

Communiqué de presse

Zurich, le 16 septembre 2026

Les cyberattaques basées sur l'IA aggravent les risques pour les PME – les conseils d'administration sont à la traîne face à cette évolution

Les cybercriminels ont de plus en plus recours à l'intelligence artificielle (IA), ce qui facilite la mise en œuvre des attaques et augmente les dommages potentiels. Or, près des trois quarts des entreprises ne disposent d'aucune stratégie explicite pour lutter contre les attaques basées sur l'IA, comme le montre la [20^e édition du swissVR Monitor](#). Parallèlement, la question de la cyberrésilience gagne en importance au sein des conseils d'administration. Cependant, nombreuses sont les instances qui manquent d'expertise, d'expérience en matière de gestion de crise et d'un système de reporting fiable, notamment dans les petites entreprises.

De plus en plus d'entreprises suisses sont prises pour cible par des cybercriminels : selon les estimations des membres des conseils d'administration, 41% des entreprises ont déjà été victimes d'une cyberattaque. Cela représente 13 points de pourcentage de plus qu'il y a trois ans. Cette hausse est presque entièrement imputable aux petites et moyennes entreprises (PME). Leur taux d'affectation est passé de 20% à 37% en 2026, alors qu'il est resté pratiquement stable pour les grandes entreprises, à hauteur de 45% et 48%. C'est ce que révèle l'enquête récente menée auprès de 281 membres de conseils d'administration dans le cadre du swissVR Monitor II/2026, réalisée par l'association des conseils d'administration swissVR, le cabinet d'audit et de conseil Deloitte et la Haute école de Lucerne.

L'importance croissante de ce sujet transparaît également dans les priorités stratégiques des conseils d'administration: selon l'enquête, l'informatique et la gestion de la sécurité, y compris la cyberrésilience, figurent parmi les dix thèmes prioritaires des conseils d'administration pour les douze prochains mois. Il est toutefois essentiel d'accorder davantage d'importance à la question suivante : selon l'étude, les interruptions d'activité, qui sont de 42%, restent de loin la conséquence la plus fréquente d'une cyberattaque (voir figure 1). Les fuites de données arrivent en deuxième position avec 22%. Dans l'ensemble, le nombre d'entreprises réellement victimes d'attaques est vraisemblablement plus élevé, car, selon l'enquête, la moitié des membres des conseils d'administration ne reçoivent pas de rapports réguliers sur les incidents cybernétiques.

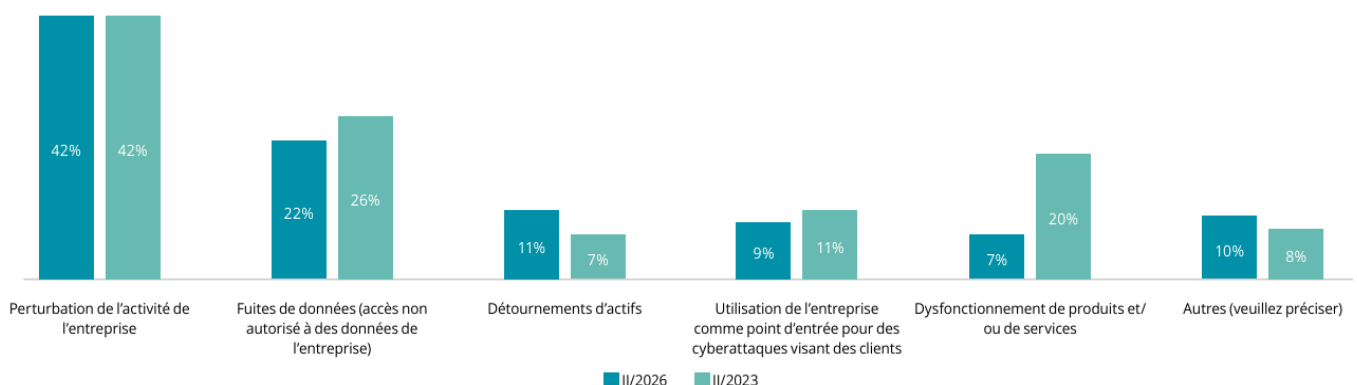


Figure 1 : Conséquences des cyberattaques dans les entreprises. Quelles ont été les conséquences de cette ou de ces attaques sur votre entreprise ?

