Télétravail et cybersécurité dans les PME suisses

Stratégies et mesures des PME suisses
de 4 à 49 collaborateurs après deux années marquées par le COVID-19

Marc K. Peter, Andreas Hölzli, Andreas W. Kaelin,
Karin Mändli Lerch, Patric Vifian et Nicole Wettstein

Étude N° 3

La transformation des PME dans le contexte du coronavirus (COVID-19)

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

Impressum

Marc K. Peter, Andreas Hölzli, 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 après deux années marquées par le COVID-19

La Mobilière, digitalswitzerland, FHNW Hochschule für Wirtschaft, SATW, Alliance Sécurité Digitale Suisse ASDS, gfs-zürich

Berne, juin 2022

Coordination de la publication : prof. Marc K. Peter, FHNW Hochschule für Wirtschaft (www.fhnw.ch/wirtschaft)

Traduction française: La Mobilière
Conception graphique : Polarstern SA, Soleure et Lucerne (www.polarstern.ch)

Les diapositives et le rapport final détaillé peuvent être téléchargés depuis les sites Internet des partenaires de l'étude.

Méthode de l'enquête

L'enquête a été réalisée par téléphone du 28 février au 30 mars 2022 auprès d'un échantillon de 504 dirigeantes et dirigeants de petites entreprises (4 à 49 collaborateurs) situées en Suisse alémanique, en Suisse romande et au Tessin.

Le panel représenté par cet échantillon couvre environ 153 000 entreprises de 4 à 49 collaborateurs dans toute la Suisse (OFS, Statistique structurelle des entreprises STATENT 2017, version du 22.08.2019).

L'intervalle de confiance de l'échantillon total est de 95 %, avec une marge d'erreur de +/- 4 % pour 50/50. Les données collectées reflétant une structure homogène du panel, 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 collaborateurs) au moyen de quotas; la répartition par taille de région a été réalisée à l'aide d'une stratification basée sur les adresses.

Le taux de réponse est de 3,6 %, ce qui correspond à la valeur habituelle pour cette méthode et ce groupe cible (22 909 appels moins 8851 contacts injoignables = 14 058 contacts pour 504 interviews réalisées, soit 2,2 % sur l'ensemble des appels passés).

Sommaire

Introduction et aperçu

La présente publication est née de l'initiative d'un groupe de projet composé de collaboratrices et collaborateurs de digitalswitzerland, de la Hochschule für Wirtschaft rattachée à la Fachhochschule Nordwestschweiz FHNW, de l'Académie suisse des sciences techniques (SATW), de l'Alliance Sécurité Digitale Suisse (ADSS), de gfs-zürich et de la Mobilière. Sur la base d'un projet de recherche et de la présente publication, les autrices et auteurs entendent contribuer à une meilleure compréhension et à un renforcement des PME suisses de 4 à 49 collaborateurs dans un contexte caractérisé par la numérisation, des environnements de travail modernes, les risques posés par la cybercriminalité et les mesures visant à renforcer la cybersécurité.

Les trois études menées de 2020 à 2022 donnent un aperçu de la situation en matière de télétravail et de cybersécurité dans les PME en lien avec la crise sanitaire vécue depuis le début de l'année 2020. La première enquête a été réalisée entre les deux premières vagues de l'épidémie, plus précisément entre le moment où le Conseil fédéral a levé la recommandation initiale de privilégier le télétravail (22 juin 2020) et celui où l'appel au télétravail a été lancé pour la deuxième fois, le 19 octobre 2020 (le télétravail est devenu obligatoire pour toutes les entreprises à partir du 18 janvier 2021). La deuxième enquête a été réalisée après la levée de l'obligation de télétravail pour les entreprises effectuant des tests réguliers (à partir du 31 mars 2021). Elle a débuté peu avant que le télétravail ne devienne une recommandation pour toutes les entreprises le 26 juin 2021 (cette deuxième enquête a été menée du 16 juin au 27 juillet 2021). Durant l'hiver 2021–2022, les employeurs suisses se sont une troisième fois vu contraints, par décision du Conseil fédéral, d'imposer le télétravail à leur personnel «[…] Lorsque la nature de l'activité le rend possible et réalisable sans efforts disproportionnés» (art. 25, al. 5, de l'ordonnance sur les mesures destinées à lutter contre l'épidémie de COVID-19 en situation particulière). Cette dernière obligation de télétravail a été en vigueur du 20 décembre 2021 au 3 février 2022 avant de passer également en recommandation. La protection contre d'éventuelles contaminations devait néanmoins continuer d'être garantie, par exemple avec l'obligation de port du masque sur le lieu de travail. La troisième étude présentée ici s'appuie sur des entretiens téléphoniques menés du 28 février au 30 mars 2022 auprès d'un échantillon de 504 dirigeantes et dirigeants de petites entreprises (4 à 49 collaborateurs) en Suisse alémanique, en Suisse romande et au Tessin. À noter que, compte tenu de la question posée, elle ne prend pas en compte les offres en matière de télétravail à temps partiel ni l'usage qui est fait de celui-ci.

L'étude révèle qu'au début de l'année 2022, il règne chez les employeurs une certaine lassitude par rapport au télétravail : les employeurs n'ont pas (ou plus) la capacité ou la volonté de proposer activement le télétravail dans leur palette de concepts en matière d'environnement de travail. Alors qu'au milieu de l'année 2020 et de l'année 2021, pour respectivement 67 % et 65 % des PME interrogées, tous les collaborateurs ou une partie d'entre eux pouvaient théoriquement télétravailler, ce pourcentage n'était plus que de 61 % début 2022. Dans ces PME, le nombre de postes adaptés au télétravail n'a cessé de baisser, passant en moyenne de 3,8 en 2020 à 3,4 en 2021, puis à 2,9 en 2022. Il se pourrait que la perception de la compatibilité des postes avec le télétravail ait évolué ou que l'expérience ait montré qu'il était préférable d'exécuter le travail sur place – ou que tel est du moins ce que l'on croit.

Il apparaissait déjà en 2021 que les dirigeants de PME tablaient sur un recul du nombre de postes de télétravail. Une tendance qui s'est confirmée : avant le premier confinement de mars 2020, 10 % du personnel des PME comptant au moins un poste adapté au télétravail travaillait depuis la maison. Cette valeur a pratiquement quadruplé pendant le premier confinement pour atteindre 38 %, avant de se replier à 16 % (soit une hausse de 60 % par rapport à la valeur d'avant-pandémie). Durant l'obligation de télétravail imposée lors du deuxième confinement, cette valeur a de nouveau progressé jusqu'à 36 %. À partir de fin 2021, elle s'est stabilisée à un niveau relativement élevé (20 %), tous secteurs confondus, puis a reculé jusqu'à 12 %, rejoignant ainsi pratiquement le niveau qui prévalait avant la pandémie (10 %). Le télétravail ne saurait toutefois être lié uniquement au COVID-19 : plus les dirigeants interrogés pensent que leur entreprise est ouverte aux innovations technologiques (les pionniers), plus leur personnel a eu tendance à faire essentiellement du télétravail.

Le regard porté en 2022 sur l'importance de la cybersécurité est le même qu'en 2021 et 2020 : environ deux tiers des sondés (64 %) considèrent la cybersécurité comme plutôt importante à très importante (valeurs 4 et 5 sur une échelle de 5), alors qu'environ un septième (14 %) la jugent peu à pas du tout importante (valeurs 1 et 2). La valeur moyenne pour l'année 2022 s'établit ainsi à 3,8,

légèrement en dessous de celle de 2021 et 2020 (3,9 respectivement). Soulignons à cet égard que la part des dirigeants de PME à considérer cette question comme très importante est en recul constant (42 % en 2020, 41 % en 2021 et 35 % en 2022). Les dirigeants de PME continuent par contre de se sentir extrêmement bien informés à ce sujet (la moitié plutôt bien ou très bien informés). Tout comme en 2021, la valeur moyenne est de 3,5. Plus les entreprises sont ouvertes aux innovations technologiques, mieux elles sont informées et plus elles mettent en place des mesures de sécurité adéquates.

Après avoir progressé de 25 % en 2020 à 36 % en 2021, la part des entreprises victimes d'une cyberattaque ayant nécessité d'importants moyens pour réparer le dommage causé a chuté de quelques points de pourcentage en 2022, à 31 %. On observe néanmoins qu'en 2022, pour la deuxième fois, le risque de subir une cyberattaque de nature à paralyser l'entreprise pendant un jour est perçu avec légèrement plus d'acuité : la valeur moyenne en 2022 s'établit à 2,5 (sur 5), contre 2,4 en 2021 et 2,1 en 2020. La part des dirigeants interrogés qui estiment un tel risque plutôt élevé voire très élevé se monte aujourd'hui à près d'un cinquième (18 %). Les entreprises ayant déjà été victimes d'une cyberattaque estiment ce risque plus élevé (2,6) que celles qui ont (pour l'instant) été épargnées. Même si le scénario d'une cyberattaque propre à menacer l'existence de l'entreprise n'est jugé réaliste que par une poignée de dirigeants, cette estimation n'en est pas moins en constante progression depuis 2020 : de 1,5 (sur 5) en 2020, la valeur moyenne est passée à 1,7 en 2021 et s'établit à 1,9 en 2022.

Afin d'accroître la cybersécurité, les entreprises continuent de privilégier des mesures techniques plutôt qu'organisationnelles, comme des mises à jour logicielles régulières (86 %) ou la sécurisation du wifi avec des mots de passe (82 %). Des moyens seront d'autant plus activement déployés que les dirigeants estimeront leur propre niveau d'information élevé. Le potentiel d'amélioration sur le front des mesures organisationnelles reste important. Les actions les plus rarement mises en œuvre sont l'instauration d'un concept de sécurité (44 %), des formations régulières du personnel (34 %) et la réalisation d'audits de sécurité informatique (32 %). Là aussi, plus les dirigeants interrogés se sentent bien informés en matière de cyberrisques, plus ils prennent des mesures organisationnelles visant à renforcer la cybersécurité de leur entreprise. Il ressort de l'étude que près d'un tiers d'entre eux (29 %) s'attendent, avec une forte probabilité, à devoir renforcer les mesures de sécurité contre la cybercriminalité dans les une à trois prochaines années. Les dirigeants ayant déjà subi une cyberattaque ont tendance à mieux vouloir se protéger que ceux qui n'en ont encore jamais été victimes.

Nous espérons que ce rapport et les résultats d'étude détaillés qui l'accompagnent (voir encadré) vous aideront à faire le point sur votre situation personnelle, à mieux comprendre votre entreprise et à la doter des outils nécessaires pour renforcer sa solidité.

Berne, juin 2022

Andreas Hölzli
Responsable du centre de compétences Cyberrisques
La Mobilière, Berne

Andreas W. Kaelin
Directeur Alliance Sécurité Digitale Suisse ASDS, Zug
Conseiller principal, digitalswitzerland, Berne

Karin Mändli Lerch
Responsable de projet
gfs-zürich, Zurich

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

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

Importance et application du télétravail

Combien de membres de votre personnel pourraient théoriquement travailler depuis la maison, p. ex. personnes qui ne doivent pas être en contact avec la clientèle sur place, ni conduire un véhicule, ni travailler sur un chantier?

Début 2022, dans 61 % des PME interrogées, tous les collaborateurs ou une partie d'entre eux pouvaient théoriquement travailler depuis chez eux (2021 : 65 %, 2020 : 67 %). Le télétravail obligatoire s'appliquait lorsque la nature de l'activité des postes le rendait possible et réalisable sans efforts disproportionnés.

Le nombre de postes compatibles avec le télétravail est en recul constant depuis 2020 : on compte en moyenne 2,9 postes de travail compatibles en 2022, contre 3,8 en 2020 et 3,4 en 2021. Ce recul marquant peut s'expliquer comme suit :

- Les employeurs ressentent une certaine lassitude vis-à-vis du télétravail : ils n'ont pas (ou plus) la capacité ou la volonté de le proposer activement dans leur palette de concepts en matière d'environnement de travail.
- La perception quant à la compatibilité d'un poste avec le télétravail a évolué ou l'expérience a montré que l'exécution du travail sur place (au bureau) était préférable – ou tel est du moins ce que l'on croit.

