N°2 | Octobre 2025

s:fi KNOWLEDGE

Swiss Finance Institute Roundups

Comprendre les bases de la cybersécurité

Éditorial

Les cybermenaces devraient coûter plus de 10'000 milliards de dollars américains en 2025, ce qui en fait l'un des défis fondamentaux de cette décennie. Dans ce *SFI Roundup*, des experts issus du monde académique et de l'industrie examinent les vulnérabilités les plus critiques ainsi que les réponses prioritaires. Le secteur financier reste particulièrement exposé en raison de systèmes hérités vieux de plusieurs décennies et des effets en cascade sur des réseaux de paiement interconnectés. Plutôt que de cantonner la cybersécurité aux départements informatiques, les conseils d'administration doivent la reconnaître comme un enjeu stratégique nécessitant des investissements soutenus et une transformation culturelle, où chaque employé comprend son rôle défensif. Alors que les gangs de rançongiciels et les acteurs soutenus par des États tendent à se confondre, et que les fournisseurs de services *cloud* centralisés créent des points de défaillance uniques particulièrement dangereux, progresser exige non seulement de meilleures technologies mais aussi de repenser l'équilibre entre efficience et résilience dans notre monde hyperconnecté.

Nous vous souhaitons une lecture instructive et stimulante.

Prof. François Degeorge
Managing Director

Contributeurs

Alain Beuchat
Alain Beuchat était, jusqu'à son départ à la retraite en juin 2025, directeur de la sécurité informatique chez Lombard Odier, où il était responsable de la cyberrésilience, de la stratégie de sécurité informatique et de la conformité réglementaire au sein de l'organisation. Il est par ailleurs membre du comité consultatif sur la cybersécurité de l'Académie suisse des sciences techniques (SATW). Il est titulaire d'un master en génie électrique de l'École polytechnique fédérale de Lausanne (EPFL).

Marc Henauer
Marc Henauer est responsable des affaires politiques et internationales à l'Office fédéral de la cybersécurité (OFCS). Auparavant, il dirigeait le Centre d'opérations et d'informations *MELANI*, où il coordonnait la surveillance des cybermenaces et a contribué à une meilleure sensibilisation à la situation en matière de cybersécurité en Suisse. Au sein de l'OFCS, il se concentre sur l'élaboration de politiques nationales et internationales en matière de cybersécurité. Il est titulaire d'un *Master of Arts in Foreign Service and National Security Studies* de *Georgetown University*.

Anastasia Kartasheva
Anastasia Kartasheva est membre du corps professoral du SFI. Elle est professeure associée à la *School of Finance* de l'Université de Saint-Gall, ainsi que directrice du *Swiss Institute for International Economics and Applied Economic Research*, également à l'Université de Saint-Gall. Avant d'occuper son poste actuel, elle a travaillé en tant qu'économiste à la Banque des Règlements Internationaux (BRI). Elle est titulaire d'un doctorat en économie de l'Université Toulouse Capitole

Olivier Scaillet
Olivier Scaillet est professeur titulaire d'une SFI *Senior Chair* et professeur de finance et de statistique à l'Université de Genève. Ses recherches portent sur la théorie économétrique et ses applications dans les domaines de la finance et de l'assurance. Outre ses activités universitaires, il met son expertise en matière de gestion des risques et de modélisation au service de plusieurs banques suisses. Il est titulaire d'un doctorat en mathématiques appliquées de l'Université Paris-Dauphine.

Beat Schär
Beat Schär est responsable de la sécurité et de l'architecture informatique à la Banque nationale suisse (BNS), où il supervise la conception et la mise en œuvre de cadres informatiques sécurisés, aligne la stratégie de cybersécurité de l'institution sur les normes réglementaires nationales et internationales et contribue aux efforts interdépartementaux visant à protéger les systèmes critiques. Il est titulaire d'un master en sciences appliquées en technologie de l'information et en génie électrique de l'École polytechnique fédérale de Zurich (ETHZ).

Fabian Schär
Fabian Schär est membre du corps professoral du SFI et professeur assistant pour la technologie des registres distribués et la Fintech à l'Université de Bâle. Il est chercheur invité au Fonds monétaire international (FMI), conseiller technique auprès du Comité sur les paiements et les infrastructures de marché, et expert invité auprès de nombreuses banques centrales, de la Banque des Règlements Internationaux (BRI), du Conseil de stabilité financière (CSF) et du G20. Il est titulaire d'un doctorat en économie de l'Université de Bâle.

Octobre 2025 (interviews réalisées en Septembre 2025)

Cette version est une traduction de la version originale en anglais. La version originale est disponible à l'adresse suivante : https://www.sfi.ch/rndp-cs25

L'essentiel

Qu'est-ce que la cybersécurité et comment est-elle structurée ?

Beat Schär: La cybersécurité désigne la protection des systèmes informatiques, des réseaux et des données contre tout accès non autorisé, toute détérioration ou toute perturbation. Si les fondements techniques, comme la protection de la confidentialité, de l'intégrité et de la disponibilité, sont communs à toutes les organisations, les priorités et les risques spécifiques dépendent de la nature de chaque activité. Par exemple, un gestionnaire de fortune doit pouvoir compter sur la sécurité des données de ses clients, une banque centrale sur la sécurité, la disponibilité et l'indépendance de ses systèmes, un fabricant sur l'intégrité de ses processus de production automatisés et une boutique en ligne doit garantir un traitement sécurisé des paiements et rester disponible même en cas de pics de trafic. Dans l'économie actuelle, presque tous les secteurs dépendent de systèmes informatiques interconnectés, de sorte que la cybersécurité est devenue une préoccupation stratégique centrale, même si son importance varie d'une entreprise à l'autre.

Alain Beuchat: Les concepts de confidentialité, d'intégrité et de disponibilité constituent les fondements de la cybersécurité. Ils sont étroitement liés et il est courant d'observer des compromis, des tensions et des défaillances complémentaires ou en cascade entre ces notions. La confidentialité protège l'identité des utilisateurs et garantit qu'ils peuvent accéder aux bonnes données. L'intégrité protège les données et les systèmes contre toute modification non autorisée. La disponibilité garantit que les utilisateurs peuvent accéder aux données et à l'infrastructure lorsqu'ils en ont besoin. Les cyberattaques peuvent cibler ces trois composantes. Par exemple, les attaques par hameçonnage *(phishing)* visent à obtenir des identifiants de connexion afin de permettre aux pirates d'accéder illégalement à des données. Les attaques par rançongiciel *(ransomware)* visent à perturber l'intégrité et la confidentialité des données. Les attaques par déni de service distribué (*Distributed Denial-of-Service* ou *DDoS*) saturent les serveurs, rendant les sites web inaccessibles aux utilisateurs légitimes. Pour assurer ces trois composantes de la cybersécurité, les organisations mettent en œuvre des contrôles de sécurité multicouches, tels que les données chiffrées, la gestion des accès, la protection contre les attaques DDoS et les logiciels malveillants *(malware)*, la surveillance des systèmes et des plans d'intervention en cas d'incident qui traitent spécifiquement les risques liés à la confidentialité, à l'intégrité et à la disponibilité.

Comment la cybersécurité s'inscrit-elle dans la thématique plus vaste de la sécurité ?

Fabian Schär: Dès que deux équipements ou logiciels informatiques interagissent, ils deviennent vulnérables aux attaques et la cybersécurité doit intervenir. Au sens large, la sécurité consiste à se protéger contre des menaces. Ces menaces peuvent prendre différentes formes, qu'elles soient physiques, numériques, émotionnelles ou institutionnelles. La cybersécurité se concentre sur la défense des systèmes informatiques et des données contre les attaques numériques, mais elle a aussi des répercussions sur d'autres domaines de la sécurité, notamment la sécurité nationale, la sécurité économique et la sécurité personnelle.

Marc Henauer: Fondamentalement, la cybersécurité consiste à gérer différents types de risques dans notre économie et notre société. Il est important de souligner que la cybersécurité ne constitue pas une couche supplémentaire de processus que nous pouvons choisir ou non d'adopter. Elle modifie plutôt la manière dont les processus existants sont exécutés. Par exemple, autrefois, les informations sensibles étaient principalement transmises par le biais de courriers scellés ou de télégrammes. Aujourd'hui, elles sont transmises via des systèmes de messagerie instantanée. La cybersécurité n'a pas créé le concept de messagerie, mais a plutôt adapté la manière dont elle est utilisée aujourd'hui afin de garantir sa sécurité.

Olivier Scaillet: Dans le secteur bancaire, le Comité de Bâle sur le contrôle bancaire fournit des orientations utiles en classant les risques en trois grandes catégories, à savoir les risques de crédit, les risques de marché et les risques opérationnels. Les cyberrisques relèvent des risques opérationnels. Cependant, ils se distinguent par leur intention malveillante, leur probabilité d'occurrence plus élevée, leur potentiel de perturbation cachée et prolongée, et leur capacité à se propager en raison de la forte interconnexion numérique. Face à ces caractéristiques, les cadres traditionnels de gestion des risques opérationnels sont insuffisants. Les cyberrisques nécessitent des stratégies dédiées et innovantes en matière de gestion, de régulation et d'assurance.

Anastasia Kartasheva: Du point de vue de l'assurance, le risque lié à la cybersécurité est aussi considéré comme un risque opérationnel en raison de son impact sur la confidentialité, l'intégrité et la disponibilité des données, ainsi que sur les infrastructures informatiques. Ces risques peuvent impliquer un accès non autorisé, entraînant des violations de données, des attaques de malware et des erreurs internes au système qui compromettent la sécurité des données. Contrairement à d'autres risques, tels que les risques sanitaires ou les risques de catastrophe naturelle, peu de méthodes de transfert des risques liés à la cybersécurité ont été développées. En conséquence, les entreprises sont peu armées face aux risques liés à la cybersécurité et se retrouvent largement livrées à elles-mêmes pour affronter les conséquences d'une cyberattaque.

En quoi les cyberattaques opportunistes diffèrent-elles des cyberattaques ciblées ?

Alain Beuchat: La plupart des cyberattaques sont opportunistes plutôt que ciblées. Les pirates recherchent sur Internet les vulnérabilités connues, les exploitent, puis identifient leur victime. Une fois qu'ils ont obtenu l'accès, les pirates, qui travaillent souvent à plusieurs niveaux, décident du montant de la rançon en fonction de la taille et de la sensibilité de la victime. La rançon doit être importante, mais pas au point que la victime soit incapable de la régler. Les attaques ciblées se distinguent en ce qu'elles impliquent une surveillance à long terme, une intention stratégique et sont souvent motivées par des considérations géopolitiques. Ces opérations, qui sont souvent liées à des acteurs étatiques, peuvent prendre des mois, voire des années, à préparer. Elles visent généralement des agences gouvernementales ou des infrastructures critiques. Ces deux types de menaces – cyberattaques opportunistes et ciblées – coexistent. Il est essentiel de comprendre leur logique afin de cartographier les risques et de planifier les réponses. Une stratégie de défense solide s'appuie non seulement sur la connaissance du mode opératoire des attaquants, mais aussi sur une analyse de leurs motivations.

