Comment le conseil d’administration renforce la cyber-résilience

swissVR Monitor II/2026
Septembre 2026

swissVR®

Deloitte.

Global Boardroom Programme | Switzerland

HSLU Hochschule Luzern

Sommaire

À propos de l'enquête
La 20e édition du swissVR Monitor repose sur un sondage réalisé auprès de 281 membres de conseils d'administration suisses. L'objectif de cette enquête est de recueillir les opinions de membres de conseils d'administration sur les perspectives conjoncturelles et commerciales ainsi que sur des questions de gouvernance d'entreprise. Chaque numéro se focalise sur un sujet d'actualité ; celui-ci a pour thème la cyber-résilience.

Cette enquête a été réalisée par l'association swissVR en collaboration avec le cabinet de conseil Deloitte et la Haute école de Lucerne, entre le 26 mai 2026 et le 5 juillet 2026. Les 281 participants représentent aussi bien des membres de conseils d'administration d'entreprises cotées en bourse que de petites et moyennes entreprises (PME), issus de l'ensemble des secteurs les plus importants de l'économie suisse. 38% des participants sont membres de conseils d'administration de petites entreprises, 28% d'entreprises de taille moyenne et 34% de grandes entreprises.

L'objectif du swissVR Monitor est, d'une part, d'orienter les membres actifs de conseils d'administration en leur permettant de comparer leur propre point de vue sur ces questions avec celui de leurs pairs. D'autre part, l'étude permet au grand public de découvrir les perspectives de membres de conseils d'administration sur des questions liées à leur activité et à la situation économique actuelle.

À propos de la méthodologie
En comparant les résultats de l'enquête avec ceux des études précédentes, il convient de tenir compte du fait que le nombre de sondés et la composition de l'échantillon des participants à l'enquête diffèrent, à chaque fois, d'une enquête à l'autre. Les pourcentages ont été arrondis de sorte que le total des réponses soit toujours égal à 100%. La taille de l'entreprise a été déterminée en fonction de ses effectifs : les petites entreprises comptent entre 1 et 49 salariés, les entreprises de taille moyenne entre 50 à 249 collaborateurs et grandes entreprises au moins 250 collaborateurs.

Préambule

Chères lectrices, chers lecteurs,

Nous avons le plaisir de vous présenter le second numéro du swissVR Monitor de l'année 2026. Pour cette édition, nous avons interrogé 281 membres de conseils d'administration (CA) suisses. Les résultats reflètent leur point de vue sur les perspectives économiques, sectorielles et commerciales, ainsi que leur opinion sur des thématiques clés liées à leur activité au sein d'un conseil d'administration.

Au vu de la fréquence et de la sophistication galopantes des cyberattaques ces dernières années, le présent numéro du swissVR Monitor se focalise à nouveau, comme ce fut déjà le cas pour l'édition II/2023, sur le thème clé de la cyber-résilience. Au regard des dommages potentiels considérables que ces attaques peuvent causer aux entreprises, il est essentiel que les membres des conseils d'administration se saisissent de la question de la cyber-résilience dans le cadre de leur mandat et acquièrent une compréhension claire de leur propre rôle et des responsabilités qui en découlent. Le présent swissVR Monitor examine notamment les conséquences possibles des cyberattaques, les mesures mises en œuvre par les entreprises pour y faire face ainsi que le reporting de la direction au conseil d'administration en matière de cybersécurité.

Les résultats du swissVR Monitor II/2026 montrent que la proportion d'entreprises ayant été victimes de cyberattaques a considérablement augmenté depuis 2023. Dans le même temps, seule une faible minorité d'entre elles se prépare à faire face à des attaques exploitant les technologies d'intelligence artificielle. Pour les conseils d'administration, les principales mesures à prendre consistent à tester leur dispositif de gestion de crise en cas de cyberattaque, garantir l'expertise nécessaire au sein du conseil d'administration et mettre en place un système complet de reporting sur la cybersécurité par la direction. Pour les petites entreprises, la marge de progression dans ces trois domaines est plus importante que pour les grandes entreprises.

Outre les résultats de l'enquête, cette édition du swissVR contient également des interviews avec :

- Marc Ruef, Head of Research chez scip et Lead Architect de VulDB
- Sandra Emme, Industry Leader Cloud Enterprise chez Google et membre des conseils d'administration de Belimo et de Zehnder Group International
- Desiere, CEO et membre du conseil d'administration de CorTec

Nous tenons à remercier chaleureusement les personnes interviewées ainsi que tous les membres des conseils d'administration qui ont participé à l'enquête. Nous vous souhaitons, chères lectrices et chers lecteurs, une lecture intéressante.

Isabelle Amschwand
Présidente de swissVR

Reto Savoia
CEO de Deloitte Suisse

Prof. Dr. Mirjam Gruber-Durrer
Chargée de cours à l'IFZ /
Haute école de Lucerne

Points-clés de l'étude

16%

des membres de conseils d'administration interrogés anticipent une évolution positive de la conjoncture suisse au cours des 12 prochains mois.

Léger redressement des perspectives économiques

- Les perspectives économiques, sectorielles et commerciales pour les 12 prochains mois se sont légèrement améliorées par rapport aux deux éditions précédentes.
- Les risques et les facteurs d'incertitude pesant sur l'économie suisse restent néanmoins présents, notamment les tensions dans le golfe Persique et la possibilité de l'instauration de nouveaux droits de douane sur les importations suisses aux États-Unis.

41%

indiquent que leur entreprise a déjà été victime d'une cyberattaque.

La cyber-résilience gagne en importance

- La proportion d'entreprises ayant déjà été victimes d'au moins une cyberattaque a presque doublé depuis 2023.
- Parmi les conséquences les plus fréquentes des attaques qui n'ont pas pu être déjouées figurent les interruptions d'activité et les accès non autorisés aux données de l'entreprise (fuites de données).

74%

ne disposent actuellement d'aucune stratégie couvrant les cyberattaques alimentées par l'IA.

La majorité des entreprises ne sont pas préparées aux cyberattaques alimentées par l'IA

- À peine une entreprise sur cinq dispose d'une stratégie contre les cyberattaques fondées sur l'IA et informe le conseil d'administration de son état de mise en œuvre et de son efficacité.
- Dans plus de la moitié des entreprises, soit il n'existe aucun plan de rétablissement des systèmes informatiques après une cyberattaque majeure, soit ces plans n'ont pas encore été testés.

68%

des conseils d'administration ne comptent aucun membre disposant d'une expertise en cybersécurité ou en informatique.

Cyber-résilience : la marge de progression est importante au sein des conseils d'administration

- Seule environ la moitié des conseils d'administration teste le dispositif de gestion de crise en cas de cyberattaque.
- La moitié des conseils d'administration n'est pas régulièrement informée par la direction des incidents de cybersécurité survenus dans l'entreprise.
- Seul un tiers des conseils d'administration dispose d'un membre possédant une expertise en cybersécurité ou en informatique.

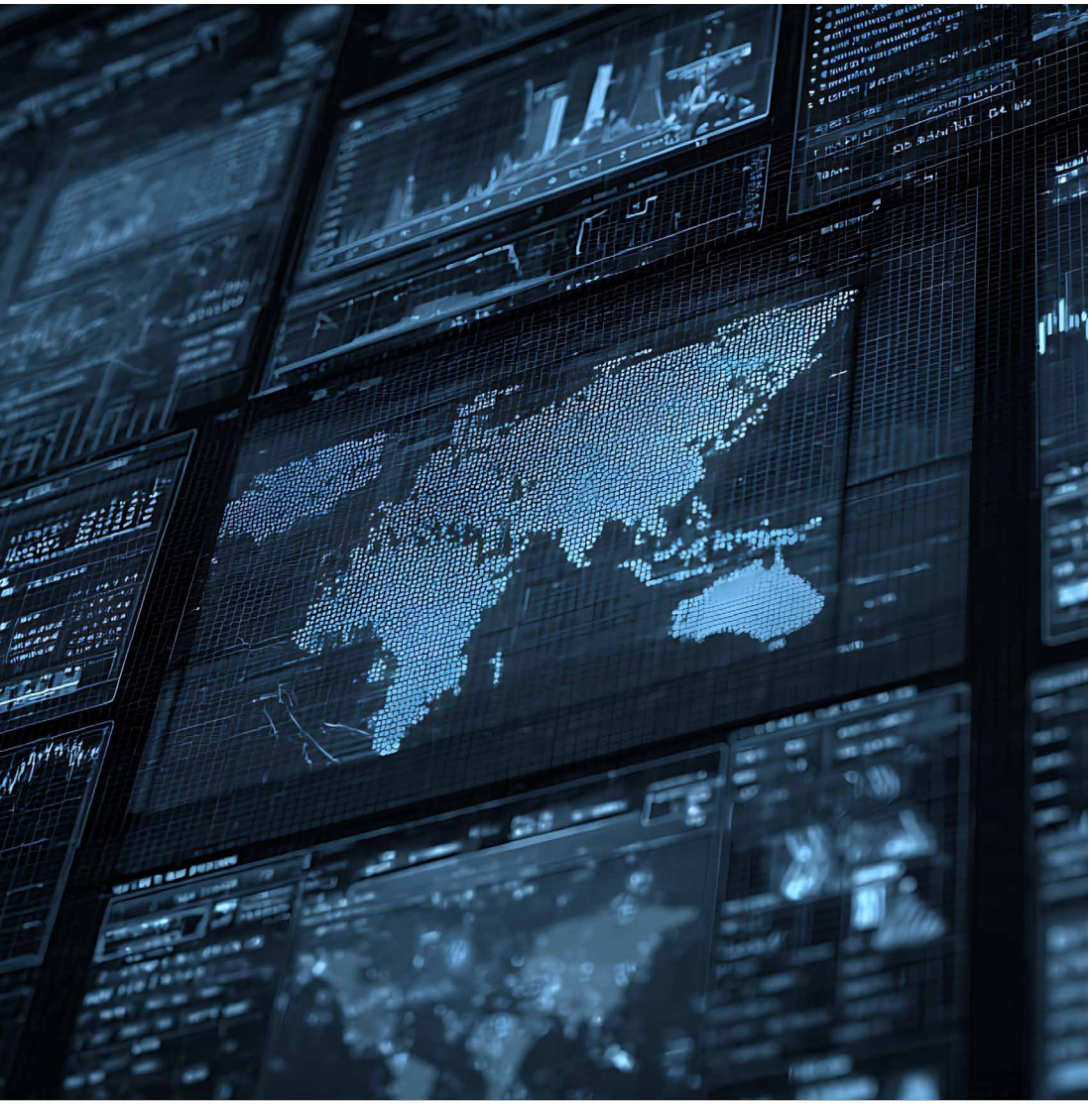
33%

considèrent l'amélioration de l'efficacité et l'optimisation des processus internes comme un enjeu prioritaire pour les 12 prochains mois.

Les priorités des conseils d'administration évoluent

- Parmi les thèmes-clés au cœur des priorités des conseils d'administration pour les 12 prochains mois, l'amélioration de l'efficacité et l'optimisation des processus internes passent de la deuxième place à la première place par rapport à l'édition précédente.
- La gestion des risques passe de la première à la deuxième place, tandis que les thématiques de la numérisation, la robotique et l'automatisation progressent de la sixième à la troisième place.

Perspectives économiques, sectorielles et commerciales



Les perspectives économiques, sectorielles et commerciales pour les 12 prochains mois se sont légèrement améliorées par rapport aux deux précédentes éditions du swissVR Monitor (voir figure 1). Un léger redressement semble se dessiner, même si, celui-ci reste pour l'heure modéré. Ce constat est d'autant plus remarquable que l'économique suisse reste exposée à de nombreux risques et facteurs défavorables, à savoir les tensions dans le golfe Persique, la possibilité de l'instauration de nouveaux droits de douane sur les importations suisses aux États-Unis, la nouvelle appréciation du franc suisse par rapport aux autres devises, ainsi que la morosité persistante de la conjoncture sur d'importants marchés étrangers.