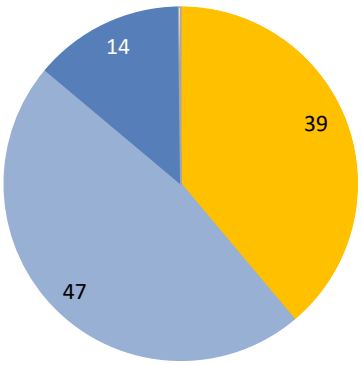
Il convient de souligner dans ce contexte les pionniers, en principe plus favorables au télétravail que les Early Followers et les Late Followers : même dans ces PME, les collaborateurs ou une partie d'entre eux ne sont plus que 69 %, en 2022, à pouvoir théoriquement faire du télétravail (85 % en 2021).

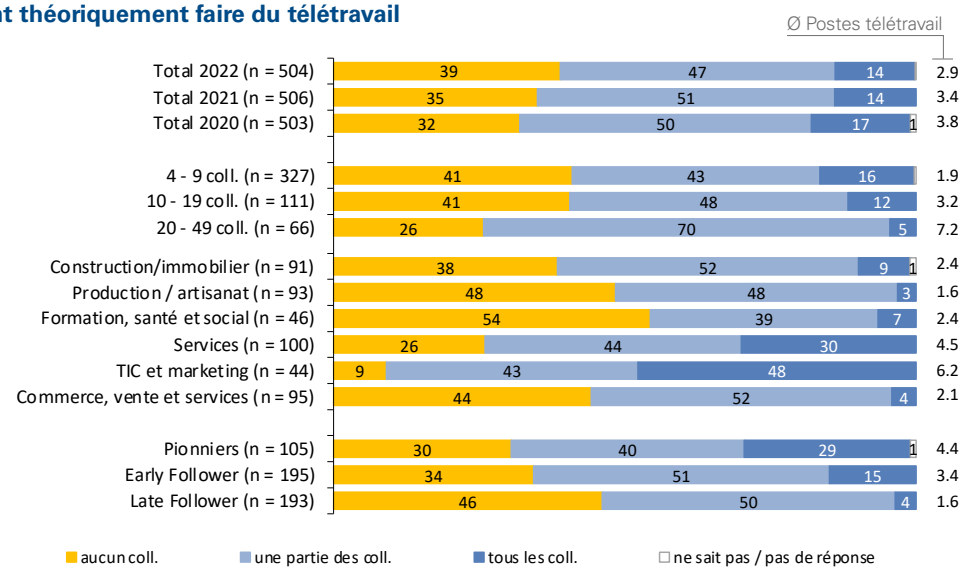
Avec respectivement 4,5 et 6,2, les branches Services et TIC/marketing sont celles qui concentrent le plus de postes adaptés au télétravail, tandis que les possibilités en la matière sont limitées dans les branches Production/artisanat (1,6) et Commerce, vente et services (2,1).

Questions posées aux PME suisses :

- Dans quelle mesure le télétravail vous permet-il d'accroître la flexibilité de vos employés, de renforcer l'attrait de votre entreprise aux yeux du personnel et de réduire votre structure des coûts?
- Avez-vous déjà discuté du télétravail avec vos employés et, sur cette base, développé des idées, identifié des potentiels et élaboré une feuille de route?
- Existe-t-il une convention de télétravail, p. ex. pour la prise en charge des frais liés à l'équipement de bureau privé?

Nombre de collaborateurs pouvant théoriquement faire du télétravail





Nombre de collaborateurs pouvant théoriquement télétravailler (n 2022 = 504, n 2021 = 506, n 2020 = 503, classement par catégories, données en pourcentage, les catégories avec un volume d'échantillonnage < 30 sont marquées d'un *)

Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

De vocation internationale avec un enseignement axé sur la pratique, la Hochschule für Wirtschaft FHNW (haute école d'économie de la Fachhochschule Nordwestschweiz) forme 3000 étudiantes et étudiants de Bachelor et de Master sur ses sites de Bâle, Brugg-Windisch et Olten. Son vaste programme de spécialisation en économie en fait l'un des leaders des hautes écoles spécialisées de Suisse.

Le professeur Marc K. Peter dirige le centre de compétences Transformation numérique à la Hochschule für Wirtschaft FHNW. Ce centre propose des prestations de recherche, de conseil et de formation en lien avec la transformation numérique, dans le but d'aider les organisations et leur personnel à développer et à mettre en place des stratégies de croissance numérique.

Outils clés pour la transformation numérique des PME (en allemand) :

Canevas d'atelier Transformation numérique
Grâce à cet outil gratuit, vous et votre personnel pouvez identifier des idées et des potentiels pour la transformation de votre entreprise.
www.digital-transformation-canvas.net

Canevas d'atelier Développement stratégique à l'ère du numérique
Avec ce canevas d'atelier, vous et votre personnel disposez d'un outil gratuit pour développer ensemble une stratégie axée sur la transformation numérique de votre entreprise.
www.act-strategy-canvas.ch

Canevas d'atelier Environnement de travail 4.0
Gratuit, cet outil vous permet d'identifier avec votre personnel des idées et des potentiels pour votre stratégie liée à l'environnement de travail.
www.arbeitswelt-zukunft.ch/workshop-canvas

Évaluation de la maturité numérique
Cet outil d'analyse gratuit permet d'évaluer votre propre maturité et celle de votre entreprise sur les points suivants : quel est votre stade d'avancement en matière de numérisation?

Avez-vous lancé ou déjà réalisé des projets dans tous les champs d'action? À quel niveau avez-vous identifié un potentiel (majeur)?
www.digitale-reife.net

Détermination des thèmes stratégiques
Le «Strategy Check» en ligne, gratuit, vous permet de définir les thèmes et les questions à discuter dans le cadre du développement stratégique à l'ère du numérique.
www.digital-strategy-check.ch

Guide pratique Développement stratégique à l'ère du numérique
Résultats de recherche, conseils pratiques, études de cas, modèles de stratégie et listes de contrôle pour la planification et la mise en œuvre de la transformation numérique :
www.strategische-transformation.ch

Guide pratique Transformation numérique pour les PME
Résultats de recherche, conseils pratiques, études de cas et listes de contrôle pour la transformation de votre PME :
www.kmu-transformation.ch

Guide pratique pour l'environnement de travail 4.0
Résultats de recherche, conseils pratiques, études de cas et listes de contrôle pour votre nouvel environnement de travail :
www.arbeitswelt-zukunft.ch

Plus d'informations :
FHNW Hochschule für Wirtschaft
Institute for Competitiveness & Communication
Prof. Marc K. Peter
Centre de compétences Transformation numérique
Riggenbachstrasse 16
4600 Olten

marc.peter@fhnw.ch
www.digitale-transformation-artikel.ch

Évolution des habitudes en matière de télétravail pendant les deux premières années de pandémie

Combien de vos collaborateurs ont principalement travaillé depuis chez eux entre le 20 décembre 2021 et le 2 février 2022, c'est-à-dire pendant l'obligation de télétravail? Combien travaillent aujourd'hui essentiellement depuis chez eux après la levée de l'obligation de télétravail?

Comment voyez-vous l'évolution à long terme: y aura-t-il davantage, autant ou moins de collaborateurs qui feront du télétravail que pendant la pandémie?

Au fil des trois enquêtes menées de 2020 à 2022, le nombre de collaborateurs en télétravail a évolué en fonction de la situation aussi bien pendant qu'après les phases de télétravail obligatoire. Avant le premier confinement de 2020, 10 % du personnel des PME comptant au moins un poste adapté au télétravail travaillait principalement depuis la maison. Cette valeur a pratiquement quadruplé pendant le premier confinement (à 38 %) avant de se replier à 16 %, soit une hausse de 60 % par rapport à la valeur d'avant-pandémie. Pendant le deuxième confinement, elle a de nouveau presque quadruplé, atteignant 36 %. Elle s'est ensuite stabilisée fin 2021 à un niveau élevé (20 %), tous secteurs confondus, puis a légèrement reculé début 2022, comme cela avait été pressenti en 2021. Durant les phases de télétravail obligatoire, le nombre de collaborateurs travaillant depuis chez eux a aussi quelque peu baissé, passant de 38 % en 2020 à 36 % en 2021 et 32 % en 2022.

Environ un tiers (32 %) des collaborateurs des PME interrogées qui comptent au moins un poste compatible avec le télétravail ont essentiellement travaillé depuis chez eux durant la période de télétravail obligatoire décrétée en 2021–2022. Leur part a été particulièrement importante dans la branche TIC/marketing (60 %), où un quart d'entre eux (25 %) sont d'ailleurs restés en télétravail par la suite. La branche Services a elle aussi enregistré un fort pourcentage de collaborateurs en télétravail: environ deux cinquièmes (43 %) du personnel y a eu recours pendant la phase de télétravail obligatoire, et un peu plus d'un huitième (13 %) a ensuite largement conservé ce mode de travail.

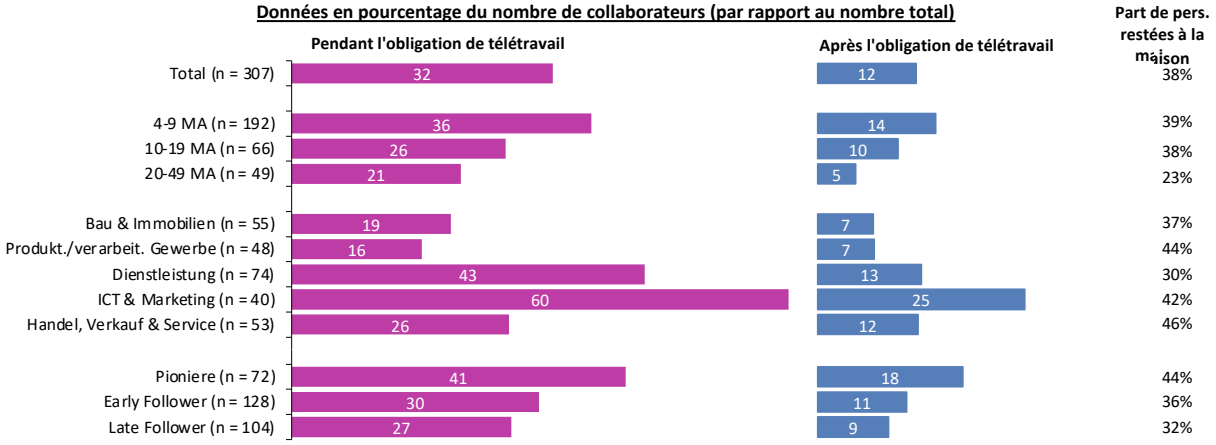
Plus les dirigeants interrogés définissent leur entreprise comme ouverte aux innovations technologiques, plus leur personnel a tendance à télétravailler. La part de collaborateurs à s'être pliés à l'injonction de télétravail a été d'environ deux cinquièmes (41 %) chez les pionniers, un tiers (30 %) chez les Early Followers et un quart (27 %) chez les Late Followers. Après la levée de l'obligation de télétravail, environ un cinquième (18 %) des collaborateurs ont continué de télétravailler chez les pionniers, contre quelque un dixième chez les Early et les Late Followers (respectivement 11 % et 9 %).

Alors que, lors de la première obligation de télétravail, près d'un dirigeant sur trois (29 %) estimait encore que les collaborateurs seraient plus nombreux à faire du télétravail à l'avenir, ils n'étaient plus que la moitié (15 %) à le penser en 2021 – une part qui n'a guère évolué en 2022 (17 %). Environ un dirigeant sur trois (30 %) s'attend à ce que le nombre de collaborateurs en télétravail baisse dans le futur, et un peu plus de la moitié des sondés (52 %) pensent que la part de collaborateurs en télétravail s'est à présent stabilisée, autrement dit que la proportion de télétravailleurs restera identique.

