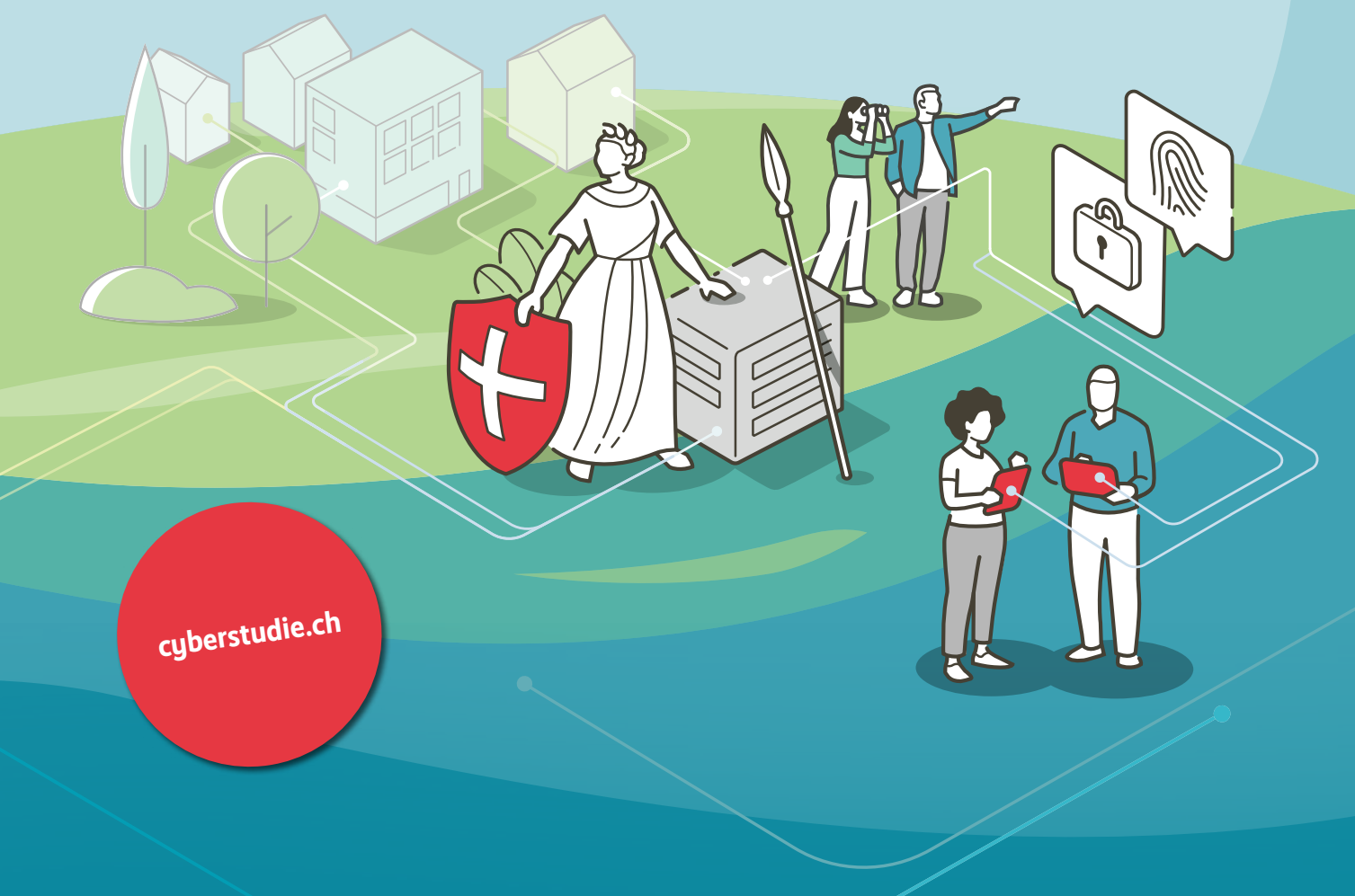


PME Cybersécurité 2026

Une étude de la Mobilière en collaboration avec l'OFCS, digitalswitzerland, la HES-SO, la HWZ et la SATW

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



cyberstudie.ch

Contenu

Introduction	3
01 Où en sont actuellement les PME suisses à l'ère du numérique?	4
02 La souveraineté numérique: un nouveau domaine thématique dans la politique mondiale actuelle	6
03 La cybercriminalité: un problème à prendre au sérieux aggravé par les nouveaux risques liés à l'IA	8
04 La cybercriminalité et les PME: plus de 35 000 entreprises touchées, et des conséquences souvent sérieuses	10
05 Connaissance des cybermenaces et des possibilités de soutien	12
06 Le thème de la cybersécurité regagne en importance	14
07 Cyberrisques: de plus en plus de PME définissent des responsabilités	16
08 Mise en œuvre de mesures techniques de cybersécurité	18
09 Mise en œuvre de mesures organisationnelles de cybersécurité	20
10 La cyberrésilience gagne toujours plus en importance, mais beaucoup de PME restent prudentes	22
Check-list pour les PME suisses	24
Outils pratiques et méthode d'enquête	26
Autrices et auteurs	27

Introduction

Ces dernières années, la transformation numérique a permis aux PME suisses de réaliser des avancées significatives. De nombreuses entreprises investissent dans des processus numériques, utilisent des services cloud, misent de plus en plus sur des stratégies numériques et travaillent avec les nouvelles technologies, comme l'intelligence artificielle (IA). Ce faisant, elles accroissent leur dépendance aux systèmes numériques, aux données et aux prestataires externes, et s'exposent donc à plus de risques. Aujourd'hui, la cybercriminalité constitue l'un des principaux défis stratégiques pour les PME suisses, et la grande majorité des entreprises s'attendent à ce que les cybermenaces continuent d'augmenter à la faveur de l'IA.

L'étude PME est réalisée tous les ans depuis 2020. Les résultats de l'étude actuelle «PME Cybersécurité 2026» révèlent des contrastes dans la situation des PME suisses. Bon nombre d'entre elles disposent de solides bases techniques: mises à jour logicielles, pare-feu, sauvegardes de données, authentification multifacteur, etc. En revanche, elles ont encore beaucoup de progrès à faire concernant les mesures organisationnelles (à l'instar des années précédentes). Elles pensent moins souvent aux plans d'urgence, aux audits de sécurité, aux évaluations des fournisseurs ou aux formations systématiques du personnel, alors même que ces éléments peuvent être essentiels pour leur résilience en cas d'urgence.

Il est réjouissant de constater que le thème de la cybersécurité revient au premier plan. De plus en plus d'entreprises définissent des responsabilités et investissent constamment dans de nouvelles mesures de protection. Le sentiment de résilience face aux cyberrisques est meilleur qu'en 2025, mais reste à un niveau inférieur à celui de 2024. L'étude montre également que de nombreuses PME considèrent encore qu'il est assez peu probable qu'un cyberincident grave survienne.

La principale conclusion à tirer est donc la suivante: la cybersécurité n'est plus une tâche purement informatique et relève désormais de la conduite. Les PME florissantes ne se contentent pas de protéger leurs systèmes et leurs données: elles pensent aussi à se préparer à faire face à une urgence au niveau organisationnel. Pour renforcer durablement sa cyberrésilience et gagner en compétitivité, il faut donc à la fois prévoir des mesures techniques de protection, définir clairement des responsabilités, former son personnel, disposer de sauvegardes testées et établir un plan d'urgence efficace.

Dans ces dix chapitres, nous présentons les principaux résultats de la dernière étude «PME Cybersécurité 2026» ainsi que des recommandations destinées à améliorer la cybersécurité et la cyberrésilience des PME. Vous trouverez les résultats détaillés de l'étude sur cyberstudie.ch.

Berne et Zurich, octobre 2026

La Mobilière, l'OFCS, digitalswitzerland, la HES-SO, la HWZ et la SATW

01 Où en sont actuellement les PME suisses à l'ère du numérique?

La dernière enquête réalisée auprès des PME révèle une situation contrastée en matière de transformation numérique en Suisse. Si beaucoup d'entreprises ont commencé à se numériser, elles n'évoluent pas toutes à la même vitesse selon leur branche, leur taille et leur disposition à innover.



Point positif: la plupart des PME estiment que leur transformation numérique est au moins moyennement avancée. Environ une entreprise sur dix considère même que sa stratégie numérique est avancée ou très avancée. Mais il reste une importante marge d'amélioration: **près d'une PME sur cinq déclare ne pas disposer de stratégie numérique ou ne pas mener de projet correspondant.**

Followers»). En outre, ces dernières ne disposent généralement pas d'une stratégie numérique. L'étude permet donc de tirer la conclusion suivante: **les entreprises qui sont parmi les premières à tester et utiliser les nouvelles technologies présentent un degré de maturité numérique nettement supérieur à celui des Late Followers.**

Les projets de numérisation en cours se concentrent sur des avantages pratiques. **Les PME investissent avant tout dans l'amélioration de la satisfaction de la clientèle et de l'utilisation des données, ainsi que dans la numérisation et l'automatisation de processus.** Ces initiatives contribuent directement à renforcer l'efficacité au travail et la compétitivité. En revanche, les entreprises sondées sont moins nombreuses à mener des projets visant à développer de nouveaux modèles d'affaires numériques, à introduire de nouvelles technologies ou à accroître l'attractivité de l'employeur.