Quels chiffres récents illustrent particulièrement bien l'ampleur des cybermenaces actuelles ?

Olivier Scaillet: Les experts prévoient que le coût mondial de la cybercriminalité dépassera les 10'000 milliards de dollars américains en 2025, ce qui représente une augmentation considérable par rapport aux 3'000 milliards de dollars américains enregistrés en 2015. Bien que ces chiffres stupéfiants soient difficiles à confirmer, ils soulignent l'ampleur considérable du problème et son taux de croissance alarmant. Avec l'augmentation des cyberattaques et de la vulnérabilité en général, certaines projections suggèrent que le coût pourrait atteindre 25'000 milliards de dollars américains d'ici 2027. La cybersécurité et les cyberrisques sont donc devenus des préoccupations majeures pour les gouvernements, les entreprises et les particuliers.

Selon vous, quels incidents récents en matière de cybersécurité illustrent le mieux l'état actuel du domaine ?

Olivier Scaillet: L'une des attaques les plus dommageables est sans doute celle de *NotPetya* en 2017. Du point de vue du risque opérationnel, elle a contraint les entreprises touchées à fermer pendant plusieurs semaines, ce qui a perturbé leur capacité à produire des biens et des services. Cet effet domino a touché leurs clients, qui ont subi des pertes importantes, quatre fois supérieures à celles des entreprises directement touchées. Ces risques opérationnels ont été particulièrement marqués pour les clients qui disposaient de peu de fournisseurs alternatifs ou dépendaient de produits hautement spécialisés. Du point de vue du risque réputationnel, cette faille de sécurité a conduit les clients à mettre fin, au fil du temps, à leurs relations commerciales avec les entreprises directement touchées. Même un an après l'attaque, les clients étaient plus enclins à rompre leurs liens avec ces entreprises, ce qui témoigne d'une érosion à long terme de la confiance et de la réputation. Les clients ont restructuré leurs chaînes d'approvisionnement afin de s'associer à des entreprises plus robustes sur le plan de la cybersécurité, ce qui indique que l'attaque a nui à la réputation des fournisseurs concernés en tant que partenaires commerciaux fiables. L'attaque NotPetya, l'une des plus sophistiquées à ce jour, illustre les conséquences considérables que de telles attaques peuvent avoir à long terme.

Anastasia Kartasheva: La cyberattaque contre l'opérateur d'oléoducs *Colonial Pipeline* en 2021 est un exemple parfait. Cette entreprise, qui fournit près de la moitié du carburant consommé sur la côte Est des États-Unis, a été victime d'une attaque par ransomware. Par mesure de précaution, elle a fermé son réseau. Même si elle a payé une rançon d'environ 4.4 millions de dollars américains en *bitcoins* dès le lendemain de l'attaque, il lui a fallu près d'une semaine pour rétablir l'intégralité de ses services, ce qui a entraîné des pénuries de carburant dans plusieurs États, des achats de panique et une hausse des prix à la pompe pouvant atteindre 10 cents par gallon. L'impact d'une attaque comme celle-ci, qui s'appuie sur la simple faiblesse d'un seul mot de passe sur une infrastructure critique, peut être considérable et affecter la vie de millions de personnes. Il est intéressant de noter le montant relativement "modeste" de la rançon par rapport au coût économique et social total résultant de cette fermeture.

Marc Henauer: L'attaque contre *Viasat*, qui a eu lieu le même jour que l'invasion de l'Ukraine par la Russie en 2022, visait à perturber les communications par satellite utilisées par des milliers d'Ukrainiens, notamment par l'armée et par des agences gouvernementales. Cette attaque ciblant l'Ukraine a eu des répercussions bien au-delà de tout ce qui aurait pu être prévu. L'ampleur des dommages collatéraux a été considérable. Environ 6'000 éoliennes ont cessé de fonctionner en Allemagne, des utilisateurs d'Internet haut débit fixe dans toute l'Europe ont subi des coupures et ont dû remplacer leur matériel, et des utilisateurs de téléphones satellitaires au Maroc et au Royaume-Uni ont été confrontés à des problèmes de connectivité.

Alain Beuchat: L'incident *CrowdStrike* de 2024, causé par une mise à jour logicielle de routine, a entraîné l'annulation de plus de 5'000 vols, le report d'interventions non urgentes dans des hôpitaux et des pannes des services bancaires en ligne dans le monde entier. Bien qu'il n'y ait aucune preuve que l'incident CrowdStrike résulte d'un acte de malveillance, l'ampleur des perturbations qu'il a causées dépasse celle de toutes les cyberattaques jamais survenues et met en évidence la vulnérabilité des systèmes informatiques centralisés. De tels incidents soulignent l'interdépendance de nos systèmes informatiques. Une défaillance, qu'elle soit intentionnelle ou accidentelle, peut avoir des répercussions non seulement sur un seul ordinateur, mais aussi sur le fonctionnement d'appareils connectés à un réseau situé à plusieurs fuseaux horaires de là. Outre les incidents susmentionnés, nous continuons d'observer un volume élevé de cyberattaques visant des organisations et leurs fournisseurs tiers. Nombre de ces violations sont dues à une absence de bonnes pratiques en matière de cybersécurité, telles qu'une gestion incohérente des correctifs ou l'absence d'une authentification multifactorielle.

Concepts fondamentaux

Comment les fonctions de cybersécurité sont-elles structurées et mises en œuvre ?

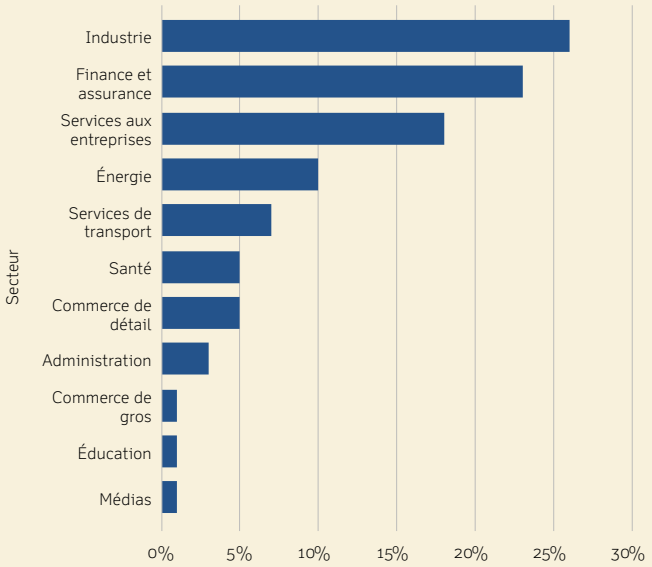
Beat Schär: La gestion des cyberrisques s'appuie souvent sur trois lignes de défense. Celles-ci comprennent la prise en charge des risques, la surveillance des risques et un audit indépendant. La première, la prise en charge des risques, consiste à identifier, évaluer et atténuer les risques liés à la cybersécurité dans le contexte spécifique de l'entreprise. Ces activités sont généralement assumées par des spécialistes internes en cybersécurité. La deuxième, la surveillance des risques, consiste à vérifier que les risques sont correctement identifiés et gérés. Cette responsabilité incombe généralement au service interne à l'entreprise chargé de la gestion des risques. La troisième ligne de défense, l'audit indépendant, fournit une évaluation externe des contrôles, des politiques et des pratiques de gestion des risques liés à la cybersécurité. Cette approche en trois étapes minimise les angles morts, instaure un contrôle mutuel entre les différentes unités organisationnelles et garantit la conformité de la gestion des cyberrisques avec les normes générales en matière de gouvernance et de conformité.

Qui sont les principaux auteurs et victimes de cyberattaques ?

Marc Henauer: Les attaquants sont très rationnels et opportunistes. Ils ciblent des victimes qui ne peuvent pas se permettre de mettre en place une sécurité de pointe, mais qui disposent de ressources financières suffisantes pour s'acquitter d'une rançon. Leurs victimes peuvent être quasiment toutes les personnes connectées à un réseau, des grandes entreprises et agences gouvernementales aux petites entreprises, en passant par les établissements d'enseignement, les instituts de recherche, les organisations à but non lucratif, les ONG et les particuliers. Toute personne disposant d'une infrastructure et de données précieuses, ainsi que de ressources financières, peut potentiellement devenir une cible. Un exemple notable est la violation du réseau d'un casino en 2017, où des pirates ont exploité un thermomètre d'aquarium mal sécurisé et connecté à Internet pour extraire 10 gigaoctets de données sur les gros joueurs du casino. Cet incident illustre la façon dont même l'appareil intelligent le plus banal peut devenir une porte d'entrée vers des informations sensibles s'il n'est pas correctement sécurisé.

Anastasia Kartasheva: Il existe un réseau complexe d'attaquants et de victimes, qui n'opèrent pas tous sur le même champ de bataille. Du côté des attaquants, nous trouvons généralement la Chine, la Corée du Nord et la Russie comme acteurs clés au niveau des États-nations, avec des stratagèmes complexes guidés par des motivations stratégiques, politiques ou financières. Au niveau des individus, les hackers sont souvent des adolescents, notamment américains, qui parlent couramment anglais et sont particulièrement doués en ingénierie sociale. Leurs actions sont généralement agressives et ciblent des secteurs économiques spécifiques pendant plusieurs semaines, avec des objectifs allant de la quête de prestige à l'activisme en passant par des intérêts lucratifs. Nous devons par ailleurs garder à l'esprit que les collaborateurs d'une entreprise peuvent également constituer une menace importante en termes de cybersécurité et causer des dommages considérables, que ce soit intentionnellement ou par négligence. Du côté des victimes, les agences gouvernementales et les opérateurs d'infrastructures critiques sont les cibles privilégiées des hackers travaillant pour des États-nations, tandis que les institutions financières et les particuliers sont généralement victimes de cybercriminels motivés par l'appât du gain. En parallèle, les entreprises, les médias et les institutions gouvernementales sont la cible des "hacktivistes", ces pirates informatiques dont les motivations sont davantage idéologiques.

