire Cybersécurité
Académie suisse des sciences techniques (SATW), Zurich
nicole.wettstein@satw.ch

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

Télétravail et cybersécurité dans les PME suisses:
Stratégies et mesures des PME suisses
de 4 à 49 collaborateurs en 2023

– La Mobilière
– digitalswitzerland
– Hochschule für Wirtschaft FHNW
– Académie suisse des sciences techniques SATW
– Alliance Sécurité Digitale Suisse ASDS
– gfs-zürich

www.cyberstudie.ch
Berne, septembre 2023