La cyberrésilience – une importance croissante pour les conseils d'administration

swissVR Monitor II/2023

Septembre 2023

swissVR®

Deloitte.

Global Boardroom Programme | Switzerland

HSLU Hochschule Luzern

Sommaire

À propos de l'enquête
La quatorzième édition du swissVR Monitor s'appuie sur un sondage réalisé auprès de 400 membres de conseils d'administration (CA) suisses. L'objectif de cette étude est de recueillir les opinions d'administrateurs et d'administratrices sur les perspectives conjoncturelles et commerciales ainsi que sur des questions de gouvernance d'entreprise. Chaque numéro traite d'un sujet d'actualité. Le thème de cette étude est la cyberrésilience des entreprises.

Cette enquête a été réalisée par swissVR en collaboration avec la société de conseil Deloitte et la Haute école spécialisée de Lucerne entre le 22 mai 2023 et le 8 juillet 2023. Au total, 400 administrateurs et administratrices de sociétés cotées en bourse mais aussi de petites et moyennes entreprises (PME) de tous les secteurs les plus importants de l'économie suisse y ont participé. Parmi ces participants, 32% sont membres de conseils d'administration de grandes entreprises, 35% de moyennes entreprises et 33% de petites entreprises.

L'objectif de l'étude swissVR Monitor est, d'une part, de proposer aux membres actifs de conseils d'administration un éclairage sur des problématiques qui les concernent en leur permettant de comparer leur propre évaluation de ces questions avec celle de leurs pairs. L'enquête permet par ailleurs au grand public de découvrir le point de vue d'administrateurs et d'administratrices sur des thématiques liées à leur activité et à la situation économique actuelle.

À propos de la méthodologie
Avant de comparer les résultats de cette enquête à ceux des études précédentes, il convient de tenir compte du fait que le nombre de personnes sondées et la composition de l'échantillon étudié diffèrent, chaque fois, d'une enquête sur 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 définie par rapport à ses effectifs : les petites entreprises comptent de 1 à 49 collaborateurs, les moyennes de 50 à 249 collaborateurs et les grandes 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 2023. Pour cette édition, nous avons interrogé 400 membres de conseils d'administration suisses. Les résultats reflètent fidèlement leur point de vue sur les perspectives conjoncturelles, sectorielles et commerciales ainsi que leur opinion sur des thématiques importantes liées à leur activité de membres de conseil d'administration.

La présente enquête est consacrée à la cyberrésilience, une thématique déjà abordée dans le numéro II/2017 qui prend de plus en plus d'importance ces dernières années. Au vu de la hausse du nombre de cyberattaques subies par les entreprises au cours de ces dernières années, il est en outre important pour les membres de conseils d'administration de se pencher sur la question de la cyberrésilience dans le cadre de leurs mandats et de bien comprendre le rôle qui leur incombe et les missions y afférentes. Ainsi, le présent numéro du swissVR Monitor aborde notamment les conséquences possibles des cyberattaques sur les entreprises, l'auto-évaluation de la cyberrésilience par le conseil d'administration et le cyberreporting de la direction à ce dernier.

Outre les résultats de l'enquête, le swissVR Monitor II/2023 contient également des interviews réalisées sur le thème clé de l'étude avec :

- Maya Bundt, présidente du comité de nomination et de rémunération de la Banque Valiant et membre des conseils d'administration de la Bâloise et de l'APG|SGA ;
- Florian Schütz, délégué fédéral à la cybersécurité et directeur du Centre national pour la cybersécurité (NCSC) ; futur directeur de l'Office fédéral de la cybersécurité à compter du 1er janvier 2024 ;
- Sonja Stirnimann, présidente du comité d'audit de la Banque cantonale de Glaris et membre du conseil d'administration d'Apiax.

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

Cornelia Ritz Bossicard
Présidente de swissVR

Reto Savoia
CEO de Deloitte Suisse

Dr. Mirjam Durrer
Professeure à l'IFZ/Haute École de Lucerne

Points-clés de l'étude

24%
des membres de CA interrogés s'attendent à une évolution favorable de la conjoncture économique en Suisse au cours des 12 prochains mois.

42%
des cybervictimes citent l'interruption d'activité comme l'une des conséquences les plus fréquentes des cyberattaques pour leur entreprise.

55%
constatent une importance croissante des questions de cyberrésilience ces trois dernières années.

Des perspectives économiques légèrement plus positives qu'en début d'année
Les membres de conseils d'administration interrogés se montrent, dans l'ensemble, légèrement plus optimistes concernant les perspectives conjoncturelles, sectorielles et commerciales pour les douze prochains mois par rapport au dernier numéro du swissVR Monitor paru en début d'année. Pour chacune des catégories de perspectives (conjoncturelles, sectorielles et commerciales), davantage de sondés s'attendent à une évolution positive plutôt que négative.

Les cyberattaques peuvent avoir de graves répercussions sur les entreprises
Les personnes interrogées, dont l'entreprise a été victime d'une cyberattaque (au moins), font état de répercussions parfois lourdes sur les processus opérationnels. La plupart du temps, les cyberattaques causent une interruption de l'activité de l'entreprise. Parmi les autres conséquences possibles, figurent la fuite de données et le dysfonctionnement de produits ou de services. En comparaison, les attaques consécutives sur les clients ou les fuites d'actifs financiers sont plus rares.

La thématique de la cyberrésilience a pris beaucoup d'importance
La quasi-totalité des membres de conseils d'administration interrogés estime que les questions de cyberrésilience ont pris davantage d'importance ces trois dernières années. Une majorité d'entre eux parle même d'une forte augmentation, et cela est d'autant plus vrai pour les administrateurs de grandes entreprises que pour ceux des petites. L'importance de la cyberrésilience n'a pas changé pour une petite minorité des personnes interrogées. Aucun membre de conseil d'administration a constaté de diminution.

46%
des entreprises ont une assurance contre les cyberrisques.

56%
des CA reçoivent des rapports sur les cyberincidents survenus dans l'entreprise de la part de la direction.

43%
créent des comités au sein du conseil d'administration.

Assurances contre les cyberrisques : un tableau contrasté
Malgré l'importance accrue de la cyberrésilience et les conséquences parfois graves des cyberattaques, à peine la moitié des entreprises a souscrit une assurance contre les cyberrisques. Les entreprises du secteur financier, de l'industrie manufacturière et du secteur de la chimie ainsi que les entreprises du bâtiment s'assurent plus souvent que la moyenne. Sur ce plan, la taille de l'entreprise n'a que peu d'importance.

Le cyberreporting régulier au conseil d'administration peut être amélioré
Selon les personnes interrogées, un peu plus de la moitié des conseils d'administration reçoivent des rapports de la part de la direction sur les cyberincidents dans l'entreprise ou sur les besoins d'action/d'investissement en matière de cyberrésilience. Dans un peu moins de la moitié des cas, un rapport est établi sur le niveau général de menace ou sur les mesures de cyberrésilience. Seul un tiers environ des conseils d'administration est régulièrement informé par la direction sur les cyberrisques majeurs ou sur la cyberstratégie/le cyberprogramme de protection.

Des comités présents surtout dans les grandes entreprises et dans le secteur de la finance
Près de la moitié des conseils d'administration créent des comités dédiés à différentes thématiques. Alors que dans les grandes entreprises, trois quarts des CA disent avoir établi ce type de comité ; dans les petites entreprises, seul un cinquième des administrateurs en ont créé. Et c'est principalement dans le secteur de la finance que des comités sont établis : les trois quarts des CA d'entreprises de la finance possèdent au moins un comité. Dans la plupart des autres secteurs, moins de la moitié des conseils d'administration dispose d'un comité. Cependant, certains membres se voient confier des domaines de spécialisation ou des questions spécifiques dans de nombreux CA.

Perspectives

Perspectives conjoncturelles, sectorielles et commerciales

S'agissant des **perspectives conjoncturelles, sectorielles et commerciales** pour les 12 prochains mois, les membres de conseils d'administration interrogés constatent que le mouvement ondulatoire de ces dernières années se poursuit (voir figure 1). En effet, alors qu'elles étaient d'abord mitigées en 2019, les perspectives se sont assombries en 2020 en raison de la crise de Covid-19, avant de s'améliorer nettement à nouveau l'année suivante, en 2021. Après un nouvel assombrissement des perspectives dû au déclenchement de la guerre en Ukraine en 2022, les membres de conseils d'administration interrogés se montrent aujourd'hui un peu plus optimistes quant aux perspectives économiques pour les 12 prochains mois. Toutefois, de nombreux facteurs d'incertitude subsistent pour l'économie suisse, notamment des risques géopolitiques persistants, des incertitudes dans le domaine de l'énergie pour l'hiver 2023/2024 et une pression inflationniste constante et supérieure à la moyenne.

Contrairement aux opinions exprimées il y a six mois (cf. swissVR Monitor I/2023), les membres de conseils d'administration se montrent, dans l'ensemble, légèrement plus optimistes par rapport aux **perspectives conjoncturelles** : 24% des personnes interrogées s'attendent à une conjoncture favorable pour les douze prochains mois, contre 10% qui expriment un avis défavorable. La majorité des membres de conseils d'administration (66%) prédisent une évolution neutre de la conjoncture. Les avis exprimés dans ce numéro étayent d'autres prévisions actuelles prévoyant une faible croissance de l'économie suisse.