Environ deux tiers des membres de conseils d'administration interrogés (68%) estiment que les perspectives économiques resteront neutres au cours des 12 prochains mois. Le solde entre les appréciations positives et négatives est nul et traduit donc, lui aussi, une appréciation neutre (16% d'opinions positives contre 16% d'opinions négatives). Ce résultat concorde avec d'autres prévisions actuelles, qui tablent certes sur une légère croissance de l'économie suisse en 2026 et 2027, mais aussi sur un rythme nettement inférieur à la moyenne de long terme.

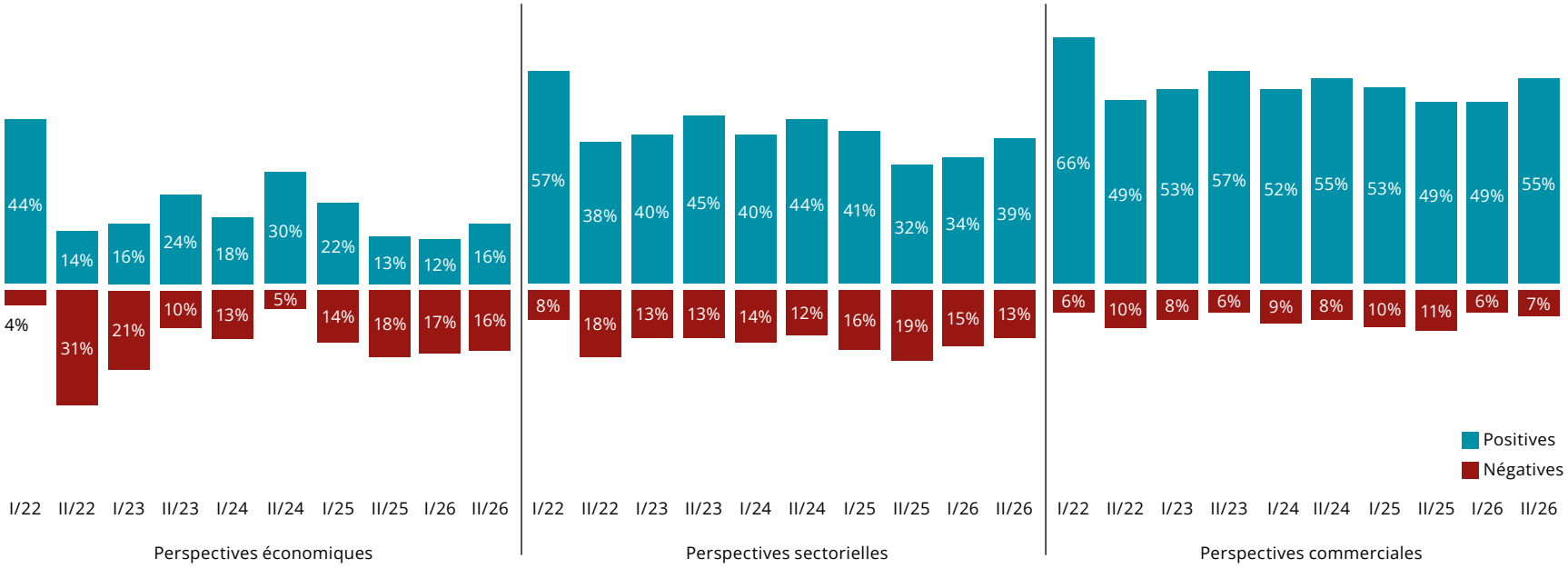
Près de la moitié des membres des conseils d'administration (48%) s'attendent à une évolution stable dans leur propre secteur au cours des 12 prochains mois. Dans le même temps, les perspectives sectorielles positives (39%) l'emportent nettement sur les prévisions négatives (13%). L'optimisme est particulièrement marqué parmi les membres des conseils d'administration du secteur des technologies de l'information et de la communication, avec 58% d'avis positifs contre 3% d'avis négatifs. Cette tendance, déjà observée ces dernières années dans un secteur porté par l'engouement pour l'intelligence artificielle, est aujourd'hui particulièrement prononcée. En revanche, les perspectives sont moins favorables dans l'industrie manufacturière et la chimie où les prévisions optimistes (20%) se plient derrière les prévisions négatives (28%). Cette situation s'explique pro-

bablement par la forte orientation à l'exportation de ces secteurs, ainsi que par la situation douanière, la vigueur du franc suisse et la demande extérieure modérée.

Concernant leur propre entreprise, plus de la moitié des membres de conseils d'administration (55%) s'attendent à une évolution positive au cours des 12 prochains mois. Une part non négligeable de 38% anticipe des perspectives commerciales neutres et seuls quelques répondants se montrent pessimistes pour les 12 prochains mois (7%). C'est dans le secteur des technologies de l'information et de la communication (73% d'opinions positives contre 3% d'opinions négatives) ainsi que dans le secteur pharmaceutique et de la santé (68% d'opinions positives contre 0% d'opinions négatives) que les membres des conseils d'administration se montrent les plus confiants pour leur entreprise. À l'inverse, les perspectives commerciales sont moins favorables que la moyenne dans l'industrie manufacturière et la chimie (24% d'opinions positives contre 16% d'opinions négatives). La baisse du solde entre les attentes positives et négatives témoigne en outre d'un recul de l'optimisme pour ces entreprises par rapport à la précédente édition du swissVR Monitor.

Fig. 1 Perspectives économiques, sectorielles et commerciales sur les douze prochains mois [swissVR Monitor I/2022 jusqu'à II/2026]

Question : Comment jugez-vous les perspectives économiques/sectorielles/commerciales sur les douze prochains mois ?
Remarque : le total n'atteint pas 100 % en raison des réponses neutres.

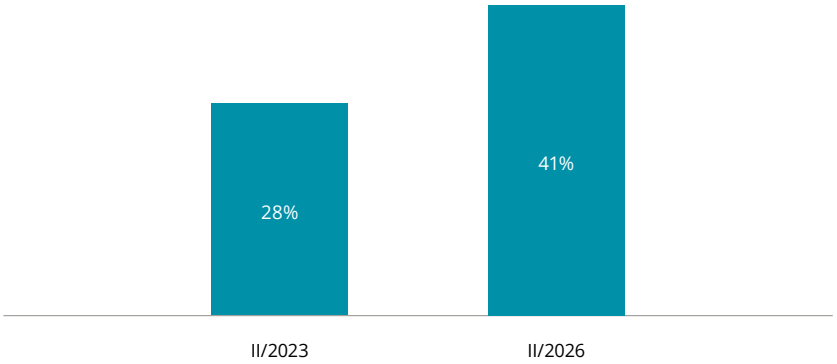


Thème clé : comment le conseil d'administration renforce la cyber-résilience

Ces dernières années, les cyberattaques visant les entreprises et autres organisations ont fortement augmenté, tant en fréquence qu'en degré de sophistication. L'un des principaux facteurs à l'origine de cette évolution est la dépendance croissante à des systèmes numériques complexes et fortement interconnectés, tels que les services cloud et les chaînes d'approvisionnement. Les progrès fulgurants de l'intelligence artificielle, avec l'apparition régulière de nouveaux modèles et d'agents plus performants, permettent par ailleurs de mener des cyberattaques plus facilement, plus rapidement et à plus grande échelle qu'auparavant. Dans ce contexte d'évolution technologique, il faut s'attendre à ce que la fréquence et l'ampleur de ces cyberattaques continuent d'augmenter. Il est donc d'autant plus important pour les membres des conseils d'administration de se saisir de la question de la cyber-résilience de leur entreprise et de la renforcer dans le cadre de leur rôle et de leurs responsabilités.

Fig. 2 Entreprises touchées par des cyberattaques

Question : À votre connaissance, votre entreprise a-t-elle déjà été victime d'une cyberattaque (par exemple : phishing, accès non autorisé à des données, piratage du site web, etc.) ?



Incidents et conséquences des cyberattaques

Quatre membres de conseils d'administration sur dix (41%) indiquent que, à leur connaissance, leur entreprise a déjà été victime d'une cyberattaque (voir figure 2). Ce chiffre a ainsi augmenté de 13 points de pourcentage en trois ans et a presque doublé (46%) par rapport à la valeur de référence de 28% enregistrée dans le swissVR Monitor II/2023.

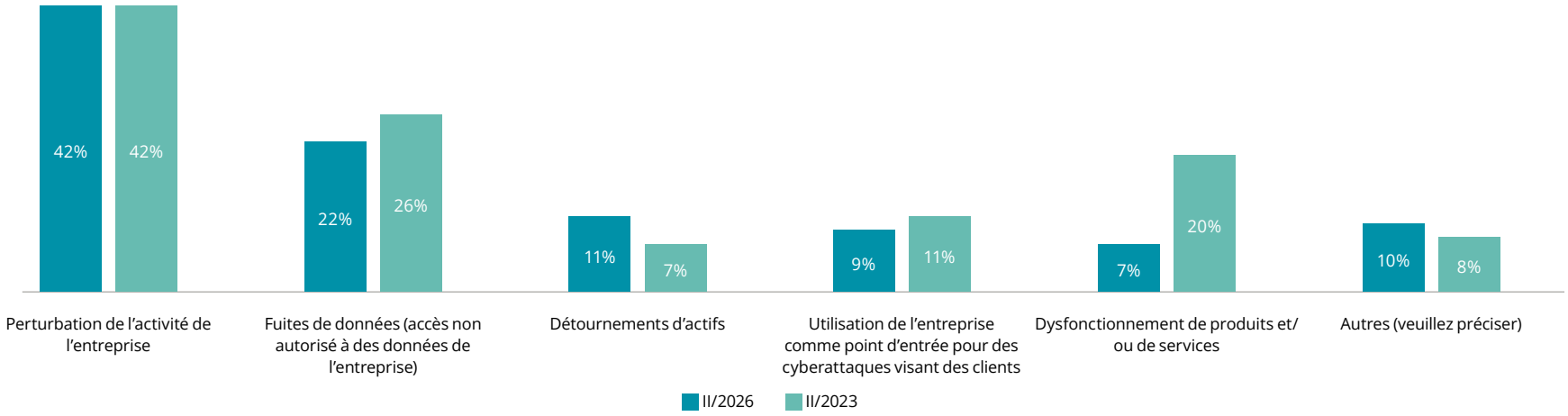
Cette progression est d'autant plus remarquable que, malgré les investissements réalisés ces dernières années par de nombreuses entreprises en matière de cyber-résilience, la proportion d'entreprises victimes de cyberattaques continue d'augmenter. Il faut en outre tenir compte du nombre potentiellement important d'incidents de cybersécurité non signalés, d'autant plus que cette enquête montre également que seul un membre du conseil d'administration sur deux reçoit régulièrement des informations de la direction à ce sujet (voir figure 9).

La hausse observée ces trois dernières années s'explique par l'augmentation du nombre de petites et moyennes entreprises victimes de cyberattaques. Leur proportion est passée de 20% à 37%, soit près du double, tandis qu'elle est restée pratiquement stable pour les grandes entreprises (II/2026 : 48% ; II/2023 : 45%). Si ces dernières restent davantage exposées en raison de leur taille, les petites et moyennes entreprises sont elles aussi de plus en plus nombreuses à être victimes de cyberattaques. L'importance de la cyber-résilience n'est donc pas une question de taille : elle revêt une importance vitale pour toutes les entreprises.

L'importance d'un niveau élevé de cyber-résilience se reflète également dans la diversité des conséquences que peuvent entraîner les attaques qui n'ont pas pu être contrées (voir figure 3). De même qu'il y a trois ans, les perturbations d'activité de l'entreprise constituent de loin la conséquence la plus fréquemment citée (42%), suivie en deuxième position par les fuites de données (22%). Les autres conséquences sont relativement rares. À l'exception des dysfonctionnements de produits et/ou de services, leur fréquence reste pratiquement inchangée par rapport à l'enquête réalisée trois ans auparavant.