Répartition des cyberattaques par secteur d'activité



Note: ce graphique illustre la répartition des cyberattaques par secteur d'activité en 2024.
Source: IBM X-Force

Quels sont les vecteurs de cyberattaques les plus répandus actuellement et comment ont-ils évolué ?

Fabian Schär: Avec l'essor de l'intelligence artificielle, l'ingénierie sociale est devenue plus sophistiquée. Les pirates informatiques utilisent davantage de données et des modèles plus avancés pour créer des attaques ciblées et sophistiquées. L'époque des courriels émaillés d'erreurs grammaticales flagrantes et de coquilles est révolue. Les attaques visant la chaîne d'approvisionnement ont également évolué, les pirates informatiques infiltrant de nombreuses organisations en ciblant leurs fournisseurs de logiciels. L'attaque *SolarWinds*, qui serait liée au gouvernement russe, en est un excellent exemple. Dans cette affaire, les hackers ont inséré un code malveillant dans la mise à jour d'un logiciel de confiance, ce qui leur a permis d'accéder à des milliers de cibles de premier plan, y compris des agences gouvernementales américaines et des entreprises du classement *Fortune 500*. Le risque de cyberattaques augmente chaque jour, à mesure que les logiciels et les entreprises deviennent de plus en plus connectés et que nous dépendons de plus en plus de solutions *cloud* et de services tiers.

Qu'est-ce qui motive les différentes catégories d'acteurs malveillants, des États-nations aux hacktivistes, à lancer des cyberattaques ?

Anastasia Kartasheva: Leurs motivations sont très diverses. L'instabilité actuelle qui règne au niveau mondial montre clairement que la propagande, la désinformation en période électorale et les attaques contre des infrastructures clés sont utilisées pour obtenir un avantage politique ou militaire. Le sabotage industriel constitue également une préoccupation majeure, en particulier pour les entreprises à forte présence internationale qui ont moins de contrôle direct sur leurs employés, sont plus exposées aux opérations et aux chaînes d'approvisionnement mondiales et doivent composer avec de multiples systèmes réglementaires complexes. La lutte contre ces différentes menaces représente un défi permanent et génère de nombreuses difficultés, notamment en ce qui concerne la collaboration avec les bons partenaires tiers, l'acquisition d'une expertise technique, la formation du personnel et la lutte contre les menaces internes.

Fabian Schär: Il est également important de tenir compte de l'horizon temporel des cyberattaques. Les attaques à court terme sont principalement motivées par des intérêts lucratifs, tandis que celles à long terme suivent des motivations stratégiques ou politiques. Le piratage et l'explosion de milliers de pagers et de talkies-walkies du Hezbollah l'année dernière, qui ont fait plus de 40 morts et plus de 3'500 blessés, montrent à quel point ces attaques peuvent être sophistiquées et bien planifiées. De nos jours, presque tous les appareils électroniques peuvent être vulnérables à une cyberattaque.

Quels sont les principes fondamentaux qui guident aujourd'hui une gouvernance efficiente en matière de cybersécurité ?

Beat Schär: La cybersécurité est une responsabilité de chaque instant. En adoptant une approche fondée sur les risques, les entreprises peuvent mettre en place une gouvernance efficiente en matière de cybersécurité. Elles doivent commencer par procéder à une évaluation approfondie des risques afin de bien comprendre leurs vulnérabilités, leurs actifs et leur exposition aux cybermenaces. Une fois cette évaluation réalisée, la direction doit hiérarchiser les mesures de sécurité, prendre les mesures nécessaires et assumer l'entière responsabilité de ses décisions. Une communication interne et ouverte est essentielle pour promouvoir une bonne conduite de tout le personnel et s'assurer que les collaborateurs sont conscients des menaces potentielles et des comportements attendus. Les évaluations des risques doivent ensuite être régulièrement mises à jour, en fonction de l'évolution des cybermenaces et de la croissance de l'entreprise.

Marc Henauer: En droit civil suisse, le conseil d'administration et la direction sont responsables de la gestion des risques. Bien qu'il y ait encore des progrès à faire, les entreprises sont de plus en plus conscientes des cyberrisques auxquels elles sont confrontées. Cependant, il est difficile de dire quelles entreprises sont en avance et lesquelles sont à la traîne. Certaines petites et moyennes entreprises, en particulier celles qui sont fortement automatisées ou numérisées, bénéficient d'une vaste expertise dans ce domaine. Et certaines grandes entreprises ont subi des pertes et des perturbations importantes. En 2017, par exemple, la compagnie maritime danoise *Maersk* a dû faire face à d'importants problèmes de capacité à l'échelle mondiale en raison de la cyberattaque NotPetya, tandis que le géant pharmaceutique *Merck* aurait perdu environ 900 millions de dollars américains en raison de pertes de revenus, de perturbations opérationnelles et de frais de recouvrement. En matière de cybersécurité, la taille ne fait pas tout. Que ce soit du côté des attaquants ou des victimes, ce sont souvent l'agilité et l'ingéniosité qui font la différence. La taille seule ne garantit pas le succès.

Quelles peuvent être les conséquences des violations majeures de cybersécurité ?

Olivier Scaillet: Les violations massives de cybersécurité peuvent avoir des conséquences considérables. Une étude menée auprès de grandes entreprises américaines cotées en bourse a révélé qu'à court terme, les cyberattaques entraînent une baisse des rendements, une augmentation du volume des transactions, une réduction de la liquidité et un élargissement des écarts entre les cours acheteurs et vendeurs. Cependant, au fil du temps, ces entreprises ont tendance à augmenter leurs investissements en matière de cybersécurité, tandis que leur valeur marchande et leurs performances globales restent relativement stables. Des recherches sur les institutions financières montrent que les cyberattaques peuvent entraîner des pertes allant jusqu'à 50% du revenu net annuel, en raison des coûts financiers directs, des perturbations opérationnelles et de l'atteinte à leur réputation. En outre, certaines violations peuvent avoir un effet domino sur les marchés financiers, ce qui augmente le risque systémique.

Anastasia Kartasheva: L'atteinte à la réputation est une préoccupation majeure, en particulier lorsque des données sensibles sont compromises. L'étendue des données compromises peut être considérable, allant de documents fiscaux et de déclarations de revenus à des antécédents médicaux, des identifiants biométriques, des données de localisation ou de la propriété intellectuelle. L'impact est variable, mais le coût de l'atteinte à la réputation et des litiges est particulièrement coûteux. Il est essentiel de se rendre compte à quel point les entreprises sont interconnectées. Les incidents cybernétiques restent rarement isolés et peuvent avoir de vastes conséquences difficiles à contrôler. En fin de compte, chaque entreprise doit non seulement gérer sa propre cybersécurité, mais aussi décider si le paiement d'une rançon vaut la peine en cas d'attaque, en tenant compte des conséquences potentielles d'un refus de payer.

Fabian Schär: L'un des effets souvent négligés d'une cyberattaque est d'ordre psychologique, en particulier l'anxiété générée par ce type d'épisode. Tout comme une personne peut se sentir très mal à l'aise longtemps après un cambriolage, même après avoir changé les serrures, un sentiment similaire peut persister après une cyberattaque. Lorsqu'un hacker s'infiltre dans les systèmes informatiques d'une organisation, un sentiment de violation peut subsister même après la mise en place de mesures préventives plus strictes. Cette crainte persistante liée à la possibilité d'une nouvelle attaque peut insidieusement affecter le comportement, la confiance et la prise de décision au sein d'une organisation.

Beat Schär: Les violations majeures de cybersécurité peuvent avoir des conséquences importantes sur le plan opérationnel, financier et réputationnel. Dans le secteur financier, un incident grave peut compromettre la situation d'une institution vis-à-vis de ses autorités de tutelle et éroder la confiance du public. En Suisse, par exemple, l'Autorité fédérale de surveillance des marchés financiers (FINMA) a le pouvoir de révoquer les licences bancaires lorsque les établissements ne respectent pas les exigences en matière de gestion des risques, y compris celles liées à la cybersécurité. Aux États-Unis, les approches réglementaires continuent d'évoluer, avec des discussions sur le bon équilibre à trouver entre les obligations de divulgation et les pratiques efficientes en matière de cybersécurité. Certaines associations professionnelles ont exprimé leur inquiétude quant au fait que certaines règles pourraient involontairement compliquer la réponse aux cyberattaques. Malgré des points de vue divergents, la réglementation vise généralement à renforcer la résilience et la responsabilité à tous les niveaux du système.

Quels sont les risques et les avantages liés au partage entre organisations des informations sur les cybermenaces ?

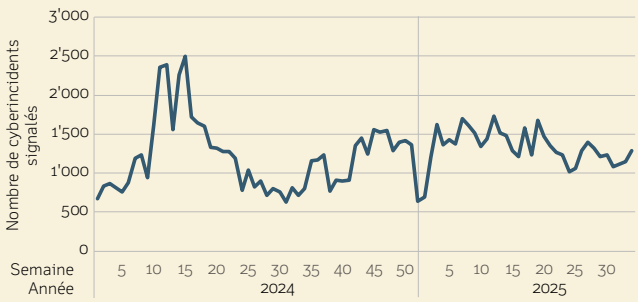
Fabian Schär: Pour faire simple, il s'agit de confiance. Il est logique que les entreprises collaborent en matière de cybersécurité et partagent leurs bonnes pratiques, mais cela implique de révéler beaucoup d'informations sur leur fonctionnement interne dans un environnement concurrentiel où vos alliés sont souvent également vos rivaux. Une initiative menée par les pouvoirs publics, permettant de partager des informations de manière anonyme et consolidée, pourrait être plus efficiente que des échanges directs et individuels.

Alain Beuchat: Il est essentiel de disposer des bonnes informations, car elles permettent de sensibiliser les organisations et les aident à évaluer leur risque d'être une cible potentielle et à se préparer à diverses menaces. Il existe deux principaux canaux pour obtenir ces informations. Elles peuvent être achetées auprès d'un tiers, ce qui permet d'adapter la recherche à son organisation, ou elles peuvent être partagées entre partenaires commerciaux grâce à l'intelligence open source (*open source intelligence* ou *OSINT*). La combinaison de ces deux canaux constitue l'approche la plus efficiente. Un autre aspect important est l'établissement de relations de confiance grâce à ces échanges, qui permettent un partage rapide et efficient des informations pertinentes en cas de cyberattaque.