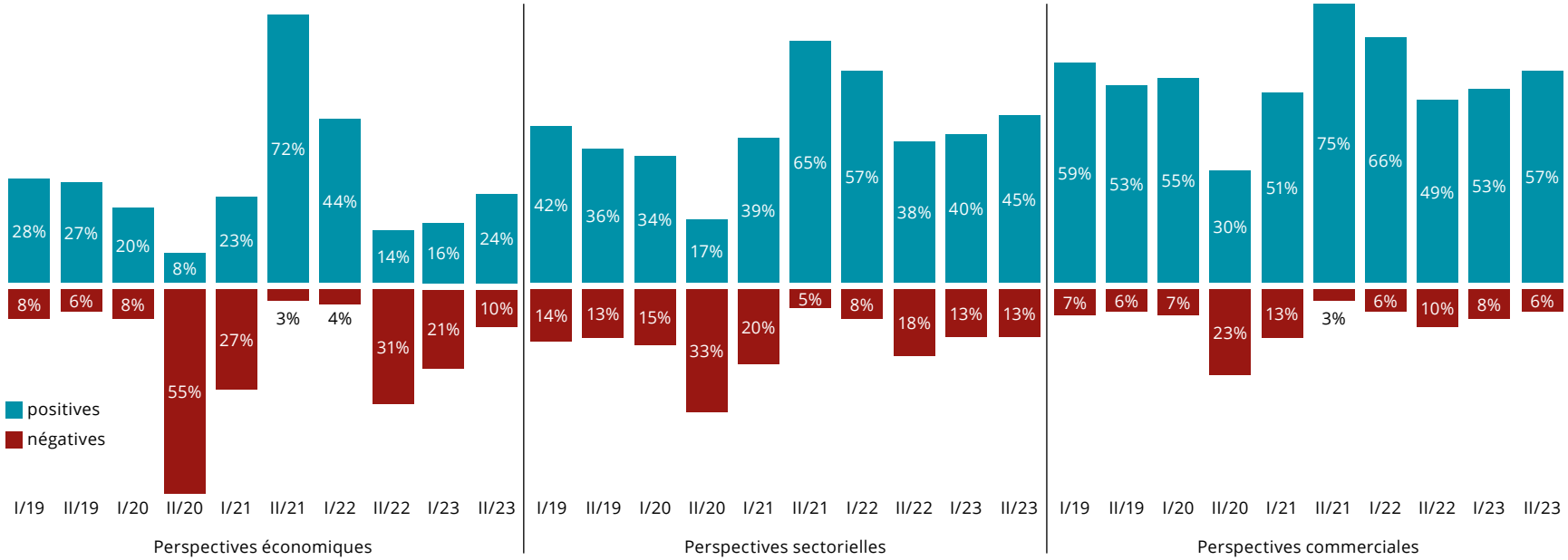
Les sondés affichent également un peu plus d'optimisme qu'il y a six mois s'agissant des **perspectives sectorielles**. 45% des membres de conseils d'administration interrogés ont un avis positif, contre 13% qui expriment un avis négatif. Ce sont surtout les personnes interrogées dans le secteur des technologies de l'information et de la communication qui se montrent optimistes (81% d'avis positifs contre 0% d'avis négatifs). Ce constat pourrait être lié aux efforts de digitalisation continus de l'économie suisse. En revanche, les membres du CA issus de l'industrie manufacturière et du

secteur de la chimie sont les administrateurs les plus pessimistes (24% d'avis négatifs contre 22% d'avis positifs). Ce résultat s'explique en grande partie par les pressions inflationnistes sur les matières premières et les produits intermédiaires, qui devraient se poursuivre, ainsi que par la situation incertaine de la demande à l'échelle internationale.

Les administrateurs se montrent également légèrement plus optimistes qu'il y a six mois concernant les **perspectives commerciales**. Un peu plus de la moitié des membres de CA interrogés (57%) estime que l'évolution de ses propres activités commerciales sera favorable au cours des douze prochains mois, tandis que seuls 6% prévoient une évolution défavorable. Une fois de plus, les membres de conseils d'administration d'entreprises issues du secteur des technologies de l'information et de la communication se montrent particulièrement optimistes (83% d'avis positifs contre 0% d'avis négatifs). Parmi tous les secteurs interrogés, c'est dans l'industrie manufacturière et la chimie que les avis sont les plus mitigés (32% d'avis positifs contre 22% d'avis négatifs).

Fig. 1 Perspectives économiques, sectorielles et commerciales sur les douze prochains mois [swissVR Monitor I/2019 bis II/2023]

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 : la cyberrésilience – une importance croissante pour les conseils d'administration

Les cyberattaques contre les entreprises ou d'autres organisations ont fortement augmenté au cours des dernières années, tant en quantité qu'en qualité. La pandémie de Covid-19 a joué un rôle déterminant dans cette hausse : une proportion inédite de salariés s'est alors retrouvée en télétravail, ce qui a accentué la vulnérabilité des infrastructures informatiques des entreprises. Ces dernières années, les médias ont également rapporté de plus en plus de cas de cyberattaques subies par de grandes entreprises de renom qui ont été affectées sur les plans opérationnel et économique. Dans un contexte de digitalisation continue et de développement de l'intelligence artificielle, une augmentation de la fréquence et de l'ampleur des cyberattaques est à anticiper. Pour toutes ces raisons, il est également important pour les conseils d'administration de s'emparer du sujet de la cyberrésilience de leur entreprise et de bien comprendre leur rôle et leurs missions dans ce domaine.

Incidents et conséquences des cyberattaques

Une minorité de 28% des membres de conseils d'administration interrogés déclarent que leur entreprise **a été victime d'une cyberattaque** dans le passé (voir figure 2). A contrario, 72% répondent par la négative ou n'en ont pas été informés. De fait, le nombre d'entreprises touchées pourrait ainsi être bien plus élevé, les membres des conseils d'administration n'étant pas toujours informés par la direction des cyberincidents via un reporting régulier (ils le sont dans 56% des cas seulement, voir figure 7), comme le révèle la présente enquête.

En la matière, la taille de l'entreprise a un impact déterminant : dans les petites entreprises, seules 18% des personnes interrogées rapportent une cyberattaque (au moins) contre leur propre entreprise, contre près d'un membre de conseil d'administration sur deux (45%) pour les grandes entreprises. Cette différence pourrait s'expliquer, par exemple, soit par une corrélation entre la taille de l'entreprise et le nombre de cyberattaques (plus l'entreprise est grande, plus les attaques sont nombreuses), soit par le fait que les membres du conseil d'administration des grandes entre-

prises sont mieux informés en matière de cyberattaques (voir la section « Le conseil d'administration et la cyberrésilience »).

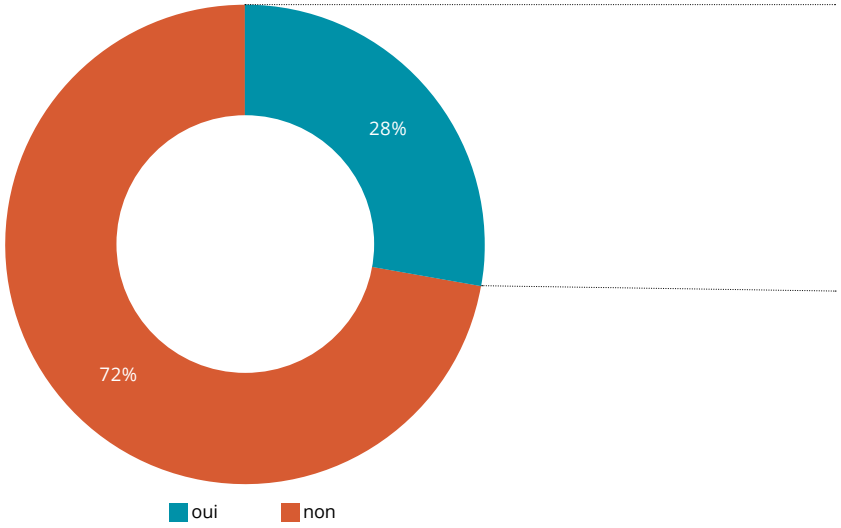
Un examen des conséquences des cyberattaques sur les entreprises (voir également figure 2) révèle que **l'interruption d'activité** (42%) est de loin la réponse la plus souvent citée. C'est surtout dans le secteur des technologies de l'information et de la communication que les membres des conseils d'administration mentionnent le plus souvent l'interruption d'activité comme conséquence des cyberattaques (69%). Les **fuites de données** (26%) et le **dysfonctionnement de produits ou de services** (20%) arrivent généralement en deuxième et troisième positions. Le fait que les sondés mentionnent fréquemment les d'interruptions d'activité et les dysfonctionnements montre que les cyberattaques ont souvent des conséquences concrètes sur les processus opérationnels de l'entreprise. Parmi les autres conséquences citées, figurent les **cyberattaques contre les clients** (11%) et les **sorties d'actifs financiers** (7%).

De l'importance des questions de cyberrésilience

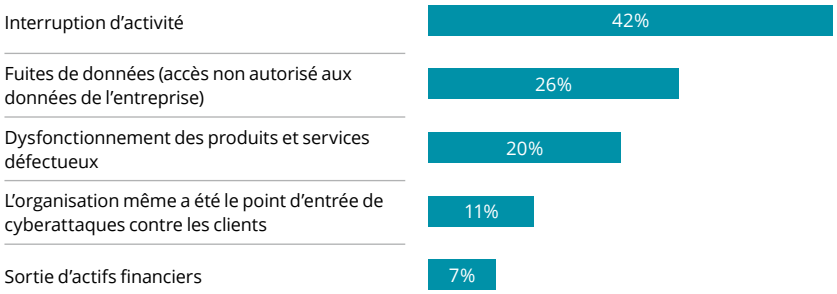
Pour les entreprises, l'importance de la cyberrésilience et des questions y afférentes s'est considérablement accrue ces dernières années selon l'avis des personnes interrogées (voir figure 3). La majorité des membres de conseils d'administration constate une **forte augmentation** (55%). 40% d'entre eux parlent d'une simple **augmentation** et le faible pourcentage restant ne voit **pas de variation** (5%). Aucune personne interrogée indique **une diminution ou une forte diminution**.

Fig. 2 Incident et conséquences d'une cyberattaque (au moins) sur l'entreprise

Question : À votre connaissance, votre entreprise a-t-elle déjà été victime d'une cyberattaque (par exemple accès non autorisé à des données ; ingérence dans la communication avec les clients ; dysfonctionnement du site internet, etc.) ?



Question : Quelles ont été les conséquences de la/des attaque(s) sur votre entreprise ? Veuillez indiquer tous les éléments applicables parmi les suivants : [n=113]



Là encore, la taille de l'entreprise joue un rôle non négligeable : dans les petites entreprises, 43% estiment que l'importance de la cyberrésilience a fortement augmenté (45% pensent que cette importance a augmenté). En revanche, 70% des personnes interrogées dans les grandes entreprises décrivent une forte augmentation de l'importance du sujet (29% parlent d'augmentation). De nouveau, ce résultat s'explique sans doute par une corrélation entre la taille de l'entreprise et le nombre de cyberattaques ou par une institutionnalisation plus forte des questions de cybersécurité dans les grandes entreprises (par exemple avec l'existence d'un département informatique ou de la fonction de CISO – Chief Information Security Officer).

De tous les secteurs, c'est dans l'industrie manufacturière et la chimie que les questions de cyberrésilience ont pris le plus d'ampleur (forte augmentation : 65%). Tous secteurs confondus, l'importance croissante de ce thème pour de nombreuses entreprises s'explique sans doute aussi par l'adoption de nouveaux modèles d'affaires et l'interconnexion croissante des personnes, des machines, des produits, des systèmes et des entreprises (Internet des objets, IdO).

Assurance contre les cyberrisques

Dès lors qu'il s'agit d'assurer une entreprise contre les cyberrisques, les avis sont divisés parmi les personnes interrogées (voir figure 4). Près de la moitié des sondés (46%) indiquent que leur entreprise a souscrit une telle **assurance** ; un pourcentage presqu'aussi important (41%) affirme que ce n'est pas leur cas. Environ un membre de conseil d'administration sur huit (13%) **ne se prononce pas** à ce sujet.