L'étude permet de dresser un constat frappant concernant l'IA: **près de la moitié des PME interrogées n'ont toujours pas mis en œuvre de projet dans ce domaine.** À l'heure où tout le monde parle d'intelligence artificielle, l'utilisation de cette

Près de la moitié des PME interrogées n'ont toujours pas mis en œuvre de projet dans le domaine de l'IA.

Le lien entre la disposition à innover et la numérisation est particulièrement intéressant. **En effet, les entreprises qui sont parmi les premières à tester et utiliser les nouvelles technologies («Entreprises pionnières») font état d'un degré de maturité numérique nettement supérieur à celui des entreprises qui les ont adoptées tardivement («Late**

technology n'en est donc encore qu'à ses débuts dans le secteur des PME suisses.

Pour les PME, l'IA offre **surtout des opportunités stratégiques** en matière de culture d'entreprise et d'innovation, de partenariats ainsi que de numérisation et d'automatisation. Enfin, les PME sont encore

plus nombreuses qu'en 2025 à permettre à leur personnel de faire du télétravail: **désormais, 61% d'entre elles offrent au moins partiellement cette possibilité.**

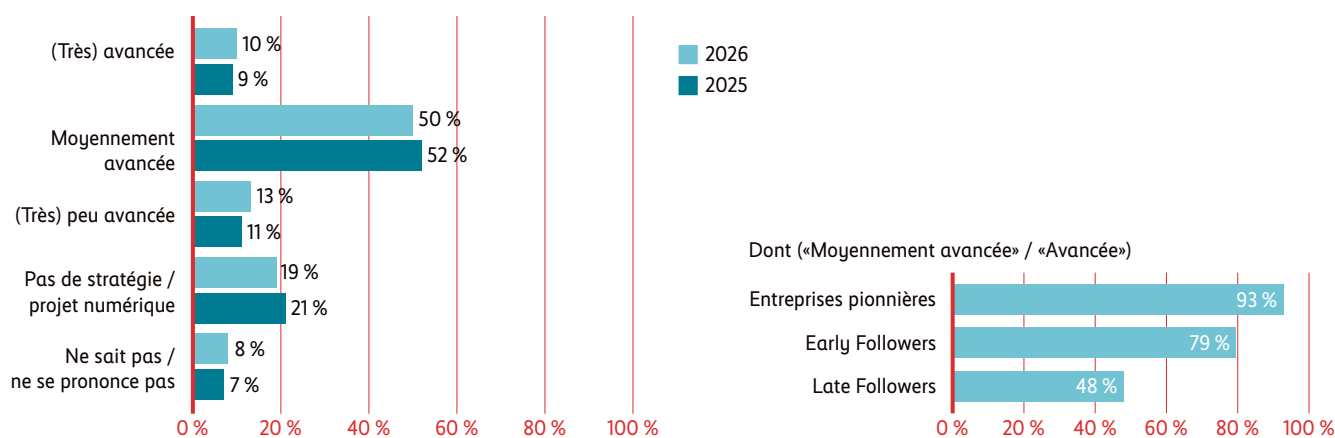
Les PME estiment que la situation politique et économique mondiale représente le plus grand risque stratégique. Environ 20 à 25 % d'entre elles considèrent l'inflation, la cybercriminalité et la pénurie de main-d'œuvre qualifiée comme des risques stratégiques. Plus l'entreprise est grande, plus elle accorde d'importance à la pénurie de main-d'œuvre qualifiée et à la cybercriminalité.

Dans l'ensemble, les résultats montrent que si les PME suisses continuent de se numériser, elles cherchent avant tout à optimiser leur activité actuelle. Pour le moment, seule une minorité d'entre elles exploite activement le potentiel le plus prometteur de la transformation numérique, que ce soit en proposant de nouvelles offres numériques, en élaborant des modèles d'affaires innovants ou en utilisant l'IA de manière ciblée. C'est peut-être là que de nombreuses entreprises trouveront les opportunités les plus intéressantes pour les années à venir.

Évolution de la stratégie numérique

Question: comment évalueriez-vous l'évolution de votre stratégie numérique ou de votre transformation numérique?

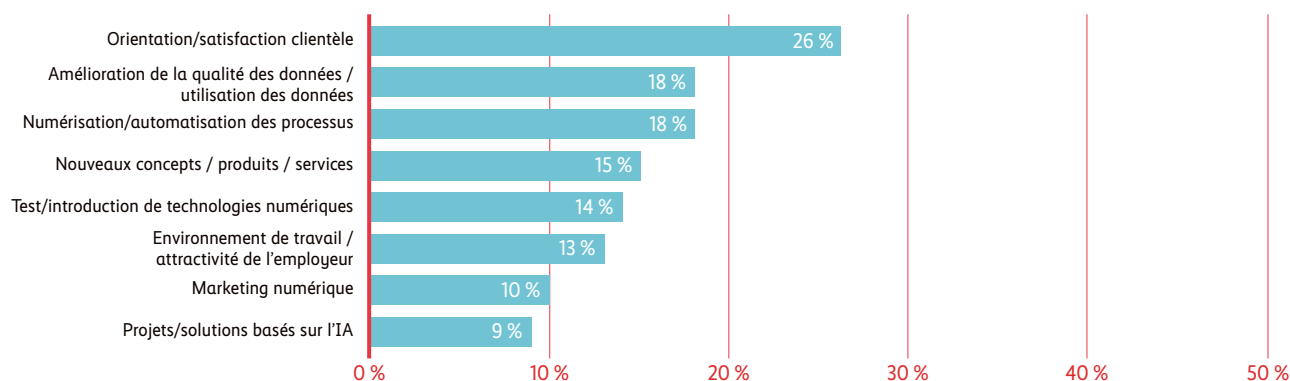
Échelle: 1-2 «(Très) peu avancée» / 3-5 «Moyennement avancée» / 6-7 «(Très) avancée».



Mesures de stratégie numérique mises en œuvre

Question: veuillez indiquer sur une échelle de 1 à 7 à quel point votre entreprise a mis en place les mesures suivantes au cours des trois dernières années.

Échelle: 1-2 «Non, (absolument) pas mise en place» / 3-5 «Partiellement mise en place» / 6-7 «(Entièrement) mise en place». Résultats représentés: échelle 6-7 «(Entièrement) mise en place»



02 La souveraineté numérique: un nouveau domaine thématique dans la politique mondiale actuelle

Ces dernières années, les changements géopolitiques ont mis en lumière un nouveau thème: la souveraineté numérique. Ce terme désigne **la capacité d'une entreprise à prendre des décisions concernant ses données, ses technologies et ses dépendances numériques avec la plus grande autonomie possible**. L'étude actuelle montre néanmoins que les PME suisses ont à peine commencé à évoluer en ce sens.

Les thèmes classiques sont ceux sur lesquels elles ont le plus avancé: **protection, souveraineté et stockage des données**. Plus d'un tiers des entreprises interrogées ont déjà pris des mesures concrètes à ce sujet. Beaucoup travaillent aussi activement sur la **protection contre les cyberrisques**. Manifestement, les PME jugent que ces domaines sont directement pertinents et essentiels pour elles.

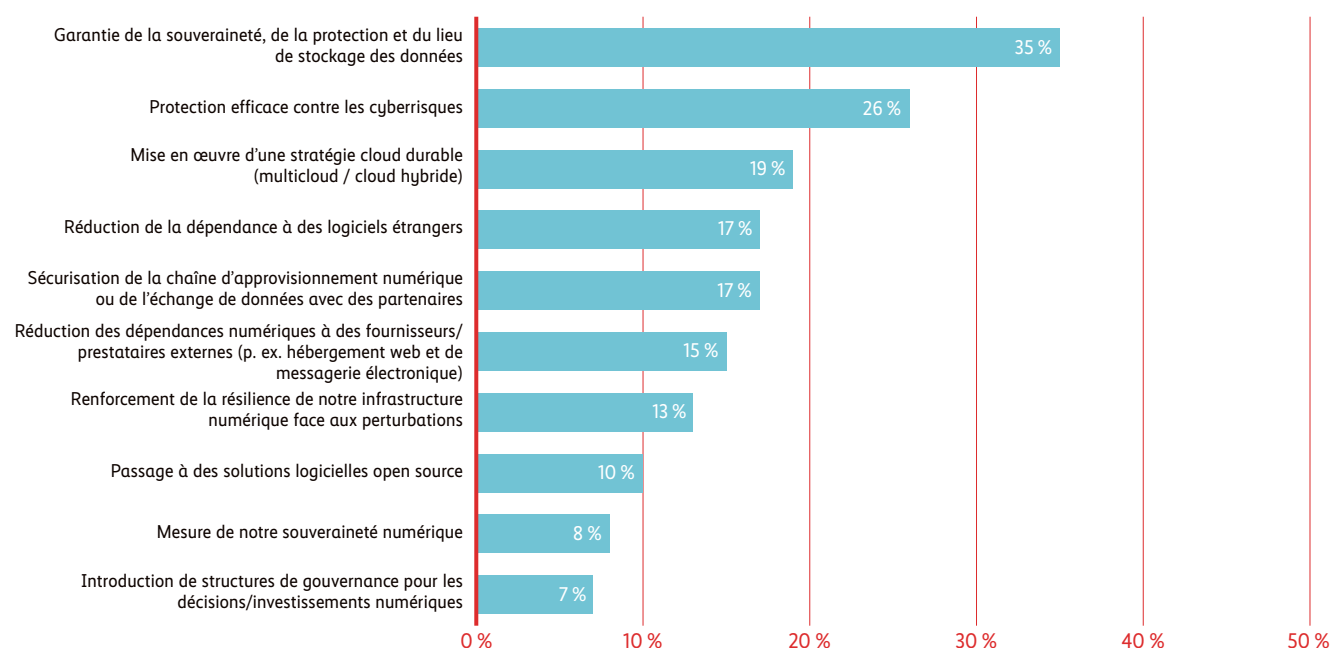
Elles sont cependant nettement moins soucieuses de **réduire leur dépendance à certains fournisseurs ou technologies**. Ainsi, seule une minorité d'entre elles ont déjà commencé à essayer de s'affranchir des logiciels étrangers, des prestataires informatiques externes ou des fournisseurs de services cloud. On peut faire le même constat en ce qui concerne des thèmes tels que la sécurisation de la chaîne d'approvisionnement numérique ou le passage à des solutions open source.

