Tous à la manœuvre face au risque cyber

Agnès Bénassy-Quéré, novembre 2026



L'attaque cyber de grande ampleur sur des frigos de supermarchés et d'hôpitaux en octobre a eu le mérite de rendre concret le risque cyber pour nos sociétés. Ce risque pèse sur tous les systèmes connectés, et le secteur financier figure au premier rang des victimes potentielles, comme l'ont montré des exemples récents.

Dans le cadre du règlement européen DORA (*Digital Operational Resilience Act*), les banques européennes sont tenues d'évaluer et protéger en continu leurs systèmes informatiques, de réaliser régulièrement des tests de sécurité et d'intrusion, d'évaluer la résilience de leurs prestataires extérieurs et, enfin, de signaler rapidement les incidents majeurs dont elles seraient victimes.

Pour l'année 2025, les Autorités de supervision européennes ont ainsi recensé 3 383 incidents majeurs ayant touché les systèmes informatiques des institutions financières européennes, dont 10 % relevant de la cybersécurité. Il y a donc eu en moyenne près d'une cyber-attaque chaque jour en Europe. En France, l'Autorité de contrôle prudentiel et de résolution (ACPR) et la Banque de France ont été notifiées d'une quarantaine de cyber-incidents majeurs d'origine supposément cybercriminelle (Banque de France, 2026).

Au-delà du dommage direct (inaccessibilité des services, vols de données, détournement de fonds et autres opérations frauduleuses, etc.), ce type d'attaque a un coût économique indirect. Par exemple, des opérations financières sont empêchées pendant l'arrêt d'un système de paiement. L'interruption des paiements de gros provoque un choc de liquidité qui se propage entre institutions financières, avec un risque de crise de liquidité (Eisenbach et al, 2021). Pour les entreprises non financières, le blocage des paiements de détail peut engendrer des pertes de revenus immédiates et fragiliser la trésorerie, d'autant plus si les banques ne sont plus en mesure d'offrir des lignes de

liquidité. Par ailleurs, le dommage réputationnel peut être important pour le secteur financier, en jetant le doute sur la sécurité des données et des actifs conservés par les intermédiaires financiers.

En 2024, le Fonds Monétaire International (FMI) identifiait trois risques principaux pour la stabilité financière :

- La perte de confiance, pouvant aller jusqu'à des ruées bancaires ;
- Le blocage de services critiques ou d'une institution centrale, sans substitut à court terme ;
- La propagation d'un cyber-incident affectant une institution via ses interconnexions au travers de liens techniques (usage de progiciels communs) ou financiers avec d'autres acteurs du secteur.

Ces perturbations peuvent affecter le secteur financier via un dysfonctionnement des marchés, une hausse de la volatilité des prix des actifs, des difficultés d'accès aux financements et des perturbations des systèmes de paiements. Ces désordres peuvent à leur tour déclencher une crise de liquidité ou des restrictions de crédit qui vont peser sur une économie réelle déjà handicapée par l'interruption des paiements ou de l'accès à des infrastructures critiques.

Plusieurs facteurs viennent accroître l'exposition des institutions financières au risque cyber, notamment :

- La concentration des fournisseurs de services tiers, particulièrement en matière de logiciels, de plateformes cloud et d'outils d'intelligence artificielle. Le risque est alors exacerbé par la dépendance d'un grand nombre d'institutions envers les mêmes fournisseurs pour des services essentiels (Pendleton et al., 2024). En 2025, la mise hors service pendant 14 heures d'*Amazon Web Services* a montré comment la défaillance d'un seul fournisseur technologique peut avoir des conséquences économiques et opérationnelles importantes, bien au-delà du seul secteur financier. Cette dépendance à un petit nombre de fournisseurs rend le risque cyber peu diversifiable par rapport aux autres risques opérationnels (Biener et al., 2015).
- L'environnement géopolitique dégradé expose ces entreprises à des menaces accrues d'actions offensives et implique une préparation renforcée. Par ailleurs, compte tenu de leur importance stratégique, certains fournisseurs de services majeurs peuvent être soumis à des pressions, des sanctions ou des restrictions à l'exportation pouvant générer des difficultés d'accès à certains services critiques. Cette fragmentation croissante augmente les risques opérationnels et de stabilité financière.