Fig. 3 Conséquences des cyberattaques sur les entreprises

Question : Quelles ont été les conséquences de cette (ces) cyberattaque(s) sur votre entreprise ? Veuillez sélectionner toutes les réponses pertinentes. (n = 113)



Intelligence artificielle, Minimal Viable Company et mesures destinées aux collaborateurs

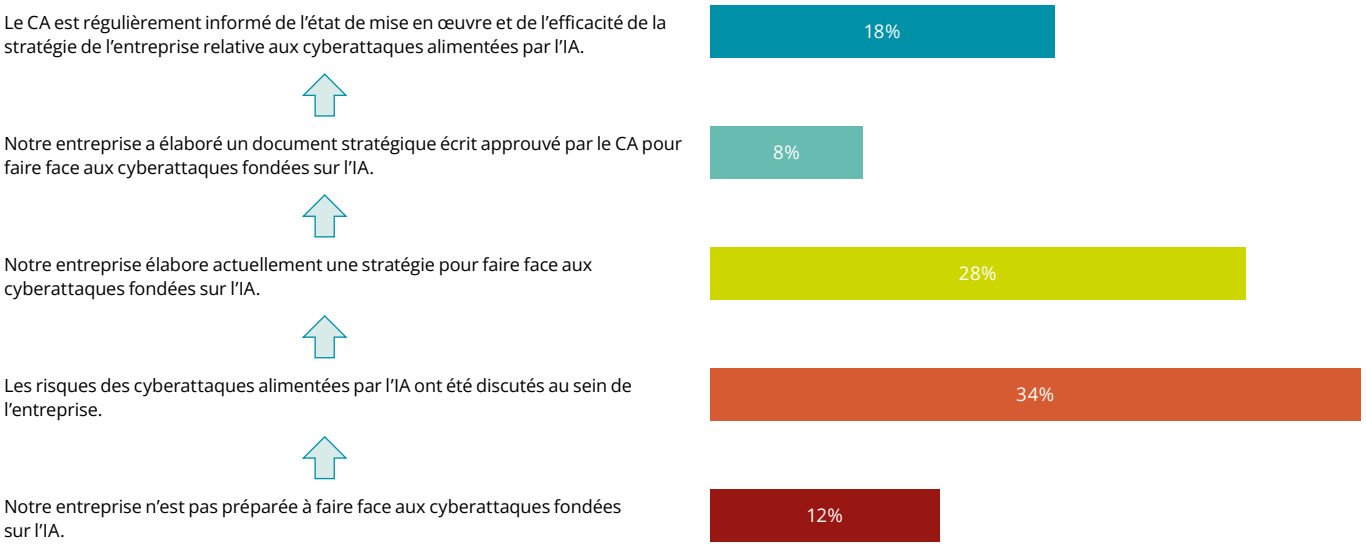
Comme indiqué précédemment, les avancées dans le domaine de l'intelligence artificielle permettent aux attaquants de causer des dommages importants plus facilement et plus rapidement. La question se pose donc de savoir dans quelle mesure les entreprises sont spécifiquement préparées à faire face à cette menace supplémentaire (voir figure 4).

Environ trois quarts des entreprises (74%, soit le cumul des trois barres inférieures) ne disposent actuellement d'aucune stratégie écrite couvrant les cyberattaques alimentées par l'IA. Parmi le quart restant, 8% disposent d'une telle stratégie, tandis que, dans la majorité des entreprises de ce groupe, le conseil d'administration est en outre informé de l'état de mise en œuvre et de l'efficacité d'une telle stratégie (18%). Il convient toutefois de souligner que l'existence d'une stratégie contre les cyberattaques alimentées par l'IA, ainsi qu'un reporting au conseil d'administration sur son efficacité, ne permettent pas, seuls, de conclure directement qu'une entreprise serait effectivement en mesure de contrer ce type d'attaques en réalité.

La taille de l'entreprise joue également un rôle déterminant dans le degré de préparation. En effet, alors que seules 18% des petites entreprises disposent d'une stratégie pour faire face aux cyberattaques fondées sur l'IA, cette proportion atteint 40% dans les grandes entreprises. Cette différence pourrait s'expliquer par un lien entre la taille de l'entreprise et le nombre de cyberattaques auxquelles elle est exposée, ou par une institutionnalisation plus poussée des enjeux cyber dans les grandes entreprises, notamment grâce à l'existence d'un département informatique ou d'une fonction de Chief Information Security Officer (CISO).

Fig. 4 Préparation à faire face aux cyberattaques alimentées par l'IA

Question : L'intelligence artificielle (IA) peut causer d'importants dommages informatiques. Dans quelle mesure votre entreprise est-elle préparée à faire face à des cyberattaques propulsées par l'IA ?



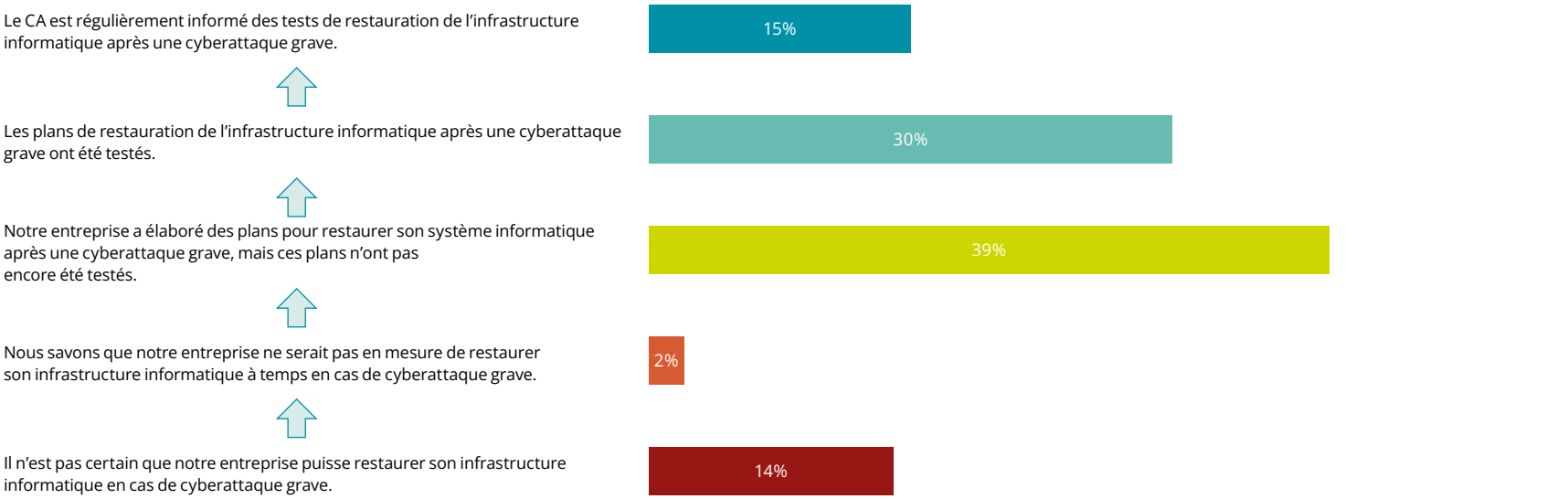
Lorsqu'il n'est pas possible, comme indiqué ci-dessus, de contrer une cyberattaque, la question se pose ensuite de savoir si les processus informatiques essentiels (Minimal Viable Company -activité minimale viable de l'entreprise) peuvent être rétablis suffisamment rapidement avant que l'entreprise ne subisse des dommages durables (voir figure 5). Dans plus de la moitié des entreprises (55%, cumul des trois barres du bas), soit il n'existe aucun plan de rétablissement des systèmes informatiques après une cyberattaque grave, soit les plans existants n'ont pas encore été testés.

À l'inverse, 45% des entreprises ont testé leurs plans visant à assurer une activité minimale viable et, parmi elles, un tiers communique également les résultats de ces tests au conseil d'administration (15%). Il convient toutefois de préciser que l'existence de plans testés et d'un reporting au conseil d'administration ne garantit pas, à elle seule, que l'infrastructure informatique pourra effectivement être rétablie.

L'influence de la taille de l'entreprise se confirme une nouvelle fois : les grandes entreprises sont près de deux fois plus nombreuses (60%) que les petites entreprises (32%) à disposer de plans testés visant à assurer une activité minimale viable. Parmi les différents secteurs, les entreprises de services financiers sont particulièrement bien préparées à la restauration de leur infrastructure informatique après une cyberattaque, avec 70% d'entre elles disposant de plans correspondants. Ce résultat s'explique par l'importance particulièrement élevée que revêt le bon fonctionnement des systèmes informatiques pour les entreprises du secteur financier, davantage encore que dans d'autres secteurs tels que la construction ou le tourisme, ainsi que par le fait que le secteur financier fait partie des infrastructures essentielles d'un État et que des normes sectorielles y sont, par conséquent, plus largement établies.

Fig. 5 Activité minimale viable de l'entreprise en cas de cyberattaque

Question : Si votre entreprise subissait une cyberattaque, ses processus informatiques clés pourraient-ils être rétablis et une activité minimale viable pourrait-elle être reprise sans coûts excessifs ni dommages inacceptables pour l'entreprise ?



Compte tenu des conséquences parfois graves des cyberattaques, les entreprises disposent d'un ensemble de mesures destinées à encadrer les pratiques des collaborateurs dans le cyberespace (voir figure 6). Ainsi, environ neuf membres de conseils d'administration sur dix (89%) indiquent que les rôles et les responsabilités en matière de cybersécurité sont clairement définis ou qu'une culture positive de la sécurité est activement promue par l'entreprise. Les collaborateurs sont régulièrement formés aux cyber-risques dans 83% des entreprises, tandis que des programmes de sensibilisation structurés, tels que des tests de phishing, existent dans environ trois entreprises sur quatre (74%). Enfin, selon six membres de conseils d'administration sur dix, l'efficacité des formations est mesurée (61%).

Ces mesures sont nettement moins souvent mises en œuvre dans les petites entreprises que dans les grandes. Ainsi, les programmes de sensibilisation, tels que les tests de phishing, ne sont présents que dans un peu plus de la moitié des petites entreprises (54%). Seul un tiers d'entre elles (36%) mesure l'efficacité de ses formations en cybersécurité. Dans presque toutes les entreprises qui comptent au moins 1000 collaborateurs, toutes les mesures présentées sont mises en œuvre.

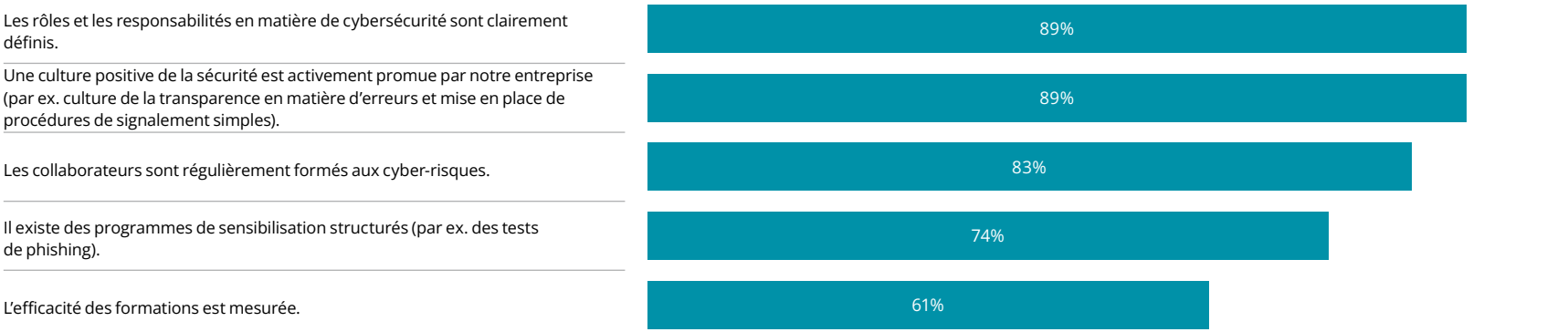
Face à la menace croissante des cyberattaques basées sur l'IA, le conseil d'administration a pour mission d'exiger de la direction une stratégie solide en la matière et d'en surveiller l'état de mise en œuvre ainsi que l'efficacité. Il doit se fixer pour objectif de savoir si l'entreprise est en mesure de contrer ce type d'attaques en situation réelle et, le cas échéant, d'engager des mesures visant à renforcer la cyber-résilience.