Questions posées aux PME suisses:

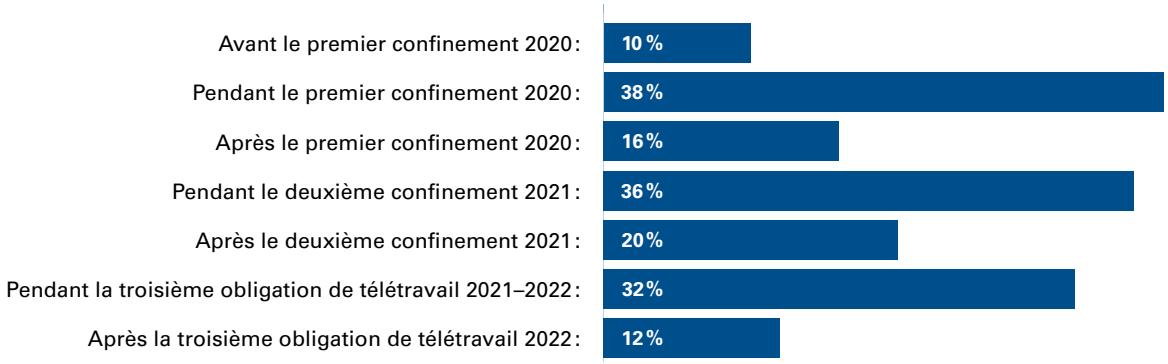
- Y a-t-il des domaines dans votre entreprise où le recours au télétravail a été jugé favorablement par les collaborateurs?
- Le télétravail pourrait-il continuer d'être proposé dans ces domaines après la pandémie?
- Avez-vous prévu un programme spécial pour le personnel (p. ex. un apéritif de bienvenue) visant à accompagner le retour au bureau sur le plan culturel et de la communication?

Évolution des habitudes en matière de télétravail pendant la pandémie en 2022



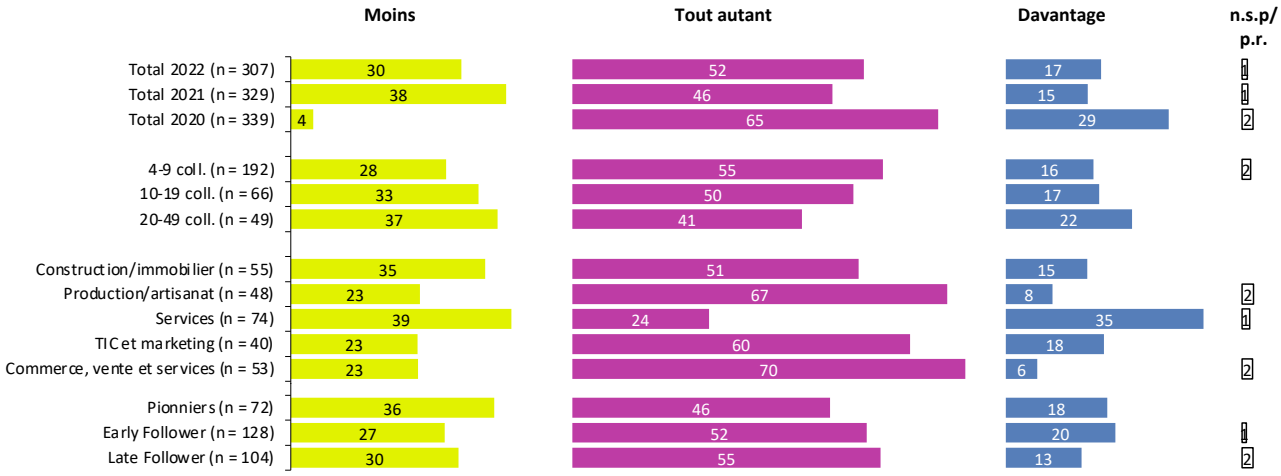
Évolution des habitudes en matière de télétravail pendant la pandémie en 2022 (n 2022 = 307, n 2021 = 329, n 2020 = 339, classement par catégories, données en pourcentage, les catégories avec un volume d'échantillonnage < 30 sont marquées d'un *, filtre : dans le cas où au moins un membre du personnel peut théoriquement faire du télétravail)

Évolution des habitudes en matière de télétravail pendant la pandémie en 2020–2022



Évolution des habitudes en matière de télétravail pendant la pandémie en 2020–2022 (n 2022 = 307, n 2021 = 329, n 2020 = 339, classement par catégories, données en pourcentage, les catégories avec un volume d'échantillonnage < 30 sont marquées d'un *, filtre : dans le cas où au moins un membre du personnel peut théoriquement faire du télétravail)

Estimation relative à l'évolution des postes en télétravail



Estimation relative à l'évolution des postes en télétravail (n 2022 = 307, n 2021 = 329, n 2020 = 339, classement par catégories, données en pourcentage, les catégories avec un volume d'échantillonnage < 30 sont marquées d'un *, filtre : dans le cas où au moins un membre du personnel peut théoriquement faire du télétravail)

Entretien sur le télétravail :

«Des inconvénients apparus au grand jour»

Les collaboratrices et collaborateurs sont toujours moins nombreux à faire du télétravail. Pourquoi?
Erika Meins, directrice du Laboratoire Mobilière d'analyse de données de l'EPF de Zurich, étudie les interactions numériques responsables. Ce recul ne la surprend pas.

Erika Meins est responsable du Laboratoire Mobilière d'analyse de données

Erika Meins, depuis cinq ans, avec votre équipe, vous étudiez les interactions entre l'humain et la machine. Il ressort de la dernière étude réalisée une nette tendance à un retour au bureau, au détriment du télétravail. Nous sommes actuellement 12 % à travailler principalement depuis chez nous, contre 38 % lors du premier confinement. Comment interprétez-vous ce résultat?
Avant la pandémie, le télétravail n'était pas un sujet prioritaire. Il était pratiqué par environ 10 % des collaboratrices et collaborateurs et seulement un jour par semaine pour la plupart d'entre eux. La situation a radicalement changé avec le confinement. Les entreprises en ont beaucoup profité. Sans le télétravail, la crise économique aurait été bien plus grave durant la pandémie. Je ne suis cependant pas surprise par ce recul du télétravail accusé après chaque obligation de télétravail. Cela tient au fait que les inconvénients du télétravail ont fini par apparaître au grand jour, sans occulter ses nombreux avantages.

Quels sont ces inconvénients?
Quand il s'inscrit dans la durée, le télétravail a ses limites. Épuisement physique, vide émotionnel pouvant aller jusqu'à une incapacité à se repérer dans le temps et dans l'espace : ces états peuvent apparaître chez les personnes qui doivent soudainement exercer une grande partie, voire l'intégralité de leurs activités en télétravail.

Comment est-ce possible?
Différentes explications sont avancées du point de vue scientifique : il s'agit tout d'abord de la «zoom fatigue», ou grande lassitude des vidéoconférences, qui a fait l'objet de nombreux travaux de recherche. Les réunions en ligne exigent de notre cerveau qu'il déploie plus d'énergie pour enregistrer les informations, car il y a de très petits décalages lors de la retransmission, la communication s'en trouve entravée. De même, le fait d'avoir toujours l'œil rivé sur un écran est fatiguant lui aussi. À cela s'ajoute la tendance au multitâche : pendant la réunion virtuelle, on répond rapidement à un e-mail ou on lit un SMS. Cela nous arrive à tous; or, paradoxalement, cela réduit notre aptitude à passer d'une tâche à l'autre et amoindrit notre mémorisation et notre performance.
Par ailleurs, les impressions visuelles, les odeurs et les bruits que nous percevons automatiquement en allant au travail ou sur notre lieu de travail disparaissent avec le télétravail. Sans ces différents stimuli sensoriels, les journées se suivent et se ressemblent, dans la grisaille, et on manque de repères. La performance en est affectée elle aussi.
Enfin, les interactions personnelles telles qu'elles nous sont familières au travail n'ont plus lieu et ce manque ne peut être compensé que partiellement dans le monde virtuel. Or, les relations sociales sont essentielles pour notre santé physique et mentale. Les contacts sociaux physiques ont sur notre système nerveux un effet apaisant et régulateur. Ils nous aident à réduire le stress. Ce sont aussi les contacts en face à face qui créent le sentiment d'appartenance sociale entre collègues de travail le plus fort. Arrivent ensuite les vidéoconférences, suivies du téléphone et, en queue de peloton, des messages.

Alors, retour au bureau pour tout le monde?
Pour une partie du moins. Cependant, si des réunions ne peuvent pas être organisées en présentiel, il vaut mieux privilégier un échange vidéo virtuel ou un appel téléphonique à l'envoi d'un e-mail ou d'un message instantané. Les nombreuses possibilités d'interaction numérique sont une énorme opportunité. Mais pour qu'elles soient utilisées de façon responsable dans un monde du travail hybride, il faut qu'employeurs et employés en aient conscience et ciblent cette utilisation.

Que peuvent faire les entreprises pour contrebalancer ces inconvénients?
Je conseille à toutes les entreprises, en particulier aux PME, d'engager un dialogue ouvert avec leur collaboratrices et collaborateurs. Il faut qu'elles identifient les besoins de leur personnel. Il est tout aussi important qu'elles formulent clairement leurs attentes, concernant par exemple les jours et les heures de présence, ainsi que les modalités de joignabilité et la marge de manœuvre de chacune et de chacun dans le cadre du télétravail. Les règles doivent être claires.

Que peuvent faire les collaborateurs pour que le télétravail se passe bien?
Il est primordial de faire des pauses afin de préserver sa performance. Si l'on passe beaucoup de temps devant un écran, on devrait avoir la possibilité de se distraire pendant les pauses : prendre l'air, lire un livre, entretenir des contacts sociaux, etc. Et il faut en finir avec le multitâche. Cela peut être utile de désactiver les messageries et de fermer des programmes que l'on n'utilise pas.

D'après vous, comment les choses vont-elles évoluer?
Le télétravail ne va pas disparaître, mais il ne remplacera pas le travail en présentiel. L'un et l'autre doivent se compléter avec pertinence et souplesse. Nous pourrons ainsi réunir le meilleur de ces deux mondes.

Laboratoire Mobilière d'analyse de données de l'EPFZ
Le Laboratoire Mobilière d'analyse de données, créé en 2013 par l'EPFZ et la Mobilière, fait partie intégrante de l'engagement sociétal de la Mobilière. Depuis sa création, différents projets de recherche interdisciplinaires ont été menés à bien aux points de contact entre l'humain et la machine. Le laboratoire s'est notamment fixé pour objectif de poursuivre l'amélioration des interactions numériques pour l'être humain et de renforcer la confiance qui leur est accordée.

Plus d'informations (en anglais) :
mobiliarlab.ethz.ch

Défis dans la mise en œuvre du télétravail

Du point de vue des entreprises, quels sont les défis majeurs posés par la mise en œuvre du télétravail?

Pour un peu plus d'un cinquième des PME, les principaux défis dans la mise en œuvre du télétravail résident dans trois facteurs: le facteur socio-émotionnel (défis d'ordre social, cohésion d'équipe, ambiance, solitude), le facteur technique (défis techniques tels que l'accès aux données et à la téléphonie) ainsi que le facteur organisationnel (problèmes d'organisation pour le personnel, p.ex. poste de travail). Près d'un dixième des PME suisses citent en outre les défis de management et les problèmes techniques liés à la sécurité.