Une absence de stratégie explicite face aux attaques perpétrées par l'IA

« L'utilisation croissante de l'IA à des fins criminelles entraîne une aggravation de la cybermenace. Les risques liés à la cybersécurité augmentent fortement et multiplient le potentiel de dommages – avec pour conséquence une sous-estimation encore importante de la part de nombreuses entreprises, mais aussi des pouvoirs publics », explique Cédric Nabé, associé cybersécurité chez Deloitte Suisse.

Malgré cela, 74% des entreprises ne disposent d'aucune stratégie explicite pour lutter contre les attaques basées sur l'IA. De plus, on observe également des différences considérables en matière d'attention portée à l'IA selon la taille de l'entreprise : seules 18% des petites entreprises sont préparées sur le plan stratégique, contre 40% des grandes entreprises.

La préparation aux situations d'urgence présente des lacunes similaires : 55% des entreprises n'ont pas de plans d'urgence, ou seulement des plans qui n'ont pas été testés, pour rétablir au plus vite les processus informatiques essentiels – ce qu'on appelle la « Minimum Viable Company » – après une cyberattaque sérieuse, avant que des dommages durables ne surviennent. Là encore, la taille de l'entreprise joue un rôle déterminant : les grandes entreprises (60%) disposent deux fois plus souvent de plans testés que les petites entreprises (32%).

« Les prestataires de services financiers sont particulièrement bien préparés : plus des deux tiers de ces entreprises disposent de plans de reprise après un sinistre informatique », explique Mirjam Gruber-Durrer, professeure en gestion normative des conseils d'administration à la Haute école de Lucerne. « Ce secteur fait partie des infrastructures critiques de la Suisse ; par conséquent, les normes de sécurité y sont mieux établies, en partie en raison d'une réglementation plus stricte. »

Un manque de compétences en matière de cybersécurité

L'enquête met également en évidence un potentiel d'amélioration au sein des conseils d'administration : certes, 86% des instances suivent les évolutions actuelles dans le domaine de la cybersécurité et 84% d'entre elles ont adopté une politique de gestion des risques pour faire face aux cyberattaques. Cependant, seule la moitié d'entre elles ont mis en place des exercices de gestion de crise en cas d'urgence – ce qui représente tout de même une nette progression par rapport aux 34% enregistrés il y a trois ans. Il existe également une marge de progression en matière d'expertise au sein des instances : 68% des conseils d'administration ne comptent aucun membre disposant d'une expertise avérée en cybersécurité ou en informatique et doivent s'appuyer sur les compétences de la direction ou d'un expert externe.

Le reporting présente lui aussi des axes d'amélioration : seul un conseil d'administration sur deux est régulièrement informé des incidents en matière de cybersécurité ; un quart d'entre eux ne reçoit aucun rapport à ce sujet. Il est inquiétant de constater que les rapports concernant les mesures à prendre et les investissements nécessaires, ainsi que la situation générale en matière de menaces, ont nettement diminué par rapport à 2023, respectivement de 18 et 13 points de pourcentage, et ce malgré une augmentation du nombre d'attaques. « Une stratégie cyber claire relève des missions essentielles de la direction, et le reporting constitue une mission de surveillance centrale permettant aux membres du conseil d'administration d'exercer leur fonction de direction. La cyber-résilience fait partie intégrante de la gestion des risques et constitue par conséquent une mission permanente de la direction, qui doit figurer sur le tableau de bord des risques et à l'ordre du jour du conseil d'administration », déclare Isabelle Amschwand, présidente de swissVR.