S'agissant des secteurs d'activité, la majorité des entreprises du secteur financier (58%), de l'industrie manufacturière et de la chimie (54%) ainsi que

Fig. 3 L'importance de la cyberrésilience pour les entreprises

Question : Quelle importance les questions de cyberrésilience ont-elles pris pour votre entreprise au cours des trois dernières années ?

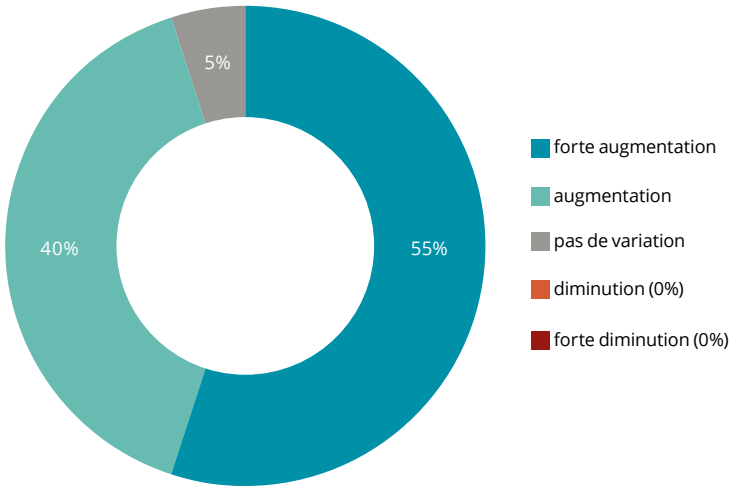
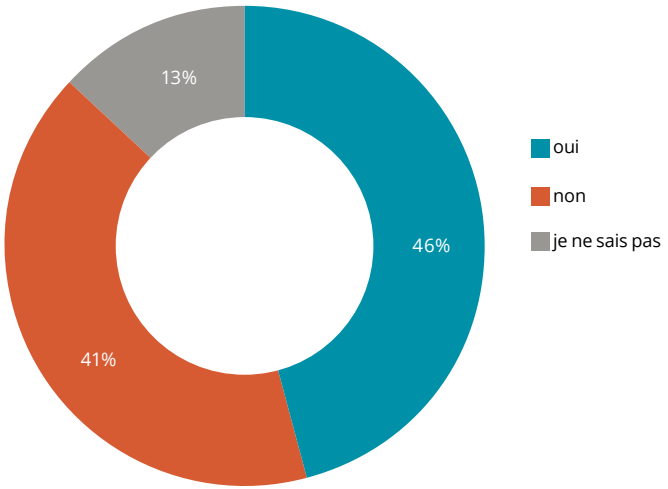


Fig. 4 Assurance contre les cyberrisques

Question : Votre entreprise a-t-elle une assurance spéciale contre les cyberrisques ?



du bâtiment (51%) sont assurées contre les cyberrisques. Dans les autres secteurs, une minorité d'entreprises souscrivent une assurance. La taille des entreprises n'a, en revanche, qu'une influence minime sur cette question.

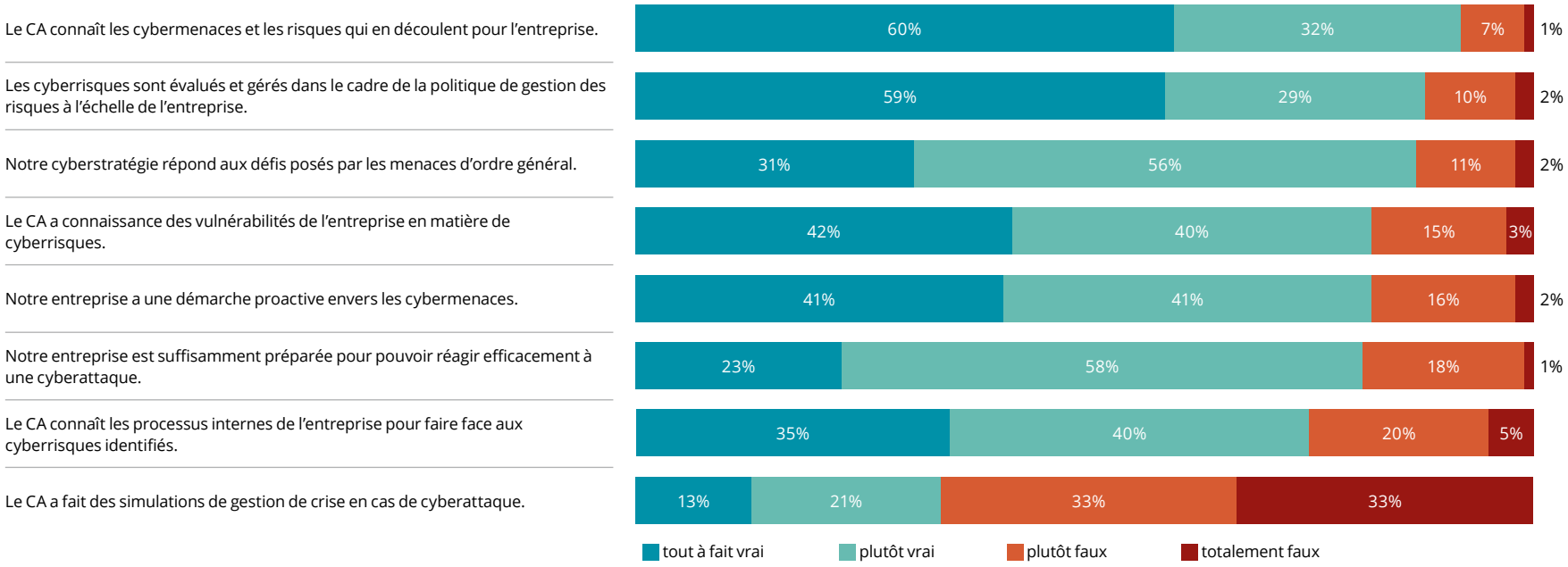
Le conseil d'administration et la cyberrésilience

En matière de cyberrésilience, les membres de conseils d'administration estiment majoritairement que leur entreprise et eux-mêmes sont bien informés et bien préparés (voir figure 5). Ainsi, pour plus de neuf personnes interrogées sur dix (92%), **les membres des conseils d'administration connaissent, pour la plupart, les cybermenaces et les risques y afférents pour l'entreprise.** Une proportion similaire d'administrateurs affirme que **les cyberrisques sont au moins partiellement évalués et gérés dans le cadre de la politique de gestion des risques à l'échelle de l'entreprise** (88%) et que la **cyberstratégie répond généralement aux défis posés par les menaces d'ordre général** (87%).

Par ailleurs, les membres de conseils d'administration estiment majoritairement que leur **conseil** est **au moins partiellement informé des vulnérabilités de l'entreprise en matière de cyberrisques** (82%), que leur entreprise adopte généralement **une approche proactive envers les cybermenaces** (82%) et qu'elle **est suffisamment préparée pour pouvoir réagir efficacement à une cyberattaque** (81%). Trois personnes interrogées sur quatre (75%) sont tout à fait ou plutôt d'accord avec l'affirmation

Fig. 5 Auto-évaluation du conseil d'administration en matière de cyberrésilience

Question : Dans quelle mesure les affirmations suivantes s'appliquent-elles à votre conseil d'administration ?



selon laquelle leur conseil d'administration connaît les processus internes de l'entreprise pour faire face aux cyberrisques identifiés.

Pour toutes les réponses proposées, le taux d'avis positifs a tendance à être supérieur à la moyenne pour les administrateurs de grandes entreprises et à l'inverse, le taux d'avis positifs est légèrement inférieur à la moyenne pour les petites entreprises. Ces résultats montrent que dans les grandes entreprises et leurs conseils d'administration, la question de la cyberrésilience est davantage institutionnalisée et systématisée.

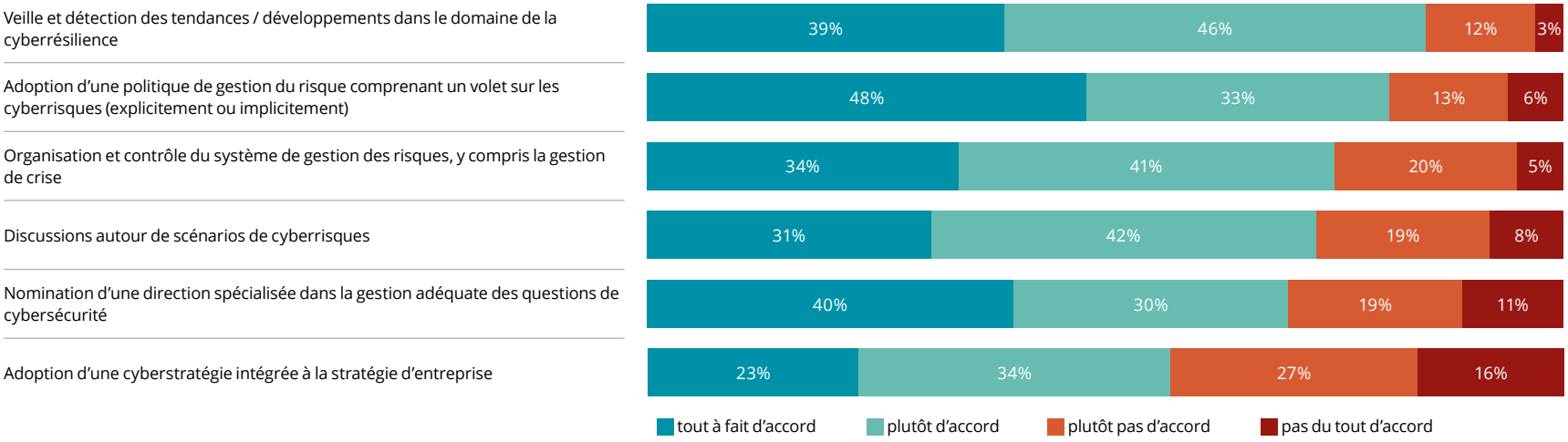
Seul un membre de conseil d'administration sur trois (34%) confirme que son propre conseil a fait, au moins partiellement, des simulations de gestion de crise en cas de cyberattaque. De telles simulations de crise sont plus souvent citées par les administrateurs de grandes entreprises (45%) que par ceux des petites entreprises (26%). Près de la moitié des membres de conseils d'administration (45%) dans l'industrie financière en parlent alors qu'ils ne sont qu'un quart environ (24%) dans le secteur des services aux entreprises et qu'un cinquième environ (19%) dans le commerce et l'industrie des biens de consommation à affirmer avoir fait un tel exercice.

S'agissant des missions et des rôles du conseil d'administration en matière de cyberrésilience, les résultats sont majoritairement positifs (voir figure 6). La très vaste majorité des personnes interrogées affirment que leur conseil d'administration suit généralement **les tendances et les dernières évolutions dans le domaine de la cyberrésilience** (85%) **et qu'il adopte** en principe **une politique de gestion des risques qui incorpore (explicitement ou implicitement) les cyberrisques** (81%).