Il est particulièrement intéressant de noter **que de nombreuses entreprises ignorent encore presque tout de certains aspects de la souveraineté numérique**. En effet, environ un quart des PME sondées ne connaissent aucune structure de gouvernance pour les décisions numériques (7 % seulement disposent d'une structure correspondante) et près

Souveraineté numérique

Question: avez-vous déjà prévu ou mis en place des mesures sur le thème de la «souveraineté numérique»?

Échelle: de 1 «Jamais entendu parler» à 4 «Déjà mise en place». Résultats représentés: échelle 4 «Déjà mise en place»



d'un tiers n'ont encore jamais entrepris de mesurer leur propre souveraineté numérique. Pourtant, ces thèmes pourraient gagner en importance à l'avenir si les entreprises décident de gérer leurs risques numériques de manière plus systématique.

L'étude permet donc de tirer la conclusion suivante: si les PME suisses ont déjà commencé à s'intéresser activement à la protection des données et à la cybersécurité, elles ne voient souvent le thème de la souveraineté numérique qu'à travers ce prisme



De nombreuses entreprises ignorent encore presque tout de certains aspects de la souveraineté numérique.

étroit. ***Bon nombre d'entre elles ne se sont toujours pas posé la question plus large de la réduction des dépendances stratégiques aux technologies, aux plateformes ou à certains fournisseurs.*** En se penchant sur ces thèmes le plus tôt possible, une entreprise peut renforcer sa résilience et agir de manière plus autonome dans un monde numérique où l'incertitude ne cesse de croître.

03 La cybercriminalité: un problème à prendre au sérieux aggravé par les nouveaux risques liés à l'IA

Cela fait longtemps que la cybercriminalité est à l'ordre du jour des organes de direction des PME suisses. Les chiffres de l'étude actuelle sont sans appel: près de neuf entreprises sur dix (88 %) considèrent qu'il s'agit d'un problème à prendre au sérieux. Quel que soit leur type, leur taille ou leur branche, elles se rejoignent largement sur un point: **les cyberattaques représentent aujourd'hui une vraie menace pour chaque PME.**

d'augmenter à la faveur de l'IA. Seule une très petite minorité d'entre elles sont d'un autre avis. Beaucoup d'entreprises estiment donc que si l'IA offre des opportunités, elle représente également un nouveau danger.

Il est intéressant de noter que les PME, toutes tailles confondues, partagent globalement cet avis: qu'elles emploient quelques personnes

Les PME bien préparées n'ont donc pas seulement davantage conscience des risques: elles se sentent aussi plus capables de les gérer.

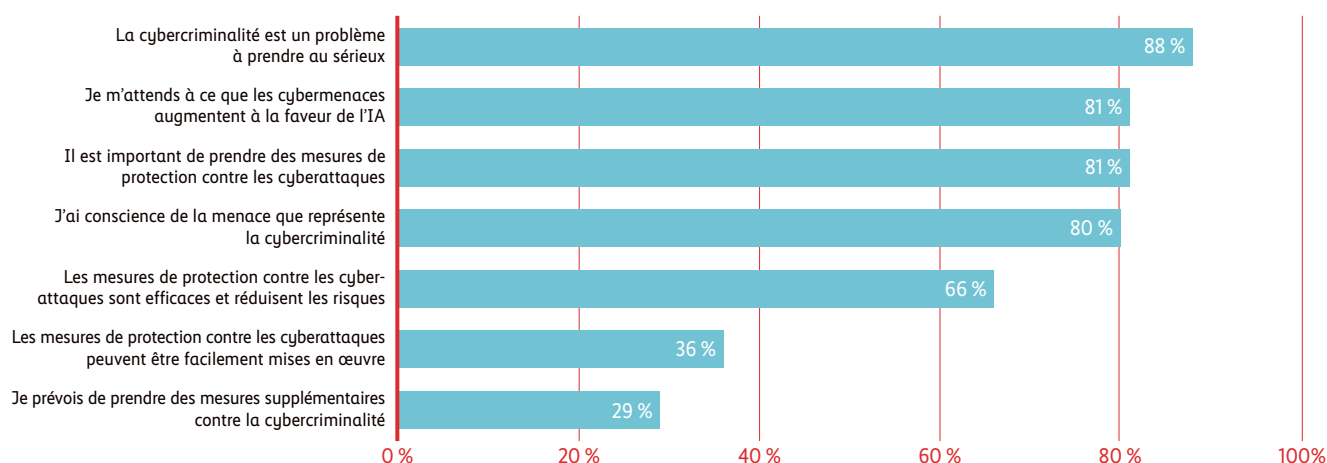
Les résultats de l'étude révèlent en outre que les cyberrisques actuels ne sont pas la seule source de préoccupation. **Quatre PME sur cinq (81 %) s'attendent à ce que les cybermenaces continuent**

ou plusieurs douzaines, leur appréciation de la menace est presque identique. Aujourd'hui, l'ensemble du secteur des PME suisses a conscience que la cybercriminalité constitue un défi.

Attitude vis-à-vis de la cybercriminalité

Question: dans quelle mesure êtes-vous d'accord avec les affirmations suivantes concernant la cybercriminalité (logiciels malveillants, escroquerie en ligne, piratage)?

Échelle: de 1 «Pas du tout d'accord» à 5 «Tout à fait d'accord». Résultats représentés: échelle 4-5 «Tout à fait d'accord»



L'étude révèle néanmoins un autre élément important: être sensibilisé à ce problème ne suffit pas. Les entreprises qui se sentent bien informées en matière de cybersécurité et qui ont déjà pris des mesures de protection techniques ou organisationnelles ne sont en effet ni plus ni moins soucieuses des cyberrisques que les autres PME. En revanche, elles sont nettement plus convaincues que l'on peut les réduire efficacement. ***Les PME bien préparées n'ont donc pas seulement plus conscience des risques: elles se sentent aussi plus capables de les gérer.***

L'étude permet donc de tirer la conclusion suivante: les PME suisses sont plus que jamais sensibilisées aux cybermenaces. Et bon nombre d'entre elles s'attendent à voir ces risques continuer d'augmenter en raison de l'évolution rapide de l'IA. Le défi de ces prochaines années ne consistera donc pas à accroître la sensibilisation à cette problématique, mais plutôt à mettre en place des mesures de protection concrètes et des formations continues correspondantes.



04 La cybercriminalité et les PME: plus de 35 000 entreprises touchées, et des conséquences souvent sérieuses



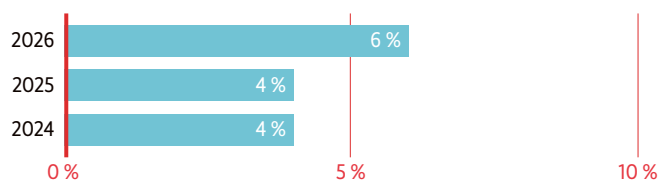
Commençons par la bonne nouvelle: ces trois dernières années, la grande majorité des PME suisses ont été épargnées par les cyberattaques graves (connues). Mais l'étude montre que la cybercriminalité peut avoir de lourdes conséquences pour les entreprises touchées. Pas moins de 6 % des PME interrogées (soit plus de 35 000 PME à l'échelle de la Suisse) déclarent avoir subi une cyberattaque au cours des trois dernières années (fourchette statistique: 35 200 à 36 700 PME). Pour bon nombre d'entre elles, cela s'est traduit par un dommage financier, une atteinte à la réputation, une importante charge de travail ou un stress considérable. Jusqu'à 16 % des entreprises employant au moins dix personnes ont été visées par de telles attaques, une proportion nettement supérieure à la moyenne.