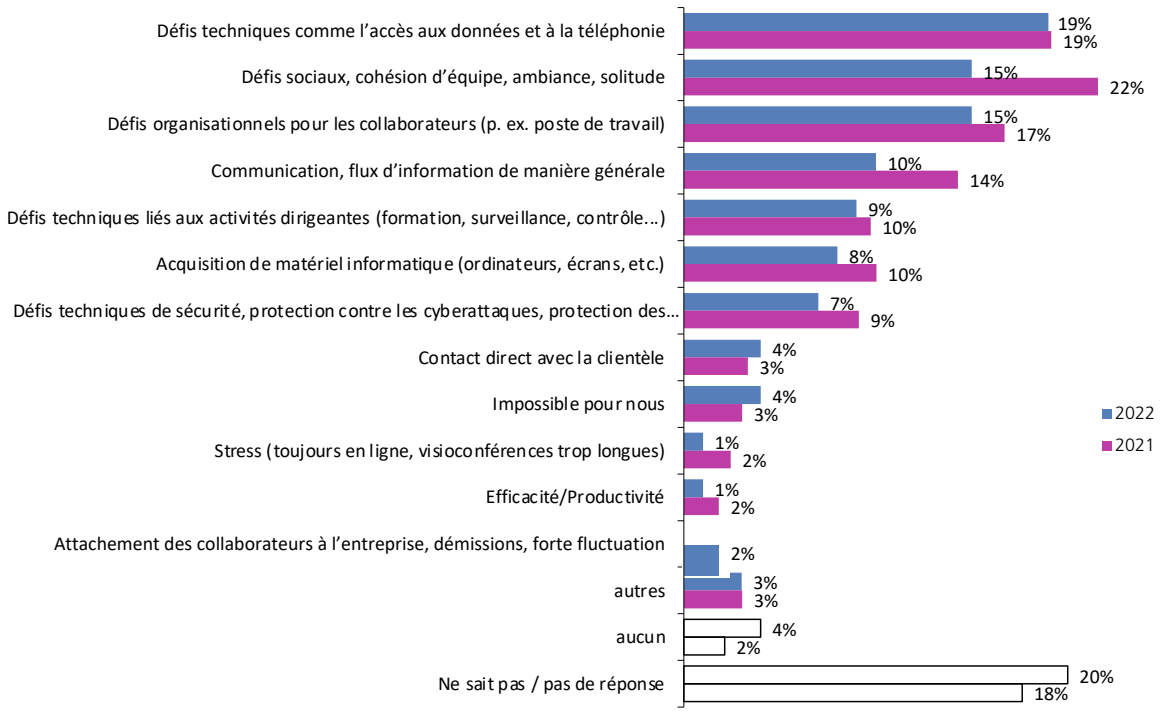
Par rapport à 2021, presque tous les défis sont perçus avec un degré de gravité moindre, ce qui peut traduire soit une amélioration de la situation, soit l'efficacité des mesures mises en place, avec pour résultat une meilleure infrastructure informatique.

Alors que la moyenne des défis cités était de 1,4 en 2021, elle s'établit à 1,2 en 2022. Le plus fort recul s'observe dans l'appréhension des défis relevant du facteur socio-émotionnel, à savoir défis d'ordre social, cohésion d'équipe, ambiance et solitude (2021: 22%, 2022: 15%). Cette dimension passe ainsi de la première à la deuxième place, qu'elle se partage avec les défis organisationnels (15% également). Les défis techniques tels que l'accès aux données et à la téléphonie arrivent donc désormais en première position, avec une valeur inchangée par rapport à 2021 (19% en 2021 et 2022).

Questions posées aux PME suisses:

- Quelles expériences positives ou négatives avez-vous tirées du télétravail pendant la pandémie? Quels enseignements en sont ressortis et quelles améliorations pourriez-vous apporter?
- Pourquoi n'avez-vous pas davantage recours au télétravail et ne l'utilisez-vous pas dans une stratégie de renouvellement de votre entreprise (p.ex. pour attirer des talents)?

Défis dans la mise en œuvre du télétravail



Défis dans la mise en œuvre du télétravail (n 2022 = 307, n 2021 = 329, n 2020 = 339, plusieurs réponses possibles, classement par catégories, données en pourcentage, les catégories avec un volume d'échantillonnage < 30 sont marquées d'un *, filtre: dans le cas où au moins un membre du personnel peut théoriquement faire du télétravail)

Utilisation des outils de communication

Parmi les outils de communication numériques cités, lesquels sont actuellement utilisés par vos collaborateurs pour communiquer avec des partenaires, la clientèle et d'autres membres du personnel?

Avec 97 % chacun, le téléphone et l'e-mail restent, en 2022, les moyens de communication les plus utilisés par les entreprises interrogées. Les écarts par rapport à 2021 sont minimes. Une comparaison avec l'année 2020 n'est possible que dans une certaine mesure, puisque d'autres catégories de réponse avaient alors en partie été définies. Entre 2020 et 2021, l'usage des outils de téléconférence a bondi de près de moitié (46 %) pour représenter presque deux tiers (64 %) des outils de communication, avant de stagner à un niveau élevé (62 %) en 2022. Les conseils et formations en ligne ont également progressé entre 2020 et 2021, jusqu'à représenter près de deux cinquièmes des outils de communication (2020 : 20 %, 2021 : 39 %). Ils se maintiennent depuis à ce niveau (2022 : 39 %).

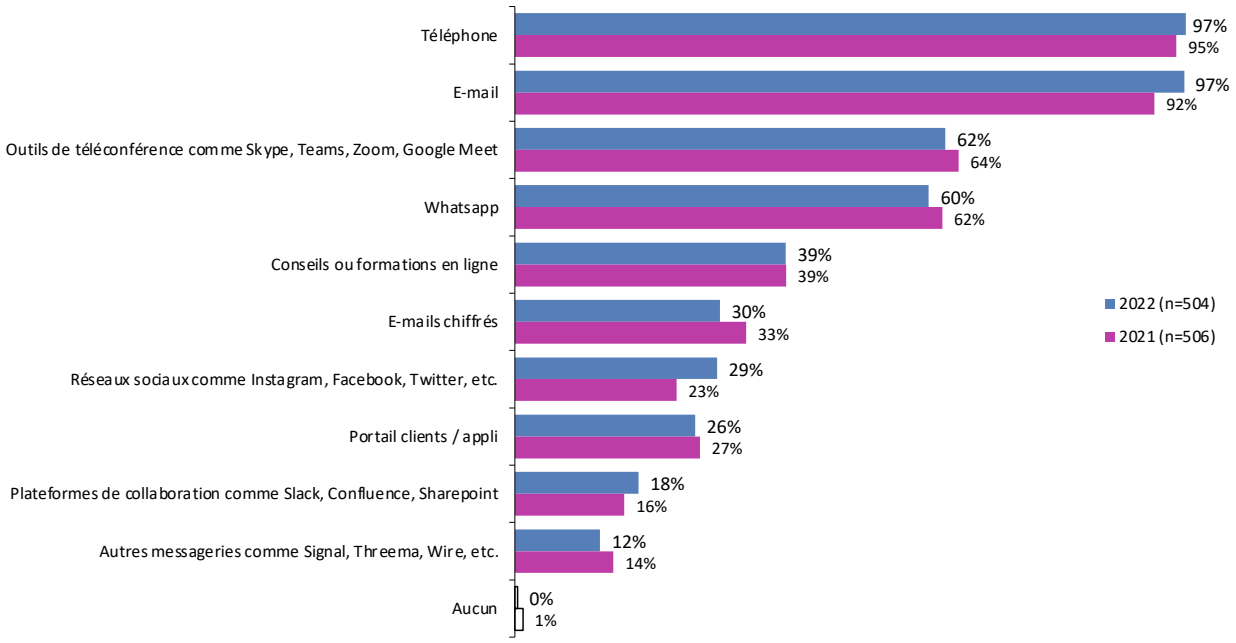
La branche TIC/marketing a bien plus souvent recours que les autres aux outils de téléconférence (91 %), aux conseils et formations en ligne (64 %) ainsi qu'aux plateformes de collaboration (64 %). Elle utilise globalement davantage d'outils de communication, comme en témoigne la valeur moyenne de 6,0 contre 4,3 à 4,9 dans les autres branches. À noter également l'ascension des réseaux sociaux, dont l'utilisation passe de 23 % en 2021 à 29 % en 2022.

De manière générale, on peut affirmer que plus il y a de collaborateurs dans une entreprise et plus ceux-ci sont nombreux à pouvoir télétravailler, plus l'usage des outils de communication est répandu. Les entreprises de 4 à 9 collaborateurs utilisent ainsi en moyenne 4,5 outils de communication, celles de 10 à 19 collaborateurs 4,8 et celles de 20 à 49 collaborateurs 5,2.
Les entreprises dépourvues de postes compatibles avec le télétravail utilisent en moyenne 4 outils de communication différents. Celles dont une partie des postes est compatible avec le télétravail en utilisent 4,9 et celles dont tous les postes sont compatibles avec le télétravail en utilisent 5,7. L'état d'esprit vis-à-vis des innovations technologiques se reflète par ailleurs sur le nombre de moyens de communication utilisés : ce nombre est en moyenne de 5,7 chez les pionniers, de 5,0 chez les Early Followers et de 3,9 chez les Late Followers.

Questions posées aux PME suisses :

- Un concept concernant l'utilisation d'outils de communication a-t-il été élaboré (et les plateformes les plus adaptées ont-elles été mises en place) ?
- Existe-t-il un concept et des directives concernant la sécurité des données pour l'utilisation professionnelle de ces plateformes de communication ?
- Les plateformes sont-elles sûres sécurisées ; quelles informations/données sont ou peuvent être échangées via quelles plateformes ?

Utilisation des outils de communication



Utilisation des outils de communication (n 2022 = 504, n 2021 = 506, plusieurs réponses possibles, classement par catégories, données en pourcentage, les catégories avec un volume d'échantillonnage < 30 sont marquées d'un *)

Degré personnel d'information concernant la thématique des cyberrisques

De façon générale, dans quelle mesure vous sentez-vous personnellement informé-e sur la question des cyberrisques?

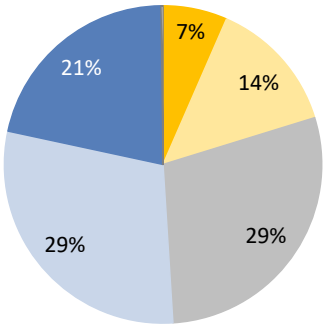
La moitié (50 %) des dirigeants interrogés s'estiment plutôt bien ou très bien informés (4 et 5 sur une échelle de 5) sur la question des cyberrisques, tandis qu'environ un sur cinq (21 %) estime être plutôt mal ou très mal informé (valeurs 1–2). La valeur moyenne s'inscrit ainsi à 3,5; inchangée par rapport à l'année précédente, elle ne varie que très légèrement par rapport à 2020 (3,4). Les plus grandes entreprises (20 à 49 collaborateurs) s'estiment les mieux informées (valeur moyenne 3,6), les deux autres catégories de PME (4 à 9 et 10 à 19 collaborateurs) sont en léger retrait avec une valeur moyenne de 3,4 (différence insignifiante). Plus les entreprises sont ouvertes aux innovations techniques et plus les mesures de sécurité techniques et organisationnelles sont résolument mises en œuvre, mieux les dirigeants se sentent informés sur les cyberrisques.

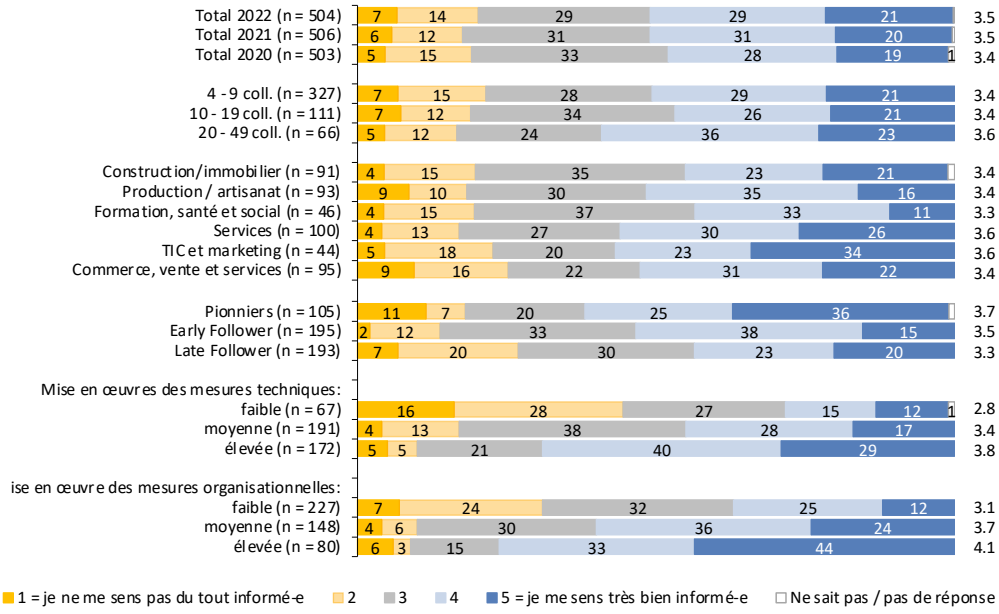
La branche TIC/marketing et celle des services ont la perception la plus positive de leur degré d'information (3,6 dans les deux cas), mais cette valeur n'est pas significativement supérieure à celle des autres branches (3,3 à 3,4). Les années précédentes (2020 et 2021), la branche TIC/marketing était encore loin devant les autres branches (2020 : 4,1, 2021 : 4,0). Elle est donc la seule branche à avoir revu à la baisse son évaluation, alors que les autres sont restées plus ou moins au même niveau.

