

Communiqué de presse

Zurich/Genève, le 4 septembre 2023

Cyberrésilience : les conseils d'administration connaissent les risques, mais doivent améliorer la prévention et le reporting

L'économie suisse est plus que jamais aux prises avec la problématique des cyberattaques. Une grande entreprise sur deux a déjà été victime d'une cyberattaque. Dans de nombreux cas, ces incidents se soldent par une interruption d'exploitation. La 14^e édition du swissVR Monitor révèle que, malgré la prise de conscience accrue des risques par les entreprises, nombreuses sont celles qui ne disposent pas d'une cyberstratégie aux contours clairs. Les cas d'incident majeur ne font que rarement l'objet d'exercices de simulation, et le reporting de la direction au conseil d'administration doit vraiment être amélioré.

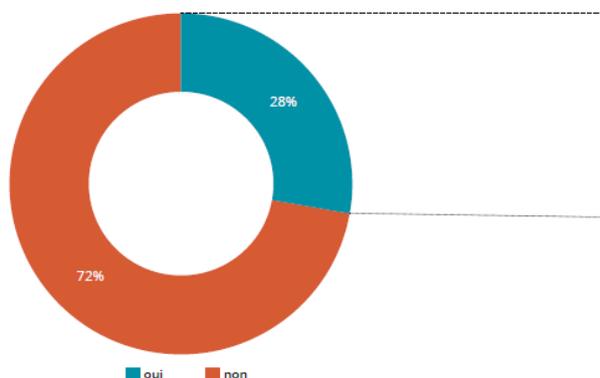
La menace des cyberattaques grandit. À cet égard, les grandes entreprises sont particulièrement visées : 45% des entreprises de plus de 250 employés ont déjà été au moins une fois victimes d'une cyberattaque. C'est ce que révèle le dernier swissVR Monitor, une enquête semestrielle réalisée par l'Association des conseils d'administration swissVR en coopération avec le cabinet d'audit et de conseil Deloitte Suisse et la Haute École de Lucerne. Dans le cadre de cette étude, pas moins de 400 membres de conseils d'administration ont été interrogés sur le thème clé de la « cyberrésilience ».

Contrairement aux grandes entreprises, les PME semblent nettement moins touchées : en effet, seulement 18% des entreprises de moins de 50 employés déclarent avoir été victimes d'une attaque grave. Le lien entre la taille de l'entreprise et la fréquence des attaques est manifeste : les grandes entreprises sont globalement plus exposées et offrent aux cybercriminels des terrains d'attaque plus vastes. Une autre raison invoquée pour expliquer pourquoi les petites entreprises seraient apparemment moins touchées réside dans le fait que les incidents de cette nature ne font pas toujours l'objet d'un reporting auprès du conseil d'administration.

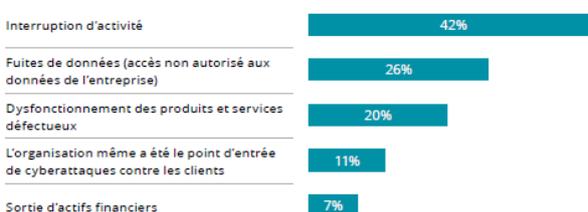
La conséquence la plus fréquente est une interruption d'exploitation

Les cyberattaques ont souvent de graves répercussions sur l'activité opérationnelle. La conséquence de loin la plus fréquente est l'interruption d'exploitation. C'est le cas pour 42% des entreprises victimes d'une cyberattaque (voir graphique 1). Sont particulièrement menacés les processus opérationnels des entreprises du secteur des technologies de l'information et de la communication. Dans cette branche, 69% des entreprises visées par une cyberattaque ont subi une interruption d'exploitation.

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]



Graphique 1 : Incident et conséquences d'une cyberattaque sur l'entreprise

Parmi d'autres conséquences fréquentes, on peut citer les fuites de données ainsi que les dysfonctionnements de produits ou de services. Les cyberattaques ont même parfois un impact qui va au-delà de l'entreprise directement touchée : ainsi, 11% des personnes interrogées déplorent des attaques « par ricochet » sur leurs propres clients. Bien que

les cas de fuite d'actifs restent rares, les conséquences financières ne doivent pas être sous-estimées pour autant. Outre les baisses de chiffre d'affaires dues aux interruptions d'exploitation, ces incidents engendrent également des coûts substantiels, par exemple pour la restauration des données.