Le type de dommages survenus mérite d'être souligné. Contrairement à ce que pense le grand public, les pertes financières ne sont pas la principale conséquence. **Les entreprises touchées citent d'abord la charge de travail importante induite par la réparation du dommage, puis le stress causé par la situation.** Ce n'est qu'après qu'elles mentionnent les dommages financiers, les atteintes à la réputation ou encore les pertes de données clientèle. Les cyberattaques sont donc avant tout chronophages, énergivores et stressantes pour les personnes qui doivent gérer leurs conséquences.

Autre enseignement important: il n'existe pas d'attaque type. **Les cybercriminels disposent de divers moyens pour parvenir à leurs fins. Le hameçonnage, le piratage de mots de passe, l'utilisation de logiciels malveillants, ainsi que les attaques visant le réseau et les serveurs sont les méthodes qui reviennent le plus souvent: chacune concerne environ un tiers des incidents.** Les PME doivent donc faire à une menace protéiforme, les cybercriminels utilisant diverses techniques pour les attaquer.

Cyberattaques et dommages

Question: au cours des trois dernières années, votre entreprise a-t-elle subi un dommage financier ou une atteinte à sa réputation ou avez-vous dû consentir des efforts importants pour réparer un dommage ou gérer une situation particulièrement stressante du fait d'une cyberattaque? (Réponse: oui)



Les entreprises touchées citent d'abord la charge de travail importante induite par la réparation du dommage.

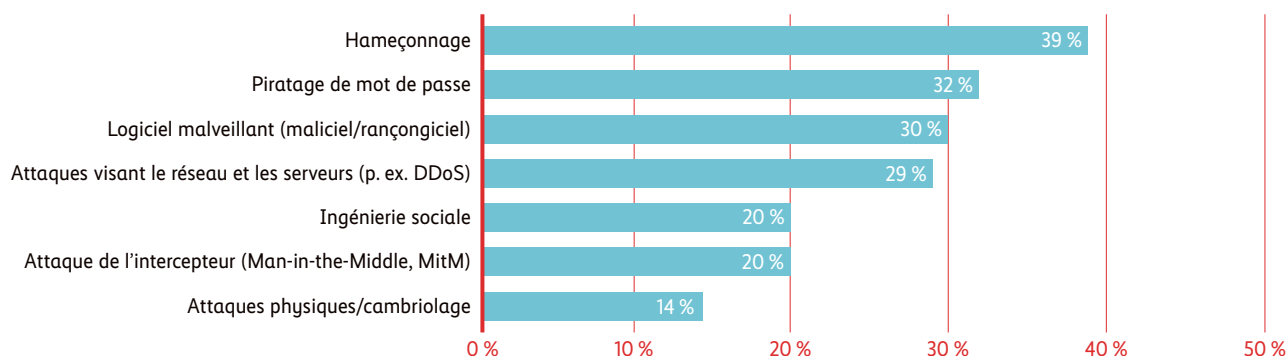
Par ailleurs, le chantage reste un thème d'actualité.

Environ 7% des entreprises interrogées (soit environ 45 000 PME à l'échelle de la Suisse) ont déjà été victimes de chantage de la part de cybercriminels (fourchette statistique: 43 300 à 45 380 PME). Les PME de grande taille ainsi que les entreprises des secteurs de la construction et de l'industrie sont particulièrement touchées. Certaines d'entre elles ont même cédé aux demandes de rançon. Autrement dit, la cybercriminalité a cessé depuis longtemps d'être un problème purement technique et constitue de plus en plus un défi qui relève de l'économie d'entreprise et de la stratégie.

Les résultats sont clairs: si seule une minorité de PME sont directement touchées par des cyberattaques, ces dernières peuvent avoir de lourdes conséquences en cas de succès. La question centrale n'est donc pas la taille de l'entreprise, mais l'efficacité des mesures prises pour pouvoir faire face à différents types d'attaques et se protéger contre les dommages financiers.

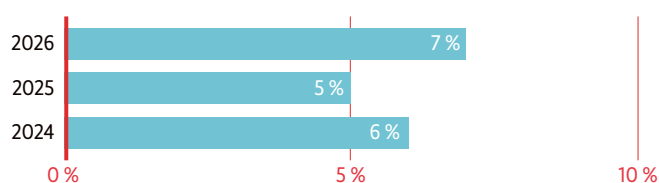
Type d'attaque

Question: quel type d'attaque avez-vous subie? (Filtre: entreprises ayant subi une cyberattaque)



Chantage

Question: votre entreprise a-t-elle déjà été victime de chantage de la part de cybercriminels? (Réponse: oui)



05 Connaissance des cybermenaces et des possibilités de soutien

Le sondage actuel révèle que beaucoup de PME suisses se sentent globalement bien armées face aux cyberrisques. **Près de la moitié d'entre elles déclarent être suffisamment informées des principales cybermenaces qui pèsent sur leur activité.** Parmi les entreprises sondées, bon nombre estime aussi savoir où trouver des informations, du soutien ou des recommandations concrètes de mesures à prendre en cas d'urgence.

Autre point positif: **40 % des entreprises se disent prêtes à signaler volontairement les cyberincidents pertinents à l'Office fédéral de la cybersécurité (OFCS).** Les PME suisses semblent donc avoir globalement conscience de l'importance de l'échange d'informations et de la collaboration.

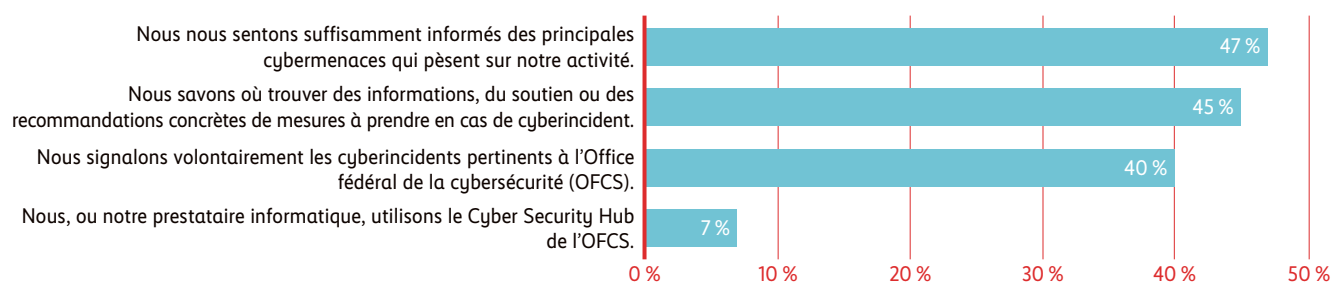
L'étude montre que les PME utilisent encore trop peu le Cyber Security Hub, en particulier les très petites entreprises. En effet, environ 7 % seulement des entreprises ou de leurs prestataires informatiques se rendent sur cette plateforme conçue par l'OFCS. Le Cyber Security Hub est principalement destiné aux exploitants d'infrastructures critiques et à leurs prestataires de services. Les PME peuvent néanmoins être elles aussi intégrées au système et utiliser cet outil.



Connaissance des cybermenaces et des possibilités de soutien

Question: dans quelle mesure êtes-vous d'accord avec les affirmations suivantes?

Échelle: de 1 «Pas du tout d'accord» à 5 «Tout à fait d'accord». Résultats représentés: échelle 4–5 «Tout à fait d'accord»



En outre, il apparaît clairement que les **PME d'une certaine taille sont plus au fait des possibilités de soutien existantes que les entreprises plus petites.**

Les entreprises employant entre 10 et 49 personnes sont nettement plus nombreuses à disposer d'informations concrètes, à savoir qui contacter en cas de cyberattaque, et à utiliser des outils tels que le Cyber Security Hub. Les entreprises de taille plus modeste se reposent vraisemblablement davantage sur leurs connaissances générales ou sur des partenaires externes.

Les PME d'une certaine taille sont plus au fait des possibilités de soutien existantes que les entreprises plus petites.

Les résultats indiquent que beaucoup de PME préfèrent s'appuyer sur leurs connaissances personnelles pour évaluer leur cyberrésilience. Sur le plan organisationnel, elles sont néanmoins parfois moins prêtes à faire face à un cyberincident.

C'est précisément là que des mesures telles que des concepts d'urgence, des processus clairs et le recours à des offres de soutien spécialisé peuvent s'avérer précieuses lorsqu'un incident survient effectivement.

Bon nombre de PME ont le sentiment d'être informées et estiment savoir qui elles peuvent contacter. Cependant, les concepts de sécurité, les plans d'urgence et les audits font souvent défaut. L'étude met donc en lumière un écart entre le sentiment de cyberrésilience des entreprises et les mesures correspondantes ancrées au niveau organisationnel.