Questions posées aux PME suisses :

- Procédez-vous à l'identification régulière du potentiel lié à l'utilisation de nouvelles technologies et avez-vous défini une stratégie/feuille de route pour la mise en place d'une nouvelle infrastructure informatique?
- Quels sont les nouveaux produits et services que vous pourriez commercialiser avec (davantage de) succès en investissant dans l'informatique et la cybersécurité?
- Répondez-vous à vos propres exigences (ou à celles du marché) en matière de cybersécurité?
- Comment procédez-vous pour vous informer régulièrement sur les dangers qui vous menacent ainsi que sur les concepts et solutions destinés à augmenter la cybersécurité?

Degré personnel d'information concernant la thématique des cyberrisques





Degré personnel d'information concernant la thématique des cyberrisques (n 2022 = 504, n 2021 = 506, n 2020 = 503, les catégories avec un volume d'échantillonnage < 30 sont marquées d'un *)

digitalswitzerland

À propos de digitalswitzerland

digitalswitzerland est une initiative nationale intersectorielle qui entend positionner la Suisse en tant que pôle d'innovation numérique de premier plan sur la scène internationale. Sous la bannière digitalswitzerland, cet objectif mobilise plus de 230 organisations composées de membres d'associations et de partenaires de fondations politiquement neutres. Véritable interlocuteur pour toutes les questions touchant à la numérisation, digitalswitzerland s'engage en faveur de solutions visant à répondre aux divers enjeux.

Outils clés pour les PME :

Test rapide de cybersécurité pour PME
cybersecurity-check.ch

Nombre de PME suisses n'ont pas conscience d'être insuffisamment protégées contre les risques sérieux liés au cyberespace. Le test rapide de cybersécurité de Cybero permet à chaque entreprise de déterminer si elle est suffisamment protégée contre les cyberrisques. Les risques potentiels peuvent être identifiés et mieux évalués. Le test rapide donne des indications sur la manière dont l'entreprise peut se comporter face aux risques :

– prévenir : p. ex. formations, logiciels antivirus
– réduire : p. ex. plan d'urgence, sauvegarde
– transférer : p. ex. par la souscription d'une assurance cybersécurité

Le test rapide de cybersécurité est soutenu par les partenaires suivants :
digitalswitzerland, Centre national pour la cybersécurité (NCSC), Alliance Sécurité Digitale Suisse (ADSS), Information Security Society Switzerland (ISSS), Académie suisse des sciences techniques (SATW), Association suisse de normalisation (SNV), Association Suisse pour Systèmes de Qualité et de Management (SQS), Association Suisse d'Assurances (ASA).

Des prestataires informatiques compétents pour une cybersécurité accrue
digitalsecurityswitzerland.ch

L'Alliance Sécurité Digitale Suisse a développé le label de qualité «Prestataire de services informatiques certifié» CyberSeal.

Le label CyberSeal atteste, au premier coup d'œil, de la fiabilité des prestataires informatiques et aide les PME dans le choix de leur partenaire informatique. Il distingue les prestataires informatiques qui garantissent à leur clientèle un niveau de protection approprié en appliquant les mesures techniques et organisationnelles requises. Le label CyberSeal renforce ainsi la sécurité numérique des PME et ancre la numérisation à un niveau de qualité supérieur.

Cyberattaques réussies et dommages consécutifs

Votre entreprise a-t-elle déjà subi une attaque par l'une des techniques suivantes, ce qui l'a contrainte à engager des frais considérables pour la réparation du dommage?

Après que la part d'entreprises attaquées a augmenté de façon significative – de 25 à 36 % – de 2020 à 2021, une baisse de quelques points de pourcentage, à 31 %, a été relevée en 2022. Comme en 2021 déjà, il n'y a pas de différences significatives entre les sous-groupes, même entre ceux qui présentent des différences notables sur d'autres points de cette étude, comme le degré d'information ou l'ouverture aux innovations techniques. Chose intéressante toutefois : plus les mesures de sécurité techniques sont résolument mises en œuvre, plus il apparaît que les entreprises concernées ont déjà été attaquées. Ce lien était déjà apparu en 2021. Cela peut notamment s'expliquer par le fait que les entreprises concernées ont mis en œuvre les mesures appropriées après l'attaque et sont dès lors à présent bien armées.

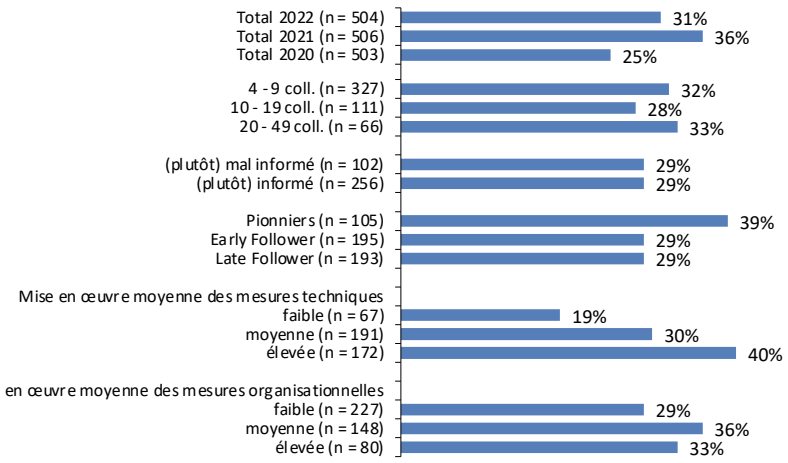
Au niveau des mesures organisationnelles, la situation est semblable, mais dans une moindre mesure : de manière générale, les entreprises qui présentent une mise en œuvre moyenne à élevée des mesures ont plus souvent été victimes d'une cyberattaque réussie par le passé que les entreprises qui n'ont que faiblement mis en œuvre les mesures nécessaires. Ce lien aussi avait déjà été relevé en 2021. S'il se vérifie que les entreprises renforcent la mise en œuvre des mesures après une attaque réussie, elles recourent alors forcément davantage aux mesures techniques qu'aux mesures organisationnelles (ou du moins prioritairement).

Comme en 2021, les attaques les plus fréquemment citées sont liées aux maliciels, aux virus et aux chevaux de Troie : une personne interrogée sur cinq (20 %) a subi une telle attaque. Cette valeur se situe entre le résultat de 2020 (18 %) et celui de 2021 (23 %). La seconde forme d'attaque la plus fréquemment mentionnée est la fraude en ligne (11 %). Cette valeur a aussi fortement augmenté en 2021, passant de 6 à 15 %, et a maintenant de nouveau légèrement diminué. Le nombre de cas de chantage ne cesse de croître depuis 2020. Mais les différences sont très minimes et pourraient être le fait du hasard. Le vol de données et la surcharge intentionnelle du réseau ou du serveur (déni de service) sont cités, de façon constante, par une entreprise sur vingt (5 %).

Questions posées aux PME suisses :

- Les collaborateurs connaissent-ils les divers types de cyberattaques? Comment les sensibilisez-vous à cette thématique?
- Quelles mesures techniques et organisationnelles avez-vous mises en place pour augmenter la cybersécurité dans votre entreprise?
- En quoi consiste l'examen régulier de vos concepts et mesures en matière de cybersécurité?

Parts de PME attaquées avec succès



Parts de PME attaquées avec succès (n 2022 = 504, n 2021 = 506, n 2020 = 503, les catégories avec un volume d'échantillonnage < 30 sont marquées d'un *)

L'Académie suisse des sciences techniques (SATW) est le principal réseau suisse d'experts dans le domaine des sciences techniques. Sur mandat de la Confédération, la SATW identifie les évolutions technologiques capitales sur le plan industriel et informe le monde politique et la société de leur importance et de leurs conséquences. En tant qu'organisation spécialisée politiquement indépendante, la SATW s'engage pour que l'ensemble des acteurs puissent évoluer dans le cyberespace en toute sécurité.

Cybersécurité : les défis pour la Suisse
À l'aide de brèves fiches d'information, les membres du comité consultatif de cybersécurité de la SATW donnent un aperçu des évolutions technologiques actuelles pertinentes du point de vue de la cybersécurité. Cette démarche est complétée par la description d'un champ d'action à court et moyen terme pour chacune des évolutions citées.
www.satw.ch/fr/cybersecurite/cybersecurity-map

Technology Outlook
La SATW identifie en amont les évolutions technologiques qui jouent un rôle central pour l'économie. Elle informe la société et la classe politique de l'importance et des conséquences de ces technologies, notamment par la voie de la publication «Technology Outlook», qui paraît tous les deux ans.
www.satw.ch/fr/to2021

Réseau d'autodétermination numérique
Le réseau d'autodétermination numérique s'engage pour une utilisation innovante et autodéterminée des données en Suisse. Son but est de saisir et de promouvoir pleinement le potentiel de notre économie et de notre société de données. La SATW a mis ce réseau sur pied conjointement avec la Direction du droit international public du DFAE, l'Office fédéral de la communication et Swiss Data Alliance.
www.satw.ch/digitale-selbstbestimmung

Promotion de la relève
À travers la promotion de la relève, la SATW entend rapprocher les jeunes des métiers technologiques. Elle s'engage en faveur d'une formation technique complète, apportant ainsi une réponse active à la pénurie de main-d'œuvre qualifiée. Un accent particulier est mis sur la promotion féminine dans les métiers techniques.
www.satw.ch/fr/promotion-de-la-releve

Pour plus d'informations :

SATW
Académie suisse
des sciences techniques
St. Annagasse 18
8001 Zurich
www.satw.ch

Risques de cyberattaques réussies

Comment évaluez-vous le risque que votre PME fasse l'objet, au cours des deux à trois prochaines années, d'une cyberattaque qui paralyserait votre entreprise durant au moins un jour?

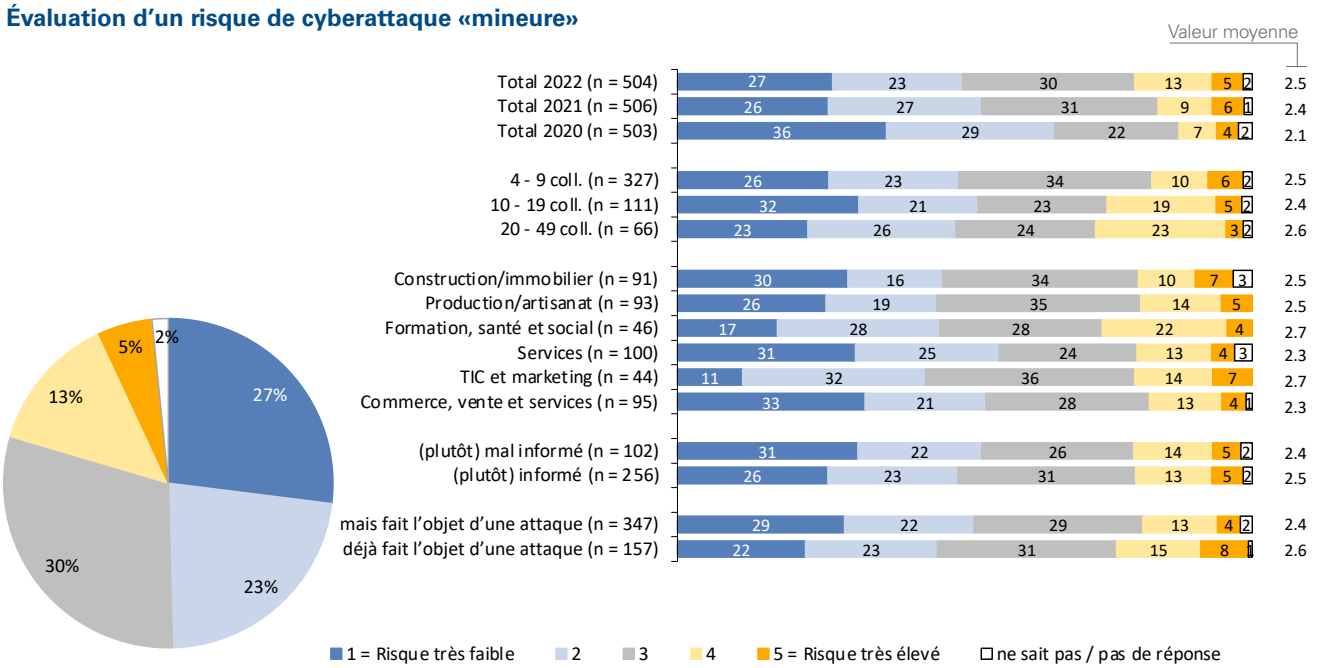
En 2002, la valeur pour l'évaluation du risque d'immobilisation pendant un jour à la suite d'une cyberattaque a légèrement augmenté pour la deuxième fois; en 2020, la valeur moyenne se situait encore à 2,1, mais elle a ensuite augmenté à 2,4 en 2021, puis à 2,5 en 2022. La part des dirigeants interrogés qui jugent le risque d'immobilisation pendant un jour à la suite d'une cyberattaque très élevé ou plutôt élevé approche aujourd'hui les 18 %, soit près d'un dirigeant sur cinq. La moitié des dirigeants interrogés (50 %) estiment ce risque plutôt faible, voire très faible.