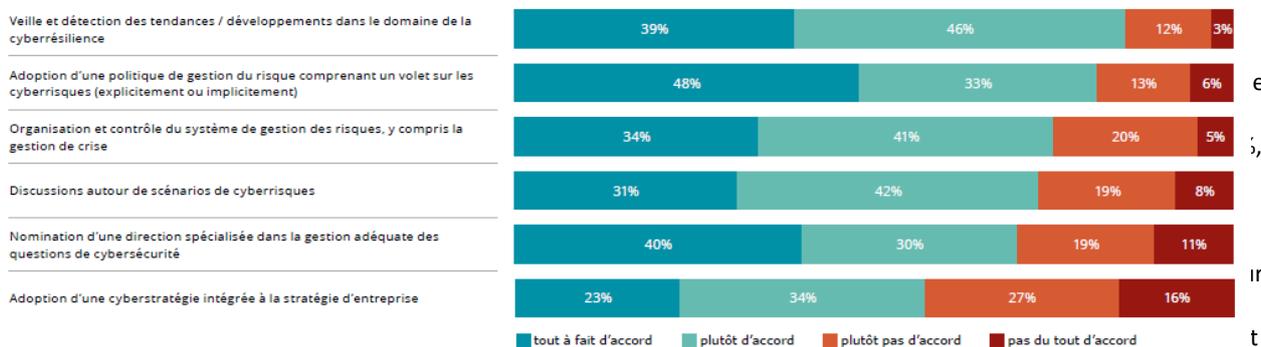
La cyberrésilience est un facteur qui compte de plus en plus

L'ampleur des conséquences illustre l'urgence pour les PME de faire face aux cyberrisques. « Cette problématique fait désormais partie intégrante de toute bonne gouvernance d'entreprise. Heureusement, de nombreuses entreprises l'ont déjà bien compris. Mais il reste encore beaucoup à faire. Notre enquête montre que la cyberrésilience devient un enjeu majeur pour toutes les branches. Il appartient à chaque entreprise d'intégrer cet enjeu dans la gestion des risques et le processus stratégique de chaque entreprise », explique Mirjam Durrer, chargée de cours à l'Institut für Finanzdienstleistungen Zug (IFZ) de la Haute École de Lucerne. 95% des membres de conseils d'administration sondés estiment que la cyberrésilience a gagné en importance pour leur entreprise au cours des trois dernières années. La majorité d'entre eux observent même une forte augmentation des enjeux liés à la cyberrésilience, qu'ils jugent dans une large mesure proportionnels à la taille de l'entreprise. On retrouve donc, là encore, une corrélation entre la taille de l'entreprise et le niveau de la menace.

La cybersécurité n'est pas encore traitée comme un enjeu crucial par tous les acteurs

Point positif : les conseils d'administration indiquent qu'ils assument la plupart de leurs responsabilités en matière de cyberrésilience. 85% des personnes interrogées confirment en effet que leur conseil d'administration suit de près les tendances et les évolutions actuelles dans le domaine de la cyberrésilience (voir graphique 2). De même, huit conseils d'administration sur dix disposent d'une politique de gestion des risques qui prend à bras-le-corps la problématique des cybermenaces. Il y a pourtant urgence à agir, rappelle avec insistance Cédric Nabe, associé Risk Advisory chez Deloitte Suisse. « La prise de conscience des risques augmente, ce qui est un signe positif. Néanmoins, tous les conseils d'administration n'ont pas encore intégré cette problématique. Par ailleurs, près de la moitié des entreprises ne disposent pas d'une cyberstratégie claire. Les entreprises suisses et leurs conseils d'administration doivent donc aller plus loin dans la prise de responsabilités dans le domaine de la cyberrésilience. »

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



Graphique 1 : Tâches du conseil d'administration en matière de cyberrésilience

les conseils d'administration voient les perspectives économiques d'un œil (plus) positif

Outre l'enquête sur cette problématique clé actuelle qu'est la cyberrésilience, le swissVR Monitor recueille deux fois par an les estimations des membres de conseils d'administration sur les perspectives économiques et commerciales. Après des attentes revues à la baisse à la suite de l'éclatement de la guerre en Ukraine en 2022, les membres de conseils d'administration sondés voient aujourd'hui les perspectives économiques pour les 12 prochains mois d'un œil légèrement plus optimiste. Lors de l'enquête, près d'un quart de l'ensemble des administratrices et administrateurs (24%) ont déclaré tabler sur une évolution positive de la conjoncture. Ils sont 10% en revanche à tabler sur une trajectoire négative. Une large majorité (66%) des personnes interrogées a émis un avis « neutre » par rapport aux prévisions conjoncturelles.