La **mise en place et le contrôle du système de gestion des risques, notamment la gestion des crises** (75%), les **discussions autour de scénarios de cyberrisques** (73%) ainsi que la **nomination d'une direction compétente en matière de gestion des questions de cybersécurité** (70%) sont d'autres missions assumées au moins partiellement par la plupart des membres de conseils d'administration **interrogés**. Lorsqu'il s'agit

Fig. 6 Tâches/rôles du conseil d'administration en matière de cyberrésilience

Question : Dans quelle mesure votre CA assume-t-il les tâches/rôles suivants en matière de cyberrésilience ?

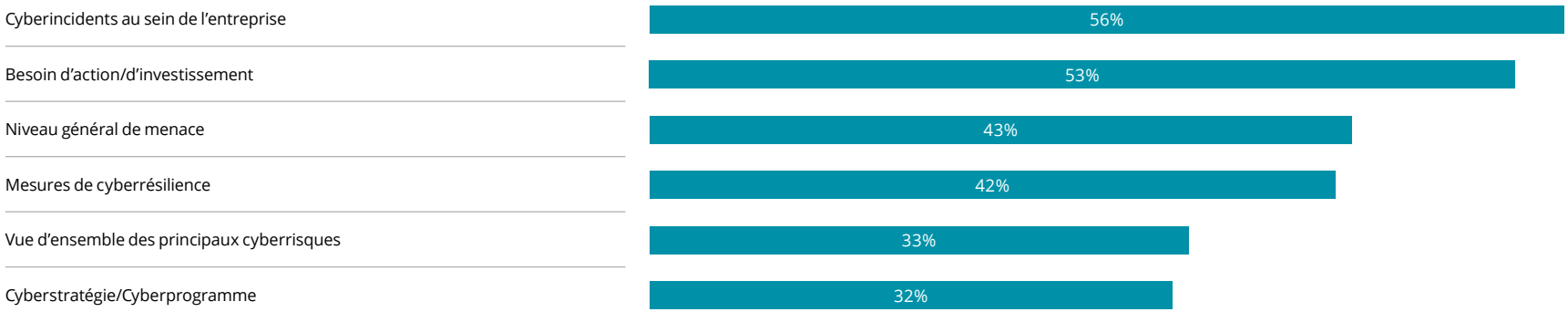


de décider de l'adoption **d'une cyberstratégie intégrée à la stratégie d'entreprise**, seule un peu plus de la moitié des personnes interrogées (57%) confirme le faire. Une fois encore, les taux de réponses positives chez les membres de conseils d'administration de grandes entreprises ont tendance à être plus élevés que chez ceux de petites entreprises.

Le conseil d'administration reçoit régulièrement des rapports sur différentes thématiques liées à la cybersécurité de la part de la direction (voir figure 7). C'est ce qu'indique un peu plus de la majorité des personnes interrogées s'agissant des **cyberincidents au sein de l'entreprise** (56%) et des **besoins d'action/d'investissement** (53%). Seule une minorité des membres de conseils d'administration sondés déclare recevoir des rapports sur le **niveau général de menace** (43%), les **mesures de cyberrésilience** (42%), une **vue d'ensemble des principaux cyberrisques** (33%) ou la **cyberstratégie/le cyberprogramme** (32%). Une fois de plus, les taux de réponses positives ou les fréquences sont plus élevé(e)s chez les administrateurs de grandes entreprises que chez les administrateurs des petites entreprises s'agissant du reporting sur les questions de cybersécurité. En revanche, les différences sont moins marquées entre secteurs.

Fig. 7 Le cyberreporting au conseil d'administration

Question : Parmi les thématiques suivantes, quelles sont celles sur lesquelles votre CA reçoit régulièrement un cyberrapport/rapport de la part de la direction ? Veuillez indiquer tous les éléments applicables parmi les suivants :



Les questions d'ordre organisationnel au sein du conseil d'administration

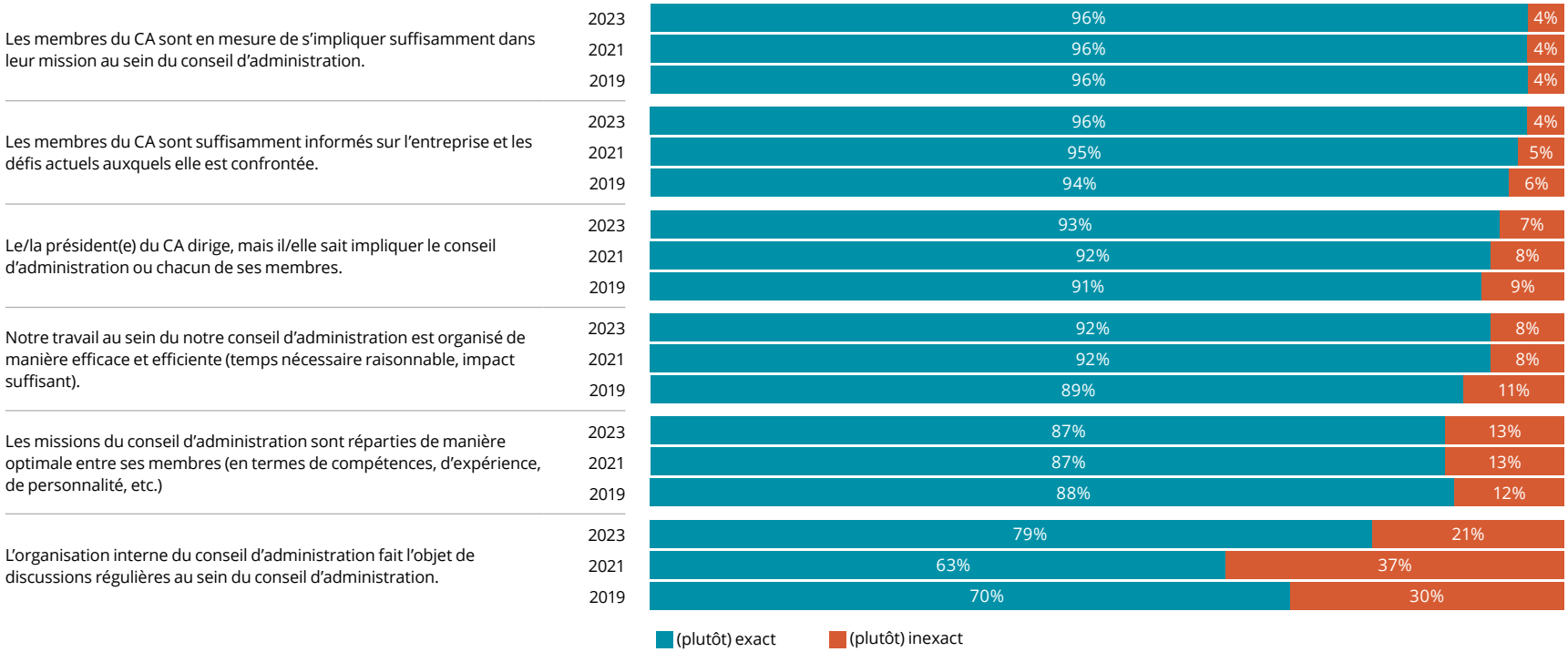
L'organisation interne au sein du conseil d'administration

L'organisation interne du conseil d'administration comprend notamment la répartition des missions et l'influence des différents membres du CA y siégeant. De même que lors des enquêtes réalisées il y a deux et quatre ans (swissVR Monitor II/2019 et II/2021), les personnes interrogées expriment un avis globalement positif sur l'organisation interne au sein de leur conseil d'administration (voir figure 8). Dans l'ensemble, le tableau reste inchangé au fil du temps : les avis des membres de conseils d'administration sont très similaires à ceux des années précédentes.

Pour l'écrasante majorité des sondés (96%), les **membres du CA** sont en mesure de **s'impliquer suffisamment dans leur mission au sein du conseil**. Un pourcentage identique de membres de conseils d'administration (96%) estime qu'eux et leurs collègues sont **suffisamment informés sur l'entreprise et ses défis actuels**. Ils sont un peu moins nombreux

Fig. 8 Organisation interne du conseil d'administration

Question : Parmi les affirmations suivantes, quelles sont celles qui s'appliquent à votre CA ?



(93%) à être d'accord avec la réponse « le/la **président(e) du CA dirige mais sait impliquer aussi les autres membres »**. S'agissant des affirmations selon lesquelles **le travail du CA est organisé de manière efficace et efficiente** (92%) et **les missions sont réparties de manière optimale entre les membres** (87%), les taux de réponses positives sont également très élevés.

Comparativement, peu de personnes interrogées (79%) indiquent que **l'organisation interne fait l'objet de discussions régulières au sein du CA**. On constate toutefois une nette augmentation du nombre de réponses positives pour cette affirmation par rapport aux années 2019 et 2021, ce qui reflète une amélioration de la situation. Pour toutes les réponses proposées, les résultats varient peu en fonction du secteur et de la taille de l'entreprise.

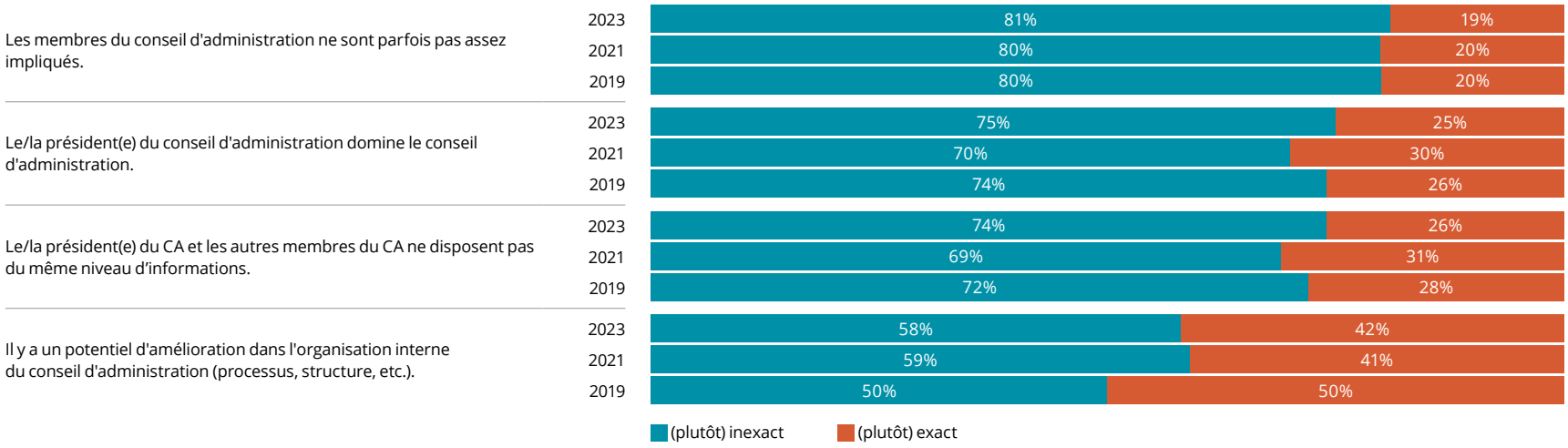
Les défis au sein du conseil d'administration

Le travail de collaboration au sein du conseil d'administration peut présenter un certain nombre de défis pour les membres. Sur la question des défis, les résultats confirment certes les opinions positives au sujet des déclarations précédentes relatives à l'organisation interne, mais révèlent également un certain potentiel d'amélioration (voir figure 9).