06 Le thème de la cybersécurité regagne en importance

Après avoir connu un recul en 2025, le thème de la cybersécurité a repris beaucoup d'importance pour les PME suisses. Cette année, 46 % des entreprises interrogées considèrent que la cybersécurité est importante ou très importante. L'année dernière, elles étaient 33 % à partager cet avis. **Cette question retrouve donc la place qu'elle occupait lors des années précédentes.**

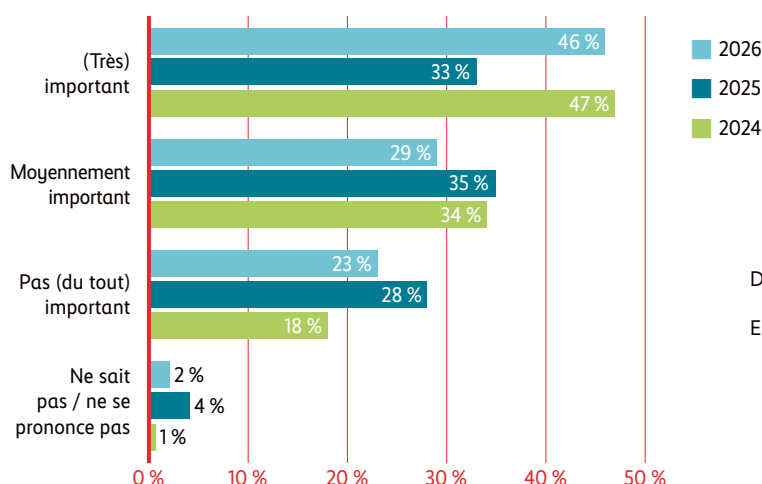
Les entreprises employant au moins dix personnes ont particulièrement évolué à ce sujet. **Dans ce groupe, environ six PME sur dix accordent beaucoup d'importance à la cybersécurité.** Les entreprises ouvertes à la technologie («Entreprises pionnières» ou «Early Followers») sont aussi nettement plus soucieuses de cette question que celles qui innovent moins («Late Followers»).

Les entreprises d'une certaine taille sont davantage sensibles aux cyberrisques.

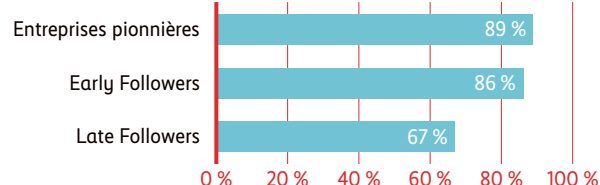
Importance de la cybersécurité

Question: à quel point le thème de la cybersécurité est-il important dans votre entreprise?

Échelle: 1-2 «Pas (du tout) important» / 3 «Moyennement important» / 4-5 «(Très) important»



Dont («Moyennement important» / «Très important»)



Cette prise de conscience ne doit rien au hasard.

L'étude actuelle montre que la cybercriminalité représente aujourd'hui l'un des principaux risques stratégiques pour les PME suisses. La cybercriminalité est mentionnée dans 23 % des réponses, ce qui la place pratiquement à égalité avec des thèmes tels que l'inflation, les hausses des coûts et la pénurie de main-d'œuvre qualifiée. Seules les incertitudes liées à la politique et à l'économie mondiales restent un peu plus souvent citées parmi les risques à long terme.

Il est frappant de noter que les entreprises d'une certaine taille sont davantage sensibles aux cyberrisques. Plus d'un tiers des PME employant entre 20 et 49 personnes considèrent déjà la cybercriminalité comme l'un des principaux risques stratégiques. Ce thème est donc nettement plus important encore dans ce groupe.

Dans l'ensemble, les résultats indiquent clairement que les PME suisses ont de plus en plus conscience que la cybersécurité n'est pas seulement une question technique que traitent des spécialistes en informatique, mais qu'elle occupe aussi une place stratégique dans leur activité. Face aux dépendances numériques croissantes, aux nouvelles menaces et aux cybercriminels professionnels, la protection des données, des processus et des relations d'affaires redevient un enjeu majeur en matière de gestion d'entreprise.



07 Cyberrisques: de plus en plus de PME définissent des responsabilités

L'étude actuelle met en évidence une évolution positive: **les PME suisses sont toujours plus nombreuses à définir des responsabilités claires en matière de cybersécurité.** Ainsi, elles confient plus souvent le traitement des cyberrisques à quelqu'un, alors qu'elles avaient tendance à s'en occuper en parallèle auparavant.

La part des entreprises déléguant à une personne responsable **une tâche partielle** correspondante a nettement augmenté. En l'espace d'une année, elle a bondi de 15 à 21%. **Et désormais, près d'une PME sur dix dispose même d'une fonction spéciale comportant des responsabilités claires du point de vue de la cybersécurité.**

Beaucoup d'entreprises décident en outre de se faire accompagner. Plus d'un quart des PME interrogées collaborent avec un partenaire externe en matière de cyberrisques. Cette mesure est particulièrement judicieuse pour les entreprises de taille plus modeste: elles peuvent ainsi pallier efficacement un manque de ressources internes ou de connaissances techniques.

Mais le principal changement concerne la part d'entreprises qui ne se sont encore jamais vraiment intéressées à cette question. En 2025, 42 % des PME sondées considéraient que les cyberrisques n'étaient pas une priorité alors qu'aujourd'hui, elles ne sont plus que 36 % à le penser. On constate le même recul chez les très petites entreprises employant une à trois personnes. **Autrement dit, ces entreprises sont elles aussi de plus en plus sensibilisées à cette problématique.**

Beaucoup d'entreprises décident de se faire accompagner.

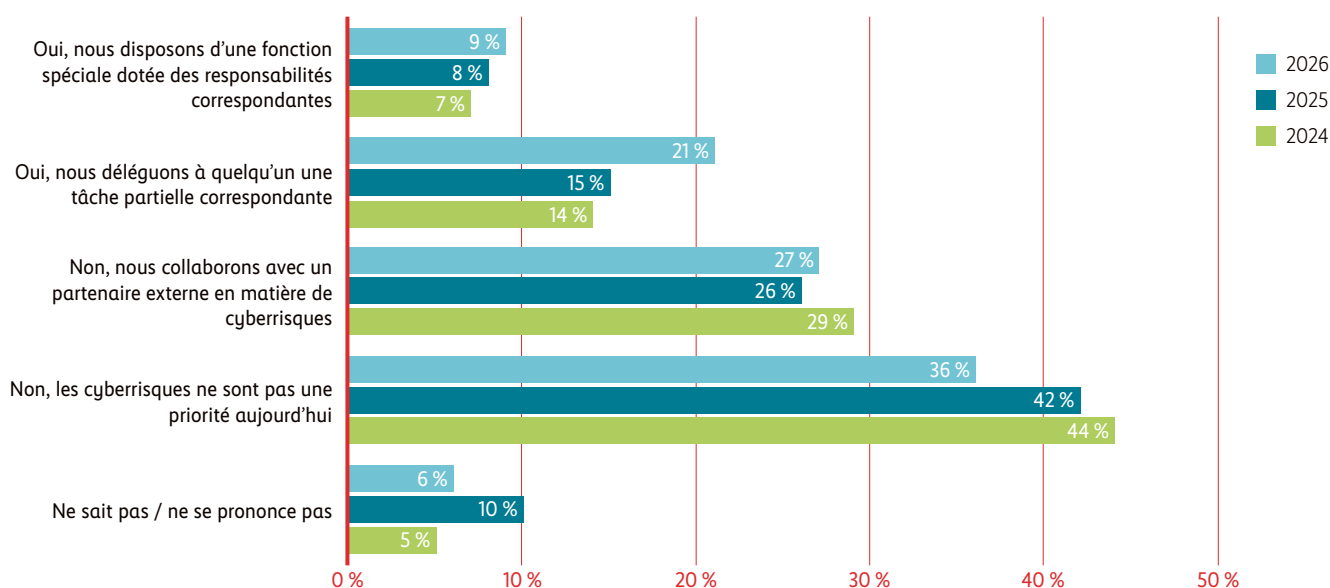


On observe de forts contrastes entre les PME selon leur taille: celles qui emploient dix personnes ou plus ont nettement plus tendance à définir des responsabilités, que ce soit en interne ou en faisant appel à des spécialistes externes. Ces entreprises sont aussi beaucoup moins nombreuses à déclarer que les cyberrisques ne sont «pas un thème prioritaire».

Dans l'ensemble, les résultats montrent que les PME suisses changent de regard sur le thème de la cybersécurité, qu'elles considèrent de plus en plus comme une tâche de gestion et de moins en moins comme une tâche purement technique. Dans ce contexte, la principale leçon à retenir est que toutes les PME n'ont pas besoin de disposer de leur propre responsable de la cybersécurité. L'essentiel est que les responsabilités soient clairement définies au sein de l'entreprise et que l'on sache qui doit intervenir en cas d'urgence.

Responsabilité concernant les cyberrisques

Question: votre entreprise a-t-elle délégué la responsabilité de la cybersécurité à une ou plusieurs personnes?



08 Mise en œuvre de mesures techniques de cybersécurité

Les PME suisses continuent d'investir avant tout dans des mesures techniques de protection éprouvées. La mise à jour régulière des logiciels est la plus courante: plus de 80 % des entreprises la mettent systématiquement en œuvre. Beaucoup d'entreprises citent également les pare-feu, les sauvegardes de données et l'authentification à deux facteurs ou multifacteur (2FA/MFA). Ces mesures constituent actuellement les piliers de la cybersécurité de la plupart des PME.