Anastasia Kartasheva: La création en 2018 par le Conseil de stabilité financière (CSF) d'un lexique définissant les termes liés à la cybersécurité a constitué une avancée majeure dans l'amélioration du partage des informations sur les risques cybernétiques à l'échelle internationale. Grâce à une compréhension commune des différences entre alertes, attaques, événements, incidents, menaces et risques, il est désormais possible de collecter et de comparer des données. Cependant, les informations cybernétiques peuvent également donner un avantage aux attaquants. Les cyberattaquants sont très intelligents et utilisent diverses tactiques pour recueillir des informations sur leurs cibles potentielles. Par exemple, notre administration locale stocke de vastes quantités de données sensibles, notamment concernant le patrimoine des ménages. Une attaque ciblée basée sur des données fiscales volées concernant un ménage spécifique sera forcément plus rentable qu'une attaque aléatoire. La sécurité globale repose sur la solidité du maillon le plus faible.

Marc Henauer: Au niveau national en Suisse, l'ordonnance sur la cybersécurité qui est récemment entrée en vigueur oblige les opérateurs d'infrastructures critiques à signaler les cyberattaques à l'Office fédéral de la cybersécurité (OFCS) dans les 24 heures suivant leur découverte et à soumettre un rapport complet dans les 14 jours. Cette règle représente une avancée significative dans l'amélioration de la visibilité de ces incidents. L'ordonnance s'applique actuellement aux entreprises de transport public, aux fournisseurs d'énergie, aux autorités fédérales, cantonales et locales, aux hôpitaux et aux fournisseurs d'eau potable, ainsi qu'à d'autres secteurs y compris le secteur financier. Toute attaque compromettant la confidentialité, l'intégrité, la disponibilité ou la traçabilité des informations doit être signalée, y compris les malwares installés avec succès sur un système, les chevaux de Troie, les attaques DDoS et l'accès non autorisé à des systèmes informatiques par le biais de failles de sécurité. L'OFCS analyse ces rapports et apporte son soutien si nécessaire. En tirant des enseignements de ces données, nous acquerrons une meilleure compréhension du paysage mondial des cybermenaces. Nous serons en mesure d'identifier rapidement les schémas d'attaques contre les infrastructures critiques et d'alerter les autres victimes potentielles en temps utile, leur permettant ainsi de prendre les mesures préventives et défensives appropriées. Bien qu'il soit encore trop tôt pour évaluer les avantages de ce processus, je suis convaincu que cette évolution réglementaire vers un meilleur partage des renseignements sera très bénéfique.

Cyberincidents signalés à l'Office fédéral de la cybersécurité



Note: ce graphique illustre le nombre hebdomadaire de cyberincidents signalés à l'Office fédéral de la cybersécurité (OFCS) entre janvier 2024 et septembre 2025.

Source: Office fédéral de la cybersécurité (OFCS)

Exposition aux cyberrisques

Comment les secteurs public et privé doivent-ils se répartir le coût et la responsabilité de la cybersécurité ?

Anastasia Kartasheva: À l'instar de la sécurité traditionnelle, la cybersécurité a des effets notables qui ont souvent un impact sur l'économie en général. Cependant, je ne m'aventurerais pas à suggérer que le secteur public finance la cybersécurité, en raison du risque moral qui pourrait en découler. Il y a une grande différence entre, d'une part, permettre aux pouvoirs publics de réglementer la construction dans les zones à risque, par exemple, et, d'autre part, leur confier la supervision de la cybersécurité. Chaque entreprise doit définir sa propre stratégie et décider du montant qu'elle est prête à investir pour réduire ses risques.

Marc Henauer: Le monde numérique est essentiellement une extension du monde physique, avec ses aspects positifs et négatifs. Comme dans la "vraie" vie, l'État a la responsabilité d'essayer de créer un environnement meilleur et plus sûr. Cependant, il n'est pas tenu d'atteindre pleinement cet objectif ambitieux et nous ne pouvons lui reprocher de ne pas y parvenir. Tout comme, dans le monde réel, nous attendons des individus qu'ils ferment leur porte à clé et assurent leur domicile, il appartient aux particuliers et aux entreprises de protéger leur environnement numérique à l'aide de mesures de cybersécurité appropriées.

Fabian Schär: Pour obtenir les meilleurs résultats, chaque partie doit se concentrer sur son domaine d'expertise. Le secteur public doit se concentrer sur la sécurisation des infrastructures clés, quels que soient leurs propriétaires, tandis que le secteur privé doit garantir le bon fonctionnement des entreprises et des différents secteurs économiques. Le rôle du régulateur est de fournir des lignes directrices claires sur les exigences minimales et l'orientation générale de l'économie. Il est également crucial d'encourager la collaboration et le partage d'informations entre les différentes parties, notamment les universitaires, les entreprises et les organismes gouvernementaux, sous la forme la plus appropriée.

Que révèlent les tendances du marché, telles que les fusions, les acquisitions et l'essor des solutions cloud "tout-en-un", sur la manière dont le secteur réagit aux cybermenaces ?

Beat Schär: La tendance à la consolidation, qu'elle passe par des fusions ou par le recours à quelques grands fournisseurs de solutions cloud, reflète une volonté de rationaliser les organisations et les systèmes informatiques. La réduction du nombre de systèmes simplifie la gestion, mais se traduit également par une concentration des risques, ce qui facilite la vie non seulement des utilisateurs, mais aussi des hackers. Les solutions cloud, bien qu'efficientes et évolutives, posent des défis quotidiens en matière de sécurité en raison de leur configuration complexe. Elles sont la cible de menaces en constante évolution. La diversification des systèmes ou l'utilisation de clouds parallèles améliore la résilience, mais ces mesures sont coûteuses et difficiles à gérer. Alors qu'une poignée de fournisseurs dominent de plus en plus le marché, cette centralisation crée une dépendance dangereuse. Si un fournisseur tombe en panne ou est piraté, les conséquences pourraient être dramatiques. En fin de compte, qu'elle passe par l'intégration ou la diversification, chaque approche nécessite un compromis en matière de cybersécurité.

En quoi l'exposition aux risques de cybersécurité diffère-t-elle entre les secteurs financier et non financier ?

Marc Henauer: Les banques ont été les premières à intégrer les technologies de l'information dans leurs activités principales, dès les années 1950. Au départ, les ordinateurs servaient à la gestion des registres et à la comptabilité, mais au fil du temps, des fonctions essentielles telles que le traitement par lots, la messagerie financière sécurisée, les distributeurs automatiques de billets, les services bancaires en ligne et le commerce électronique ont été ajoutées. Cette adoption précoce a créé des infrastructures fragmentées et lourdement chargées en systèmes hérités. Cela dit, le secteur financier a tendance à adopter des cycles de remplacement structurés de manière plus cohérente que de nombreux secteurs non financiers. Les systèmes informatiques des secteurs financier et non financier ont tendance à se développer de manière organique, souvent sans feuille de route à long terme ni cadre réglementaire définissant les infrastructures devant être mises en place au cours de la prochaine décennie.

Comment les organisations se sont-elles mieux préparées aux cyberattaques et quels sont les défis qui restent à relever ?

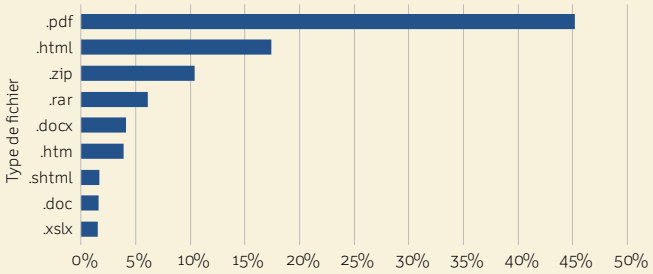
Alain Beuchat: Les entreprises ont accompli des progrès significatifs dans la mise en place de protocoles de cyberhygiène de base et dans le choix d'outils de sécurité adaptés. En théorie, les principes de base sont clairs. Ils consistent à corriger rapidement les vulnérabilités connues, à déployer une protection et une surveillance anti-malware, à mettre en œuvre une authentification multifactorielle et à veiller à ce que les données sauvegardées soient stockées de manière sécurisée. Dans la réalité, cependant, ces mesures apparemment simples sont difficiles à mettre en œuvre à grande échelle. Le défi consiste à les appliquer de manière cohérente sur tous les systèmes. Ce qui complique la cyberdéfense, ce n'est pas tant un manque de connaissances que la complexité même de la mise en œuvre de mécanismes de défense sur de grands réseaux. Les erreurs humaines, la fragmentation des processus et les retards dans l'application des correctifs continuent de créer des vulnérabilités, même lorsque des mesures de défense sont en place. Être véritablement prêt ne consiste pas tant à créer la bonne liste de contrôle qu'à l'appliquer de manière cohérente et rapide.

Olivier Scaillet: À mesure que les mesures de cybersécurité deviennent plus complexes et plus coûteuses, les services informatiques sont soumis à une pression croissante pour créer de la valeur pour l'organisation. Les entreprises doivent décider ce qu'elles doivent protéger, comment elles doivent le protéger et ce qu'elles peuvent se permettre de ne pas protéger. Chacune de ces décisions est intrinsèquement lourde de risques et d'incertitudes. Dans le même temps, les dirigeants et les membres du conseil d'administration doivent rester vigilants, car les incidents cybernétiques ont des conséquences importantes en matière de gouvernance. Des études montrent que les cyberattaques réussies augmentent le risque de remplacement des dirigeants, en particulier des directeurs des investissements et des responsables de la sécurité informatique. Elles peuvent même entraîner des départs de membres du conseil d'administration lorsque des lacunes en matière de surveillance ou de préparation sont mises en évidence. Ces défis montrent bien que ce ne sont pas seulement les organismes de réglementation, mais aussi les actionnaires qui tiennent les dirigeants responsables de défaillances en matière de cybersécurité.

Beat Schär: Les attaques commanditées par des États sont plus sophistiquées. Les pirates informatiques introduisent discrètement des codes malveillants dans les mises à jour logicielles de fournisseurs tiers de confiance, ce qui leur permet de cibler un large éventail de victimes. Ces attaques montrent comment des partenaires de confiance peuvent devenir une menace. Elles soulignent l'importance des principes d'architecture informatique *Zero Trust* et d'une gestion rigoureuse des risques liés aux tiers. Ces attaques étant très complexes, la probabilité de les détecter à temps ou de les éviter est très faible. Cette complexité souligne la nécessité d'une vigilance continue, d'une modélisation proactive des menaces et de simulations basées sur des scénarios afin de tester et d'améliorer la résilience de l'organisation.

Marc Henauer: Les dirigeants d'entreprise doivent comprendre que les compétences en cybersécurité sont hautement spécialisées et qu'il faut du temps et des efforts pour en saisir les implications et reconnaître les scénarios. Chaque employé a un rôle à jouer en matière de cybersécurité. Il est donc essentiel de former son personnel. En matière de communication, il s'agit d'aller au-delà d'une approche purement descendante, en interne comme en externe. Il est nécessaire de disposer de canaux efficients permettant aux utilisateurs finaux de signaler les problèmes informatiques suspects de manière ascendante. La préparation à la cybersécurité doit vraiment être intégrée à l'ensemble de la culture organisationnelle et ne pas se limiter au service informatique.