Il en va de même pour la garantie de l'activité minimale viable de l'entreprise : le conseil d'administration doit, là encore, être en mesure de comprendre les plans de rétablissement des systèmes informatiques après une cyberattaque majeure ainsi que les résultats des tests réalisés. Sur cette base, il peut déterminer si l'activité minimale viable de l'entreprise est assurée et si des mesures supplémentaires sont nécessaires.

Des informations et recommandations complémentaires sur ces thèmes figurent dans les interviews suivantes :
- Marc Ruef, sur les évolutions actuelles en matière de cyber-résilience
- Frank Desiere, sur l'importance de l'intelligence artificielle dans le contexte des cyberattaques

Fig. 6 Mesures encadrant l'utilisation du cyberespace par les collaborateurs

Question : Êtes-vous d'accord avec les affirmations suivantes relatives à la mise en œuvre de mesures encadrant les pratiques des collaborateurs de l'entreprise en matière de cybersécurité ?



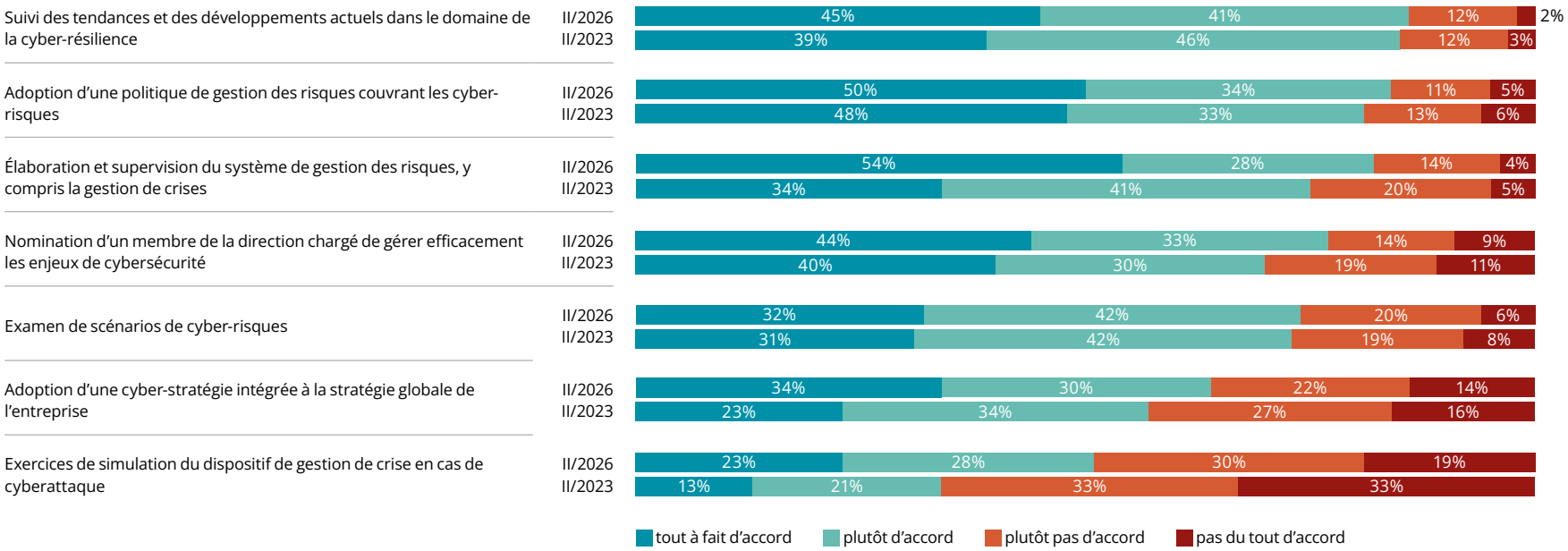
Le conseil d'administration et la cyber-résilience

En matière de cyber-résilience, le conseil d'administration assume différentes missions et différents rôles (voir figure 7). Une très grande majorité des personnes interrogées indiquent que leur conseil d'administration assure le suivi des tendances et des développements actuels dans le domaine de la cyber-résilience (86%) et adopte une politique de gestion des risques couvrant les cyber-risques (84%).

Parmi les autres responsabilités assumées au moins en partie par la majorité des membres de conseils d'administration figurent l'élaboration et la supervision du système de gestion des risques, y compris la gestion de crises (82%), la nomination d'un membre de la direction chargé de gérer efficacement les enjeux de cybersécurité (77%), ainsi que l'examen de scénarios de cyber-risques (74%). S'agissant de l'adoption d'une cyber-stratégie intégrée à la stratégie globale de l'entreprise, près de deux tiers des personnes interrogées indiquent que leur conseil d'administration assume cette mission (64%). Des améliorations restent toutefois possibles en ce qui concerne la gestion de crise en cas de cyberattaque : des exercices de simulation du dispositif de gestion de crise en cas de cyberattaque ne sont réalisés que dans la moitié des cas (51%). Ce chiffre reflète néanmoins une nette progression par rapport à l'enquête menée trois ans auparavant (34% au deuxième semestre 2023).

Fig. 7 Missions et rôles du CA

Question : Dans quelle mesure votre CA assume-t-il les missions/rôles suivants en matière de cyber-résilience ? Veuillez indiquer pour chaque réponse votre degré d'accord/de désaccord.



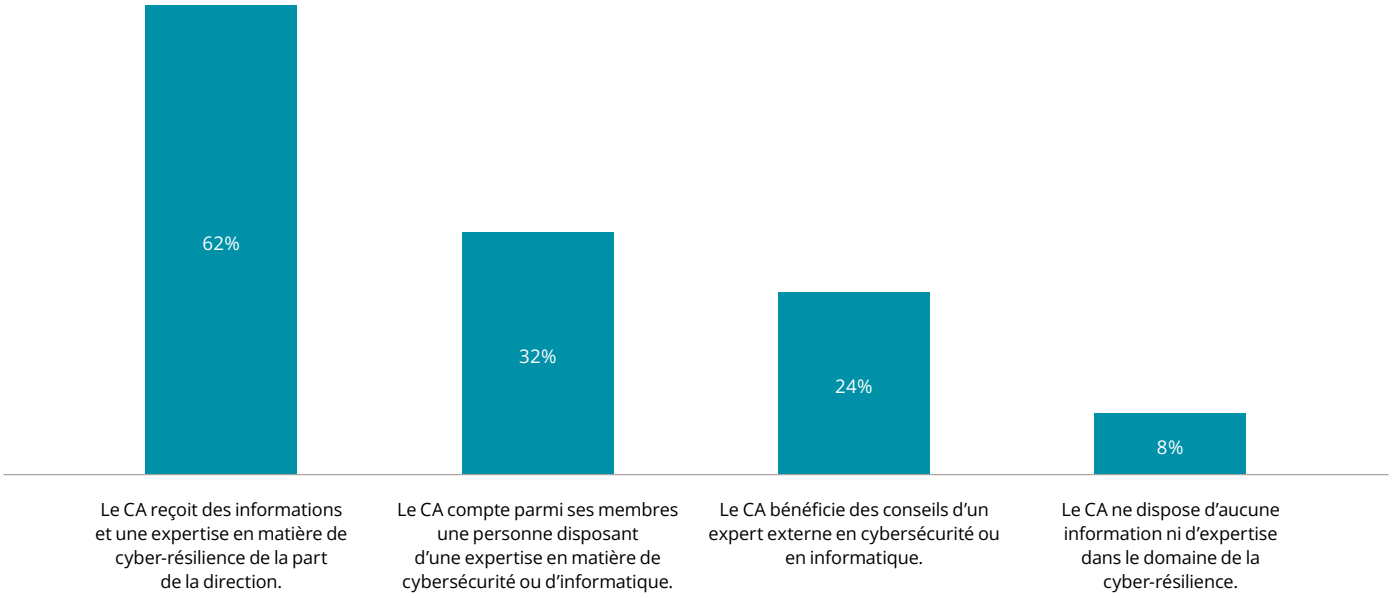
Une fois encore, les réponses des administrateurs des grandes entreprises affichent généralement des taux d'approbation plus élevés que celles des membres de conseils de petites entreprises. Par ailleurs, la comparaison avec l'enquête du swissVR Monitor II/2023 montre qu'aujourd'hui, plus de conseils d'administration s'intéressent aux enjeux de cyber-résilience qu'à l'époque.

Le conseil d'administration peut développer son expertise en matière de cyber-résilience en puisant dans différentes sources (voir figure 8). La majorité des conseils d'administration s'appuie sur la direction générale pour obtenir les informations et l'expertise nécessaires dans ce domaine (62%). Seul un tiers des personnes interrogées (32%) indique que leur conseil compte un membre disposant d'une expertise en matière de cybersécurité ou d'informatique. Dans un quart des cas (24%), le conseil d'administration bénéficie des conseils d'un expert externe en cybersécurité ou en informatique, tandis que 8% des conseils d'administration ne disposent d'aucune information, ni expertise dans le domaine de la cyber-résilience.

Étant donné que les grandes entreprises comptent un plus grand nombre de conseils d'administration que les petites entreprises, il n'est guère surprenant que leurs conseils comptent également plus fréquemment des membres disposant d'une expertise en cybersécurité ou en informatique (41% contre 28%). Cette expertise est particulièrement présente chez les membres de CA d'entreprises des technologies de l'information et de la communication (53%) ainsi que chez ceux opérant dans le secteur des services aux entreprises (41%). À l'inverse, le secteur de la construction (20%), le secteur pharmaceutique et de la santé (19%) ainsi que l'industrie manufacturière et de la chimie (16%) affichent des valeurs inférieures à la moyenne.

Fig. 8 L'expertise du CA en matière de cyber-résilience

Question : Qui fournit à votre CA les informations et l'expertise nécessaires en matière de cyber-résilience ? Veuillez sélectionner toutes les réponses pertinentes.



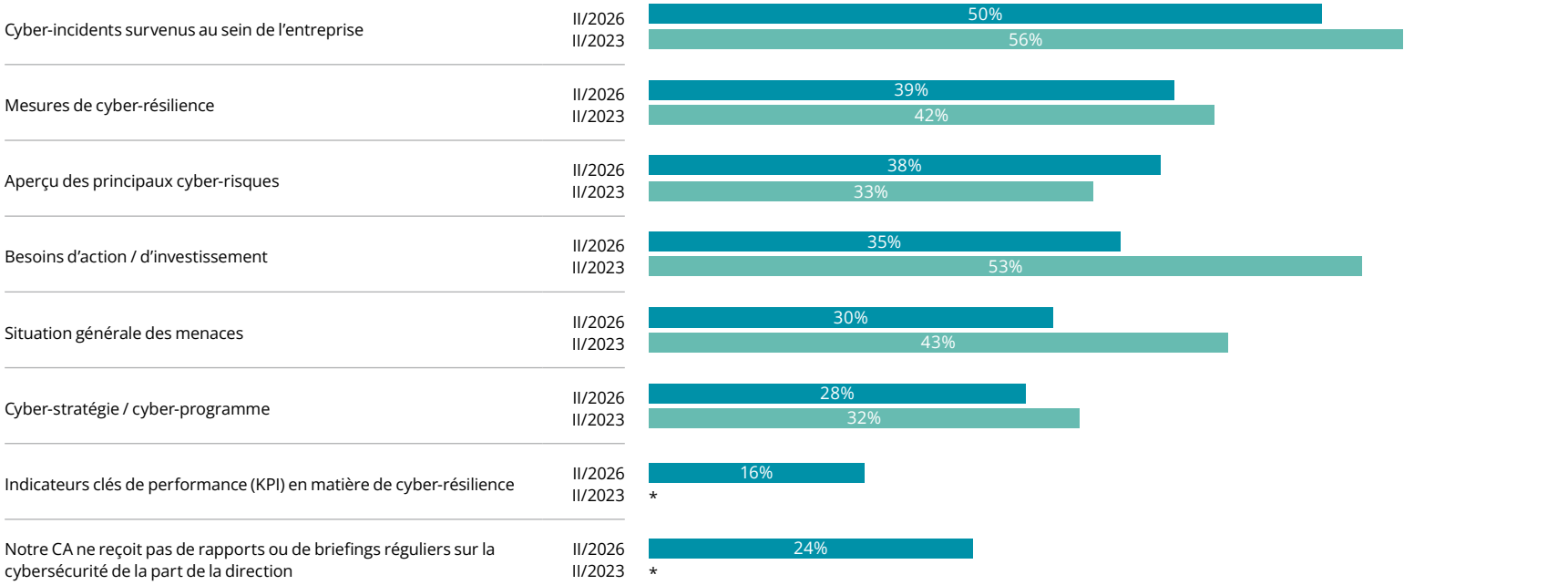
Le conseil d'administration reçoit régulièrement de la part de la direction des rapports sur différents thèmes liés à la cybersécurité, mais des améliorations restent possibles dans ce domaine (voir figure 9). Ainsi, seule environ la moitié des conseils d'administration est informée des incidents de cybersécurité survenus au sein de l'entreprise (50%). Et ce n'est que dans une minorité des cas qu'un reporting est assuré s'agissant de d'autres problématiques de cybersécurité. Par ailleurs, un quart des personnes interrogées (24%) indiquent que leur conseil d'administration ne reçoit pas de rapports ou de briefings réguliers sur la cybersécurité de la part de la direction.