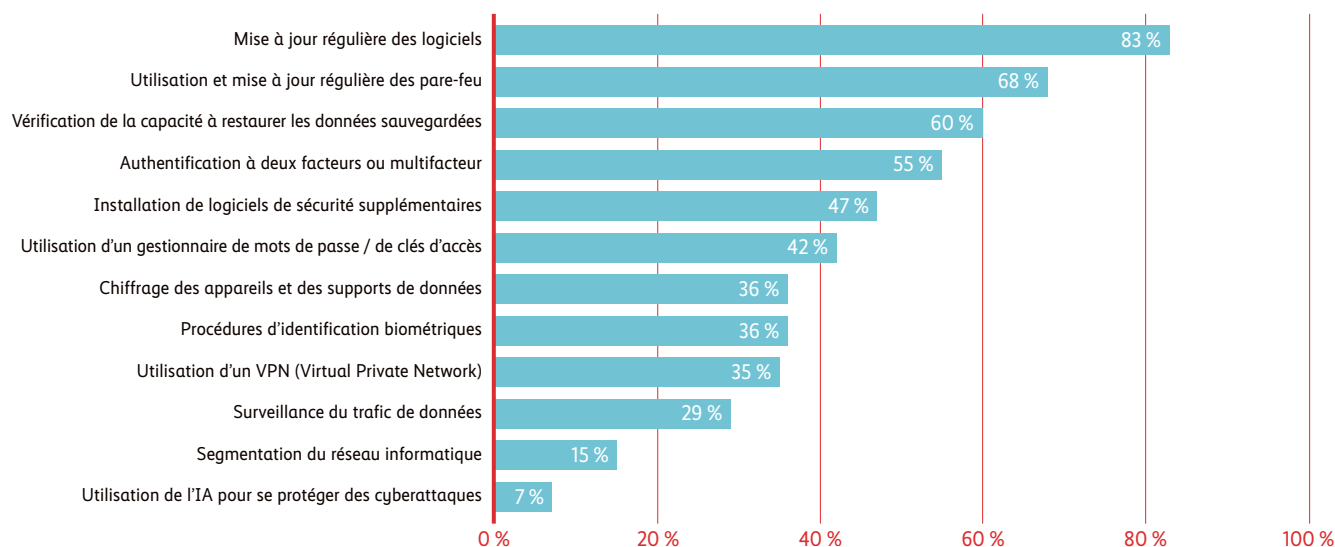
En revanche, les mécanismes avancés de protection (surveillance du trafic de données, segmentation réseau, utilisation de l'IA pour se protéger contre les cyberattaques, etc.) sont nettement moins répandus. C'est justement sur ces thèmes que l'on observe un écart important entre les PME plus

innovantes et celles qui sont davantage à la traîne. Si les précurseurs technologiques adoptent de plus en plus de telles mesures, bon nombre d'entreprises se limitent toujours aux fondamentaux classiques.

Il est particulièrement réjouissant de noter que **neuf PME suisses sur dix sauvegardent régulièrement des données** aujourd'hui – désormais, seules 4 % des entreprises ne le font pas. En outre, de plus en plus d'entreprises effectuent des sauvegardes de données à la fois en local et dans le cloud. Cette combinaison renforce la sécurité en cas de défaillance et réduit le risque de perte totale de données.

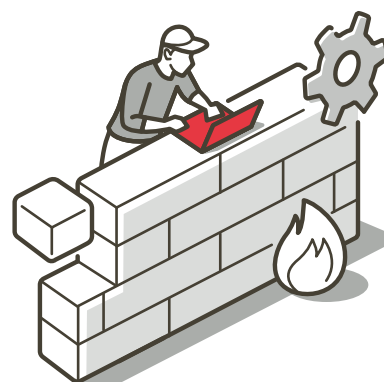
Mesures techniques de cybersécurité

Question: jusqu'à quel point les mesures techniques suivantes destinées à accroître la cybersécurité ont-elles été mises en œuvre dans votre entreprise?
Échelle: 1-2 «(Absolument) pas mise en œuvre» / 3-5 «Partiellement mise en œuvre» / 6-7 «(Entièrement) mise en œuvre». Résultats représentés: échelle 6-7 «(Entièrement) mise en œuvre»



L'endroit où les PME sauvegardent leurs données est aussi intéressant: **environ les trois quarts d'entre elles le font en Suisse**. Rares sont celles qui choisissent un lieu en dehors de l'Europe. Autrement dit, beaucoup de PME tiennent à garder le contrôle sur leurs données sensibles et sont attachées à leur souveraineté en la matière.

Cette approche présente néanmoins un point faible majeur: une sauvegarde ne peut être utile que si elle fonctionne effectivement en cas d'urgence. Si effectuer des sauvegardes de données fréquentes est devenu la norme aujourd'hui, **seul un quart des PME vérifie régulièrement si les données sauvegardées peuvent vraiment être restaurées**. Ainsi, de nombreuses entreprises ne sont pas certaines de pouvoir récupérer leurs données après une cyberattaque, un problème technique ou une erreur de manipulation.



Neuf PME suisses sur dix sauvegardent régulièrement des données aujourd'hui.

Dans l'ensemble, les résultats de l'étude indiquent que beaucoup de PME mettent en œuvre des mesures techniques de base. En revanche, elles négligent encore souvent les thèmes de la protection des accès, de la surveillance, de la segmentation et de la vérification de la capacité à restaurer les données. Ces dernières années, des progrès considérables ont été réalisés concernant la sauvegarde de données. Mais ce n'est pas suffisant: les entreprises doivent à présent comprendre qu'il est aussi crucial de tester régulièrement ces sauvegardes afin de s'assurer de pouvoir vraiment récupérer leurs données. Car en cas d'urgence, de telles sauvegardes ne sont utiles que si elles fonctionnent bel et bien.

09 Mise en œuvre de mesures organisationnelles de cybersécurité



L'étude actuelle montre qu'en matière de cybersécurité, les PME suisses se concentrent avant tout sur des mesures techniques de protection. **Les mesures organisationnelles sont quant à elles beaucoup moins répandues.** Parmi ces dernières, la plus courante consiste à respecter des règles de conduite de base: gestion prudente des informations personnelles, utilisation de mots de passe sécurisés, contrôle des documents ou des e-mails suspects, etc. Aujourd'hui, la grande majorité des entreprises ont intégré ces principes.

Mais elles sont beaucoup moins nombreuses à appliquer des structures et des processus supérieurs. **Environ un tiers des PME seulement réalise systématiquement l'inventaire de ses systèmes informatiques et de ses services cloud ou forme**

régulièrement son personnel. Elles sont encore plus rares à disposer de plans d'urgence garantissant la continuité des activités, à évaluer la sécurité informatique de leurs fournisseurs, à mettre en œuvre des concepts de sécurité formels ou à classifier les données selon le degré de protection requis. **La réalisation d'audits de sécurité est la mesure la moins fréquente.**

On observe de forts contrastes entre les entreprises selon leur taille. Si l'ensemble des PME a bien intégré les règles de conduite de base, le degré de professionnalisation augmente nettement avec le nombre de collaboratrices et de collaborateurs. Les entreprises employant entre 10 et 49 personnes disposent beaucoup plus souvent de concepts d'urgence, de support technique pour la sécurité informatique, de directives de sécurité et d'audits réguliers que les toutes petites entreprises.

Environ un tiers des PME seulement réalisent systématiquement l'inventaire de leurs systèmes informatiques et de leurs services cloud ou forment régulièrement leur personnel.

Une autre tendance notable concerne les connaissances en matière de cybersécurité. Les entreprises qui estiment être bien informées sur les cyberrisques sont bien plus nombreuses que les autres à prendre des mesures organisationnelles de cybersécurité. Cela vaut pour presque tous les domaines examinés, des formations pour le personnel aux concepts de sécurité, en passant par les plans d'urgence. Les audits de sécurité ainsi que la classification des données sensibles sont les deux seules exceptions. Ainsi, le niveau d'information est corrélé positivement au degré de mise en œuvre des mesures organisationnelles de protection.