Ce sentiment de sécurité est uniformément réparti entre les sous-groupes / au sein de l'intervalle de confiance. Seules quelques différences significatives ont été relevées : les Late Followers (valeur moyenne 2,2) jugent le risque nettement moins élevé que les pionniers (2,8) et les Early Followers (2,6). L'évaluation des Late Followers n'a pas changé par rapport à l'année précédente, tandis que les Early Followers et les pionniers jugent le risque un peu plus élevé en 2022 qu'en 2021 (pionniers : 2,7, Early Followers : 2,5). Les entreprises qui ont déjà été victimes d'une cyberattaque jugent ce risque plus élevé que celles qui n'ont pas (encore) été attaquées.

Questions posées aux PME suisses :

- Quelle est l'infrastructure informatique critique pour la fourniture de prestations dans votre entreprise ou quelle importance attachez-vous à la cybersécurité?
- Quelles sont les prestations que vous ne seriez pas en mesure de fournir en cas de défaillance des systèmes informatiques?
- Quelle protection de votre infrastructure informatique avez-vous définie?
- De quels concepts/plans d'urgence disposez-vous ou quels éléments vous manquent?

Évaluation d'un risque de cyberattaque «mineure»



Évaluation d'un risque de cyberattaque menaçant l'existence de l'entreprise (n 2022 = 504, n 2021 = 506, n 2020 = 503, les catégories avec un volume d'échantillonnage < 30 sont marquées d'un *)

Risques de cyberattaques menaçant l'existence de l'entreprise

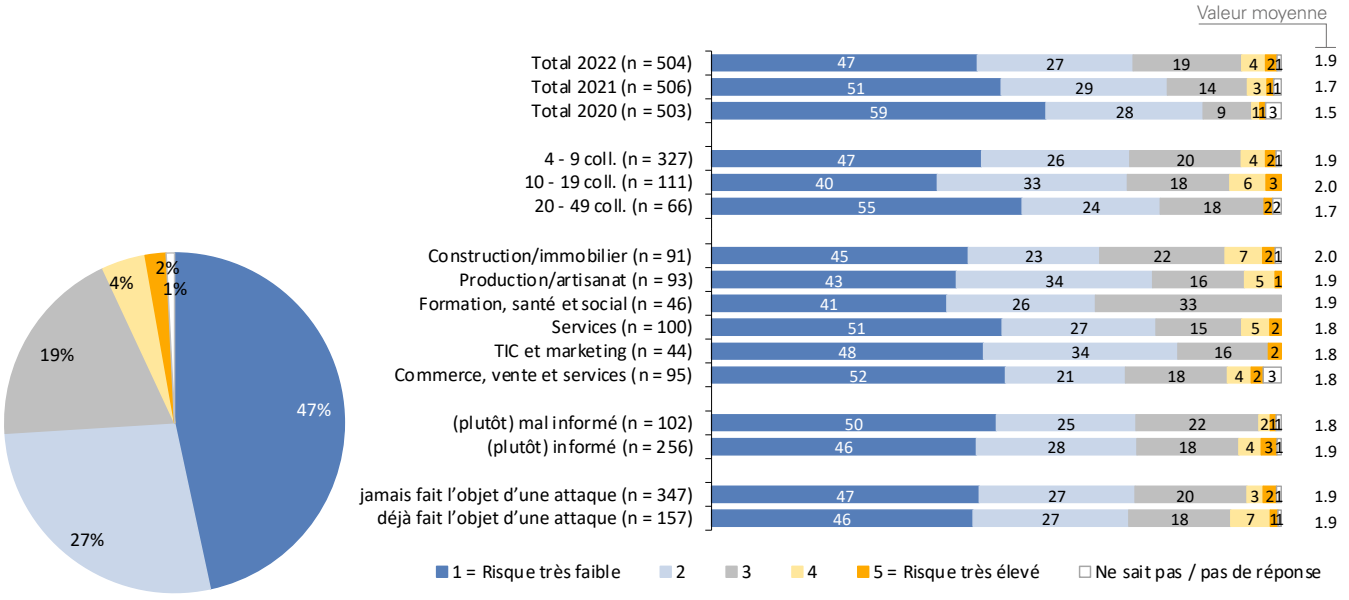
Comment évaluez-vous le risque qu'au cours des deux ou trois prochaines années, votre PME soit victime d'une cyberattaque propre à menacer son existence?

Même si le scénario d'une cyberattaque propre à menacer l'existence de l'entreprise n'est jugé réaliste que par une poignée de dirigeants, cette estimation n'en est pas moins en constante progression depuis 2020. À l'époque, la valeur moyenne s'élevait encore à 1,5, contre 1,7 en 2021 et 1,9 en 2022. La part de dirigeants interrogés qui jugent le risque d'une cyberattaque menaçant l'existence de l'entreprise plutôt élevé ou très élevé se situe autour d'un sur vingt (6 %). Près de trois quarts des dirigeants interrogés (74 %) jugent le risque plutôt faible ou très faible. Un seul sous-groupe présente une différence significative: les entreprises de Suisse alémanique et romande (2,0 et 1,8) jugent le risque significativement plus élevé que les entreprises tessinoises (1,4). Contrairement à la question précédente, il n'y ici aucune différence entre les entreprises ayant ou non fait l'objet de cyberattaques (1,9 dans les deux cas); les dirigeants d'entreprise victimes de cyberattaques citent donc un risque supérieur de cyberattaques de nature à immobiliser l'entreprise pendant un jour, mais pas de cyberattaques menaçant l'existence de leur entreprise.

Questions posées aux PME suisses:

- Quelles solutions alternatives (concepts de restauration des données) avez-vous mises au point?
- Si votre entreprise est fortement dépendante de l'informatique, serait-il judicieux d'investir dans une infrastructure informatique parallèle (ce que l'on appelle un «hot site»?
- De quels concepts/plans d'urgence disposez-vous ou quels éléments vous manquent?

Évaluation d'un risque de cyberattaque menaçant l'existence de l'entreprise



Évaluation d'un risque de cyberattaque menaçant l'existence de l'entreprise (n 2022 = 504, n 2021 = 506, n 2020 = 503, les catégories avec un volume d'échantillonnage < 30 sont marquées d'un *)

Mesures techniques visant à renforcer la cybersécurité

Jusqu'à quel point les mesures techniques suivantes destinées à accroître la cybersécurité ont-elles été mises en œuvre chez vous?

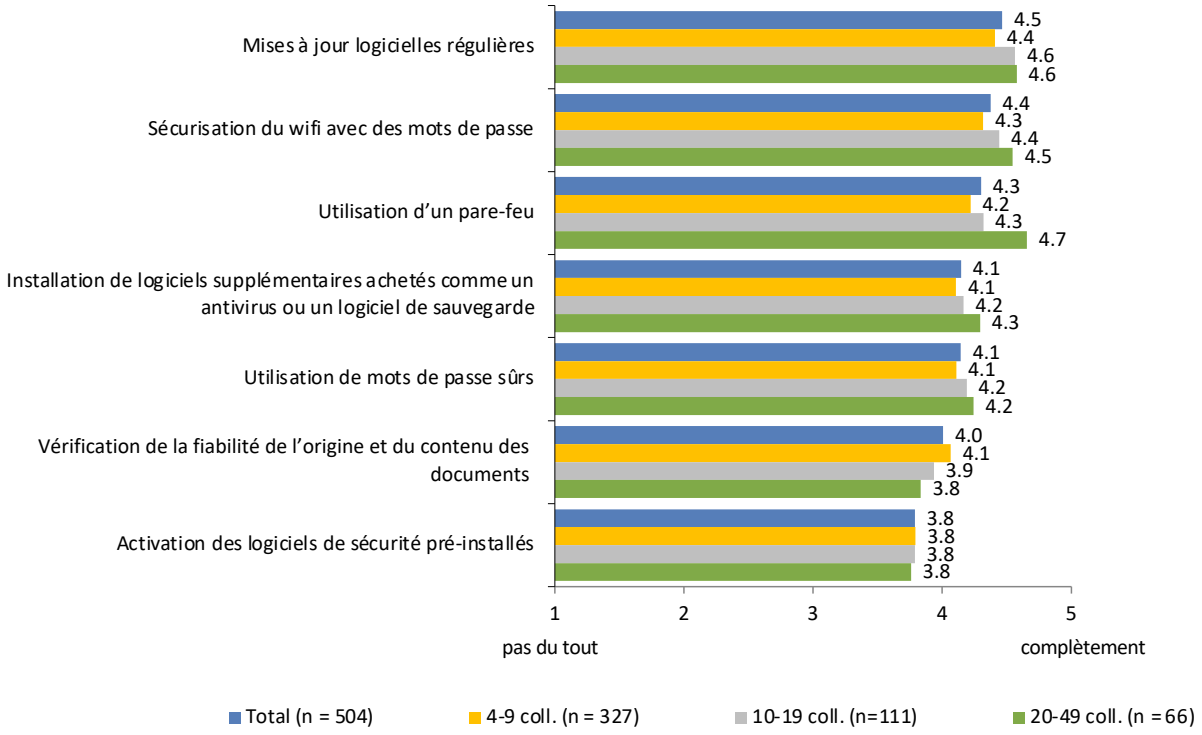
Les degrés de mise en œuvre des différentes mesures engagées se situent entre 3,8 et 4,5 et n'accusent donc qu'un recul minime par rapport à 2021. Les mises à jour logicielles régulières affichent le degré de mise en œuvre le plus élevé (86 % presque entièrement ou complètement mises en œuvre, valeur moyenne 4,5), suivies par la sécurisation du wifi avec des mots de passe (82 % presque entièrement ou complètement mise en œuvre, valeur moyenne 4,5). L'activation des logiciels de sécurité pré-installés (60 % presque entièrement ou complètement mise en œuvre, valeur moyenne 3,8) affichent le degré de mise en œuvre le plus bas et une valeur moyenne inférieure à 4,0. Toutes mesures confondues, une constante apparaît: plus les dirigeants interrogés s'estiment informés, plus le degré de mise en œuvre des mesures est élevé.

Dans certaines circonstances, les mesures non mises en œuvre ou mises en œuvre a minima peuvent constituer un risque de sécurité considérable: d'une part pour les entreprises elles-mêmes, de l'autre pour les propriétaires des données susceptibles d'être volées (données clients, mots de passe, etc.). Sachant cela, il faut aussi tenir compte des faibles valeurs d'échelle: ainsi, huit entreprises sur 100 n'ont pas de pare-feu, sept n'ont acheté aucun logiciel de sécurité additionnel et plus d'une sur dix n'active pas les logiciels de sécurité pré-installés. Une certaine imprécision liée au faible niveau de connaissance des dirigeants interrogés doit toutefois être prise en considération.