Une nouvelle fois, les répondants de grandes entreprises indiquent généralement des taux et des fréquences de reporting en matière de cybersécurité plus élevés que ceux des petites entreprises. Les différences entre secteurs sont en revanche moins marquées.

Malgré l'augmentation du nombre d'entreprises ayant déjà été victimes de cyberattaques et la menace croissante que représentent les attaquants recourant à l'IA, le reporting consacré aux besoins d'action et d'investissement (–18 points de pourcentage) ainsi qu'à la situation générale des menaces (–13 points de pourcentage) a diminué

Fig. 9 Reporting de la direction en matière de cybersécurité

Question : Sur quelles questions votre CA reçoit-il régulièrement des informations en matière de cybersécurité de la part de la direction ? Veuillez sélectionner toutes les réponses pertinentes.



* aucune donnée collectée

par rapport à l'enquête du swissVR Monitor II/2023. Cette évolution pourrait indiquer que, dans de nombreuses entreprises, la cyber-résilience est davantage considérée, dans le reporting de la direction au conseil d'administration, comme une tâche ponctuelle que comme un processus continu.

Compte tenu du risque élevé que leur entreprise soit victime d'une cyberattaque, les conseils d'administration ont tout intérêt à tester leur dispositif de gestion de crise en prévision d'un tel incident. Cela inclut, par exemple, la question de savoir quelles mesures doivent être mises en œuvre en collaboration avec la direction afin de garantir l'activité minimale viable de l'entreprise.

S'agissant de la composition du conseil d'administration, il est recommandé de compter au moins un membre disposant d'une expertise en cybersécurité ou en informatique, ou de faire appel à des experts externes dans ce domaine. Le conseil d'administration peut ainsi pleinement assumer son rôle de partenaire de réflexion de la direction et contribuer au renforcement de la cyber-résilience de l'entreprise.

Le devoir de haute surveillance du conseil d'administration exige également un reporting régulier en matière de cybersécurité de la part de la direction. Ce reporting doit couvrir des éléments clés, tels que des informations relatives aux cyberincidents survenus au sein de l'entreprise. Si ces informations ne sont pas communiquées, le conseil doit les exiger.

Des informations et recommandations complémentaires sur ces thèmes figurent dans les interviews suivantes :

- Sandra Emme, sur le rôle du conseil d'administration en matière de cyber-résilience
- Frank Desiere, sur l'importance de l'intelligence artificielle face aux cyberattaques

Questions stratégiques et structurelles au sein du conseil d'administration

Fonctions, nombre de séances, temps consacré au mandat et assurance responsabilité civile des mandataires sociaux

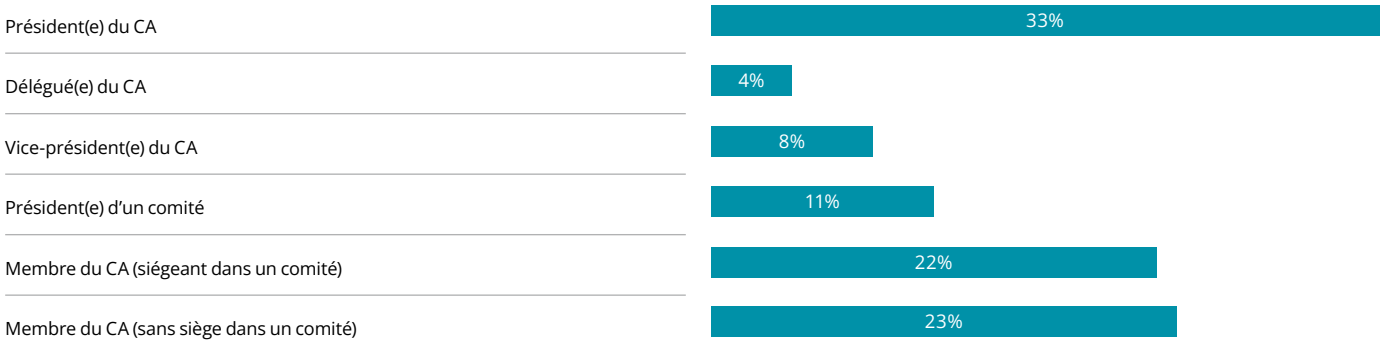
Des personnes exerçant différentes fonctions au sein de conseils d'administration ont participé au swissVR Monitor II/2026 (voir figure 10). Les membres de conseils d'administration siégeant ou non au sein d'un comité constituent ensemble le groupe le plus représenté parmi les sondés (45%). Un tiers des participants à la présente enquête sont des présidentes ou présidents de conseils d'administration (33%). L'enquête comprend également d'autres fonctions, telles que les présidentes ou présidents de comité (11%), les vice-présidentes ou vice-présidents de conseils d'administration (8%) ou les membres délégués de conseils d'administration (4%).

Le nombre de séances annuelles des conseils d'administration — hors réunions des comités — peut varier considérablement (voir figure 11). Près de trois quarts des conseils d'administration (72%) se réunissent entre trois et six fois par an, tandis qu'environ un quart (26%) se réunit plus souvent. Le nombre de réunions du conseil d'administration tend à augmenter avec la taille de l'entreprise : les conseils d'administration des petites entreprises se réunissent en médiane cinq fois par an, contre six fois pour ceux des grandes entreprises. Par rapport à l'édition II/2024, la médiane pour l'ensemble des entreprises est passée de cinq à six séances.

Outre le nombre de séances, le temps consacré chaque année au mandat de membre du conseil d'administration varie lui aussi considérablement (voir figure 12). En incluant les séances, les réunions des comités, le travail de préparation, les activités de représentation ainsi que les formations initiales et continues, le temps consacré au mandat s'élève en moyenne à 22 jours, avec une médiane de 15 jours. Ces chiffres montrent que certains membres de conseils d'administration investissent beaucoup de temps dans leur mandat. Ces valeurs ex-

Fig. 10 Fonction(s) au sein du conseil d'administration

Question : Quelle est votre fonction au sein du conseil d'administration ? [Cocher les fonctions applicables]



trêmes sont regroupées dans la catégorie « > 30 jours » et concernent environ un septième des personnes interrogées (15%). Près des deux tiers de ce sous-groupe (61%) sont des présidentes ou présidents de conseils d'administration. Par rapport aux éditions II/2022 et II/2024 du swissVR Monitor, la moyenne et la médiane du temps annuel consacré au mandat de membre du conseil d'administration n'ont pas évolué de manière significative.

Un mandat d'administrateur implique une responsabilité importante, tant pour l'entreprise que pour la personne qui l'exerce. Il existe par exemple le risque d'être poursuivi à titre personnel en cas de sinistre dans le cadre d'une action en responsabilité. Afin de se prémunir contre les coûts liés à la défense contre des actions en responsabilité, des réclamations infondées et d'éventuels versements d'indemnités, les membres du conseil d'administration et les entreprises peuvent

Fig. 11 Nombre de réunions annuelles du CA

Question : Combien de réunions annuelles du CA sont organisées au sein de votre entreprise (en dehors de celles des comités) ?

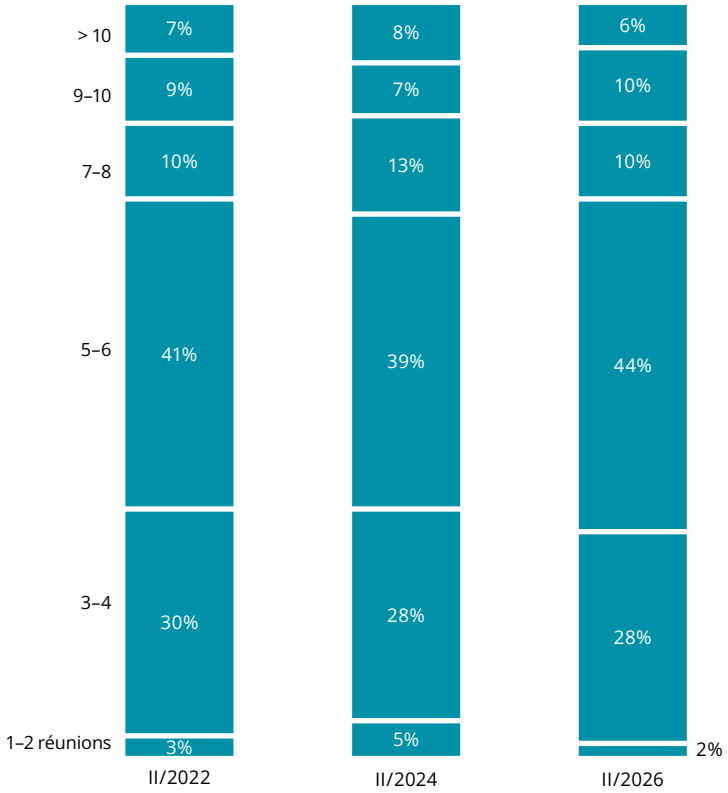
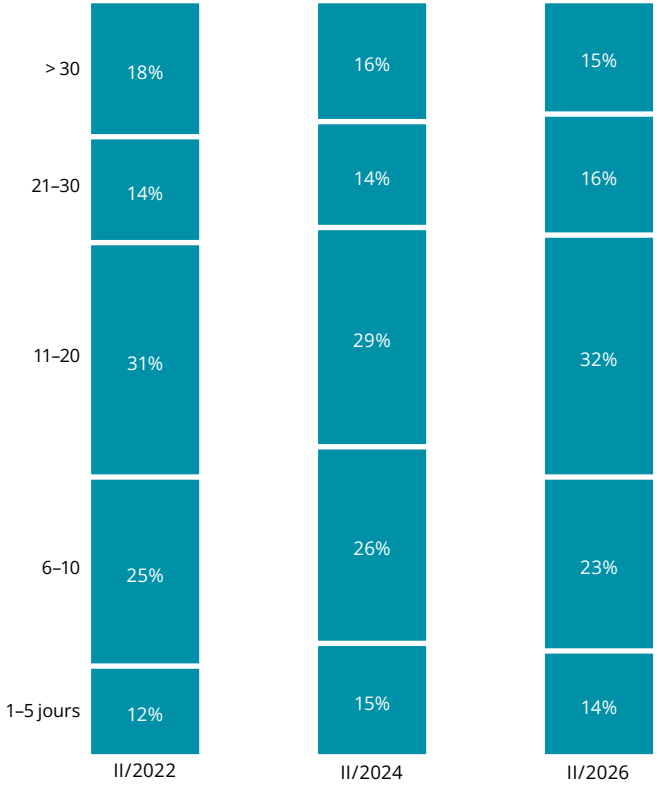


Fig. 12 Temps consacré au mandat du CA par an

Question : Combien de temps consacrez-vous chaque année à votre mandat de membre du CA (y compris les réunions, les comités, les préparatifs, la représentation, la formation, etc.) ?



souscrire une assurance responsabilité civile des mandataires sociaux (assurance D&O).

