

Communiqué de presse

Zurich, le 20 août 2026

Les PME suisses sous-estiment considérablement les cyberrisques : la protection de base et la couverture d'assurance restent lacunaires

Grâce à l'IA, les cyberattaques gagnent en rapidité et peuvent être déployées à plus grande échelle. Dans le même temps, de nombreuses PME suisses sont insuffisamment protégées et sous-assurées. [C'est ce que révèle une enquête représentative menée par Deloitte auprès des collaborateurs de PME suisses](#) : de nombreuses entreprises sous-estiment les risques et ne mettent pas systématiquement en œuvre les mesures de protection élémentaires. De plus, les petites entreprises, en particulier, sont encore trop peu nombreuses à disposer d'une cyberassurance.

La situation en matière de cybermenaces pour les entreprises suisses s'aggrave considérablement. Les cyberattaques sont en forte augmentation et, grâce à l'intelligence artificielle (IA), elles sont de plus en plus ciblées et efficaces. Les petites et moyennes entreprises (PME) sont particulièrement vulnérables : elles disposent souvent de moins de ressources, sous-estiment les risques auxquels elles sont exposées, mettent en œuvre moins de mesures de cybersécurité et sont également moins bien assurées. C'est ce que révèle une étude sur la cybersécurité des PME suisses menée par le cabinet d'audit et de conseil Deloitte.

Les résultats mettent en évidence un écart significatif entre les cybermenaces auxquelles les entreprises sont effectivement confrontées et la perception du risque (voir figure 1) : 49% des collaborateurs de PME interrogés ont été confrontés à un cyberincident grave chez leur employeur au cours de ces trois derniers mois, mais seuls 22% d'entre eux estiment que le cyberrisque pesant sur leur entreprise est élevé. Cet écart de perception est particulièrement marqué chez les micro-entreprises comptant entre 1 et 9 salariés : si 38% d'entre elles font état de cyberincidents graves, seuls 15% estiment que le risque de cyberattaque est élevé.

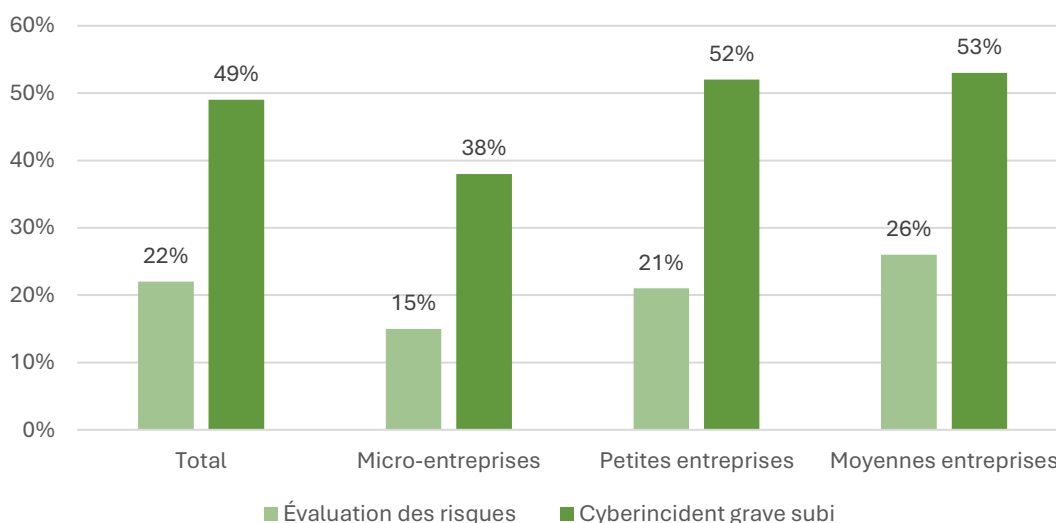


Figure 1 : Pourcentage des personnes interrogées estimant que le cyberrisque est très élevé ou élevé, ainsi que pourcentage des personnes interrogées ayant été confrontées à un cyberincident grave chez leur employeur au cours de ces trois derniers mois.