Canaux de distribution des logiciels malveillants par type de fichier



Note: ce graphique illustre la répartition des méthodes de diffusion des logiciels malveillants par type de fichier en 2024.
Source: IBM X-Force

Quelles sont les tendances récentes en matière d'investissement dans la cybersécurité qui ont le plus influencé les pratiques du secteur ?

Marc Henauer: Nous nous rendons de plus en plus compte de l'importance de mener des tests continus. Ces tests doivent couvrir à la fois les aspects techniques et procéduraux, y compris les simulations d'attaques. En élargissant l'environnement de test afin d'inclure d'autres acteurs que des experts en cybersécurité, nous pouvons garantir que la communication, essentielle pour rassurer les tiers, les investisseurs et les régulateurs, soit également prise en compte et améliorée. L'intelligence artificielle est de plus en plus utilisée pour renforcer les fonctions de sécurité et pour simuler des attaques. Les investissements dans la cybersécurité et le coût des cyberincidents apparaissent plus clairement dans les états financiers, à travers l'augmentation des dépenses opérationnelles et les répercussions des cyberincidents.

Fabian Schär: Outre les tests, les instantanés *(snapshots)* et les sauvegardes multiples constituent une défense solide contre les problèmes de contamination et les attaques par ransomware capables de détruire tout un système. Il semble cependant que de nombreuses petites et moyennes entreprises, pourtant très exposées à ces risques, n'aient pas mis en place un système de sauvegarde complet. Si les sauvegardes et les instantanés ne constituent pas une solution complète en matière de cybersécurité, ils offrent néanmoins un moyen simple et peu coûteux de protéger l'infrastructure informatique contre une grande partie des menaces actuelles. Ils ne protègent toutefois pas contre les attaques telles que l'extorsion de données ou la double extorsion, où les données sont d'abord chiffrées, puis l'attaquant exige une rançon pour qu'elles restent confidentielles.

Comment les institutions financières décident-elles du montant à investir dans la cybersécurité et quels sont les facteurs qui influencent ces décisions ?

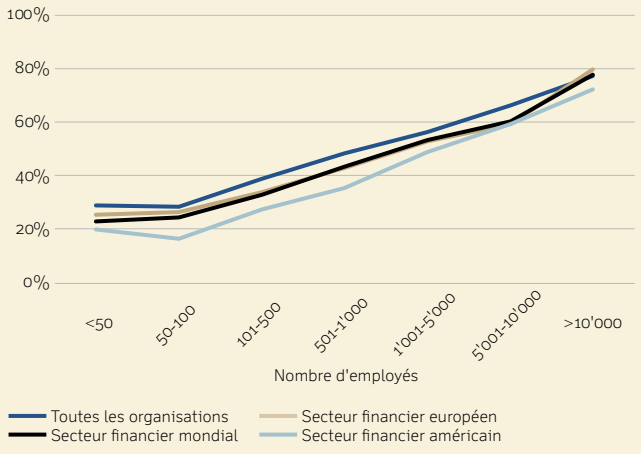
Olivier Scaillet: Les décisions d'investissement dans la cybersécurité sont motivées par le niveau de risque auquel les institutions financières estiment être exposées. Une analyse des entreprises cotées aux États-Unis montre que cette perception est influencée par plusieurs facteurs, notamment les cyberattaques passées, les caractéristiques de l'entreprise et du secteur dans lequel elle évolue, la qualité de la gouvernance et la pression réglementaire ou du marché. Il est intéressant de noter que les entreprises présentant un risque de cybersécurité plus élevé ont tendance à surperformer leurs pairs d'environ 10% par an, mais qu'elles sous-performent fortement lorsque les cyberrisques se concrétisent. Cette différence suggère qu'il existe un facteur de cyberrisque distinct qui est pris en compte par le marché. Compte tenu de leur rôle essentiel et de leur exposition accrue au risque, les institutions financières doivent reconnaître l'existence de cette menace en constante évolution et veiller à ce que leurs investissements en matière de cybersécurité soient à la fois proactifs et proportionnés à leur profil de risque.

Marc Henauer: Il est probable que des facteurs tels que les expériences passées, les dirigeants et les intérêts du conseil d'administration jouent tous un rôle important dans ces décisions. Les régulateurs financiers ont également une influence majeure, en établissant les exigences de base à respecter. Un facteur clé pour renforcer la cybersécurité est de disposer d'un plan à long terme décrivant les investissements financiers réalisés au fil du temps, ce qui permet à la direction de l'entreprise de suivre les progrès et les étapes clés.

Quelles sont les conséquences possibles d'une cyberattaque sur les systèmes bancaires centraux ou sur les systèmes d'information financiers ?

Fabian Schär: Les banques commerciales doivent pouvoir servir leurs clients en traitant les transactions financières et paiements 24 heures sur 24. Les plus grandes banques mondiales traitent jusqu'à 100 millions de transactions par jour, y compris les virements électroniques, les paiements par carte de crédit et les transactions mobiles. Lorsque les activités de base d'une grande banque sont prises pour cible, cela a un impact immédiat sur le marché, provoquant des fluctuations erratiques des flux monétaires sur les marchés financiers et réels jusqu'à ce que d'autres banques prennent le relais. Le système principal de compensation et de règlement est la colonne vertébrale de tout système financier. Tout problème affectant un réseau de messagerie ou un système de règlement (*SWIFT, TARGET2, Fedwire* ou le système *SIX Interbank Clearing*) peut avoir des conséquences considérables et semer la panique dans le secteur financier et dans le monde réel, sans distinction de frontières internationales.

Exposition aux vulnérabilités connues exploitées par taille d'entreprise : ensemble de l'économie et secteur financier



Note: ce graphique illustre la proportion des organisations ayant au moins une vulnérabilité connue exploitée détectée dans leur infrastructure en 2023, ventilée par taille d'entreprise. Il comprend un indice de référence pour l'ensemble de l'économie couvrant tous les secteurs, ainsi que des chiffres agrégés pour le secteur financier mondial et ses composantes européenne et américaine. Les catégories de taille des entreprises sont définies en fonction du nombre d'employés.

Source: Bitsight

Comment les institutions financières mesurent-elles les cyberrisques afin de les gérer ?

Beat Schär: Compte tenu des nombreux éléments variables et inconnus, quantifier avec précision ces risques nécessite des efforts considérables et peut n'apporter que des avantages limités. Une approche globale basée sur des scénarios constitue probablement la manière la plus efficiente d'évaluer la situation et semble être aujourd'hui la norme. Étant donné que la communication sur la cybersécurité est déjà complexe et que la gestion quantitative des cyberrisques en est encore à ses débuts, il est préférable de communiquer de manière claire et concise avec les dirigeants de l'entreprise.

Quels sont les risques liés à la cybersécurité introduits par des prestataires de services tiers ?

Alain Beuchat: Le recours à des prestataires tiers, qu'il s'agisse de fournisseurs de services cloud, d'externalisation informatique ou de logiciels, est devenu indispensable. Cela ajoute cependant un nouveau niveau de risque qui est plus difficile à gérer. Les régulateurs attendent de nous que nous appliquions à nos fournisseurs le même niveau de contrôle que celui que nous appliquons au sein de la banque. Concrètement, cela se traduit par des audits continus, de longs questionnaires à l'attention des fournisseurs et des suivis réguliers afin de faire respecter les normes au-delà de notre périmètre direct. Plus le recours à l'externalisation se développe, plus la surface d'attaque s'élargit. Pour les institutions financières, cela pose un double défi qui consiste à la fois à appliquer des contrôles sur les tierces parties tout en gérant les questions de cybersécurité en interne.

Quelles sont les limites et les évolutions probables du marché de la cyberassurance ?

Beat Schär: Il est relativement facile d'évaluer l'impact d'une cyberattaque, mais il est extrêmement complexe de déterminer la probabilité d'être ciblé. Cette complexité rend difficile d'évaluer précisément le risque global d'une entreprise. Une approche pragmatique consiste à comparer votre configuration de cybersécurité avec celle de vos pairs du secteur et à viser à les surpasser. Comme dans de nombreux domaines de la gestion des risques, l'objectif est de garder une longueur d'avance. Cela dit, nous devons être réalistes. Toute police d'assurance comporte des lacunes, et la cyberassurance ne fait pas exception. Un autre sujet de préoccupation pour les assureurs est le risque de concentration. Certains fournisseurs de services cloud représentent à eux seuls une part importante de la capacité informatique mondiale. Ce niveau de concentration soulève de sérieuses questions quant à la manière dont les assureurs peuvent gérer leur exposition au risque systémique dans un écosystème numérique aussi interconnecté.

Alain Beuchat: Le marché de la cyberassurance est en phase de maturité rapide, mais nous nous rendons également compte de ses limites. Au début, les polices de cyberassurance étaient bon marché et peu contraignantes. Aujourd'hui, les compagnies d'assurance effectuent des vérifications rigoureuses, posent des questions techniques détaillées et sont promptes à contester les demandes d'indemnisation. Elles ne s'intéressent pas seulement à des questions de coût, mais aussi de fiabilité. Si une attaque contre une entreprise est due à une machine mal configurée ou à un anti-malware obsolète, les assureurs peuvent invoquer des clauses d'exclusion et réduire les indemnités accordées, quelles que soient les bonnes pratiques générales de l'entreprise. Dans de nombreux cas, des conséquences douloureuses pour l'entreprise, comme les atteintes à la réputation et la perte de clientèle, ne sont pas couvertes par les assurances. Face à l'augmentation des primes et à la multiplication des clauses d'exclusion, certaines institutions commencent à considérer la cyberassurance comme un dernier recours plutôt que comme la pierre angulaire de leur stratégie de gestion des risques.