De même que dans le cadre des enquêtes réalisées il y a deux et quatre ans (swissVR Monitor II/2019 et II/2021), près d'un cinquième des membres de conseils d'administration (19%) estiment qu'eux-mêmes ou certains de leurs collègues de CA **ne sont parfois pas assez impliqués**. Environ une personne interrogée sur quatre estime que la **domination du président ou de la présidente du CA** (25%) ou que les **différences de niveau d'information entre le/la président(e) du CA et les autres membres** (26%) constituent un défi notable. Avec un résultat de 42%, une proportion relativement élevée de membres de conseils d'administration estime qu'il existe un **potentiel d'amélioration en matière d'organisation interne**

Fig. 9 Les défis du conseil d'administration

Question : Parmi ces affirmations, lesquelles sont exactes ?



(processus, structure, etc.). Ces résultats montrent que, malgré des opinions de base positives, l'organisation au sein du CA et la collaboration entre les membres du CA doivent être améliorées. Là encore, les résultats varient relativement peu selon le secteur et la taille de l'entreprise.

Responsabilités spécifiques et comités

Environ deux tiers des personnes interrogées (63%) indiquent que certains membres se voient confier des **responsabilités spécifiques ou des domaines de spécialisation** au sein de leurs conseils d'administration (voir figure 10). Ce chiffre est pratiquement identique à ceux enregistrés il y a deux et quatre ans (swissVR Monitor II/2019 : 59%, swissVR Monitor II/2021 : 62%).

La part des conseils d'administration au sein desquels les membres se voient confier des responsabilités particulières ou des domaines de spécialisation dépend, entre autres, de la taille de l'entreprise. Dans les grandes entreprises, dans sept cas sur dix (70%), les conseils ont confié des responsabilités spécifiques à leurs membres et ont mis en place des comités alors que, dans les petites entreprises, seule un peu plus de la moitié des conseils d'administration (58%) attribue des missions spécifiques à certains membres du CA. Ces résultats s'expliquent notamment par le nombre plus élevé de membres de conseils d'administration dans

Fig. 10 Responsabilités spécifiques / spécialisations et comités

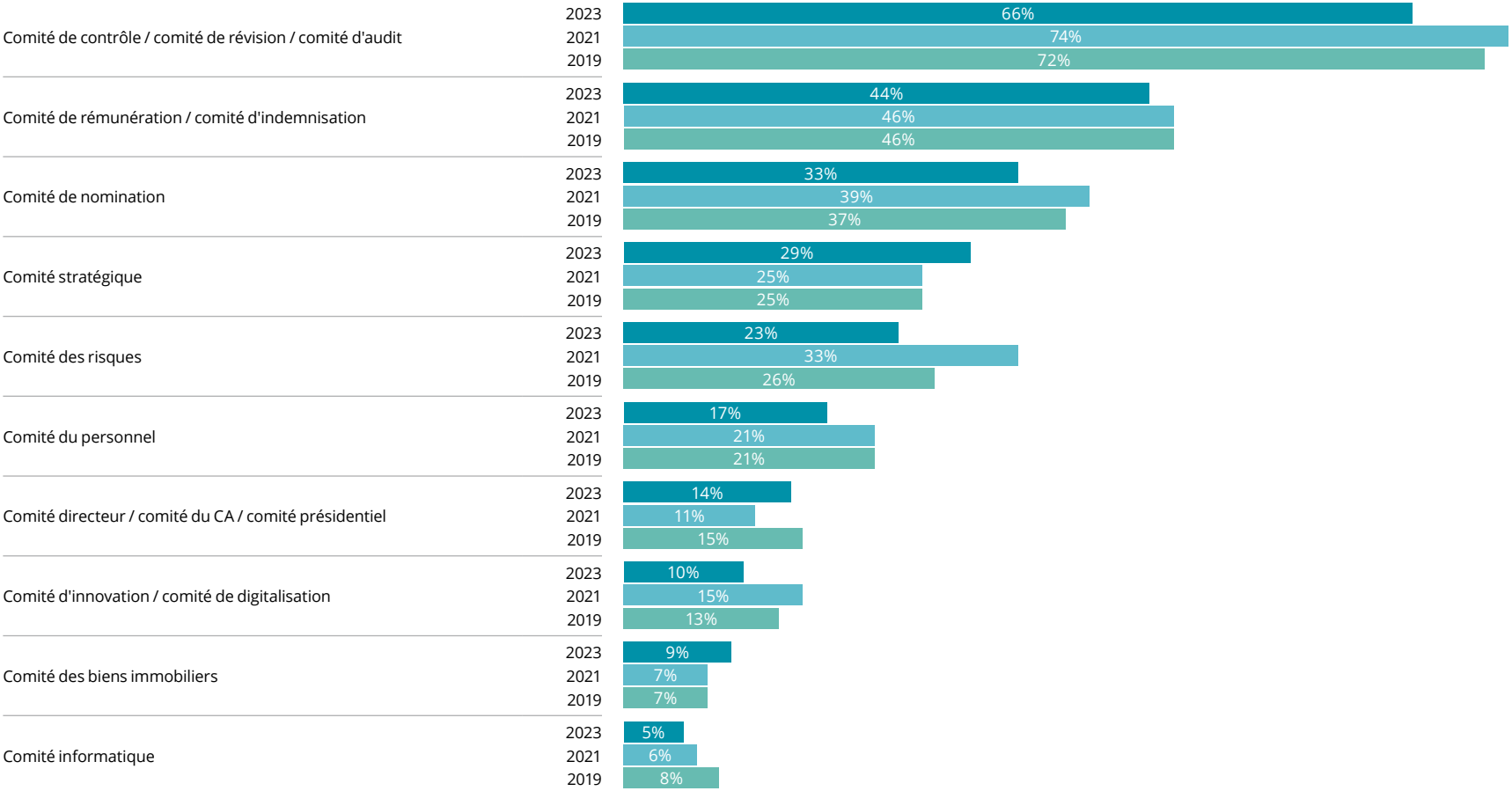
		Nous avons attribué des responsabilités particulières ou des domaines de spécialisation aux membres du conseil	Nous avons mis en place des comités au sein du conseil d'administration
Total II/2023		63%	43%
Total II/2021		62%	43%
Total II/2019		59%	41%
Par taille d'entreprise (II/2023)	Petites entreprises	58%	20%
	Entreprises de taille moyenne	63%	35%
	Grandes entreprises	70%	75%
Par secteur d'activité (II/2023)	Services aux entreprises	56%	18%
	Commerce / industrie des biens de consommation	76%	41%
	Services financiers	65%	75%
	Pharmaceutique / sciences du vivant / medtech / santé	65%	43%
	Production / produits chimiques	51%	38%
	Technologies de l'information et de la communication	65%	15%
	Construction / immobilier	60%	35%

les grandes entreprises par rapport aux petites entreprises (7 membres contre 4). S'agissant du secteur d'activité, l'attribution de responsabilités particulières ou de domaines de spécialisation est particulièrement fréquente dans le commerce et l'industrie des biens de consommation (76%) et inférieure à la moyenne dans l'industrie manufacturière et la chimie (51%).

Environ quatre personnes interrogées sur dix (43%) indiquent que leur conseil d'administration a mis en place **des comités ou des commissions**. De même, ce pourcentage est presqu'identique à ceux enregistrés il y a deux et quatre ans (swissVR Monitor II/2019 : 41%, swissVR Monitor II/2021 : 43%).

Fig. 11 Types de comités

Question : Quels sont les comités existants ? [Plusieurs réponses possibles, n=170]