Quatre entreprises sur cinq (81%) ont souscrit une assurance responsabilité civile des mandataires sociaux couvrant les membres de leur conseil d'administration, tandis que 3% des personnes interrogées ont elles-mêmes souscrit une telle assurance (voir figure 13). Toutefois, un sixième des répondants (16%) ne bénéficie d'aucune protection par une assurance D&O en cas d'action en responsabilité. Dans les grandes entreprises, neuf membres de conseils d'administration sur dix bénéficient de cette protection (89% par l'intermédiaire de l'entreprise et 1% à titre personnel), contre trois quarts dans les petites entreprises (70% par l'intermédiaire de l'entreprise et 5% à titre personnel).

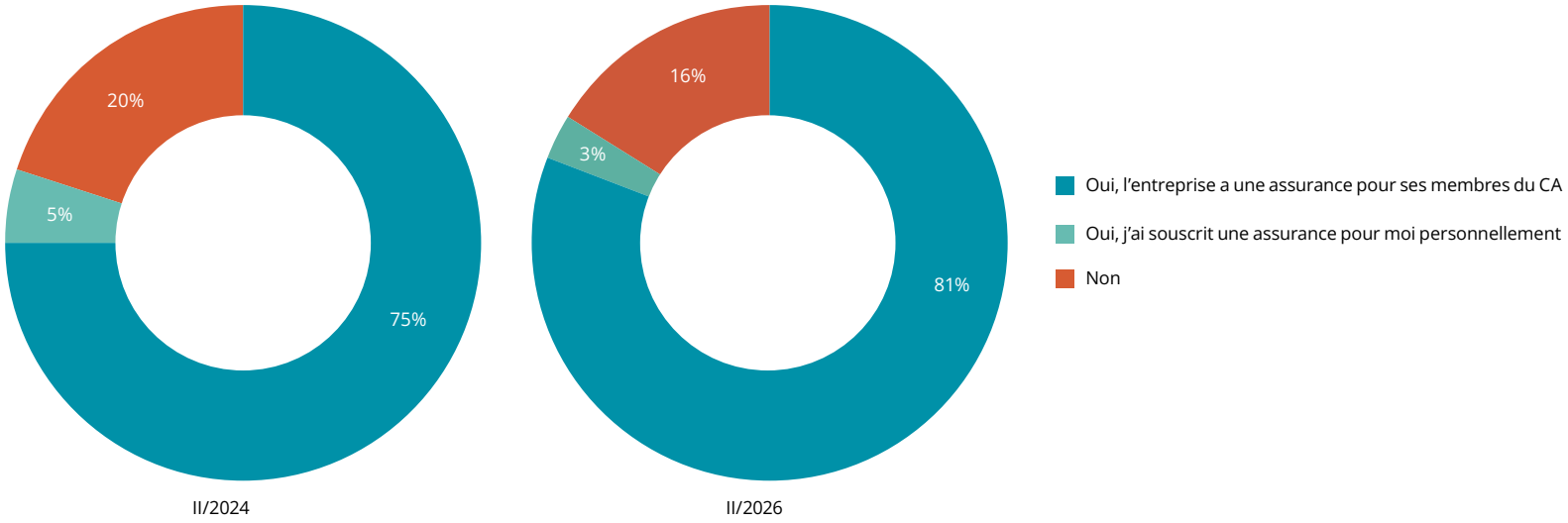
Par rapport à l'enquête du swissVR Monitor II/2024, la situation s'est, dans l'ensemble, légèrement améliorée. Cette évolution pourrait notamment s'expliquer par le fait que les membres de conseils d'administration demandent de plus en plus à leur entreprise de mettre en place une assurance responsabilité civile des mandataires sociaux.

Thèmes-clés au cœur des préoccupations du conseil d'administration

En tête des thèmes que les conseils d'administration souhaitent aborder au cours des 12 prochains mois figure le gain de performance / l'optimisation des processus internes (33%, voir figure 14). Ce thème gagne ainsi trois places par rapport à l'édition précédente. Comme cela avait été analysé en détail dans cette dernière, cette évolution

Fig. 13 Assurance responsabilité civile des mandataires sociaux

Question : Avez-vous une assurance responsabilité civile des mandataires sociaux (assurance D&O) ?



est probablement liée en premier lieu à l'introduction et au développement de l'intelligence artificielle au sein des entreprises.

Aux deuxième et troisième rangs des thématiques clés que les conseils d'administration souhaitent traiter au cours des 12 prochains mois figurent la gestion des risques (29%) ainsi que la numérisation / robotique / automatisation (28%). Par rapport à l'édition précédente, la gestion des risques recule ainsi d'une place, tandis que les thèmes liés à la numérisation progressent de trois rangs.

Il convient notamment de relever la progression de l'informatique (19%), de la gestion de la sécurité, y compris la cyber-résilience (18%) et de la mise sur le marché (stratégie marketing et commerciale) (18%), trois thèmes qui ne figuraient pas auparavant parmi les dix thèmes-clés. À l'inverse, l'élaboration d'une nouvelle stratégie d'entreprise enregistre le recul le plus marqué du classement, passant de la deuxième à la huitième place (18%).

Fig. 14 Les 10 thèmes-clés du CA

Questions : Au cours des 12 derniers mois, quelles ont été les problématiques les plus importantes traitées par votre CA ? Selon vous, quels seront les thèmes-clés dont votre CA s'occupera au cours des 12 prochains mois ?

12 prochains mois		Rang au II/2026	Thème
1 (33%)	▲	**4** (27%)	**Gain de performance / Optimisation des processus internes**
2 (29%)	▼	**1** (38%)	**Gestion des risques**
3 (28%)	▲	**6** (23%)	**Numérisation / robotique / automatisation**
4 (27%)	▲	**5** (25%)	**Adaptation aux tendances du marché / Attitude concurrentielle**
5 (24%)	▲	**7** (22%)	**Talents (y compris le recrutement, la rétention)**
6 (22%)	▼	**3** (28%)	**Défis en matière de personnel au niveau de la direction**
7 (19%)	▲	– (15%)	**Informatique**
8 (18%)	▲	– (16%)	**Gestion de la sécurité, y compris la cyber-résilience**
8 (18%)	▲	– (13%)	**Mise sur le marché (stratégie marketing et commerciale)**
8 (18%)	▼	**2** (36%)	**Élaboration d'une nouvelle stratégie d'entreprise**

« – » signifie « ne fait pas partie des 10 thèmes-clés ».

Interviews

Évolutions actuelles en matière de cyber-résilience

Marc Ruef, Head of Research chez scip et Lead Architect de VulDB

« Il faut absolument prendre le temps et garder son calme afin de se préparer à une situation de crise. […] Ne pas s'y atteler suffisamment tôt est désastreux, car lorsque la crise survient, on se bat alors, selon les cas, pour sa survie même et on n'a alors plus le temps de prendre les bonnes décisions avec discernement, et encore moins de planifier quoi que ce soit. »

Marc Ruef travaille dans le domaine de la cybersécurité depuis la fin des années 1990 et a fondé, avec computec.ch, le portail germanophone de référence consacré à la sécurité informatique. À 18 ans, il a publié son premier livre. Ont notamment suivi Hacking Intern, aux éditions Data Becker, et Die Kunst des Penetration Testing, aux éditions C&L. Au cours des 25 dernières années, il a contribué à 16 ouvrages, publié plus de 275 articles spécialisés dans sept langues différentes et accordé plus de 200 interviews. Il est considéré comme l'un des auteurs germanophones les plus lus dans son domaine. Il enseigne également dans plusieurs universités et hautes écoles, notamment à l'ETH, à la HWZ, à la HSLU et à l'IKF. Il est cofondateur de scip AG à Zurich, qui offre depuis 2002 des services de conseil en cybersécurité. Il y est responsable du département de recherche, qui mène principalement des projets non conventionnels, tels que le piratage automobile ou l'évaluation de dispositifs médicaux.

swissVR Monitor : Vous êtes un expert reconnu en cybersécurité. À votre avis, comment la cyber-résilience des entreprises a-t-elle évolué ces dernières années ?

Marc Ruef : La cyber-résilience s'est globalement améliorée. De nombreuses entreprises considèrent désormais la cybersécurité comme un élément important du risque d'entreprise. Les membres de la direction se préoccupent aujourd'hui beaucoup plus des risques et des exigences réglementaires dans le domaine numérique. Parallèlement, la cybercriminalité s'est elle aussi professionnalisée. Les groupes de ransomware opèrent aujourd'hui comme des prestataires de services industriels, avec des rôles spécifiques, une répartition des tâches et des modèles économiques bien définis. Ainsi, la course entre attaquants et défenseurs se poursuit.

swissVR Monitor : Selon notre enquête menée auprès des membres de conseils d'administration, plus d'un tiers des entreprises ont été victimes à ce jour d'une cyberattaque préjudiciable. Selon vous, quelles sont les principales vulnérabilités et pistes d'amélioration des entreprises ?

Marc Ruef : Le vol d'identifiants reste le risque le plus important. Les attaques réussies par phishing, via des infostealers ou des comptes compromis peuvent avoir des conséquences dévastatrices. Ce qui est relativement nouveau, c'est la prise de conscience croissante des risques liés aux prestataires tiers et aux chaînes d'approvisionnement. La complexité croissante des systèmes modernes entraîne des risques qui, à première vue, passent inaperçus et sont donc souvent négligés.

swissVR Monitor : Il y a trois ans, dans le cadre de la même enquête, la proportion d'entreprises ayant été victimes d'une cyberattaque s'élevait encore à environ un quart. Comment expliquez-vous cette hausse dans un contexte où les entreprises accordent une attention accrue aux cyberattaques ?

Marc Ruef : Cette augmentation n'est pas en contradiction avec une meilleure compréhension des cyber-risques. Mais fondamentalement, la complexité des systèmes – et donc leur surface d'attaque – s'est accrue. Les protéger n'est donc pas devenu plus facile. De plus, la cybercriminalité s'est transformée en un véritable modèle économique qui s'est systématiquement développé et perfectionné. Nous observons actuellement les premiers effets, déjà très concrets, de l'IA dans le domaine de la cybersécurité. Tant les défenseurs que les attaquants tirent profit de ces nouvelles possibilités.

swissVR Monitor : Selon vous, quelles sont les mesures les plus efficaces pour préparer les collaborateurs à faire face aux cyberattaques ?

Marc Ruef : La mise en œuvre réussie de la cybersécurité ne commence pas par l'acquisition de technologies coûteuses. C'est avant tout la culture de sécurité de l'entreprise qui dicte les possibilités et les modalités en la matière. La formation du personnel est un élément essentiel pour réduire le degré de vulnérabilité aux attaques. Et diverses mesures techniques, qui ont fait leurs preuves au fil des décennies, peuvent être mises en œuvre et optimisées en permanence. Il s'agit notamment de mécanismes classiques tels que les pare-feux, la segmentation des réseaux, les solutions antivirus et l'installation de mises à jour.

swissVR Monitor : Selon notre dernière enquête, plus de la moitié des entreprises ne sont pas en mesure de garantir que leurs processus informatiques essentiels pourront être rétablis en cas de cyberattaque sans entraîner de coûts ou de dommages inacceptables. À quoi devraient concrètement ressembler les plans prévus pour un tel scénario et comment devraient-ils être testés ?

Marc Ruef : Le sang-froid et la discipline sont des conditions essentielles à la sécurité d'une entreprise. Il faut absolument prendre le temps et garder son calme afin de se préparer à une situation de crise. Il faut identifier les processus clés, déterminer les risques qui les menacent et élaborer des mesures visant à limiter les répercussions ou à assurer la reprise des activités. Ne pas s'y atteler suffisamment tôt est désastreux, car lorsque la crise survient, on se bat alors, selon les cas, pour sa survie même et on n'a alors plus le temps de prendre les bonnes décisions avec discernement, et encore moins de planifier quoi que ce soit.

Le rôle du conseil d'administration dans la cyber-résilience

Sandra Emme, Industry Leader Cloud Enterprise chez Google et membre des conseils d'administration de Belimo et de Zehnder Group International

« De nombreux conseils d'administration ne sont pas conscients du rôle important qui leur incombe. [...] Garantir la cyber-résilience n'est pas une tâche informatique délégable, mais fait partie intégrante de la haute direction de l'entreprise, dont la responsabilité est inaliénable. »

swissVR Monitor : Quel rôle incombe généralement au conseil d'administration lorsqu'il s'agit d'assurer la cyber-résilience des entreprises ?