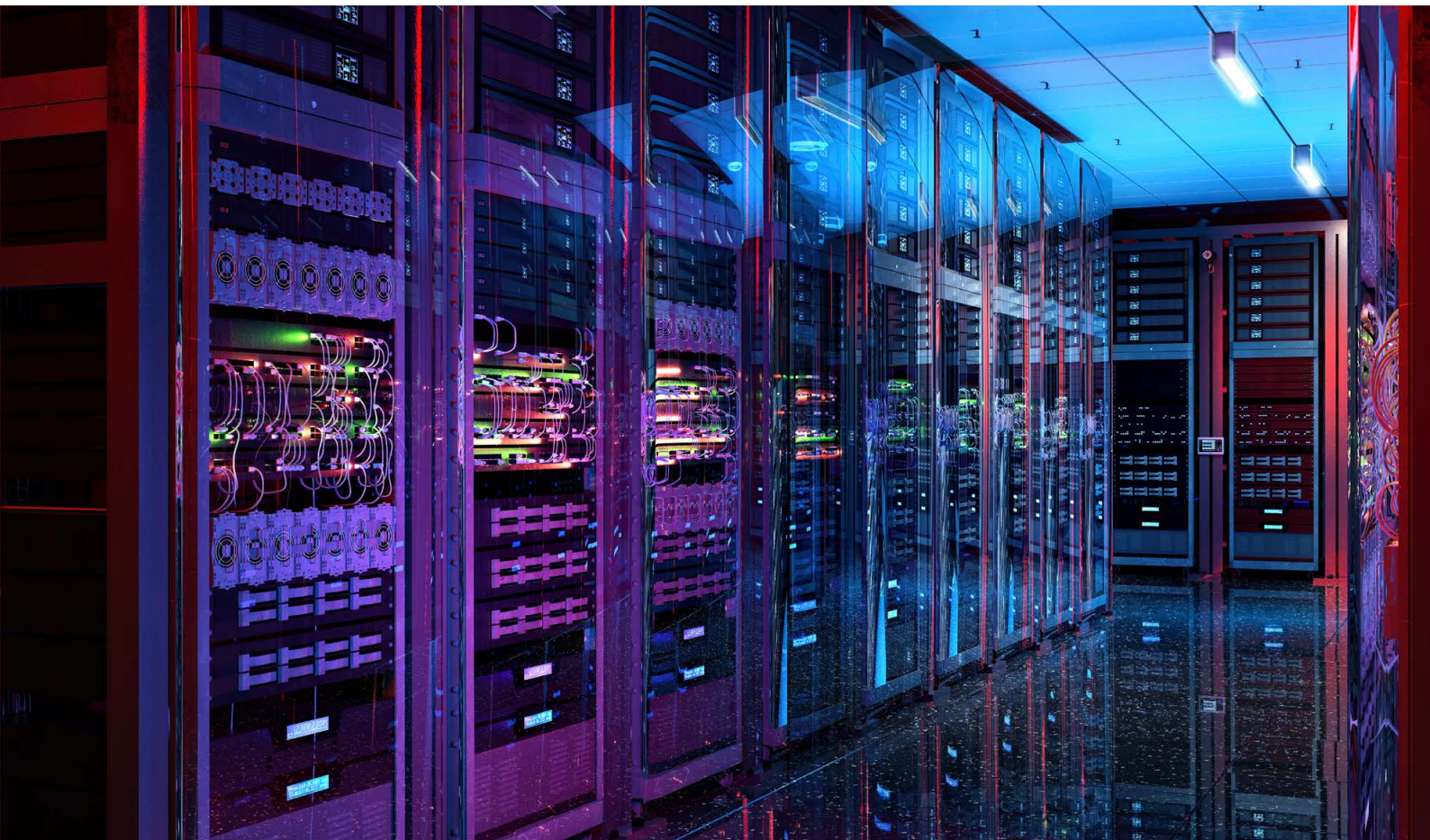
Anastasia Kartasheva: Les cyberrisques sont influencés par une combinaison de distributions de pertes à queue épaisse, de modèles incertains et d'informations inégales. Contrairement aux risques assurables classiques, les cyberévénements peuvent se produire au niveau mondial, être très rapides et délibérément adaptatifs, ce qui les rend particulièrement difficiles à prévoir et à modéliser. Leur coût élevé et leur nature changeante ajoutent à leur complexité. Ces caractéristiques posent des défis majeurs aux assureurs, mais cela peut aussi signifier que le marché recèle un certain potentiel. Parmi les nouvelles solutions, nous pouvons citer la création d'intermédiaires qui évaluent la cyberrésilience d'une entreprise, à l'instar des notations de crédit sur les marchés obligataires.

Olivier Scaillet: Le marché de la cyberassurance est en train de devenir un segment distinct. Pour comprendre cette évolution, nous pouvons nous intéresser à l'équilibre entre un investissement interne dans la cybersécurité et le transfert des risques via une assurance. Les compagnies d'assurance ne se contentent plus d'offrir une couverture, elles aident également les organisations à gérer leurs cyberrisques directement ou par l'intermédiaire de tiers. À mesure que ces modèles se développent, j'anticipe une pression croissante sur le secteur de la réassurance, en raison de la hausse des coûts et de la complexité des cyberrisques. Cette trajectoire pourrait finalement conduire à la mise en place de mécanismes mondiaux de partage des risques, tels que des syndicats d'assurance ou des marchés secondaires pour les cyberrisques, à l'instar des obligations catastrophes *(Cat Bonds)*. Ces mécanismes de partage des risques permettraient aux investisseurs de négocier des titres liés à la cybersécurité et élargiraient la capacité au-delà de l'assurance traditionnelle.

À l'avenir, quelles stratégies avancées les institutions financières devraient-elles adopter pour atténuer le risque de cyberattaques ?

Marc Henauer: Les institutions financières ont une connaissance approfondie du paysage de la cybersécurité et du fonctionnement du système financier interconnecté, ainsi que de ses vulnérabilités potentielles. Quelle que soit leur taille, toutes les banques peuvent en cas de cyberattaque créer un effet domino sur l'ensemble de l'infrastructure bancaire et financière. Elles sont également conscientes que toute atteinte réputationnelle a des répercussions sur chaque établissement. Si une banque est gravement touchée, c'est l'ensemble du secteur financier qui en ressent les conséquences. Il n'y a aucun gain individuel à tirer d'une telle situation. Cette réalité les incite à collaborer de manière proactive et à communiquer de manière ouverte et efficiente.

Olivier Scaillet: À l'avenir, les institutions financières devront adopter des stratégies de défense avancées et multicouches, telles que la détection des menaces basée sur l'intelligence artificielle, les cadres Zero Trust et la formation continue de leurs employés, afin de garder une longueur d'avance pour se protéger face à des cybermenaces de plus en plus sophistiquées. Mais au-delà de leur propre protection, les banques sont particulièrement bien placées pour saisir les nouvelles opportunités commerciales qui se présentent dans le domaine de la cybersécurité. À mesure que le cyberrisque devient un actif mesurable et coté, les institutions financières peuvent prendre l'initiative de développer et de proposer des produits financiers innovants, tels que le tranchage du cyberrisque sur le modèle des obligations adossées à des actifs (*Collateralized Debt Obligations* ou *CDO*). En structurant les risques en couches qui absorbent les pertes en fonction de leur gravité, les banques peuvent faciliter la diversification basée sur le marché, proposer des instruments adaptés liés à la cyberassurance et aider leurs clients à se couvrir contre les cyberrisques. Ce faisant, elles passent du statut de cibles passives à celui d'acteurs actifs sur le marché en pleine évolution de l'économie des cyberrisques.



Thématiques d'avenir

Les initiatives de finance décentralisée *(DeFi)* renforcent-elles la cybersécurité ou créent-elles au contraire des points de vulnérabilité ?

Fabian Schär: La finance décentralisée et la finance centralisée présentent des profils de risque distincts en matière de cybersécurité, sans qu'aucune des deux ne soit clairement avantagée. D'un côté, les systèmes décentralisés offrent certains avantages en matière de sécurité, notamment l'impossibilité pour un acteur unique de modifier unilatéralement le registre public, ce qui élimine de nombreux vecteurs d'attaque courants dans les architectures centralisées. En revanche, ils introduisent des vulnérabilités uniques. Par exemple, les systèmes DeFi reposent fortement sur des clés privées, ce qui signifie que si un utilisateur perd ou divulgue la sienne, il n'a aucun recours. Ses actifs peuvent être volés de manière irréversible et les attaquants peuvent même utiliser son identité compromise pour créer de nouveaux contrats intelligents. L'attrait fondamental de la DeFi réside dans l'absence de tiers de confiance, dans des processus rationalisés et dans des transactions plus rapides. Autant de caractéristiques qui peuvent être très avantageuses d'un point de vue commercial. Cependant, l'absence d'intermédiaires transfère également la charge du risque vers l'individu. Les utilisateurs doivent non seulement sécuriser leurs clés, mais aussi naviguer dans un système complexe où les protections courantes proposées dans la finance traditionnelle, telles que les annulations de transactions ou le règlement des litiges, sont largement absentes. En ce sens, la DeFi élargit l'éventail des possibilités, mais introduit également une nouvelle catégorie de risques opérationnels et de cybersécurité qui doit être comprise et gérée activement.

Olivier Scaillet: Comme pour toute innovation technologique, il y a des avantages et des inconvénients. Des études ont montré que les attaques par ransomware sont le type de cyberattaque le plus courant et qu'un petit nombre de groupes de cybercriminels dominent le secteur. Ces gangs sont devenus des entreprises sophistiquées avec des noms élaborés, des bureaux, des centres d'appel et des opérations de franchise. Ils reçoivent généralement les rançons en cryptomonnaies et doivent blanchir les fonds à l'aide de stratagèmes complexes. Le bitcoin étant traçable, les pirates lui préfèrent des cryptomonnaies moins transparentes, comme *Monero* ou *Zcash*. Selon certaines informations isolées, des gangs exigeraient une majoration de 20% lorsque les victimes insistent pour payer en bitcoins. Une solution qui empêcherait complètement l'utilisation abusive des cryptomonnaies dans le contexte de la cybercriminalité n'est guère réaliste, car une interdiction totale de toutes les cryptomonnaies dans un pays annulerait leurs avantages et désavantagerait le pays sur le plan technologique.

Quelles sont les différences en termes de risques de cybersécurité entre la monnaie centrale, la monnaie commerciale et les crypto-actifs ?

Anastasia Kartasheva: Il ne s'agit pas seulement de voler de la monnaie électronique ou des actifs, mais aussi de les blanchir pour pouvoir les encaisser. Le braquage de la Banque du Bangladesh en 2016 est un excellent exemple. Des pirates informatiques ont infiltré le système informatique de la banque centrale et ont accédé à son réseau SWIFT pour envoyer de fausses instructions de transfert pour un montant total de 951 millions de dollars américains. Environ 81 millions de dollars américains ont été envoyés aux Philippines, puis blanchis via un réseau complexe et coûteux de sociétés écrans et de casinos. Les autres transferts, d'une valeur de plus de 850 millions de dollars américains, ont été interceptés grâce à une faute de frappe dans le message, ce qui a éveillé des soupçons. S'il est relativement facile de convertir des actifs non réglementés comme les bitcoins dans des pays où la réglementation est faible, cette opération reste risquée et opaque. L'utilisateur final se retrouve souvent avec de la "fausse monnaie".