Questions posées aux PME suisses:

- Avez-vous réalisé un inventaire de votre infrastructure informatique? Disposez-vous d'une liste répertoriant le matériel informatique et les logiciels (avec numéros de série, date et prix d'achat, version logicielle, etc.)?
- Quelle infrastructure informatique fait l'objet de mises à jour? Qui s'en charge et à quelle fréquence?
- Quelle protection de votre infrastructure informatique avez-vous définie pour garantir la continuité des activités en cas d'attaques ou d'autres problèmes?

Mesures techniques visant à renforcer la cybersécurité



Mesures techniques visant à renforcer la cybersécurité selon le nombre de collaborateurs (n 2022 = 504)

Mesures organisationnelles visant à renforcer la cybersécurité

Jusqu'à quel point les mesures organisationnelles suivantes destinées à accroître la cybersécurité ont-elles été mises en œuvre dans votre entreprise?

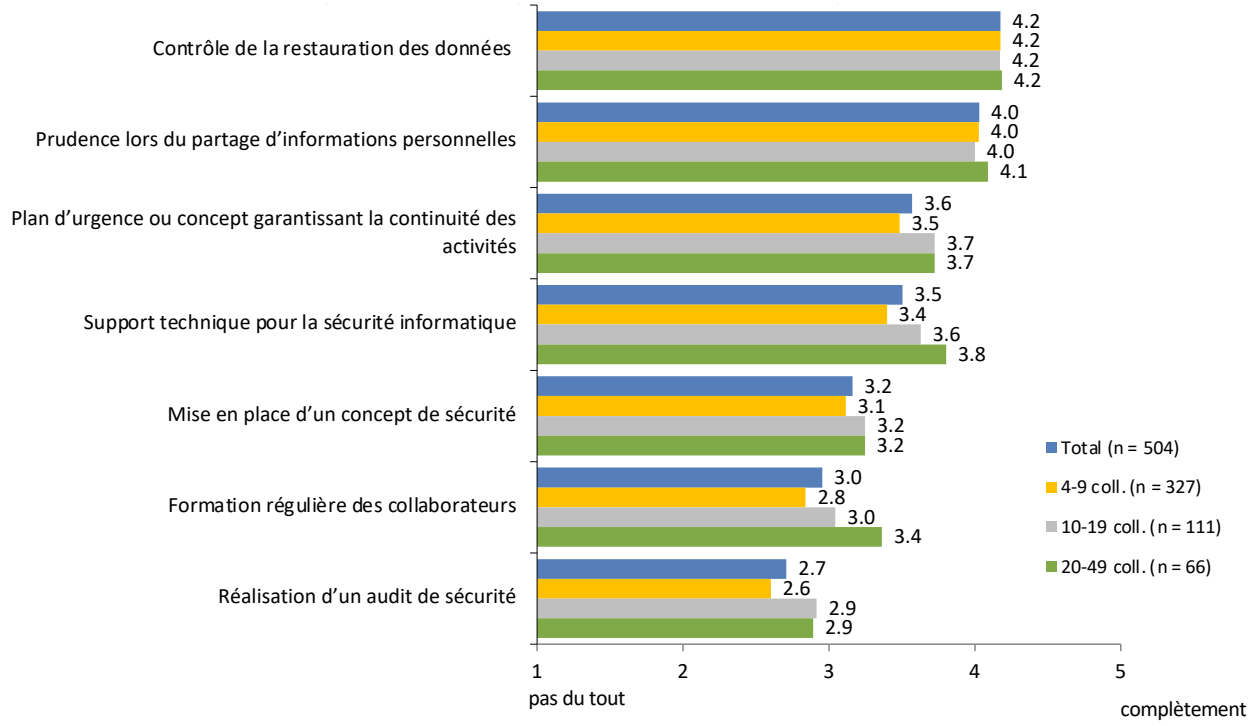
Comme l'étude de l'année précédente l'avait déjà révélé, les entreprises appliquent toujours nettement moins de mesures organisationnelles que de mesures techniques. La mesure organisationnelle la plus fréquemment appliquée est le contrôle de la restauration des données (4,2). Environ trois quarts (76 %) des dirigeants interrogés l'ont presque entièrement ou complètement mise en œuvre (2021 : 77 %). Par comparaison, la mesure organisationnelle la plus souvent intégralement appliquée – les mises à jour logicielles régulières – a été presque entièrement ou complètement mise en œuvre par plus de quatre cinquièmes (86 %) des dirigeants interrogés. En deuxième position des mesures organisationnelles appliquées figure la prudence lors du partage d'informations personnelles : près de trois quarts des dirigeants interrogés (73 %) l'ont presque entièrement ou complètement mise en œuvre (2021 : 74 %). En troisième position, gagnant ainsi une place, on trouve le plan d'urgence ou le concept garantissant la continuité des activités, avec un peu plus de la moitié (57 %) des dirigeants interrogés déclarant que cette mesure a été presque entièrement ou complètement mise en œuvre (2021 : 58 %). Suit alors le support technique pour la sécurité informatique avec environ la moitié (53 %) des dirigeants interrogés déclarant avoir mis cette mesure presque entièrement ou complètement en œuvre (2021 : 61 %). La mise en place d'un concept de sécurité (presque entièrement ou complètement mise en œuvre par 44 % des dirigeants interrogés), la formation régulière des collaborateurs (presque entièrement ou complètement mise en œuvre par 34 % des dirigeants interrogés) et la réalisation d'audits de sécurité (presque entièrement ou complètement mise en œuvre par 32 % des dirigeants interrogés) sont les mesures les moins appliquées. Les différences par rapport à l'année précédente sont minimes et non significatives.

Pour la grande majorité des mesures organisationnelles, il apparaît que les entreprises de Suisse alémanique les ont plus volontiers appliquées que les entreprises de Suisse romande, les pionniers, plus volontiers que les Early et Late Followers et les entreprises qui ont déjà fait l'objet de cyberattaques plus volontiers que les entreprises qui ne sont pas dans le cas. Mieux les dirigeants interrogés sont informés sur la thématique des cyberrisques, plus ils prennent des mesures organisationnelles pour améliorer la cybersécurité (significatif dans toutes les mesures). Ce constat avait également déjà été posé dans l'étude 2020/2021.

Questions posées aux PME suisses :

- Quelles mesures organisationnelles concrètes devraient être planifiées et mises en œuvre?
- Votre prestataire informatique est-il certifié ou suffisamment compétent pour vous assister?
- Devriez-vous éventuellement réaliser un audit de sécurité informatique et souscrire une cyberassurance?

Mesures organisationnelles visant à renforcer la cybersécurité



Mesures organisationnelles visant à renforcer la cybersécurité selon le nombre de collaborateurs (n 2022 = 504)

la Mobilière

Le Groupe Mobilière («la Mobilière») est le leader suisse de l'assurance standard et le numéro un des assurances ménage, PME et vie risque.
Fondée en 1826, la Mobilière est la plus ancienne société d'assurances privée de Suisse et opère encore, à ce jour, sur une base coopérative.
Pas moins de 80 agences générales entrepreneuriales possédant leur propre service des sinistres offrent des prestations de proximité à plus de 2,2 millions de clientes et clients sur 160 sites. Une entreprise sur trois et un ménage sur trois en Suisse sont ainsi assurés à la Mobilière.

Aperçu de l'offre de cyberprotection pour les PME

Scanner de points faibles Cyber RedBox
Les cybercriminels peuvent mettre à profit les failles dans l'infrastructure informatique pour pénétrer dans les systèmes de votre entreprise. La RedBox identifie de tels points faibles, de manière à pouvoir y remédier avant qu'un incident ne se produise.
Le scanner de points faibles RedBox est un service numérique innovant qui a été spécialement développé pour les PME. Il vous aide à mieux protéger votre entreprise contre les cyberattaques. Il scanne en permanence votre infrastructure informatique et vous avertit s'il détecte de nouveaux points faibles.

Plus d'informations sous
www.mobiliar.ch/redbox

Cyberformation pour les entreprises
Il suffit de peu de choses : un collaborateur ouvre un e-mail douteux et toute l'entreprise se retrouve paralysée. Cette formation sensibilise les collaborateurs aux risques liés à l'utilisation d'Internet et de l'e-mail.
À l'issue du cours, les collaborateurs connaissent les méthodes utilisées par les pirates informatiques et savent comment réagir en cas d'attaque.
Le programme de sensibilisation aux cyberrisques se compose de différents modules :

- séquences d'exercices en ligne pour apprendre comment réagir face aux menaces d'Internet
- simulation d'attaques par phishing avec évaluation de la réaction des collaborateurs
- rapport rassemblant les principaux résultats de la formation

Plus d'informations sous
www.mobiliere.ch/cyberformation

Cyberassurance
La cyberassurance consiste en un paquet complet de mesures qui permet de sécuriser l'exploitation d'une PME à la suite d'une cyberattaque. Cette assurance intervient comme suit :

- prise en charge des frais des spécialistes qui suppriment les maliciels, restaurent l'accès aux données et s'emploient à empêcher la divulgation de celles-ci;
- indemnisation d'une éventuelle interruption d'exploitation dont la durée excède douze heures;
- soutien financier et juridique si un client;
- reproche à la PME d'avoir provoqué un dommage en raison d'un e-mail contenant un virus;
- l'assistance IT vous aide de manière simple et rapide en cas de problèmes informatiques. Un expert intervient à distance pour résoudre les problèmes informatiques.

Plus d'informations sous
www.mobiliere.ch/cyberprotection-entreprises

Votre PME est-elle parée pour faire face aux cyberrisques?
Faites le point sur votre situation actuelle et découvrez où des améliorations doivent être apportées en procédant à un check-up cyberfitness.
www.mobiliere.ch/cyberfit

Renforcement des mesures de sécurité contre la cybercriminalité

Quelle est la probabilité que vous renforciez les mesures de sécurité contre la cybercriminalité dans les une à trois prochaines années?

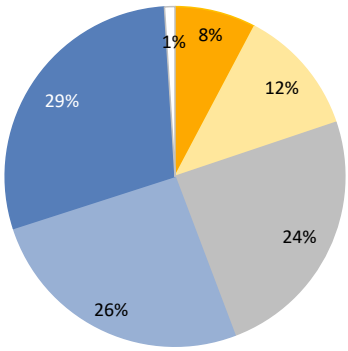
Près d'un tiers (29 %) des dirigeants interrogés pensent qu'il est très vraisemblable (valeur de 5 sur une échelle de 5) qu'ils renforcent leurs mesures de sécurité contre la cybercriminalité dans les une à trois prochaines années. Depuis l'année dernière (19 %), cette part a donc augmenté de moitié environ. Un autre quart environ (26 %) des dirigeants interrogés jugent un renforcement de la sécurité plutôt vraisemblable (valeur d'échelle 4). Par rapport à l'année précédente, la valeur moyenne a augmenté de 3,2 à 3,6.

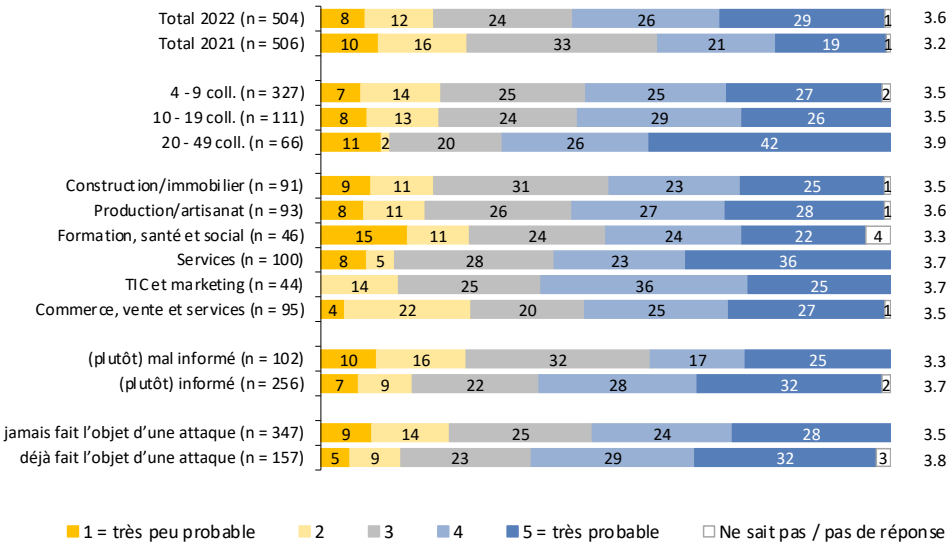
Les pionniers (3,9) et les Early Followers (3,7) tablent nettement plus souvent sur un renforcement des mesures de sécurité que les Late Followers (3,3) et les dirigeants interrogés plutôt bien à très bien informés sur les cyberrisques souhaitent davantage accroître leurs mesures de sécurité (3,7) que les dirigeants plutôt mal à très mal informés (3,3). De plus, les dirigeants qui ont déjà été victimes d'une attaque sont plus enclins à renforcer les mesures (3,8) que ceux qui n'en ont jamais fait l'objet (3,5).