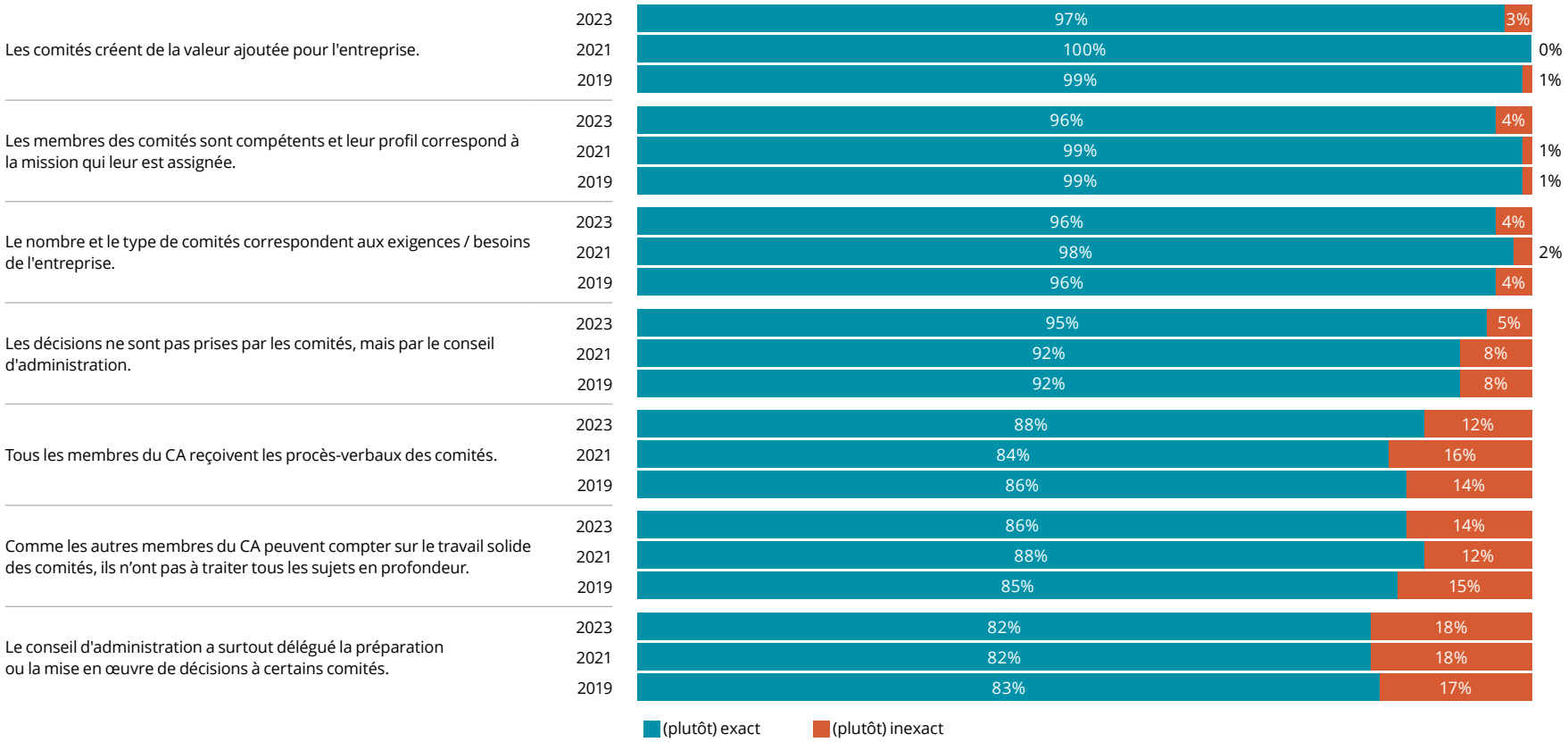


S'agissant des comités, les différences sont encore plus marquées selon la taille de l'entreprise et le secteur d'activité que pour les responsabilités spécifiques et les domaines de spécialisation. Ainsi, dans les grandes entreprises, trois conseils d'administration sur quatre (75%) établissent des comités, alors que le pourcentage n'est que d'un cinquième environ dans les petites entreprises (20%). S'agissant des différents secteurs d'activité, c'est surtout dans l'industrie financière que les conseils d'administration forment des comités (75%), ce qui s'explique notamment par le fait que la FINMA impose aux banques à partir d'une certaine taille de mettre en place un comité d'audit et de risque. En revanche, les conseils d'administration issus des secteurs des services aux entreprises (18%) et des technologies de l'information et de la communication (15%) forment relativement rarement des comités.

Parmi les conseils d'administration qui disposent d'au moins un comité, deux tiers (66%) indiquent avoir un **comité d'audit** (comité de contrôle ou

Fig. 12 Évaluation des comités

Question : Veuillez indiquer quelles affirmations concernant les comités de votre CA sont exactes : [n=170]



comité de révision) (voir figure 11). Il s'agit de loin du comité le plus répandu, ce qui pourrait être lié, d'une part, à la charge de travail correspondante, d'autre part à la recommandation relative à la bonne gouvernance des entreprises cotées en bourse (par exemple Economiesuisse), mais aussi aux prescriptions des régulateurs (par exemple, celles de la FINMA). Il en va de même pour les **comités de rémunération** (44%) prescrits par la loi pour les entreprises cotées en bourse. Par ailleurs, il existe une grande diversité de types de comités créés qui reflète les différents besoins de chaque entreprise et de son conseil d'administration.

Dans l'ensemble, les proportions des divers types de comités dans les conseils d'administration sont relativement similaires à celles enregistrées il y a deux et quatre ans. Il convient de souligner la nette diminution du nombre de **comités des risques** (23%) par rapport à l'enquête de 2021 (33%). Si cette évolution peut surprendre car elle entre en contradiction avec l'importance croissante de la gestion des risques, que ce soit par exemple dans le domaine de la cybersécurité (voir figure 3) ou en lien avec les évolutions géopolitiques (voir swissVR Monitor II/2022), elle signifie également que la gestion des risques est moins souvent déléguée à un comité et qu'elle est de plus en plus souvent prise en charge par l'ensemble des membres des conseils d'administration.

De plus, les avis des membres de conseils d'administration interrogés sur le travail des comités sont globalement très positifs (voir figure 12). Presque tous les sondés (97%) estiment que les comités de leur conseil d'administration créent de la valeur ajoutée pour leur entreprise. Le taux d'avis positifs est tout aussi élevé en ce qui concerne la **compétence des membres et l'adéquation de leur profil à leur mandat** ainsi que **l'adéquation du nombre et du type de comités avec les besoins de l'entreprise** (96% dans les deux cas).

Presque tous les membres de conseils d'administration interrogés (95%) indiquent que les **décisions ne sont pas prises par les comités, mais par le conseil d'administration**. Ce résultat correspond aux dispositions légales selon lesquelles le conseil d'administration peut uniquement « répartir entre ses membres, pris individuellement ou groupés en comités, la charge de préparer et d'exécuter ses décisions ou de surveiller certaines affaires. » (CO 716a/2).

Lorsqu'il s'agit de **recevoir les procès-verbaux des comités** (88%), de **pouvoir compter sur le travail solide des comités** (86%) et de **déléguer la préparation ou la mise en œuvre de décisions à certains comités** (82%), les taux d'avis positifs sont un peu plus faibles mais restent néanmoins élevés. Dans l'ensemble, les avis des personnes interrogées sur le travail des comités rejoignent ceux des années 2019 et 2021. Ces résultats montrent que le swissVR Monitor est un baromètre fiable et solide des opinions des membres de conseils d'administration au fil du temps.

Interviews

Le rôle du conseil d'administration en matière de cyberrésilience

Maya Bundt, présidente du comité de nomination et de rémunération de la Banque Valiant et membre des conseils d'administration de la Bâloise et de l'APG|SGA.

« Il est important que le conseil d'administration ne circonscrive pas uniquement les cyberrisques ou les risques numériques au domaine informatique, mais qu'il les considère comme des sujets de premier ordre sur le plan stratégique et pour l'entreprise dans son ensemble. En effet, les grandes décisions stratégiques ont quasiment toujours un impact sur la cyberempreinte de l'entreprise »

Dirigeante et administratrice expérimentée, **Maya Bundt** est passionnée par les questions cybernétiques, l'innovation et l'humain. Pendant près de 20 ans, elle a travaillé pour Swiss Re, société de réassurance mondiale, à différents postes au sein des équipes IT, Stratégie et Réassurance. À partir de 2014, elle devient responsable du développement de la stratégie de cyber-assurance et réussit à créer la fonction et l'équipe chargées des solutions cyber et numériques. Elle a également présidé le Cyber Council de Swiss Re. À l'été 2022, elle quitte l'entreprise pour se concentrer sur ses mandats d'administratrice. Maya soutient plusieurs initiatives nationales et internationales en matière d'économie numérique et de cyberrisques ; elle est aussi l'autrice de plusieurs articles publiés à ce sujet. Elle est très engagée auprès de la communauté en tant que Présidente du Cyber Resilience Chapter de la Swiss Risk Association, membre de la commission cybersécurité de digitalswitzerland qui contribue au Geneva Dialogue, et en tant que partenaire du Governance of Digital Risks à l'International Center for Corporate Governance.

swissVR Monitor : Quelles sont les dernières évolutions ou tendances en matière de cyberattaques dirigées contre des entreprises ?

Maya Bundt : Si l'on consulte les statistiques du NCSC (Centre national pour la cybersécurité), la fraude se situe, de loin, en tête de liste. Elle concerne aussi bien les particuliers que les entreprises et depuis des années, il s'agit là du sujet de préoccupation absolu.

D'autres attaques sont toutefois beaucoup plus médiatisées. Depuis quelques années, ce sont surtout les attaques par ransomware, avec ou sans vol de données, qui occupent le devant de la scène. Les criminels cryptent les données de l'entreprise au moyen de logiciels malveillants, appelés rançongiciels ou ransomwares, et exigent ensuite une rançon. Depuis peu, il n'est pas rare que des données soient aussi dérobées dans la foulée et qu'ensuite, les auteurs de l'attaque menacent de les publier. Ces menaces accroissent la pression sur les entreprises pour qu'elles paient.

Enfin, des attaques par « déni de service distribué » (attaques DDos pour Distributed Denial of Service) ont de nouveau été récemment rendues publiques. Elles consistent, par exemple, à bombarder des pages web publiques de demandes massives de données pour les rendre inaccessibles aux clients. C'est ce que nous avons pu constater en juin, lorsque divers

services de la Confédération et des CFF sont tombés en panne pendant quelques heures.

swissVR Monitor : Quel est le rôle du conseil d'administration en matière de cyberrésilience ?

Maya Bundt : De manière générale, le conseil d'administration définit les grandes lignes de la gestion durable de l'entreprise dans l'intérêt de ses propriétaires. La cyberrésilience en fait également partie. À cet égard, le CA doit évaluer les opportunités et les risques liés à la numérisation pour l'entreprise et les activités commerciales. Il est important de comprendre que la sécurité absolue n'existe pas ! Aussi, cela signifie qu'il faut non seulement prendre des mesures de protection classiques mais aussi en adopter d'autres qui favorisent la détection des intrus. Par ailleurs, il est nécessaire de se préparer aux situations d'urgence afin de pouvoir sortir d'une situation de crise le plus rapidement possible et sans préjudice.

Il incombe au conseil d'administration de veiller à ce que la gestion des risques, l'organisation et le budget soient mis en œuvre de sorte à permettre à l'entreprise de se protéger contre les cyberrisques en fonction de son modèle d'entreprise et de survivre à un cyberincident.

swissVR Monitor : Quelles sont les mesures que vous conseillez aux conseils d'administration en matière de cyberrésilience ?

Maya Bundt : Il est important que le conseil d'administration ne circonscrive pas uniquement les cyberrisques ou les risques numériques au domaine informatique, mais qu'il les considère comme des sujets de premier ordre sur le plan stratégique et pour l'entreprise dans son ensemble. En effet, les grandes décisions stratégiques ont quasiment toujours un impact sur la cyberempreinte de l'entreprise, qu'il s'agisse d'une expansion sur un nouveau marché, d'activités de fusion et d'acquisition, de participation à un écosystème numérique ou, plus généralement, de la poursuite de la transformation digitale.

En outre, le conseil d'administration doit comprendre où se situent les principaux cyberrisques dans l'entreprise, doit connaître leur ampleur et doit savoir comment les éviter, les atténuer ou les transférer. À cet égard, il est également important de déterminer l'appétit au risque, car c'est la seule façon de prendre des décisions fondées sur des faits, qu'il s'agisse, par exemple, de déterminer comment la cybersécurité doit être organisée dans l'entreprise ou la nécessité de souscrire une cyber-assurance.

Je préconise toujours au conseil d'administration de rencontrer la personne responsable de la sécurité de l'information, généralement le CISO (Chief Information Security Officer). Le connaître présente plusieurs avantages. Premièrement, le fait qu'il y ait un CISO signifie qu'il existe quelqu'un qui s'occupe à plein temps de la sécurité de l'entreprise. Deuxièmement, les questions stratégiques et opérationnelles liées à la cybersécurité sont davantage mises en avant si le CISO participe régulièrement aux réunions du conseil d'administration. Troisièmement, le conseil d'administration peut ainsi bâtir une relation avec cette personne clé. Ces liens sont tout aussi importants à mes yeux que ceux avec la direction générale des risques ou des ressources humaines.