Comment l'intelligence artificielle exacerbe-t-elle les menaces en matière de cybersécurité ?

Anastasia Kartasheva: L'intelligence artificielle est une arme à double tranchant. Les cyberattaquants sont devenus beaucoup plus intelligents. L'époque où nous recevions des courriels en masse avec des adresses aléatoires, des fautes de frappe et des logos mal conçus est depuis largement révolue. En parallèle, les cibles potentielles peuvent tirer parti de l'intelligence artificielle pour renforcer leur équipe et automatiser leurs défenses. Le secteur cherche à déployer des outils d'intelligence artificielle dans l'ensemble du système informatique. Il est essentiel de sensibiliser les utilisateurs partout dans le monde aux menaces actuelles et futures et de les former.

Fabian Schär: Le développement rapide des *deepfakes*, alimenté par les systèmes d'apprentissage profond, me préoccupe tout particulièrement. Le seul mécanisme de défense efficace aujourd'hui est la signature cryptographique. De nos jours, des milliers d'heures de vidéos mettant en scène des figures politiques sont disponibles en ligne. Il est relativement simple pour un modèle d'intelligence artificielle d'usurper l'identité de ces personnes et de leur faire dire tout ce que nous voulons. Je pense que nous allons bientôt nous retrouver dans un monde où les discours ne seront plus prononcés en personne, mais écrits et présentés par l'intermédiaire d'un système d'intelligence artificielle, avec un message crypté pour garantir son authenticité.

Comment les institutions financières gèrent-elles aujourd'hui à l'aide de l'intelligence artificielle les menaces liées à la cybersécurité ?

Fabian Schär: Il est difficile pour les entreprises financières de garder une longueur d'avance dans ce domaine et ce pour deux raisons principales. Premièrement, la concurrence est très vive. Deuxièmement, les banques sont souvent des organisations pérennes, ce qui signifie qu'elles se retrouvent avec des systèmes hérités complexes qui sont difficiles à sécuriser. L'intelligence artificielle les aidera à détecter les activités suspectes et à réagir plus rapidement. Il faut cependant admettre que les cybercriminels semblent avoir une longueur d'avance dans ce domaine.

Olivier Scaillet: Plusieurs évolutions intéressantes sont en cours. L'intelligence artificielle offre de nombreux avantages, tels que l'efficience, l'évolutivité et l'adaptabilité en matière de cybersécurité. Ces avantages facilitent l'identification des activités frauduleuses potentielles sur la base des comportements des clients, permettent d'anticiper les menaces en tirant des enseignements des données historiques et rendent possible la mise en place de systèmes de réponse automatisés qui isolent les problèmes et réduisent les temps de réponse. Cependant, toute notre base de connaissances actuelle devra être revue lorsque l'informatique quantique deviendra la nouvelle norme.

À quelle échéance pouvons-nous de manière réaliste anticiper l'apparition des menaces liées à l'informatique quantique ?

Anastasia Kartasheva: La puissance et la vitesse de calcul sont des éléments cruciaux dans le monde cybernétique. Certains experts prédisent que des attaques plus sophistiquées provenant d'ordinateurs quantiques se généraliseront au cours de la prochaine décennie. Cependant, même si les cyberattaques sont, par définition, menées via des systèmes informatiques, elles intègrent toujours une composante humaine. La capacité de calcul n'est pas le seul facteur à prendre en compte. Du côté des cybercriminels comme des cibles potentielles, tout le monde devra monter en compétences.

Quelles mesures spécifiques les institutions financières devront-elles prendre pour se préparer à une cybersécurité capable de résister à l'informatique quantique ?

Fabian Schär: Les banques doivent toujours se préparer aux défis futurs. À mon avis, elles doivent approfondir leur compréhension du système actuel et du système émergent. Le cadre informatique bancaire actuel est un modèle consolidé qui a été établi dans les années 1950 et qui a traversé de nombreuses fusions et acquisitions. Contrairement à de nombreux autres secteurs, l'importance d'un système centralisé est cruciale dans le secteur bancaire et les systèmes anciens posent des problèmes considérables. J.P. Morgan Chase, par exemple, résulte de fusions et d'acquisitions de plus de 1'200 institutions au cours de son histoire.

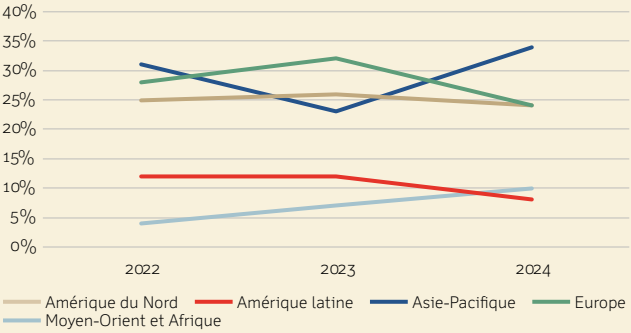
Olivier Scaillet: La préparation à l'avenir quantique comporte plusieurs étapes. Tout d'abord, les banques doivent dresser un inventaire clair de leurs blocs cryptographiques actuels afin de comprendre leur configuration et leurs vulnérabilités. Vient ensuite la phase de développement, au cours de laquelle les banques collaborent avec les fournisseurs de systèmes et les propriétaires de systèmes internes afin de tester de manière approfondie la nouvelle technologie quantique. Puis vient la phase de remplacement de l'ancienne technologie par la nouvelle. L'approche actuelle pour faire face aux risques liés à la cryptographie post-quantique (*post-quantum cryptography* ou *PQC*) et aux faiblesses potentielles des nouveaux algorithmes résistants à la PQC consiste à combiner les anciennes et les nouvelles méthodes en mettant en œuvre des protocoles hybrides qui appliquent simultanément les deux technologies.

Quelles sont les différences entre les pays et les secteurs en termes de moyens mis en œuvre pour garantir la cybersécurité ?

Fabian Schär: Les différences entre les pays et les secteurs sont importantes et tiennent souvent à des facteurs liés à l'histoire, à la géographie et à la conception institutionnelle. Dans le secteur financier, par exemple, les nouveaux centres financiers bénéficient souvent d'un avantage structurel. Leurs systèmes ont été construits à l'ère des marchés mondiaux et du commerce électronique, ce qui leur a permis de se doter d'infrastructures informatiques plus modernes. En revanche, les banques établies de longue date s'appuient souvent sur des systèmes anciens, parfois vieux de plusieurs décennies, qui sont difficiles et coûteux à maintenir. Il en résulte des mosaïques complexes, plus difficiles à sécuriser et à maintenir. Au niveau national, si les pays occidentaux disposent généralement de capacités plus solides en matière de cybersécurité, des disparités persistent. Certains pays attirent davantage d'attention sur le plan géopolitique et sont donc plus souvent la cible de cyberattaques, notamment les États-Unis. D'autres, comme la Suisse, bénéficient d'une position géopolitique plus neutre, d'institutions dotées de ressources importantes et d'une coopération public-privé solide. Ces différences déterminent à la fois l'exposition aux cyberrisques et la résilience face à l'évolution des menaces.

Anastasia Kartasheva: Le niveau de préparation en matière de cybersécurité varie non seulement d'un pays à l'autre, mais aussi d'un secteur à l'autre, d'une entreprise à l'autre et d'un individu à l'autre, en fonction de la manière dont les responsabilités sont plus ou moins clairement définies et les ressources plus ou moins bien coordonnées. Dans certains pays, le secteur public a pris l'initiative en établissant des normes claires, en finançant des centres de coordination et en facilitant le partage des informations concernant les cybermenaces. Dans d'autres, en particulier dans les marchés émergents ou les économies en transition, les entreprises sont souvent livrées à elles-mêmes, avec peu de directives ou de clarté réglementaire. Cette situation conduit à une protection inégale. Certaines grandes entreprises disposent de défenses de classe mondiale, tandis que d'autres, en particulier les petites entreprises et les institutions publiques, restent très vulnérables en raison de budgets limités et de systèmes fragmentés. En fin de compte, l'efficience d'un cadre de cybersécurité dépend autant de la gouvernance nationale et de la maturité institutionnelle que de la technologie utilisée ou des dépenses consenties.

Répartition des cyberattaques par région géographique



Note: ce graphique illustre la répartition des cyberattaques par région géographique entre 2022 et 2024. En 2024, les pays les plus ciblés dans chaque région étaient les États-Unis (86% de l'Amérique du Nord), le Japon (66% de l'Asie-Pacifique), l'Arabie saoudite (63% du Moyen-Orient et de l'Afrique), le Brésil (53% de l'Amérique latine) et le Royaume-Uni (25% de l'Europe).

Source: IBM X-Force

Comment décririez-vous le rôle des normes internationales dans les efforts transfrontaliers en matière de cybersécurité ?

Marc Henauer: Les normes internationales jouent un rôle très important dans la coopération transfrontalière en matière de cybersécurité en fournissant une terminologie commune, des attentes partagées et des références techniques pour la gestion des risques. Bien que leur mise en œuvre varie selon les régions et les secteurs, ces normes, telles que la norme ISO 27001 (de l'Organisation internationale de normalisation) et le cadre de cybersécurité du *National Institute of Standards and Technology (NIST)* aux États-Unis, contribuent à réduire la fragmentation et à faciliter la collaboration entre les gouvernements, les secteurs et les chaînes d'approvisionnement. Comme en matière de politique climatique, la cybersécurité nécessite un alignement mondial sur le plan des principes, mais la traduction de ces principes communs en actions coordonnées reste un défi complexe. Pour accomplir de réels progrès, il s'agit de miser sur une réciprocité et une confiance entre les pays et les secteurs et non sur l'imposition de modèles uniformes. Le risque de perdre des institutions importantes telles que MITRE, un organisme de recherche à but non lucratif qui gère des infrastructures communes telles qu'un répertoire mondialement utilisé des vulnérabilités informatiques connues (*Common Vulnerabilities and Exposures* ou *CVE*), montre la fragilité des systèmes centralisés. Ce risque souligne la nécessité d'adopter des approches plus résilientes, distribuées et coopératives en matière de gouvernance mondiale pour la cybersécurité.

Beat Schär: Les normes internationales sont extrêmement précieuses en tant que références, car elles aident les organisations à s'auto-évaluer et à déterminer comment s'améliorer. L'existence d'initiatives diverses dans différents secteurs et pays permet de proposer des ressources sur les défis auxquels d'autres sont confrontés et les solutions qu'ils mettent en œuvre. Dans le domaine de la cybersécurité, aucun acteur ne détient toutes les réponses. Apprendre en continu les uns des autres est non seulement utile, mais indispensable.