Questions posées aux PME suisses :

- La hausse du télétravail a-t-elle aggravé la vulnérabilité informatique de votre entreprise?
- Quelles mesures de sécurité devriez-vous mettre en œuvre le plus rapidement possible en prévision des prochains mois (et dans l'optique de projets à venir)?
- Quelles autres mesures devraient être planifiées pour augmenter durablement la cybersécurité?
- Une collaboratrice ou un collaborateur a-t-il été désigné responsable de la protection des données et des règlements/processus correspondants ont-ils été introduits?

Renforcement des mesures de sécurité contre la cybercriminalité





Renforcement des mesures de sécurité contre la cybercriminalité (n 2022 = 504, n 2021 = 506, les catégories avec un volume d'échantillonnage < 30 sont marquées d'un *)

Mise en œuvre pratique pour les PME suisses

Thématiques et questions pour une mise en œuvre dans votre entreprise

À partir de l'étude, des thématiques identifiées et des défis posés aux PME, les autrices et auteurs ont établi la liste de contrôle ci-dessous, destinée à servir de base de discussion et d'outil dans le cadre d'un travail de projet.

Nous vous souhaitons beaucoup de succès dans la mise en œuvre de ces thématiques clés.

Stratégie concernant l'environnement de travail et mise en place du télétravail

- ☐ Dans quelle mesure le télétravail vous permet-il d'accroître la flexibilité de vos collaborateurs, de renforcer l'attrait de votre entreprise aux yeux du personnel et de réduire votre structure des coûts?
- ☐ Avez-vous déjà discuté du télétravail avec vos collaborateurs et, sur cette base, développé des idées, identifié des potentiels et élaboré une feuille de route?
- ☐ Y a-t-il des domaines dans votre entreprise où le recours au télétravail a été commenté favorablement par les collaborateurs?
- ☐ Existe-t-il une convention de télétravail, p. ex. pour la prise en charge des frais liés à l'équipement de bureau privé?
- ☐ Avez-vous identifié et défini les exigences posées par le «New Work» (environnement de travail 4.0) en matière de culture, de conduite et de communication?
- ☐ Avez-vous élaboré une stratégie et une feuille de route correspondante pour votre environnement de travail 4.0?
- ☐ Quelles expériences positives et/ou négatives avez-vous tirées du télétravail pendant la pandémie de COVID-19? Quels enseignements pouvez-vous en tirer et quelles améliorations pouvez-vous apporter?
- ☐ Le télétravail pourrait-il continuer d'être proposé dans ces domaines après la pandémie?
- ☐ Avez-vous prévu un programme spécial pour le personnel (p. ex. un apéritif de bienvenue) visant à accompagner le retour au bureau sur le plan culturel et de la communication?
- ☐ Un concept a-t-il été élaboré pour l'utilisation des outils de communication (et les plateformes les plus appropriées ont-elles par la suite été implémentées)?
- ☐ Avez-vous élaboré un concept et des directives sur la sécurité des données dans le cadre de l'utilisation des plateformes de communication à des fins professionnelles?
- ☐ Ces plateformes sont-elles sécurisées? Quelles sont les données/informations qui sont ou peuvent y être échangées, et quelle est la nature de ces plateformes?

Stratégies et mesures de cybersécurité

Acquisition de connaissances et sensibilisation

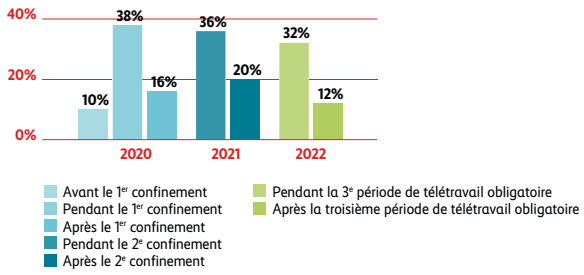
- ☐ Procédez-vous à l'identification régulière du potentiel lié à l'utilisation de nouvelles technologies et avez-vous défini une stratégie/feuille de route pour la mise en place d'une nouvelle infrastructure informatique?
- ☐ Quels sont les nouveaux produits et services que vous pourriez commercialiser avec (davantage de) succès en investissant dans l'informatique et la cybersécurité?
- ☐ Répondez-vous à vos propres exigences (ou à celles du marché) en matière de cybersécurité?
- ☐ Comment procédez-vous pour vous informer régulièrement sur les dangers qui vous menacent ainsi que sur les concepts et solutions destinés à augmenter la cybersécurité?
- ☐ Les collaborateurs connaissent-ils les divers types de cyberattaques? Comment les sensibilisez-vous à cette thématique?
- ☐ Quelles mesures techniques et organisationnelles avez-vous mises en place pour augmenter la cybersécurité dans votre entreprise?
- ☐ En quoi consiste l'examen régulier de vos concepts et mesures en matière de cybersécurité?
- ☐ Votre prestataire informatique est-il certifié ou suffisamment compétent pour vous assister?

Concepts et mesures

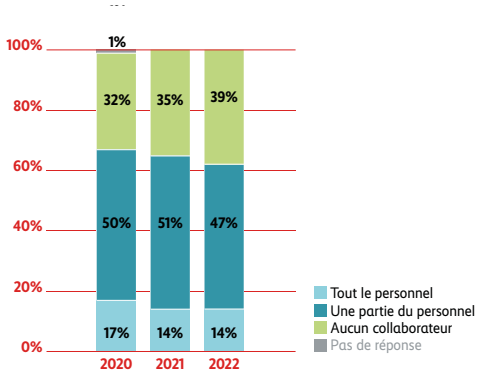
- ☐ Quelle est l'infrastructure informatique critique pour la fourniture de prestations dans votre entreprise ou quelle importance attachez-vous à la cybersécurité?
- ☐ Quelles sont les prestations que vous ne seriez pas en mesure de fournir en cas de défaillance des systèmes informatiques?
- ☐ Quelle protection de votre infrastructure informatique avez-vous définie?
- ☐ Quelles solutions alternatives (concepts de restauration des données) avez-vous mises au point?
- ☐ De quels concepts/plans d'urgence disposez-vous ou quels éléments vous manquent?
- ☐ Avez-vous réalisé un inventaire de votre infrastructure informatique? Disposez-vous d'une liste répertoriant le matériel informatique et les logiciels (avec numéros de série, date et prix d'achat, version logicielle, etc.)?
- ☐ Quelle infrastructure informatique fait l'objet de mises à jour? Qui s'en charge et à quelle fréquence?
- ☐ Quelle protection de votre infrastructure informatique avez-vous définie pour garantir la continuité des activités en cas d'attaques ou d'autres problèmes?
- ☐ Quelles mesures organisationnelles concrètes devraient être planifiées et mises en œuvre?
- ☐ Devriez-vous éventuellement réaliser un audit de sécurité informatique et souscrire une cyberassurance?
- ☐ Quelles solutions alternatives (concepts de restauration des données) avez-vous mises au point?
- ☐ Si votre entreprise est fortement dépendante de l'informatique, serait-il judicieux d'investir dans une infrastructure informatique parallèle (ce que l'on appelle un «hot site»)?
- ☐ Quelles mesures de cybersécurité devriez-vous impérativement ou immédiatement mettre en œuvre en prévision des prochains mois?
- ☐ Quelles autres mesures devraient être planifiées pour augmenter durablement la cybersécurité?
- ☐ Une collaboratrice ou un collaborateur a-t-il été désigné responsable de la protection des données et des règlements/processus correspondants ont-ils été introduits?

Infographie «Télétravail et cybersécurité dans les PME suisses 2022»

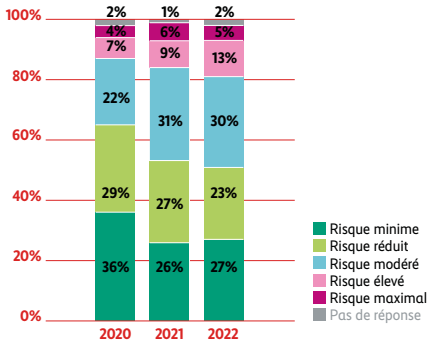
Évolution du télétravail depuis la période avant la pandémie jusqu'à ce jour



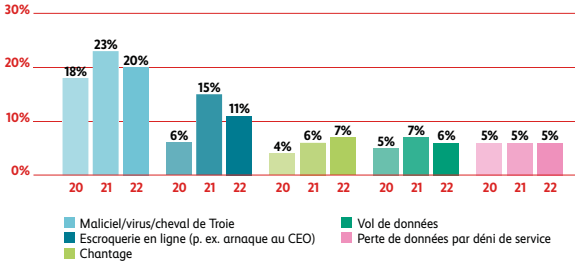
Proportion de collaboratrices et de collaborateurs qui peuvent potentiellement télétravailler



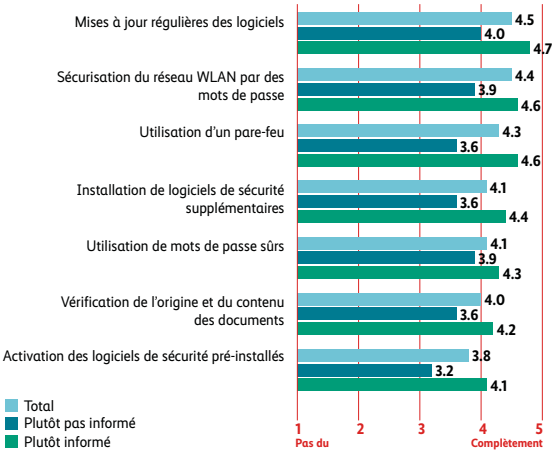
Évaluation du risque lié aux cyberattaques



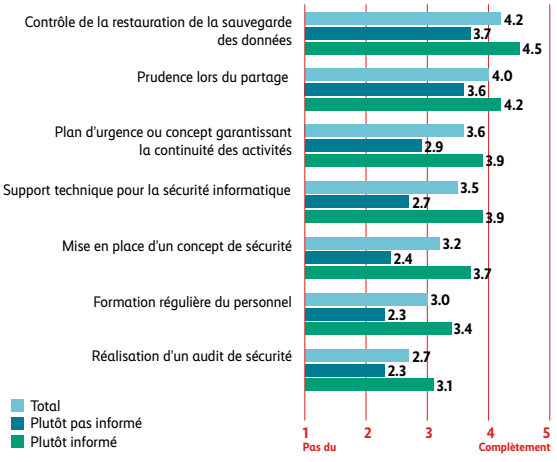
Types de cyberattaques



Mise en œuvre de mesures techniques



Mise en œuvre de mesures organisationnelles



Contact/autrices/auteurs

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

Andreas Hölzli
Responsable du centre de compétences Cyberrisques
La Mobilière, Berne
andreas.hoelzli@mobi.ch

Andreas W. Kaelin
Directeur Alliance Sécurité Digitale Suisse ASDS, Zug
Conseiller principal, digitalswitzerland, Berne

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, Andreas Hölzli, Andreas W. Kaelin, Karin Mändli Lerch, Patric Vifian & Nicole Wettstein :

Télétravail et cybersécurité dans les PME suisses : stratégies et mesures des PME suisses de 4 à 49 collaborateurs après deux années marquées par le COVID-19

— La Mobilière
— digitalswitzerland
— Hochschule für Wirtschaft (FHNW)
— Académie suisse des sciences techniques (SATW)
— Alliance Sécurité Digitale Suisse (ADSS)
— gfs-zürich

www.cyberstudie.ch
Berne, juin 2022