Comparativement, les avis concernant les perspectives sectorielles (45%) et les perspectives commerciales (57%) sont beaucoup plus positifs que les jugements portés sur la situation conjoncturelle globale. Cornelia Ritz Bossicard, présidente de swissVR, partage néanmoins le constat suivant : « Un grand nombre de facteurs continuent de peser sur l'économie suisse, parmi lesquels on peut citer des risques géopolitiques persistants, une situation énergétique incertaine pour l'hiver prochain ainsi que des pressions inflationnistes supérieures à la moyenne et qui s'avèrent durables. La place économique suisse a démontré sa résilience dans les périodes difficiles. Cet atout qualitatif se doit d'être préservé face à l'émergence de ces nouveaux défis, tels que les cyberrisques décrits ici. Car une chose est sûre : les nouveaux défis, notamment dans le domaine cyber, sont voués à croître. »

Contact : Cornelia Ritz Bossicard
Titre : présidente de swissVR
Tél. : +41 41 757 67 11
E-mail : cornelia.ritz@swissvr.ch

Contact : Dr. Mirjam Durrer
Titre : Chargée de cours de Normative Board Management à l'Institut des services financiers de Zoug de la Haute École de Lucerne IFZ
Tél. : +41 41 228 41 73
E-mail: Mirjam.durrer@hslu.ch

Contact : [Michael Wiget](#)
Responsable Communication externe
Tél. : +41 58 279 70 50
E-mail: mwiget@deloitte.ch

Contact : [Kevin Capellini](#)
External Communications Specialist
Tél. : +41 58 279 59 74
E-mail: kcapellini@deloitte.ch

À propos du swissVR Monitor

[L'enquête semestrielle swissVR Monitor](#) vise à recueillir les avis de membres de conseils d'administration sur les perspectives commerciales, les stratégies et des thèmes d'ordre structurel, ainsi que – dans cette édition – sur le thème clé « Le facteur de succès humain et la gestion des talents de l'avenir ». La 14e enquête a été réalisée par swissVR en collaboration avec Deloitte et la Haute école de Lucerne entre le 22 mai et le 8 juillet 2023. Les 400 participants représentent des conseils d'administration d'entreprises cotées en bourse et de PME et proviennent de tous les secteurs pertinents.

swissVR

swissVR s'engage pour la professionnalisation, la mise en réseau et la prise en compte des intérêts des conseils d'administration. swissVR est une association indépendante d'administratrices et d'administrateurs suisses, de conseils d'administration pour les conseils d'administration. Au travers de ses prestations, elle contribue à la professionnalisation des conseils d'administration, favorise les échanges d'expérience entre les administratrices et administrateurs d'entreprises de tous les secteurs et propose à ses plus de 1'200 membres une offre d'informations et de formations adaptée à leurs besoins. swissVR s'adresse uniquement aux personnes assumant un mandat actif d'administratrice ou d'administrateur. www.swissvr.ch

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

La Haute École de Lucerne est la haute école des six cantons de la Suisse centrale. L'institution, qui compte quelque 8'300 étudiantes et étudiants en formation initiale, 5'200 en formation continue, presque 400 projets de recherche et environ 2'000 collaboratrices et collaborateurs, est l'établissement d'enseignement le plus important en Suisse centrale. « Governance, Risk and Compliance » est une spécialité de l'Institut des services financiers de Zoug, Haute École de Lucerne – Économie ; dans ce cadre, cet institut propose aussi des formations continues pour les administratrices et administrateurs. www.hslu.ch/ifz

Deloitte Schweiz

Deloitte offre des services intégrés en Audit & Assurance, Consulting, Financial Advisory, Risk Advisory et Tax & Legal. Nous associons notre vision et nos capacités d'innovation dans de multiples disciplines à notre connaissance du monde des affaires et de l'industrie pour accompagner nos clients dans leur trajectoire vers l'excellence, partout dans le monde. Avec environ 2'700 collaborateurs répartis sur les sites de Bâle, Berne, Genève, Lausanne, Lugano et Zurich (siège), Deloitte propose ses services à des entreprises et à des institutions de toutes formes juridiques et de toutes tailles, opérant dans tous les secteurs d'activité.

Deloitte SA est une filiale de Deloitte North and South Europe (NSE), société affiliée de Deloitte Touche Tohmatsu Limited (DTTL) qui emploie plus de 415'000 collaborateurs dans plus de 150 pays.

Lisez d'autres [communiqués de presse](#), contactez les [personnes de l'équipe communication](#) ou visitez le [site web de Deloitte Suisse](#).

Note à la rédaction

Dans le présent communiqué de presse, la désignation Deloitte fait référence aux filiales suisses de Deloitte NSE LLP, une société affiliée de Deloitte Touche Tohmatsu Limited (DTTL), une « UK private company limited by guarantee » (une société à responsabilité limitée de droit britannique). DTTL et son réseau de sociétés affiliées forment chacune une entité juridique indépendante et séparée. DTTL et Deloitte NSE LLP ne fournissent pas elles-mêmes de services aux clients. Pour une description de la structure juridique de DTTL et de ses sociétés affiliées, veuillez consulter le site www.deloitte.com/ch/about.

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

Les informations contenues dans ce communiqué de presse étaient correctes au moment de l'envoi.