Pour conclure

Quel rôle les conseils d'administration et les comités exécutifs, ainsi que les instances de réglementation, devraient-ils jouer dans l'élaboration de la gouvernance de la cybersécurité ?

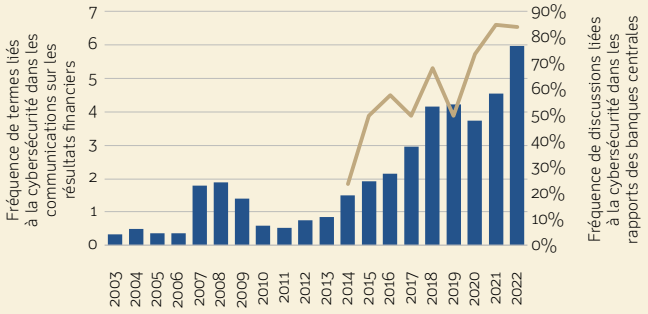
Alain Beuchat: La réglementation suisse exige que les stratégies en matière de cybersécurité soient approuvées au niveau du conseil d'administration. L'implication du conseil d'administration dans le domaine de la cybersécurité représente cependant plus qu'une simple exigence de conformité. Il s'agit d'une question de survie stratégique. Autrement dit, une implication formelle ne se traduit pas toujours par une surveillance efficiente. De nombreux membres de conseils d'administration peinent à saisir à quel point leur organisation dépend de son infrastructure informatique, et sont rarement au fait des thématiques complexes liées à la cyberdéfense. Bien qu'ils soient généralement conscients de l'impact que peuvent avoir les cyberattaques, souvent du fait de leur couverture médiatique, ils ont du mal à faire le lien entre ces menaces et les vulnérabilités et réalités spécifiques à leur propre organisation. Pour combler ce fossé, il faudra plus que de simples briefings. Les membres du conseil d'administration doivent disposer de connaissances de base leur permettant de poser des questions pertinentes, de remettre en question les compromis et de comprendre le profil de risque de leur entreprise. Tant que les conseils d'administration n'auront pas acquis une meilleure maîtrise des questions cybernétiques, la gouvernance restera à la traîne par rapport à l'évolution des menaces.

Olivier Scaillet: Dans le contexte suisse, les organismes de réglementation tels que la FINMA jouent un rôle important dans l'élaboration de la gouvernance de la cybersécurité, en particulier dans le secteur financier. Si certaines institutions sont en avance grâce à des ressources plus importantes ou à une meilleure compréhension des cyberrisques, la réglementation reste relativement peu stricte dans des domaines tels que les solutions cloud et les chaînes d'approvisionnement. Une prochaine étape importante consisterait à clarifier les rôles et les responsabilités de tous les niveaux de direction en cas de défaillance de la cybersécurité, afin de promouvoir une plus grande responsabilisation des dirigeants. En parallèle, les conseils d'administration et les dirigeants ne doivent pas considérer la cybersécurité comme une simple question technique déléguée à leurs équipes informatiques. Les conseils d'administration doivent être régulièrement informés des principaux incidents et développements et mener des tests réguliers pour s'assurer qu'ils sont prêts à prendre des décisions éclairées sous pression. La cybersécurité touche presque tous les aspects de l'entreprise et de la société. Les dirigeants ont donc le devoir de s'engager tôt et de manière proactive pour mieux comprendre cette thématique, plutôt que d'attendre qu'une crise les oblige à agir.

Anastasia Kartasheva: Il est essentiel de disposer d'un bon plan de crise. Ce plan doit répondre à des questions clés, telles que la rapidité avec laquelle les systèmes peuvent être restaurés, si l'attaquant a toujours accès au réseau, quelles pertes pourraient être couvertes par l'assurance cybersécurité et si des sanctions réglementaires ou des amendes pourraient être infligées. Il n'existe pas de solution universelle, mais il est essentiel de sensibiliser de manière proactive les dirigeants d'entreprise aux risques liés à la cybersécurité.

Fabian Schär: Comme souvent, il peut être utile de prendre des mesures raisonnables, mais aller trop loin peut avoir l'effet inverse. S'il y a une leçon à tirer des bannières obligatoires annonçant l'utilisation de *cookies* sur les sites web, c'est qu'en matière de conformité réglementaire, nous nous contentons souvent de cocher des cases, sans vraiment protéger le plus important. Au final, ni les entreprises ni les individus ne peuvent externaliser leur responsabilité. La réglementation fixe un seuil minimum et non maximum pour une cybersécurité efficace.

Mentions de concepts liés à la cybersécurité par les entreprises et les banques centrales



Note: ce graphique présente deux mesures de l'attention accordée par les institutions à la cybersécurité entre 2003 et 2022. Les barres indiquent la fréquence d'utilisation de termes liés à la cybersécurité (cyberattaque, cybermenace, cybersécurité, logiciel malveillant, perte de données, ransomware, etc.) dans les communications sur les résultats financiers des entreprises, normalisée par 10'000 phrases (axe de gauche). La ligne indique la proportion des rapports sur la stabilité financière et des rapports annuels publiés par les banques centrales du G20 qui incluent une discussion approfondie sur la thématique de la cybersécurité (axe de droite).

Sources: Advisen, NL Analytics et Fonds Monétaire International (FMI)

Comment anticipez-vous que la réglementation façonne la capacité du secteur financier à gérer les risques cybernétiques ?

Marc Henauer: En Suisse, l'OFCS joue un rôle crucial dans le renforcement de la cyberrésilience du pays. Son travail s'articule autour de quatre objectifs principaux. Il s'agit d'améliorer la compréhension des menaces, d'encourager la prévention, de minimiser l'impact des incidents et de sécuriser les produits et services numériques. Une étape importante a récemment été franchie avec l'introduction d'une obligation de signalement dans les 24 heures des cyberattaques visant des infrastructures critiques, une mesure destinée à générer des données plus précises et à éclairer une réglementation plus intelligente. Cette nouvelle obligation de signalement permettra d'obtenir des informations plus claires sur les menaces, d'apporter un soutien plus ciblé et de renforcer les bases de la gestion des cyberrisques dans un cadre national coordonné. Il sera intéressant de voir comment cette obligation évoluera au fil du temps.

Fabian Schär: Bien qu'il soit difficile de tirer des conclusions définitives, l'expérience passée suggère que la réglementation en matière de cybersécurité dans le secteur financier a généralement été efficace. Cependant, même les cadres réglementaires et les mesures de protection techniques les plus robustes ne peuvent éliminer le risque d'erreur humaine. Il est donc essentiel de former et de sensibiliser les collaborateurs en continu. À l'avenir, les obligations de signalement obligatoire et la transparence accrue des données continueront probablement à façonner les normes réglementaires, améliorant ainsi notre compréhension collective des cybermenaces. Cela dit, le respect des délais de signalement rapides, par exemple dans les 24 heures, reste difficile. En effet, les entreprises ont souvent besoin de plus de temps pour évaluer pleinement l'impact d'un incident, notamment lorsqu'elles doivent coordonner leurs actions avec des parties externes.

Olivier Scaillet: Dans le secteur financier, chacun sait que nous devons nous concentrer sur le moment où la prochaine attaque aura lieu et sur la manière d'en minimiser l'impact, et non sur la question de savoir si une attaque aura lieu. Cela est frustrant, mais le fait d'être confronté à cette dure réalité permet aux entreprises et au secteur de se préparer. Au sein des entreprises, il convient d'avoir des discussions franches sur la rapidité avec laquelle elles peuvent se remettre d'une attaque. Entre entreprises, il faut réfléchir à la manière de limiter les risques communs en utilisant une gamme plus large de matériels et de logiciels. Si la réglementation peut imposer bon nombre de ces mesures, elle n'a toutefois qu'un pouvoir limité pour contraindre le secteur à adopter des systèmes différents. Je m'inquiète de la baisse constante du nombre de fournisseurs et de l'absence de solution viable pour inverser cette tendance.

Quels types de menaces émergentes en matière de cybersécurité auront le plus d'impact sur la société au cours de la prochaine décennie ?

Fabian Schär: Au cours des prochaines années, les progrès de l'intelligence artificielle, du *Big Data* et de l'informatique quantique feront passer notre cybersécurité à un niveau supérieur. Je suis fermement convaincu que nous devons exploiter tout le potentiel des programmes de primes pour transformer les "méchants" en "gentils". Les attaques par ransomware sont souvent motivées par des intérêts financiers. Il est donc logique que les entreprises récompensent les personnes qui les aident à améliorer leur sécurité plutôt que de payer des rançons pour sauver leur entreprise. Le jeu du chat et de la souris existe depuis toujours et il n'y a aucune raison de penser que l'avenir sera différent, si ce n'est que les outils évolueront.

Anastasia Kartasheva: Au cours de la prochaine décennie, le secteur financier sera confronté à des menaces de cybersécurité de plus en plus complexes, sous l'effet de l'interdépendance numérique croissante et d'une exposition au risque mondialisée. L'un des principaux défis consistera à vérifier l'identité des tiers, qu'il s'agisse d'entreprises ou de particuliers, surtout au niveau transfrontalier dans un contexte où différentes normes et réglementations numériques coexistent. Dans le même temps, la surface d'attaque potentielle s'étendra en raison de la prolifération des appareils connectés, de la consolidation des systèmes informatiques et de l'adoption généralisée du cloud. Ces tendances, combinées aux progrès de l'intelligence artificielle, de l'apprentissage automatique et de l'informatique quantique, donneront plus de moyens à des adversaires plus sophistiqués. Ensemble, elles obligeront à repenser en profondeur les concepts de confiance, de vérification et de résilience en matière de cybersécurité.

Swiss Finance Institute

Avec le soutien de ses fondateurs – le secteur bancaire suisse, la Confédération et les principales universités suisses – le Swiss Finance Institute (SFI) assure une promotion active d'une recherche et d'un enseignement de classe mondiale dans les domaines de la banque et de la finance en Suisse. En combinant excellence académique et expérience pratique, le SFI contribue au renforcement de la place financière suisse.

Editeur et contact
Dr. Cyril Pasche
Senior Director Publications and Topic Development
+41 22 379 88 25
cyril.pasche@sfi.ch

swiss:finance:institute

Walchestr. 9, CH-8006 Zurich, T +41 44 254 30 80
c/o University of Geneva, 42, Bd du Pont d'Arve, CH-1211 Geneva 4, T +41 22 379 84 71
www.sfi.ch

Version 10/2025