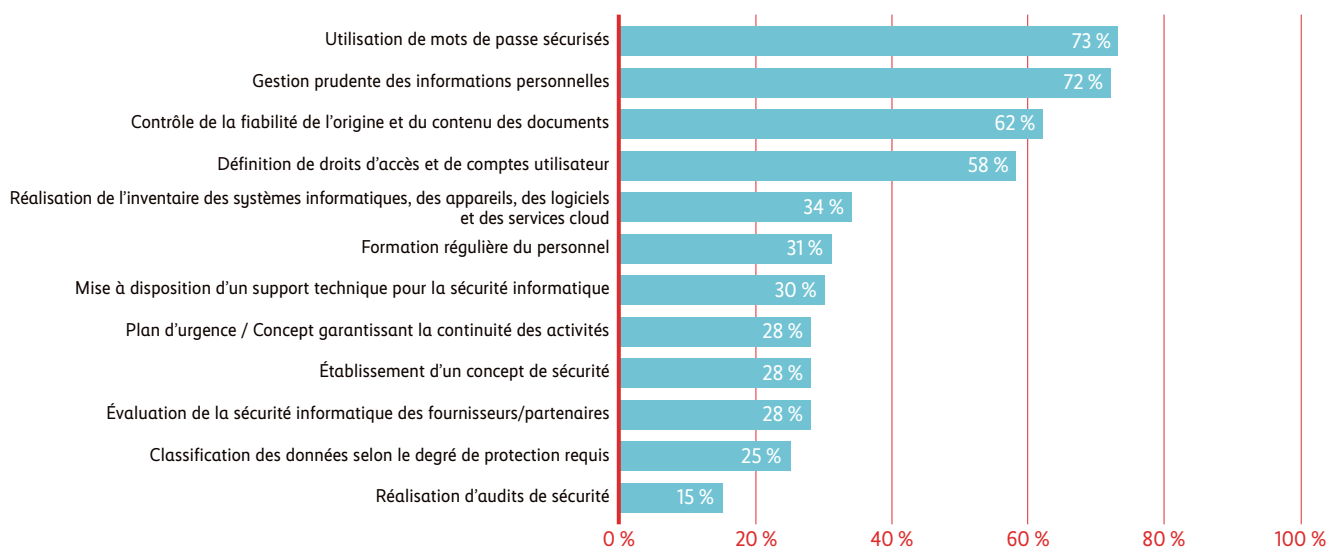
La culture de l'innovation joue également un rôle important. Les entreprises ouvertes à la technologie ainsi que les «Early Followers» ont nettement

plus tendance que les «Late Followers» à mettre en œuvre de telles mesures. Les «Late Followers» sont beaucoup plus rares à disposer de processus de sécurité structurés et ont tendance à négliger les mesures organisationnelles de protection.

Dans l'ensemble, les résultats indiquent clairement que la plupart des PME savent quelles règles de prudence appliquer au quotidien. **Le vrai défi consiste à intégrer la cybersécurité du point de vue organisationnel.** Mettre en place des plans d'urgence, former le personnel, évaluer les fournisseurs et réaliser des audits de sécurité réguliers constituent des mesures que l'on remarque souvent moins que l'utilisation de pare-feu, mais en cas d'urgence, elles peuvent déterminer la vitesse de réaction d'une entreprise à un cyberincident et sa capacité à maintenir son exploitation.

Mesures organisationnelles de cybersécurité

Question: jusqu'à quel point les mesures techniques suivantes destinées à accroître la cybersécurité ont-elles été mises en œuvre dans votre entreprise?
Échelle: 1-2 «(Absolument) pas mise en œuvre» / 3-5 «Partiellement mise en œuvre» / 6-7 «(Entièrement) mise en œuvre». Résultats représentés: échelle 6-7 «(Entièrement) mise en œuvre»



10 La cyberrésilience gagne toujours plus en importance, mais beaucoup de PME restent prudentes

L'étude actuelle dresse un tableau plutôt positif de la cyberrésilience dans le secteur des PME suisses. Une entreprise sur deux considère être bien ou très bien protégée contre les cyberattaques et se sent prête à y faire face. Cette estimation a même légèrement progressé par rapport à l'année dernière. Les entreprises d'une certaine taille et les PME ouvertes à la technologie se montrent particulièrement confiantes. **Les entreprises pionnières en matière de numérisation font état d'un niveau de résilience nettement plus élevé que les «Late Followers», qui sont beaucoup plus critiques sur ce point.**



marquée dans les entreprises employant plus de dix personnes. Les PME innovantes ont elles aussi tendance à se soucier davantage de ce sujet.

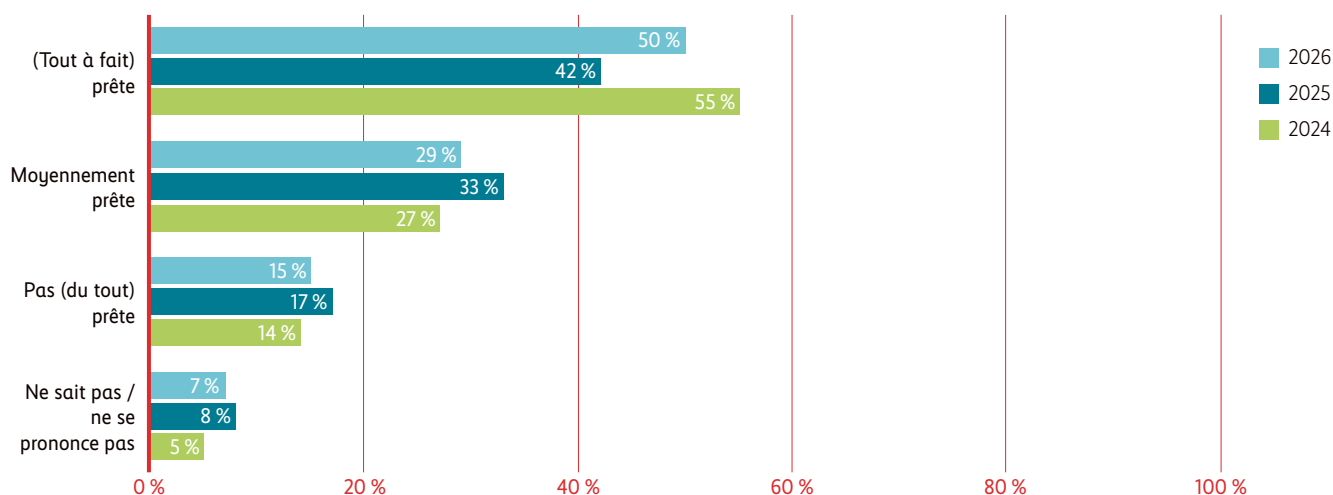
Dans le même temps, la cybersécurité retrouve de l'importance sur le plan stratégique. Si l'intérêt pour ce thème a diminué entre 2024 et 2025, près d'une PME sur deux considère désormais que la cybersécurité est une question importante ou très importante. Cette évolution est particulièrement

L'avenir s'annonce prometteur: **environ deux PME sur cinq jugent (très) probable l'adoption de mesures de sécurité supplémentaires d'ici un à trois ans.** La taille et le niveau d'information de l'entreprise influencent positivement cette disposition. Les entreprises qui estiment être bien infor-

Cyberrésilience

Question: d'après vous, votre entreprise est-elle bien protégée contre les cyberattaques et prête à y faire face?

Échelle 1-2 «Pas (du tout) prête» / 3 «Moyennement prête» / 4-5 «(Tout à fait) prête»



La cyberrésilience ne se limite pas à prévenir les attaques: elle permet aussi aux entreprises de réagir rapidement et de rester opérationnelles après un incident.

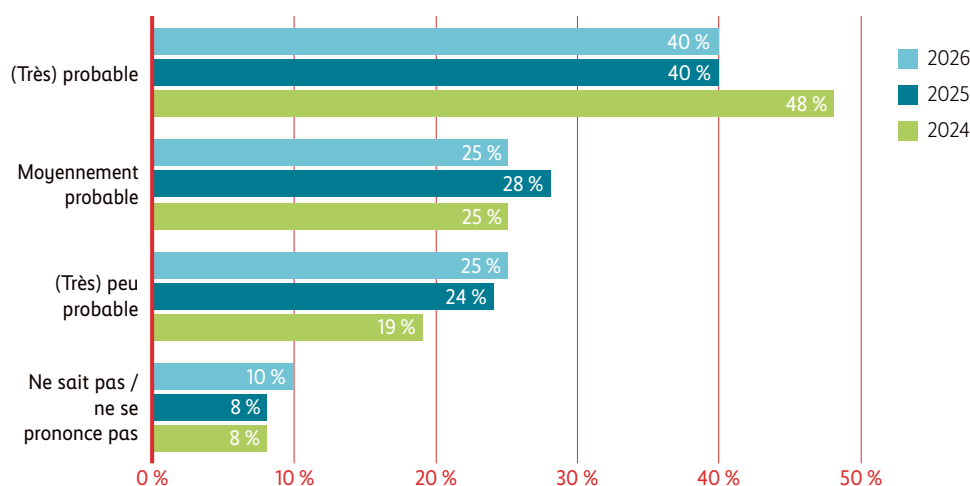
mées sur les cyberrisques ont nettement plus tendance que les autres à planifier de nouveaux investissements.

Mais ce haut niveau de sensibilisation doit être nuancé par un autre constat. Si certaines parties du sondage révèlent que les PME suisses ont clairement conscience que la cybercriminalité est une menace à prendre au sérieux, une majorité d'entre elles estime assez peu probable de subir une interruption d'exploitation d'au moins un jour à la suite d'une cyberattaque dans les deux à trois prochaines années. Environ une entreprise sur dix seulement juge que le risque est élevé. Cette estimation n'est supérieure que chez les PME d'une certaine taille.

Les résultats indiquent que si beaucoup d'entreprises ont aujourd'hui davantage confiance en leur propre résilience, elles sont aussi nombreuses à sous-estimer potentiellement les conséquences d'un éventuel incident. **La cyberrésilience ne se limite pas à prévenir les attaques: en cas d'incident, elle permet aussi aux entreprises de réagir rapidement et de rester opérationnelles.** C'est précisément pourquoi les thèmes de l'amélioration continue des mesures de protection, de la mise en place de plans d'urgence et de la réalisation d'audits de sécurité réguliers continueront de gagner en importance dans les prochaines années.