Le conseil d'administration devrait également réfléchir à la manière de renforcer la cyberexpertise au sein de l'organe, en suivant par exemple une formation continue sur le sujet ou en comptant sur la présence de membres intéressés par les questions « cyber ». Je pense que, de nos jours, les membres de conseils d'administration devraient avoir des connaissances de base sur le sujet. Par ailleurs, grâce à des connaissances approfondies et, surtout, un intérêt pour la question, il est possible d'éviter de noyer le sujet dans le flot des thématiques traitées par le conseil d'administration et de s'assurer qu'il y aura toujours quelqu'un pour poser les questions pertinentes.

swissVR Monitor : Selon vous, sous quelle forme les informations relatives à la cyberrésilience doivent-elles être présentées au conseil d'administration ?

Maya Bundt : De nombreuses entreprises traitent de la question des cyberrisques surtout au sein d'un comité, généralement le comité des risques ; mais il existe aussi parfois un comité chargé des questions technologiques et de la cybersécurité. C'est un point important, car les comités disposent généralement de davantage de temps pour traiter de ces questions par rapport au CA dans son ensemble et les membres des comités concernés peuvent se pencher encore plus en profondeur sur la question.

En règle générale, les rapports doivent être pertinents, compréhensibles et adaptés au CA. Il est souvent utile que le CISO ne se perde pas dans des détails techniques, mais offre un aperçu général des risques et de la manière de les gérer d'un point de vue opérationnel. Outre les informations et les KPI spécifiques à l'entreprise, il est souvent intéressant et utile pour le conseil d'administration d'inclure un tableau général de la situation et des éléments de comparaison avec d'autres entreprises.

swissVR Monitor : Que pensez-vous des assurances contre les cyber-risques ? Dans quels cas sont-elles utiles ?

Maya Bundt : Il convient en premier lieu de noter que les cyber-assurances font partie intégrante de la gestion des cyberrisques mais ne peuvent jamais s'y substituer. J'ai froid dans le dos lorsque j'entends des déclarations telles que : « Nous n'avons pas besoin de nous préoccuper de notre cybersécurité. Il suffit de souscrire une assurance. » Non, ça ne marche pas du tout comme ça. Aujourd'hui, je suis aussi certaine qu'aucune assurance ne proposerait une police à une entreprise qui n'aurait pas mis en œuvre un minimum de mesures de cybersécurité.

La gestion des risques consiste notamment à prévenir, atténuer, transférer ou accepter les risques. Pour pouvoir souscrire une assurance à bon escient, il faut par conséquent comprendre les risques et les avoir quantifiés dans une certaine mesure avant de décider de céder ou non une partie du risque résiduel à une assurance. Ce qui est transféré après les mesures d'atténuation du risque, c'est la part excédant encore l'appétence au risque définie. Mais il existe aussi certaines entreprises qui, après avoir mené de telles réflexions, décident ensuite de ne pas souscrire de cyber-assurance.

Les cyber-assurances incluent souvent des services qui apportent une aide concrète aux assurés en cas d'urgence. Par exemple, si une entreprise est victime d'une attaque par ransomware, elle peut appeler un numéro d'urgence et obtenir rapidement le soutien nécessaire pour faire face à cette situation de crise. Pour certaines entreprises, ce service peut tout à fait constituer un argument en faveur d'une cyber-assurance.

Les cybermenaces en 2023 et les mesures que les entreprises doivent prendre

Florian Schütz, délégué fédéral à la cybersécurité et directeur du Centre national pour la cybersécurité (NCSC) ; futur directeur de l'Office fédéral de la cybersécurité à compter du 1er janvier 2024.

« En principe, toutes les entreprises sont menacées, quels que soient leur taille et leur secteur d'activité. Toutefois, de nombreuses PME sont confrontées au problème suivant : en raison de leurs moyens financiers et humains restreints, le savoir-faire et l'infrastructure nécessaires en matière de cybersécurité sont très limités, voire inexistants. »

Florian Schütz, délégué fédéral à la cybersécurité, est responsable de la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques et de la coordination de toutes les cyberactivités de l'administration fédérale. Il joue le rôle d'interlocuteur auprès des cantons, des entreprises et des universités sur les questions cybernétiques et préside le centre de compétences de la Confédération, le Centre national pour la cybersécurité (NCSC). Florian Schütz est titulaire d'un master en informatique et d'un master of advanced studies en politique de sécurité et gestion de crise de l'EPF de Zurich. Il a plus de dix ans d'expérience en tant que dirigeant dans le domaine de la sécurité informatique dans le secteur privé.

Source de l'image : Keystone-SDA / Gaëtan Bally

swissVR Monitor : Comment l'importance de la cyberrésilience a-t-elle évolué pour les entreprises au cours des dernières années ? Et comment évaluez-vous le niveau général de menace en 2023 ?

Florian Schütz : La sensibilisation aux questions de cybersécurité s'est accrue ces dernières années et de nombreuses entreprises sont conscientes des cyberrisques. Il existe toutefois de grandes disparités entre les entreprises : certaines prennent la cybersécurité très au sérieux et mettent en œuvre les mesures de protection nécessaires alors que d'autres ne s'en préoccupent guère.

Le nombre de cyberincidents signalés au NCSC a atteint aujourd'hui un niveau élevé, avec une moyenne d'environ 700 signalements par semaine. Cette hausse est, selon nous, en partie liée à une plus grande sensibilisation de la population. Mais nous constatons également une légère augmentation du nombre de cyberattaques. Actuellement, les signalements d'escroqueries sont particulièrement fréquents. Ainsi, les courriels de pseudo-extorsion prétendument envoyés par des autorités et contenant des menaces de poursuite pénale (fake extortion e-mails), représentent environ un tiers des signalements reçus par le NCSC.

Le NCSC a également observé une légère augmentation du nombre d'attaques par ransomware au cours des dernières semaines. Un redoublement est à craindre à l'avenir. Cela s'explique notamment par le fait que la guerre en Ukraine a provoqué un certain ralentissement des attaques par ransomware car certains groupes de hackeurs se sont engagés dans la guerre et n'ont ainsi plus eu de temps à consacrer aux tentatives de chantage à l'étranger. Mais les attaques par ransomware devraient désormais regagner en intensité, car ces groupes auront très probablement besoin de générer de nouvelles ressources financières.

swissVR Monitor : La cyberrésilience des petites et moyennes entreprises (PME) est moins médiatisée. Les PME sont-elles moins souvent visées par des cyberattaques ?

Florian Schütz : En principe, toutes les entreprises sont menacées, quels que soient leur taille et leur secteur d'activité.

Toutefois, de nombreuses PME sont confrontées au problème suivant : en raison de leurs moyens financiers et humains restreints, le savoir-faire et l'infrastructure nécessaires en matière de cybersécurité sont très limités, voire inexistants.

Par ailleurs, les pirates informatiques effectuent, eux aussi, des calculs coûts-bénéfices. Ils veulent obtenir le maximum avec le moins d'efforts possible. Ainsi, les PME sont plutôt dans la ligne de mire des pirates, car les attaques contre les infrastructures informatiques complexes des grandes entreprises nécessitent souvent des dépenses plus importantes de la part des pirates.

En outre, de nombreuses PME décident de ne pas communiquer publiquement après une cyberattaque. Les craintes de voir leur réputation ternie jouent souvent un rôle important. Les entreprises de plus grande taille ont modifié leur façon de voir les choses à ce propos. Récemment, certaines d'entre elles ont rendu leurs affaires publiques et les médias se sont emparés du sujet.

swissVR Monitor : Quelles mesures recommandez-vous aux entreprises qui souhaitent développer ou renforcer leur cyberrésilience ?

Florian Schütz : La cybersécurité est une affaire de chefs ! Elle doit être abordée au niveau de la direction et chaque entreprise doit adopter une politique de gestion des cyberrisques. Les éventuels risques résiduels doivent être signalés à la direction. La direction de l'entreprise doit connaître les risques résiduels et les consigner par écrit. Le financement des principales mesures doit être défini et leur mise en œuvre assurée. Les investissements nécessaires à cet effet semblent conséquents. Mais toutes les mesures ne doivent pas être mises en œuvre en même temps. Il est important d'établir des priorités. La priorité numéro un est le maintien des systèmes à jour. La plupart des attaques par ransomware réussies exploitent des failles connues pour lesquelles des mesures correctives existent déjà.

Hormis les mesures techniques de protection élémentaire, la création de sauvegardes et l'installation de mises à jour, ainsi que la sensibilisation des collaborateurs jouent également un rôle important. En effet, souvent, les cyberattaques ne visent pas l'infrastructure dans un premier temps mais s'adressent à une personne travaillant pour l'entreprise. Au moyen de procédés d'« ingénierie sociale », les collaborateurs sont incités, par exemple, à ouvrir une pièce jointe à un courriel malveillant ou à divulguer un mot de passe.

swissVR Monitor : Dans quelle mesure la Confédération et plus précisément le Centre national pour la cybersécurité (NCSC) soutiennent-ils les entreprises en matière de cyberrésilience ?

Florian Schütz : Sur son site web, le NCSC met à disposition de nombreuses directives et listes de contrôle expliquant comment se protéger contre les cyberattaques et réagir en cas d'attaque effective. Par ailleurs, le NCSC publie régulièrement des informations notamment sur les nouvelles formes d'attaques et les failles de sécurité par le biais de ses canaux comme son site web et LinkedIn.

La campagne nationale de sensibilisation S-U-P-E-R, que la Confédération mène avec divers partenaires, reprend les cinq thèmes « Sauvegarder », « Utiliser ses mises à jour », « Protéger », « Équiper ses accès d'un mot de passe fort » et « Réduire ». Elle fournit de nombreux conseils sur la manière de se protéger contre les cybermenaces.

swissVR Monitor : La nouvelle loi sur la protection des données entrera en vigueur le 1er septembre 2023 sans période transitoire. Qu'est-ce qui va changer pour les entreprises en matière de cyberrésilience ?

Florian Schütz : La nouvelle loi sur la protection des données assurera l'adéquation entre la législation suisse et le droit européen. C'est important pour que l'UE continue à considérer la Suisse comme un État tiers disposant d'un niveau conforme de protection des données et pour que les flux transfrontaliers de données restent possibles à l'avenir sans exigences supplémentaires. Cette évolution est cruciale pour la Suisse si elle veut conserver sa position sur le marché et sa compétitivité.

Le facteur humain en matière de cyberrésilience

Sonja Stirnimann, présidente du comité d'audit de la Banque cantonale de Glaris et membre du conseil d'administration d'Apiax.