Sandra Emme : Ce qui me frappe souvent dans mes échanges avec des membres de conseils d'administration, c'est que beaucoup d'entre eux ne sont pas conscients du rôle important qui leur incombe. Permettez-moi d'aller un peu plus loin. Garantir la cyber-résilience n'est pas une tâche informatique délégable, mais fait partie intégrante de la haute direction de l'entreprise, dont la responsabilité est inaliénable, conformément à l'article 716a du Code suisse des obligations.

Le conseil d'administration doit considérer les cyber-risques, au même titre que les risques financiers ou opérationnels, comme des risques stratégiques pour l'entreprise et les intégrer de manière structurée dans la gestion des risques à l'échelle de l'entreprise. Sa mission principale réside dans le pilotage stratégique : il définit la tolérance au risque, met à disposition les ressources financières nécessaires et garantit une gouvernance claire.

Sandra Emme a débuté sa carrière entrepreneuriale en France en tant que cofondatrice de plusieurs start-ups informatiques qui se sont développées à l'international avant d'être revendues avec succès. Elle travaille chez Google depuis quinze ans et y occupe actuellement le poste d'Industry Leader, dans le cadre duquel elle conseille des entreprises industrielles sur leur stratégie de transformation, de cybersécurité et de données. En 2018, elle est devenue membre du conseil d'administration de Panalpina Welttransport Holding AG, puis, en 2019, de Metall Zug AG. Elle exerce actuellement des mandats au sein des conseils d'administration de Belimo Holding AG (depuis 2018) et de Zehnder Group AG (depuis 2022). Elle est également membre du comité directeur de digitalswitzerland, chargée de cours en transformation numérique des entreprises à l'IMD, et titulaire de certifications en gouvernance d'entreprise (HSG) ainsi qu'en ESG (Competent Boards).

Le conseil d'administration doit également recevoir régulièrement des informations sur la situation en matière de menaces, exiger des indicateurs de sécurité et vérifier l'efficacité des plans d'urgence. Il est conseillé de documenter ce processus afin de pouvoir démontrer les responsabilités fiduciaires, le devoir de diligence et la continuité. En cas d'incident, les obligations légales de déclaration doivent être respectées, ce que le conseil d'administration doit superviser dans le cadre de sa haute surveillance.

swissVR Monitor : D'après notre enquête menée auprès des membres de conseils d'administration, seule la moitié environ des conseils d'administration teste son dispositif de gestion de crise en cas de cyberattaque. Quels sont les risques concrets pour l'autre moitié des conseils d'administration ?

Sandra Emme : Si un conseil d'administration néglige fondamentalement la question de la cyber-résilience, il manque à son devoir légal de diligence. En cas de cyberattaque grave entraînant des pertes financières considérables, le conseil d'administration s'expose à une responsabilité civile personnelle engageant son patrimoine privé, ainsi qu'à des conséquences pénales si les obligations légales de déclaration n'ont pas été respectées.

Par ailleurs, les exercices de simulation de crise destinés au conseil d'administration ne visent expressément pas à ce que celui-ci intervienne sur le plan opérationnel en cas d'urgence – cela serait contre-productif et entraverait le travail de la cellule de crise de la direction. Il s'agit plutôt de vérifier si l'organisation est préparée et si les flux d'information vers le conseil d'administration fonctionnent correctement. Sans exercice préalable, le conseil risque, en cas d'urgence, de prendre de mauvaises décisions stratégiques et de perdre un temps précieux.

Les risques concrets sont au nombre de quatre. Le premier est la responsabilité juridique : le conseil d'administration n'est pas responsable de l'attaque elle-même, mais d'une préparation insuffisante ou d'erreurs stratégiques commises pendant la crise, telles que la violation des obligations de publication ad hoc ou des obligations de déclaration en matière de protection des données. Dans de tels cas, les assurances cyber et les assurances de responsabilité civile des mandataires sociaux (D&O) peuvent également refuser de couvrir les dommages.

Le deuxième risque réside dans l'incapacité à agir en situation de crise : sans entraînement, le conseil d'administration ne sait pas quelles décisions stratégiques il doit prendre sous une pression énorme en termes de temps (par exemple, déblocage de fonds exceptionnels, information des actionnaires majoritaires ou des autorités de régulation). Le troisième risque est le dilemme lié à une demande de rançon : sans discussion préalable, le conseil d'administration ne sait pas, au moment de l'attaque, s'il doit céder aux demandes de rançon ni comment s'y prendre, et ne dispose pas des ressources nécessaires à cette fin.

Le quatrième risque concerne les préjudices financiers et les dommages réputationnels : un incident de cybersécurité entraîne presque toujours une atteinte à la réputation, même en cas de bonne gestion de crise. Toutefois, si le conseil d'administration n'est pas préparé et que la communication manque de coordination, ce préjudice s'amplifie considérablement et peut menacer l'existence même de l'entreprise, en particulier pour les PME.

Mon conseil : organisez des exercices de simulation de crise (tabletop exercises) et assurez-vous que la direction a conclu un contrat de réponse aux incidents (Incident Response Retainer), c'est-à-dire un contrat de disponibilité avec des experts externes pour une aide immédiate. Un tel contrat est souvent considéré comme un atout par les assureurs cyber, voire exigé.

swissVR Monitor : De même, seule la moitié environ des membres du conseil d'administration reçoit de la part de la direction des informations sur les incidents de cybersécurité survenus au sein de l'entreprise. Outre ces incidents, sur quels autres aspects le conseil d'administration devrait-il recevoir un reporting régulier de la part de la direction en matière de cybersécurité ?

Sandra Emme : Un reporting qui se contente, par exemple, d'énumérer les incidents passés ne répond pas aux exigences stratégiques du conseil d'administration. L'accent doit être mis sur la gestion des risques. Le conseil d'administration doit prendre des décisions d'investissement concrètes et fondées. Le mieux est de quantifier les cyber-risques en francs suisses : quel niveau de risque sommes-nous prêts à accepter ?

Un reporting prospectif devrait couvrir les dimensions suivantes. Premièrement, les principaux cyber-risques et les mesures de mitigation, c'est-à-dire la réponse aux questions suivantes : quelles sont actuellement les plus grandes menaces pour le modèle économique et quelles mesures la direction prend-elle pour réduire ces risques ?

La deuxième dimension concerne la protection des « joyaux de la couronne » : dans quelle mesure nos systèmes les plus critiques pour l'activité et nos données les plus précieuses sont-ils protégés ? Les co-

pies de sauvegarde, par exemple, doivent impérativement être séparées du réseau principal – et donc protégées contre tout chiffrement externe.

La troisième dimension concerne la capacité de réaction (résilience) ou les indicateurs relatifs au délai moyen de détection : en d'autres termes, combien de temps faut-il en interne pour se rendre compte que le réseau de l'entreprise a été attaqué ? Combien de temps faut-il pour réagir ? Et : lorsqu'un éditeur de logiciels externe signale une faille de sécurité, combien de temps faut-il à l'équipe interne pour corriger cette vulnérabilité critique ?

La quatrième dimension porte sur la chaîne d'approvisionnement et les tiers, c'est-à-dire l'évaluation des cyber-risques tout au long de la chaîne d'approvisionnement, laquelle représente souvent une porte d'entrée majeure. La cinquième dimension concerne les risques liés aux personnes et à l'IA : les résultats des formations ainsi que l'évaluation stratégique de la sécurité des outils d'IA utilisés.

La sixième et dernière dimension englobe un regard externe indépendant, à savoir les résultats d'audits de cybersécurité indépendants, de tests d'intrusion ou d'évaluations du niveau de maturité, ainsi que les scores de sécurité, afin d'obtenir une référence objective.

swissVR Monitor : **La grande majorité des conseils d'administration ne compte aucun membre disposant d'une expertise en cybersécurité. Dans quels cas un conseil d'administration devrait-il recruter une personne possédant une expertise en cybersécurité ou en informatique ?**

Sandra Emme : Tous les membres d'un conseil d'administration ne doivent pas nécessairement être des experts en informatique, mais une « cécité technologique » au sein de l'ensemble du conseil s'accompagne d'énormes risques stratégiques. Un recrutement ciblé est particulièrement conseillé lorsque le « déficit de mise en œuvre » s'accentue. Le conseil d'administration a besoin d'un membre qui joue le rôle de « traducteur » afin d'examiner d'un œil critique les déclarations de la direction en matière d'informatique.

Les transformations en profondeur constituent une autre raison justifiant un recrutement ciblé : par exemple, lors d'une migration mondiale vers de nouveaux systèmes ERP, dans le cadre d'une stratégie « cloud first » ou lorsque l'IA bouleverse le modèle économique principal. Un membre du conseil d'administration disposant de l'expertise requise est également indispensable lorsqu'il existe un retard à combler en matière de maturité cyber. Si des audits cyber mettent en évidence des lacunes, les conseils d'administration ne doivent pas attendre que l'entreprise soit victime d'une attaque majeure et que les actionnaires exigent des changements au niveau du personnel et le renforcement de l'expertise au sein du conseil.

Pour les entreprises cotées, un recrutement ciblé est également pertinent, car les investisseurs et les conseillers en vote exigent de plus en plus des administrateurs dotés de compétences numériques. Au moins un membre devrait posséder une expérience avérée dans les domaines de la technologie et de la cybersécurité.

Dans les entreprises de taille moyenne, il est souvent plus difficile de trouver un expert informatique à temps plein au sein du conseil d'administration, et un tel profil risque de mobiliser de manière trop spécifique l'un des rares sièges disponibles. Il est recommandé de constituer un comité consultatif externe ou de solliciter un RSSI externe en tant qu'intervenant invité afin d'assurer un regard indépendant sur les rapports en matière de cybersécurité.

swissVR Monitor : **Dans quels cas est-il judicieux pour un conseil d'administration de créer un comité chargé de la cybersécurité ou de l'informatique ?**

Sandra Emme : De manière générale, la mise en place d'un tel comité s'impose de plus en plus comme une bonne pratique dans tous les secteurs. La création d'un comité informatique ou cyber dédié devient toutefois impérative lorsque la complexité de l'environnement informatique est telle que l'ensemble du conseil d'administration ou le comité d'audit classique ne dispose pas du temps nécessaire pour en acquérir une compréhension approfondie. Cela vaut en particulier dans le cas d'une convergence OT/IT. Lorsque, dans les entreprises manufacturières, les installations de production (Operational Tech-

nology) et l'informatique classique fusionnent, de nouveaux vecteurs d'attaque extrêmement complexes apparaissent dans l'automatisation industrielle.

D'autres raisons justifient la création d'un tel comité lorsque l'entreprise doit réduire une dette informatique importante, investit massivement dans l'IA ou doit gérer des intégrations informatiques complexes à la suite d'acquisitions.

Un comité dédié à l'informatique ou à la cybersécurité est également utile pour les analyses approfondies : il permet d'approfondir des sujets présentant un intérêt stratégique particulier pour une entreprise, par exemple les stratégies SOC (Security Operations Center), la protection de la chaîne d'approvisionnement, les développements en matière de cybersécurité ou d'IA/IoT dans le cadre de la stratégie d'innovation.

Enfin, la pression réglementaire peut également justifier la mise en place d'un tel comité. Pour les entreprises cotées en bourse ou fortement réglementées, un « Technology & Cyber Committee » est essentiel pour examiner en profondeur les questions d'architecture, les budgets informatiques importants et les audits de sécurité, puis pour formuler des recommandations étayées à l'intention de l'ensemble du conseil d'administration.

L'importance de l'intelligence artificielle dans les cyberattaques

Frank Desiere, CEO et membre du conseil d'administration de CorTec

« Les enquêtes – y compris le swissVR Monitor – indiquent qu'une part considérable des conseils d'administration ne reçoit pas de reporting régulier sur l'utilisation de l'IA et les risques qui y sont associés. Sans ce reporting, une surveillance efficace est tout simplement impossible. »

swissVR Monitor : Comme dans d'autres domaines d'application, l'intelligence artificielle (IA) est également de plus en plus utilisée pour les cyberattaques. Comment l'IA a-t-elle modifié la qualité et la quantité des cyberattaques ces dernières années ?