À propos du swissVR Monitor

L'enquête semestrielle swissVR Monitor vise à recueillir les avis de membres de conseils d'administration sur les perspectives commerciales, les stratégies et des thèmes d'ordre structurel. [Dans le cadre de la 20^e édition intitulée « Comment le conseil d'administration peut-il renforcer la cyberrésilience »](#), swissVR, en collaboration avec Deloitte et la Haute école de

Lucerne, a mené une enquête en ligne auprès de 281 membres de conseils d'administration entre le 26 mai 2026 et le 5 juillet 2026. Les participants représentent des conseils d'administration d'entreprises cotées en bourse et de PME, et proviennent de tous les secteurs pertinents de l'économie. 34% des participants sont des membres de conseil d'administration de grandes entreprises, 28% représentent des entreprises de taille intermédiaire et 38% des petites entreprises.

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

swissVR

swissVR s'engage pour la compétence, la mise en réseau et la prise en compte des intérêts des conseils d'administration. swissVR est une association indépendante d'administratrices et d'administrateurs suisses, de conseils d'administration pour les conseils d'administration. Grâce à son offre de prestations, swissVR contribue à la professionnalisation de l'activité des conseils d'administration, favorise les échanges d'expérience entre les administratrices et les administrateurs d'entreprises de tous les secteurs, fournit des informations ciblées et propose des formations à ses membres. swissVR compte plus de 1'400 membres. Pour plus d'informations, rendez-vous sur www.swissvr.ch

Haute École de Lucerne – la haute école de la Suisse centrale

La Haute École de Lucerne est la haute école spécialisée des six cantons de la Suisse centrale et réunit les départements Technique & Architecture, Économie, Informatique, Travail social, Design Cinéma Art, Musique ainsi que le département Santé. Avec près de 8'700 étudiantes et étudiants et environ 13'000 participantes et participants à des formations continues (dont 5'600 MAS, DAS, CAS), 274 nouveaux projets de recherche par an et 2'144 collaboratrices et collaborateurs, elle est la plus grande institution de formation au cœur de la Suisse. « Governance, Risk and Compliance » est une spécialité de l'Institut des services financiers de Zoug, Haute École de Lucerne, qui propose des formations continues pour les administratrices et les administrateurs, et notamment le cours de certificat « CAS Verwaltungsrat ». Pour plus d'informations, rendez-vous sur www.hslu.ch/ifz-verwaltungsrat / www.hslu.ch/cas-vr / www.hslu.ch/ifz

Deloitte Suisse

Deloitte propose des services intégrés en Audit & Assurance, Tax & Legal, Strategy, Risk & Transactions et Technology & Transformation. Avec environ 2'500 personnes réparties sur six sites à Bâle, Berne, Genève, Lausanne, Lugano et Zurich (siège social), Deloitte accompagne les entreprises et les organisations de toutes formes juridiques et de toutes tailles, issues de tous les secteurs d'activité en Suisse.

Nos équipes obtiennent des résultats mesurables et durables qui contribuent à renforcer la confiance du public dans les marchés financiers et permettent à notre clientèle de se développer et de réussir. Fort de plus de 180 ans d'histoire, Deloitte est présent dans plus de 150 pays et territoires et emploie environ 470 000 personnes à travers le monde.

Le terme « Deloitte » désigne Deloitte Touche Tohmatsu Limited (« DTTL »), son réseau mondial de sociétés membres et de sociétés affiliées (collectivement dénommées « Deloitte Organisation »). DTTL, ses sociétés membres et ses sociétés affiliées sont des entités juridiquement autonomes et indépendantes qui ne peuvent s'engager ni s'obliger mutuellement vis-à-vis de tiers. DTTL, ses sociétés membres et ses sociétés affiliées ne sont responsables que de leurs propres actes et omissions. DTTL ne fournit pas de prestations à ses clients en son nom. Pour plus d'informations, rendez-vous sur 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.