« L'univers « cyber » a au moins 40 ans. Par rapport à d'autres risques opérationnels, c'est encore un « terrain inconnu » pour de nombreux décideurs. Ce que je constate, c'est que ce sujet tabou actuel perd son caractère effrayant lorsqu'il peut être discuté dans un cadre sécurisé avec des personnes ayant la même vision à l'échelle du conseil d'administration et de la direction. »

swissVR Monitor : Beaucoup d'entreprises semblent ne pas vraiment comprendre la nécessité d'agir en matière de cyberrésilience jusqu'à ce qu'elles soient victimes d'une cyberattaque. Les entreprises sous-estiment-elles ou occultent-elles souvent les cyberrisques ?

Sonja Stirnimann : Je constate que cette thématique est encore trop souvent réservée aux responsables informatiques et n'est pas vraiment considérée comme un pilier stratégique. Et ce, à tort selon moi car elle revêt une importance considérable dès lors qu'il s'agit de protéger les actifs, la réputation et la capacité d'action des entreprises et de leurs décideurs. La cyberrésilience est l'un des principaux avantages concurrentiels d'une entreprise (et de ses décideurs) ; cette perspective est, elle aussi, encore trop peu prise en compte de nos jours au moment de définir des mesures préventives dans le but de parer aux situations d'urgence.

Je ne me permettrais pas de juger s'il s'agit d'un refoulement conscient ou d'une mauvaise estimation, mais il est humain d'éviter les sujets que l'on ne maîtrise pas encore vraiment. Cette attitude (inconsciente) peut entraîner des conséquences fatales dans le domaine de la cyberrésilience. Si nous examinons maintenant la question sous l'angle de la responsabilité du conseil d'administration, il est indispensable de lui accorder toute l'attention nécessaire.

Économiste et experte-comptable diplômée, **Sonja Stirnimann** est titulaire d'un *eMBA Financial Services & Insurance* de la HSG et du *Board of Director Diploma* de l'IMD et est *Certified Fraud Examiner* (CFE). Experte dans les domaines de la gouvernance, du risque et de l'audit, elle intervient auprès des entreprises sur des questions d'intégrité et de gestion de crise liées à la non-conformité, la criminalité économique et la cybercriminalité. Forte d'une expérience professionnelle de plus de trois décennies, Sonja Stirnimann a travaillé pour des multinationales telles que LafargeHolcim, UBS, Deloitte et EY dans son domaine d'expertise. Elle est également membre indépendante du conseil d'administration et présidente des comités d'audit de plusieurs sociétés privées cotées en bourse. Elle enseigne dans différentes institutions, universités et associations professionnelles dans le monde ainsi que dans des entreprises d'envergure internationale. La deuxième édition de son livre *Der Mensch als Risikofaktor bei Wirtschaftskriminalität. Handlungsfähig bei Non-Compliance und Cyberkriminalität* a été publiée par Springer.

swissVR Monitor : Quel rôle le facteur (de risque) humain joue-t-il dans la cyberrésilience ?

Sonja Stirnimann : Contrairement à la résistance, qui touche beaucoup plus les thèmes liés à la sécurité informatique, l'infrastructure informatique et les dispositifs de défense, y compris le monitoring, la résilience d'une entreprise est essentielle lorsqu'il s'agit de savoir à quelle vitesse et sous quelle forme nous sommes à nouveau en mesure d'agir pour nos parties prenantes.

Il n'est pas rare que la capacité d'action soit gravement menacée. Celle-ci

dépend fortement de la réaction des décideurs dans ces situations souvent exceptionnelles. Tous les décideurs, et donc leur entreprise, ne sont pas tous préparés avec professionnalisme à de telles situations d'urgence. Cette capacité d'action doit être également assurée au niveau du conseil d'administration et de la direction et il en va de notre responsabilité. Par ailleurs, il n'est pas non plus inutile de s'exercer à ce type de situation et d'intégrer dans le processus les connaissances en résultant afin de l'améliorer.

La cyberrésilience, au sens où nous l'entendons dans le langage courant, se réfère à la capacité d'une organisation à détecter des cyberattaques, à y réagir, à s'en remettre et à conserver sa capacité opérationnelle. Si l'on approfondit la question, il apparaît que la différence entre la résistance et la résilience est visible dans le cycle de vie des incidents cybercriminels.

La résistance se concentre sur la prévention ou le blocage des attaques afin d'éviter tout préjudice. Elle comprend la mise en œuvre de mesures de sécurité telles que les pares-feux, les systèmes de détection d'intrusion et les politiques de sécurité. Même si la résistance est primordiale, elle ne peut cependant pas garantir qu'une attaque sera totalement évitée. De nos jours, chacun d'entre nous doit considérer qu'il est continuellement soumis à des attaques. La résistance regroupe les mesures préventives de protection/minimisation des risques.

La résilience désigne la capacité d'une organisation à réagir rapidement après une attaque ou une perturbation, à se rétablir et à poursuivre ses activités. La résilience englobe la détection (detection) des attaques, la réaction rapide (reaction), la restauration des systèmes et le fonctionnement continu de l'entreprise. Elle consiste à limiter les répercussions et, donc le plus souvent les dommages engendrés par les attaques et à se rétablir rapidement, plutôt que de miser uniquement sur la prévention (résistance). Et c'est là que la capacité d'action joue un rôle essentiel.

swissVR Monitor : Les entreprises ne communiquent pas toujours ouvertement sur les cyberincidents. Comment les entreprises peuvent-elles se détacher de cette approche taboue et opter pour davantage de transparence ?

Sonja Stirnimann : L'univers « cyber » a au moins 40 ans. Par rapport à d'autres risques opérationnels, c'est encore un « terrain inconnu » pour de nombreux décideurs. Ce que je constate, c'est que ce sujet tabou actuel perd son caractère effrayant lorsqu'il peut être discuté dans un cadre sécurisé avec des personnes ayant la même vision à l'échelle du conseil d'administration et de la direction. Pour ce faire, comme je l'ai indiqué, un cadre protégé et une volonté d'échanger sur ses expériences et d'apprendre sont nécessaires. Dans la pratique, on constate que les responsables apprécient ces échanges qui leur permettent d'apprendre beaucoup les uns des autres. Ces discussions sont utiles surtout si elles sont intersectorielles.

swissVR Monitor : Qui est concerné par le sujet de la cyberrésilience dans l'entreprise, et à quel niveau devrait-il être traité ?

Sonja Stirnimann : Comme il ne s'agit pas encore (ou uniquement depuis peu) d'un sujet auquel sont confrontées de nombreuses entreprises, il est selon moi important de le prendre en compte au même titre que les risques opérationnels au niveau du conseil d'administration et de la direction, où ils doivent être traités. Et ce, en même temps que la cyberrésistance, qui se situe en amont de la résilience. Selon le degré de maturité de chaque entreprise et de ses organes, un délai d'apprentissage plus ou moins court est nécessaire. Le conseil d'administration et la direction doivent généralement jouer le rôle de modèles et cela vaut également en matière de cyberrésilience.

swissVR Monitor : La première action que vous recommandez aux entreprises est de sensibiliser. Qu'est-ce que cela signifie dans le cadre de la cyberrésilience ?

Sonja Stirnimann : La sensibilisation commence là où l'on parle activement d'un sujet, où l'on informe et où l'on forme à tous les niveaux hiérarchiques. Nous apprenons par le biais de cas pratiques qui sont analysés et discutés et qui peuvent nous aider à identifier nous-mêmes les risques. Cette approche requiert une ouverture d'esprit sur le sujet et la prise de conscience que nous serons tous concernés. Tôt ou tard. Souvent, ces discussions ne débutent qu'après coup, au lieu d'être préventives. Je constate qu'il y a de bons résultats – s'agissant de la protection des actifs – au sein des entreprises qui se soucient déjà en amont de ces questions stratégiques et entrepreneuriales et qui souhaitent développer et préserver leur avantage concurrentiel.

Contacts et auteurs

swissVR

Cornelia Ritz Bossicard
Présidente de swissVR
+41 41 757 67 11
cornelia.ritz@swissvr.ch

Dr. Brigitte Maranghino-Singer
CEO de swissVR
+41 41 228 41 19
brigitte.maranghino@swissvr.ch

Deloitte SA

Reto Savoia
CEO de 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
Économiste, équipe Recherche
+41 58 279 64 35
dlaude@deloitte.ch

Haute école de Lucerne

Dr. Mirjam Durrer
Professeure de Normative Board Management, Institut des services financiers de Zoug (IFZ)
+41 41 228 41 73
mirjam.durrer@hslu.ch

swissVR s'engage en faveur de la professionnalisation, du réseautage et de la défense des intérêts des conseils d'administration. swissVR est une association indépendante regroupant des membres de conseils d'administration en Suisse, créée par des administrateurs/trices pour des administrateurs/trices. Son action contribue à la professionnalisation des conseils d'administration. swissVR promeut le partage d'expériences entre les membres de conseils d'administration d'entreprises de tous les secteurs d'activité. Elle propose à ses plus de 1 200 membres une offre d'informations et de formations continues adaptée à leurs besoins. swissVR s'adresse exclusivement aux personnes exerçant un mandat actif dans un conseil d'administration. Vous trouverez des informations complémentaires sur le site www.swissvr.ch.

Deloitte SA est une filiale de Deloitte NSE LLP, une société affiliée de Deloitte Touche Tohmatsu Limited (« DTTL »), une société à responsabilité limitée de droit britannique (UK private company limited by guarantee). DTTL et son réseau de sociétés affiliées forment chacune une entité juridiquement indépendante et autonome. Les sociétés DTTL et Deloitte NSE LLP, en tant que telles, ne fournissent pas directement de services aux clients. Une description détaillée de la structure juridique est disponible à l'adresse www2.deloitte.com/ch/fr/pages/about-deloitte/articles/about-deloitte.html. Deloitte SA est une société d'audit agréée et supervisée par l'Autorité fédérale de surveillance en matière de révision (ASR) et l'Autorité fédérale de surveillance des marchés financiers (FINMA).

La Haute école de Lucerne est l'université des sciences appliquées des six cantons de Suisse centrale. Avec actuellement près de 8 300 étudiants inscrits en formation initiale et plus de 5 200 en formation continue, 400 projets de recherche en cours et quelque 2 000 collaborateurs, il s'agit du plus grand établissement d'enseignement de Suisse centrale. L'Institut des services financiers de Zoug (IFZ) du département Économie de la Haute école de Lucerne est spécialisé dans les questions de gouvernance, de risques et de conformité. Il propose également des cursus de formation continue pour les membres de conseils d'administration dans ces domaines, notamment le CAS Verwaltungsrat, le certificat d'études avancées pour administrateurs. D'autres informations sont disponibles en ligne sur www.hslu.ch/ifz-verwaltungsrat, www.hslu.ch/cas-vr et www.hslu.ch/ifz.

swissVR®

Deloitte.

Global Boardroom Programme | Switzerland

HSLU Hochschule Luzern