Le phishing touche des entreprises de toutes tailles

Le phishing, c'est-à-dire la tentative de voler des données ou de déclencher des paiements à l'aide de messages frauduleux, est la cybermenace la plus fréquemment signalée, avec 25%. Il est frappant de constater que le phishing est presque aussi fréquent dans les micro-entreprises que dans les PME en général. Cela démontre bien que même les très petites entreprises sont exposées aux cyberrisques. Les collaborateurs signalent également des logiciels malveillants (malware), des arnaques au président (CEO fraud), des usurpations d'identité, des soupçons de fuites de données et des perturbations de l'activité. Ces risques touchent les entreprises de toutes tailles.

« De nombreuses PME sous-estiment à quel point les cyberattaques ont évolué. Aujourd'hui, les attaques peuvent être menées à grande échelle, elles sont automatisées et touchent des entreprises de toutes tailles. Le phishing, les identifiants compromis ou la manipulation des processus de paiement, en particulier, peuvent avoir des conséquences graves même pour les petites entreprises », explique Florian Widmer, associé Cyber Risk chez Deloitte Suisse. « La capacité d'une organisation à résister aux cyberattaques commence donc par les bases : il faut notamment une authentification forte, des droits d'accès restrictifs, des formations régulières, des sauvegardes testées ainsi qu'un plan d'urgence solide. »

Les mesures de sécurité élémentaires ne sont pas encore généralisées

L'indice de cybersécurité des PME de Deloitte, établi pour la première fois sur la base de cette étude, mesure le degré d'adoption de six mesures de sécurité fondamentales liées au personnel et s'établit à 58 points sur 100 (voir figure 2). Autrement dit : en moyenne, les mesures de sécurité en question ne sont mises en œuvre qu'à hauteur de 58%, ce qui révèle une lacune importante au niveau des mesures de protection élémentaires.

Les failles sont particulièrement importantes dans les méthodes d'authentification modernes. Seuls 45% des entreprises ont mis en place des méthodes d'authentification sans mot de passe, telles que les techniques biométriques. L'authentification multifactorielle est certes plus répandue (66%), mais elle est encore loin d'être généralisée. Parallèlement, lorsque des mesures sont en place, elles sont perçues comme efficaces par les collaborateurs : 88% des personnes interrogées dont l'entreprise utilise des alertes par e-mail les jugent utiles. L'enquête mesure ici la perception des collaborateurs, et non l'efficacité réelle. Elle montre également que toutes les entreprises n'utilisent pas encore ce type d'avertissement.

Indice de cybersécurité des PME de Deloitte

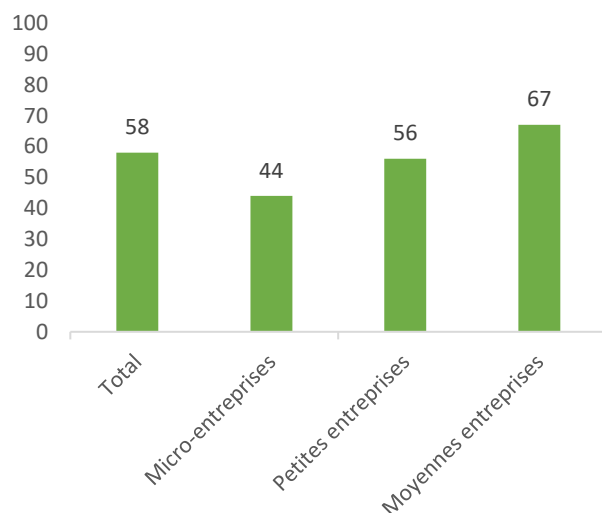


Figure 2 : Moyenne non pondérée de l'adoption de six mesures de sécurité. Le niveau de protection de base contre les cyberattaques augmente avec la taille de

La couverture d'assurance reste lacunaire

Outre la perception des risques et la mise en œuvre de mesures de protection, l'étude de Deloitte met en évidence une troisième lacune : la couverture d'assurance. Si les cyberassurances gagnent du terrain en Suisse, leur pénétration du marché reste toutefois faible. Selon les chiffres récents de l'Association Suisse d'Assurances (ASA), environ 72'000 polices d'assurance pour entreprises avaient été souscrites en 2025. Ainsi, seuls 11,5% des entreprises domiciliées en Suisse sont assurées contre les cyberrisques.

La couverture d'assurance est particulièrement lacunaire chez les micro-entreprises et les petites entreprises. Ce sont pourtant ces entreprises qui peuvent être particulièrement touchées par des

cyberincidents, car les dommages peuvent peser proportionnellement plus lourd au regard de leur chiffre d'affaires. Or, de nombreuses PME ne disposent pas des mesures de sécurité élémentaires requises pour souscrire une cyberassurance. D'autres facteurs compliquent également l'accès aux cyberassurances, notamment la complexité des procédures de souscription et le faible attrait commercial, les commissions versées pour les cyberassurances étant souvent modestes pour les petites entreprises.