Frank Desiere : Je décrirais cela comme une évolution de l'économie des cyberattaques. Sur le plan quantitatif, l'IA fait quasiment tomber à zéro le coût marginal d'une attaque : la reconnaissance, la recherche de cibles et la création de contenus convaincants peuvent être automatisées et déployées à grande échelle, à volonté. Ce qui nécessitait autrefois une équipe spécialisée est aujourd'hui à la portée d'acteurs moins expérimentés.

Sur le plan qualitatif, le changement est peut-être encore plus radical. Le rapport d'IBM « Cost of a Data Breach Report 2025 » estime que près de 16% des violations de données examinées impliquaient déjà l'IA du côté des attaquants – principalement du phishing généré par l'IA et l'usurpation d'identité par deepfake. Les messages d'attaque ne se repèrent plus à leurs fautes de langue : ils sont désormais personnalisés et parfaitement adaptés au contexte ; les deepfakes vocaux et vidéo rendent les fraudes classiques au faux dirigeant particulièrement convaincantes.

Dr. Frank Desiere est CEO de CorTec et exerce également la fonction de Non-Executive Director (membre du conseil d'administration). Cette double fonction façonne sa vision de la gouvernance : il connaît aussi bien les responsabilités liées à la direction opérationnelle que les missions de surveillance et de contrôle du conseil d'administration — et donc l'interface où se construit une gouvernance d'entreprise efficace. Avec WE TALK BOARD, sa newsletter et son podcast, il s'adresse aux membres de conseils d'administration, aux présidences, aux cadres dirigeants ainsi qu'aux futurs membres de conseils. Il y aborde principalement l'efficacité des conseils d'administration, la gouvernance responsable et la formation continue des Non-Executive Directors, avec une perspective résolument suisse et européenne. Parallèlement à ses activités de direction et de surveillance, Dr Desiere intervient comme conférencier et anime des sessions destinées aux dirigeants sur des thèmes liés à la gouvernance, notamment dans le cadre du Deloitte Board Program. Son objectif est de proposer des repères pratiques et solides à toutes les personnes qui assument des responsabilités au sein d'un conseil d'administration.

Pour le conseil d'administration, le facteur décisif est le raccourcissement du délai entre la découverte d'une vulnérabilité et son exploitation. Cela fait évoluer la stratégie de défense : il ne s'agit plus seulement de « protection du périmètre » mais de « détection et (de) confinement rapides ». La cybersécurité n'est donc plus une simple question informatique, mais une question de résilience – et celle-ci doit figurer à l'ordre du jour de l'instance.

swissVR Monitor : Nous sommes aujourd'hui à la transition entre l'ère de l'IA agentique et celle de l'IA multi-agentique. Que signifie cette évolution technologique pour le risque de cyberattaques à l'avenir ?

Frank Desiere : La différence est qualitative, et non graduelle. L'IA générative a fourni de meilleurs outils aux attaquants, tout en laissant l'humain aux commandes. L'IA agentique repousse précisément cette limite : l'agent planifie, agit, observe et s'adapte – en grande partie sans intervention humaine.

Anthropic a révélé en novembre 2025 à quel point cette évolution est concrète : il s'agit de la première campagne d'espionnage documentée, largement orchestrée par l'IA, menée selon l'entreprise par un acteur proche de l'État, dans laquelle l'IA a exécuté elle-même environ 80 à 90% des étapes opérationnelles et où les humains ne sont intervenus qu'à quelques rares moments décisionnels. Une trentaine de cibles à travers le monde, avec des attaques menées à la vitesse des machines plutôt que manuellement.

Les systèmes multi-agents font passer cela au niveau supérieur : des agents spécialisés qui exécutent une chaîne d'attaques selon une répartition des tâches et réagissent en temps réel aux mesures de défense. Nous nous dirigeons vers une dynamique « machine contre machine », dans laquelle une défense reposant entièrement sur l'intervention humaine est structurellement trop lente.

Conséquence pour le conseil d'administration : la défense doit elle-même être automatisée – et les agents que nous déployons nous-mêmes, avec leurs autorisations, leur mémoire et leurs accès aux outils, deviennent à leur tour une cible d'attaque à part entière. C'est le revers de la médaille de toute initiative d'efficacité basée sur l'IA approuvée par l'instance.

swissVR Monitor : Notre enquête auprès des membres de conseils d'administration montre que seule une petite minorité d'entreprises dispose d'une stratégie concrète contre les cyberattaques fondées sur l'IA. Comment évaluez-vous le risque pour les entreprises qui ne prennent pas encore spécifiquement en compte les cyberattaques menées par l'IA ?

Frank Desiere : Il est considérable mais je tiens à préciser où réside réellement le risque, car il existe deux failles. La première : ceux qui ne tiennent pas compte des attaques alimentées par l'IA se défendent contre un nouveau modèle de menace avec des outils d'hier. La détection basée sur les signatures est inefficace face aux logiciels malveillants adaptatifs, et les attaquants ont déjà industrialisé leurs méthodes.

La deuxième faille est d'origine interne et est sous-estimée : l'utilisation non maîtrisée de l'IA au sein même de l'entreprise. Le rapport d'IBM de 2025 montre qu'environ une violation de données sur cinq était liée à une « IA fantôme » et que ces incidents coûtaient en moyenne environ 670 000 dollars américains ; 63% des entreprises concernées ne disposaient d'aucune politique de gouvernance de l'IA. Le risque ne provient pas ici d'un attaquant, mais de collaborateurs qui intègrent des données clients ou de la propriété intellectuelle dans des modèles externes.

Je mets toutefois en garde contre toute précipitation. Toutes les entreprises n'ont pas besoin d'une « stratégie cyber-IA » distincte sous la forme d'un document autonome. Ce qui est déterminant, c'est son intégration dans le cadre de la gestion des risques existant et la gestion de la cybersécurité en tant qu'enjeu d'entreprise, et non comme un simple enjeu informatique – en s'appuyant sur des normes reconnues telles que le NIST CSF 2.0 ou la norme ISO 27001. Les PME sont particulièrement exposées : non seulement en raison de ressources plus limitées, mais aussi, de plus en plus, en tant que cibles via les chaînes d'approvisionnement, notamment dans le sillage de la réglementation européenne NIS2. Celles qui adoptent une attitude attentiste risquent de devenir le prochain cas d'école.

swissVR Monitor : Quelles mesures concrètes les entreprises devraient-elles prendre pour se protéger contre les cyberattaques alimentées par l'IA ?

Frank Desiere : Je distingue cinq priorités, délibérément classées dans cet ordre. Premièrement : contrer l'IA par l'IA. La détection basée sur le comportement et les anomalies, ainsi que la réaction automatisée, sont nécessaires pour pouvoir réagir à la vitesse des machines. Selon IBM, les organisations qui utilisent largement l'IA et l'automatisation dans leur défense économisent en moyenne environ

1,9 million de dollars US par incident et limitent les attaques nettement plus rapidement.

Deuxièmement : une approche « Zero Trust » associée à une gestion rigoureuse des identités et des autorisations – y compris expressément pour les identités machines et les agents d'IA, qui se voient de plus en plus souvent attribuer leurs propres droits d'accès. Troisièmement : une authentification résistante au phishing, comme les clés d'accès, combinée à un principe obligatoire de double contrôle et de rappel pour les paiements et les modifications d'autorisations. Face aux fraudes au faux dirigeant fondées sur les deepfakes, il ne faut pas se fier à son intuition, mais à un processus.

Quatrièmement – et c'est souvent sous-estimé : l'humain. La sensibilisation doit être repensée ; la règle empirique consistant à « repérer les fautes de frappe » ne tient plus la route lorsque les messages sont parfaitement rédigés. Cinquièmement : les mesures d'hygiène de base restent cruciales – gestion des correctifs, sauvegardes immuables, segmentation du réseau et plan de réponse aux incidents régulièrement mis en pratique, et pas seulement documenté.

Deux éléments supplémentaires qui relèvent du niveau de la direction : la sécurisation de la chaîne d'approvisionnement et la gouvernance des applications d'IA de l'entreprise contre les fuites de données et l'injection de prompts. L'ordre est important : d'abord les fondamentaux, puis le perfectionnement. Et le conseil d'administration devrait recevoir un reporting sur le niveau de maturité pour chacun de ces points, et non pas simplement des activités menées.

swissVR Monitor : Quel rôle joue le conseil d'administration pour garantir qu'une entreprise soit toujours à la pointe des évolutions technologiques et préparée aux menaces qui en découlent, telles que les cyberattaques fondées sur l'IA ?

Frank Desiere : Les risques liés à la cybersécurité et à l'IA relèvent de la responsabilité du conseil d'administration, tant sur le plan juridique que dans les faits. Ils touchent à la haute direction, qui est une fonction intransmissible, et au devoir de diligence prévu aux articles 716a et 717 du CO. La mise en œuvre opérationnelle peut être déléguée à la direction ou au RSSI, mais pas la surveillance ; en cas de manquement à une obligation, le conseil d'administration est personnellement responsable en vertu de l'article 754 du CO. Une couverture D&O ne dispense pas le conseil de son devoir de diligence ; elle suppose au contraire que celui-ci soit respecté.

Le conseil d'administration ne doit pas nécessairement posséder l'expertise technique la plus pointue, mais il doit en savoir suffisamment pour poser les bonnes questions et exiger des réponses étayées de la part de la direction. Il doit également s'assurer que les compétences nécessaires sont présentes au sein du conseil d'administration ou par le biais de conseillers externes. Concrètement, cela signifie : des responsabilités clairement définies au sein d'un comité des risques ou d'audit ; un reporting régulier et structuré plutôt qu'un compte rendu établi uniquement après coup ; un plan de crise rodé, dans lequel le rôle du conseil est également clarifié ; des ressources adaptées à l'appétence au risque ; et une veille attentive de l'horizon réglementaire – la LPD révisée, les répercussions de la directive NIS2 et la législation européenne sur l'IA.

C'est précisément là que se situe la véritable vulnérabilité. Les enquêtes – y compris le swissVR Monitor – indiquent qu'une part considérable des membres des conseils d'administration ne reçoit pas de reporting régulier sur l'utilisation de l'IA et les risques qui y sont associés. Sans ces informations, une surveillance efficace est tout simplement impossible.

Mon principe, en tant que CEO comme en tant que membre de conseil d'administration, est le suivant : notre mission n'est pas d'assurer nous-mêmes la sécurité, mais de veiller à ce que les bonnes questions soient posées avec constance et à ce que l'entreprise considère la cybersécurité comme un enjeu de résilience dynamique et non comme une simple question informatique ponctuelle. C'est précisément sur ces questions de gouvernance que j'approfondis régulièrement la réflexion dans ma newsletter LinkedIn « WE TALK BOARD ».

Auteurs

swissVR

Isabelle Amschwand
Présidente de swissVR
+41 41 757 67 11
isabelle.amschwand@swissvr.ch

Dr. Brigitte Maranghino-Singer
Directrice générale de swissVR
Chargée de cours, Institut des services financiers de Zoug (IFZ), Haute école spécialisée de Lucerne HSLU
+41 41 228 41 19
brigitte.maranghino@swissvr.ch

Deloitte SA

Reto Savoia
CEO Deloitte Suisse
+41 58 279 60 00
rsavoia@deloitte.ch

Dr. Michael Grampp
Économiste en chef et directeur de la recherche
+41 58 279 68 17
mgrampp@deloitte.ch

Dr. Daniel Laude
Project & Research Manager
+41 58 279 64 35
dlaude@deloitte.ch

Haute École de Lucerne

Prof. Dr. Mirjam Gruber-Durrer
Chargée de cours en Board Management normatif, Institut des services financiers de Zoug (IFZ), Haute école spécialisée de Lucerne (HSLU)
+41 41 228 41 73
mirjam.gruber-durrer@hslu.ch