Renforcement des mesures de cybersécurité

Question: quelle est la probabilité que vous renforciez les mesures de sécurité contre la cybercriminalité dans les une à trois prochaines années?
Échelle: 1-2 «(Très) peu probable» / 3 «Moyennement probable» / 4-5 «(Très) probable»



Mise en œuvre

Check-list: cybersécurité et cyberrésilience pour les PME suisses

Les résultats de l'étude montrent que beaucoup de PME maîtrisent les bases techniques. Aujourd'hui, la principale marge d'amélioration concerne souvent la mise en place de mesures organisationnelles et de plans d'urgence ainsi que la réalisation d'audits réguliers de l'efficacité des mesures de protection existantes. Cette check-list a été conçue pour vous aider à renforcer votre cyberrésilience.

Mesures techniques de cybersécurité

1. Sécuriser les bases

- ☐ Effectuer des mises à jour régulières de tous les systèmes d'exploitation, applications et appareils.
- ☐ Utiliser des pare-feu mis à jour en continu.
- ☐ Activer l'authentification multifacteur (MFA) pour l'accès aux e-mails, aux services cloud et aux systèmes critiques.
- ☐ Utiliser des logiciels de sécurité supplémentaires (ERD / Endpoint Protection, antivirus).
- ☐ Utiliser des gestionnaires de mots de passe ou des clés d'accès.

2. Protéger les données

- ☐ Effectuer régulièrement des sauvegardes de données.
- ☐ Stocker les sauvegardes en local et dans le cloud.
- ☐ Dans la mesure du possible, veiller à stocker les sauvegardes en Suisse.
- ☐ Vérifier régulièrement que les données sauvegardées peuvent être restaurées. En cas d'urgence, une sauvegarde n'est utile que si elle fonctionne bien.
- ☐ Chiffrer les appareils, les supports de données et les données sensibles.

3. Sécuriser l'infrastructure

- ☐ Utiliser des solutions VPN pour les accès externes.
- ☐ Utiliser des procédures d'identification biométriques lorsque cela s'avère pertinent.
- ☐ Surveiller le trafic de données et les activités suspectes.
- ☐ Isoler les systèmes critiques les uns des autres via la segmentation réseau.
- ☐ Étudier le potentiel des solutions de protection basées sur l'IA.

Mesures organisationnelles de cybersécurité

1. Sensibiliser le personnel

- ☐ Définir des règles claires en matière de gestion des informations personnelles et confidentielles.
- ☐ Imposer des règles de sécurité en matière de mots de passe.
- ☐ Contrôler la fiabilité des e-mails, des liens et des documents.
- ☐ Former régulièrement le personnel en matière de cyberrisques.

2. Définir des structures et des responsabilités

- ☐ Définir des responsabilités claires en matière de cybersécurité.
- ☐ Gérer systématiquement les droits d'accès et les comptes utilisateur.
- ☐ Réaliser l'inventaire de tous les systèmes informatiques, appareils, paquets de logiciels et services cloud.
- ☐ Prévoir un support technique interne ou externe pour la sécurité informatique.
- ☐ Documenter le concept de sécurité de l'entreprise.

3. Renforcer la résilience

- ☐ Élaborer un plan d'urgence et un concept garantissant la continuité des activités.
- ☐ Définir les responsabilités en cas de crise.
- ☐ Déterminer à qui demander un soutien en cas d'urgence (prestataire informatique, assureur, Office fédéral de la cybersécurité (OFCS)).
- ☐ Signaler à l'OFCS les cyberincidents pertinents.

4. Contrôler régulièrement les risques

- ☐ Évaluer la sécurité informatique des fournisseurs et des partenaires commerciaux.
- ☐ Classifier les données selon le degré de protection requis.
- ☐ Réaliser des audits de sécurité réguliers.
- ☐ Contrôler les dépendances numériques à des prestataires, plateformes ou services cloud spécifiques.

La cyberrésilience ne se limite pas à prévenir les attaques. Les entreprises exemplaires savent identifier une attaque, limiter le dommage, relancer rapidement l'exploitation et tirer des leçons de l'incident.

Outils pratiques pour renforcer la cybersécurité

Cybertest pour les PME

- Avec ce test d'autoévaluation, découvrez pourquoi les pirates s'intéressent à votre PME, et obtenez des conseils en sécurité adaptés à votre profil.
<https://www.mobiliere.ch/campagne/cybertest>
- Avec ITSec4KMU, déterminez votre Cyber Score et obtenez des mesures concrètes pour améliorer votre cybersécurité.
<https://itsec4kmu.ch/>

Office fédéral de la cybersécurité (OFCS)

- Informations destinées aux entreprises et aux autorités concernant la protection et les mesures à prendre en cas de cyberincident, ainsi que l'obligation de signaler.
<https://www.bacs.admin.ch/fr/infos-entreprises-et-autorites>
- Informations concernant le Cyber Security Hub (CSH)
<https://www.bacs.admin.ch/fr/informations-concernant-csh>

Cybersecurity Map

- La **Cybersecurity Map** offre aux décideurs politiques une vue d'ensemble concise des développements technologiques qui sont particulièrement pertinents du point de vue de la cybersécurité.
<https://www.satw.ch/fr/themes/cybersecurity/cybersecurity-map>

Méthode d'enquête

L'enquête visait à recueillir l'avis des PME suisses sur les thèmes de la cybercriminalité, de la cybersécurité et de la numérisation.

Durant la période allant du 24 juin au 10 juillet 2026, 507 entretiens ont été menés avec des dirigeantes et des dirigeants de PME employant de 1 à 49 personnes. Tous ont été réalisés à l'aide de questionnaires en ligne. La procédure d'invitation se base sur le panel Internet de YouGov (environ 115 000 membres).

L'échantillon a été prélevé de manière non proportionnelle avec des quotas définis selon la taille de l'entreprise et la région linguistique, puis pondéré de manière proportionnelle.

Le panel représenté par cet échantillon couvre environ 614 400 entreprises employant de 1 à 49 personnes (Office fédéral de la statistique, STATENT, 2025) dans toute la Suisse. L'intervalle de confiance de l'échantillon total est de 95 %, avec une marge d'erreur de +/- 4,4 % pour 50/50.

L'échantillon pondéré 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.

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

Autrices et auteurs



Marc K. Peter
Professeur en Digital Business
HES-SO Valais-Wallis – Haute École de Gestion
marckurt.peter@hes-so.ch



Romain Geiser
Program Manager NCS
Office fédéral de la cybersécurité
ncs@ncsc.admin.ch



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



Léonard Marbe
Senior Marketing Manager
La Mobilière
leonard.marbe@mobiliere.ch



Anna V. Rozumowski
Chargée de cours et responsable de filière
HWZ Hochschule für Wirtschaft Zürich
anna.rozumowski@fh-hwz.ch



Tobias Schlegel
Responsable Tech Intelligence
Académie suisse des
sciences techniques SATW
tobias.schlegel@satw.ch



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

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

PME Cybersécurité 2026

Une étude de la Mobilière en collaboration
avec l'OFCS, digitalswitzerland, la HES-SO, la HWZ
et la SATW

- Office fédéral de la cybersécurité (OFCS)
- La Mobilière
- digitalswitzerland
- HES-SO Valais-Wallis – Haute École de Gestion
- HWZ Hochschule für Wirtschaft Zürich
- Académie suisse des sciences techniques SATW
- YouGov

cyberstudie.ch
Berne et Zurich, octobre 2026

Impressum

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

PME Cybersécurité 2026:

Une étude de la Mobilière en collaboration avec l'OFCS, digitalswitzerland, la HES-SO, la HWZ
et la SATW

Office fédéral de la cybersécurité (OFCS), la Mobilière, digitalswitzerland, HES-SO Valais-Wallis –
Haute École de Gestion, HWZ Hochschule für Wirtschaft Zürich, Académie suisse des sciences
techniques SATW, YouGov
Berne et Zurich, octobre 2026

Malgré le soin apporté à la rédaction de la présente publication, les autrices, les auteurs et les partenaires
de recherche impliqués déclinent toute responsabilité quant à l'exactitude des données, informations
et conseils ainsi qu'à d'éventuelles erreurs d'impression.

Tous droits réservés, y compris la traduction dans d'autres langues.
Les droits attachés aux marques citées demeurent auprès de leurs propriétaires respectifs.

Aucune partie de cette publication ne peut être reproduite, transcrite et/ou traduite dans un langage
informatique, notamment un langage de traitement de l'information, sous quelque forme que ce soit,
sans l'autorisation écrite préalable des autrices ou auteurs.

Coordination: Marc K. Peter,
HES-SO Valais-Wallis – Haute École de Gestion

Avec la collaboration de Thomas Burkhardt (YouGov), Michèle C. Kaufmann (YouGov), Kenza Leclerc
(OFCS), Bettina Mavrommatis (OFCS) et David Torcasso (digitalswitzerland).

Conception: équipe conception média, la Mobilière
Illustration: Livia Lüthi

La présentation contenant tous les résultats de l'enquête est disponible sur les sites Internet des partenaires
de l'étude et sur cyberstudie.ch.