« Pour les PME, une cyberassurance se révèle utile bien avant qu'une cyberattaque ne survienne », explique Marcel Thom, associé au sein du département Assurance chez Deloitte Suisse. « Sa valeur ajoutée réside dans la combinaison de la prévention, d'une aide d'urgence rapide et d'une protection financière. Les petites entreprises ont justement besoin de produits clairs, d'exigences transparentes et de processus de souscription simples et assistés par des outils numériques. C'est ainsi qu'une cyberassurance peut devenir un élément central de la résilience des entreprises. »

Des exigences plus contraignantes, mais pas de réglementation rigide

Cette étude met également en évidence des attentes claires quant au rôle de l'État. 87% des personnes interrogées sont favorables à un renforcement des prescriptions en matière de cybersécurité. Dans le même temps, seuls 19% sont favorables à des prescriptions plus strictes, exclusivement étatiques et fixant des normes minimales. Il en résulte pour la Suisse une mission pragmatique : la Confédération devrait fixer des normes minimales claires et faciliter la coopération entre les entreprises, les associations professionnelles, les assureurs et les prestataires de services informatiques.

À propos de l'étude

[L'étude Deloitte « Sous-estimés, non protégés, sous-assurés : les cyberrisques pour les PME en Suisse »](#) s'appuie sur une enquête en ligne représentative menée auprès de 924 employés d'entreprises suisses comptant jusqu'à 249 collaborateurs, qui utilisent un ordinateur dans le cadre de leur activité professionnelle. L'enquête a été réalisée en avril 2026. Par ailleurs, des entretiens ont été menés en juin et juillet 2026 avec des experts en cybersécurité issus du secteur des assurances. Selon la classification de l'Office fédéral de la statistique, les entreprises comptant jusqu'à 249 collaborateurs sont considérées comme des PME.

Contact : Michael Wiget
Responsable Communication Externe
Tél. : +41 58 279 70 50
E-mail : mwiget@deloitte.ch

Contact : Kevin Capellini
Communication externe
Tél. : +41 58 279 59 74
E-mail : kcapellini@deloitte.ch

[Deloitte Suisse](#)

Deloitte propose des services professionnels intégrés en Audit & Assurance, Tax & Legal, Strategy, Risk & Transaction Advisory et Technology & Transformation. Avec environ 2'500 collaborateurs répartis sur les sites de Bâle, Berne, Genève, Lausanne, Lugano et Zurich (siège), Deloitte propose ses services à des entreprises et à des institutions de toutes formes juridiques et de toutes tailles, opérant dans tous les secteurs d'activité en Suisse.

Nos équipes fournissent des résultats mesurables et durables qui contribuent à renforcer la confiance du public dans les marchés financiers et permettent à nos clients d'évoluer et de prospérer. Fort de plus de 180 ans d'histoire, Deloitte est présent dans plus de 150 pays et territoires et emploie environ 470'000 professionnels dans le monde entier.

Note à la rédaction

La désignation Deloitte fait référence à une ou plusieurs des entités suivantes : Deloitte Touche Tohmatsu Limited (« DTTL »), son réseau mondial de cabinets membres et leurs entités liées (collectivement désignés sous le nom d'« organisation Deloitte »). DTTL ainsi que chacun de ses cabinets membres et chacune de leurs entités liées constituent des entités juridiques distinctes et indépendantes, qui ne peuvent s'engager ou se lier mutuellement à l'égard de tiers. DTTL, chacun de ses cabinets membres et chacune de leurs entités liées ne sont responsables que

de leurs propres actes et omissions, et ne sauraient être tenus responsables des actes ou omissions des autres entités. DTTL ne fournit pas lui-même de services aux clients. Pour en savoir plus, veuillez consulter le site www.deloitte.com/about.

Deloitte SA est une société d'audit agréée et surveillée par l'Autorité fédérale de surveillance en matière de révision (ASR) et par l'Autorité fédérale de surveillance des marchés financiers (FINMA).

Les informations contenues dans ce communiqué de presse étaient exactes au moment de sa publication.



© 2026 Deloitte SA