Si les risques ont clairement augmenté, les attaques ne sont pas nouvelles et les institutions financières investissent depuis longtemps pour protéger leurs systèmes d'information, ce qui les rend paradoxalement moins vulnérables que d'autres secteurs d'activité (Aldasoro et al., 2020). En outre, des initiatives internationales existent pour limiter la vulnérabilité du secteur financier.

Coordination G7

Le secteur financier est particulièrement interconnecté, en Europe mais aussi avec le reste du monde. C'est pourquoi, depuis 2019, le G7 a conduit trois exercices de coordination transfrontière face à une hypothétique attaque touchant l'un des pays du G7 et se propageant aux autres. Le dernier en date s'est déroulé entre mars et mai 2026 sous la présidence française du G7. L'idée est de tester la capacité des autorités du G7 à partager rapidement des informations critiques, à agir de manière coordonnée et à communiquer de concert de manière à limiter les dommages et

promptement rétablir un fonctionnement normal. Une communication coordonnée réduit le risque de mouvement de panique, notamment *via* les réseaux sociaux.

Placé sous la responsabilité conjointe du Royaume-Uni et des États-Unis, le groupe d'experts en risque cyber au sein de la filière finances du G7 promeut l'harmonisation des stratégies de cyber-résilience pour protéger l'intégrité et la stabilité du secteur financier. À ce titre, le groupe diffuse des bonnes pratiques auprès du secteur, afin d'améliorer les dispositifs de réaction aux possibles attaques, de protéger les systèmes pendant l'attaque, d'assurer la continuité du service en mode dégradé, puis, de reconnecter les systèmes et de rétablir le fonctionnement normal. À charge pour les différentes autorités nationales de décliner ces bonnes pratiques et de s'assurer de leur mise en œuvre par les acteurs financiers et leurs prestataires.

Les experts insistent sur l'importance de maintenir une « hygiène informatique » irréprochable s'appuyant, parmi nombre d'autres mesures, sur une mise à jour des systèmes à un rythme d'autant plus rapide que les équipements sont exposés sur Internet et que les failles sont activement exploitées. Cette approche doit s'accompagner d'une gestion suffisamment anticipée de l'obsolescence des systèmes, d'une politique de gestion stricte des droits d'accès, du recours à des mécanismes d'authentification forte pour l'accès aux systèmes critiques, d'une segmentation rigoureuse des réseaux, de mesures de durcissement des configurations des différents systèmes et équipements, ainsi que de chiffrement des données… À ces mesures s'ajoutent naturellement la sensibilisation régulière des utilisateurs et la mise en œuvre de sauvegardes immuables et déconnectées.

Ces éléments destinés à protéger les systèmes doivent être complétés par des processus permettant de détecter efficacement les attaques, puis d'y répondre au plus vite. Il faut aussi savoir relancer rapidement les systèmes et activités après la résolution d'un incident, notamment lorsqu'un établissement aurait été compromis. Ces procédures sont régulièrement testées dans le cadre des plans de continuité et de reprise d'activité.

Au-delà de la sécurisation de ses propres systèmes d'information, il importe enfin de s'assurer de la résilience cyber des principaux fournisseurs de services – logiciels, télécommunications, cloud, etc.

IA et informatique post-quantique

L'émergence des intelligences artificielles dites « de pointe » accentue les risques en augmentant à la fois la rapidité et l'envergure des attaques. L'automatisation de la recherche de failles et de voies de contournement des protections rend les systèmes plus vulnérables. Ce constat a conduit le Comité européen du risque systémique à publier une alerte dédiée à ces risques, qualifiés de systémiques (ESRB, 2026).

En parallèle, le développement des échanges en crypto-actifs, notamment via des portefeuilles non hébergés (c'est-à-dire, gérés par les individus eux-mêmes, hors des plateformes d'échange), facilite le déploiement d'une véritable industrie des services de cyber-criminalité.

Dans les années qui viennent, la mise en service d'ordinateurs quantiques démultipliera la puissance de calcul disponible, permettant à de potentiels attaquants de briser les clés cryptographiques qui protègent les systèmes. C'est pourquoi le secteur financier doit se préparer en passant à la cryptographie post-quantique, notamment en faisant évoluer les solutions de chiffrement et de signature qui protègent ses données, ses communications et ses transactions. En janvier 2026, le groupe d'experts du G7 sur le risque cyber a publié une feuille de route visant

à guider la transition du secteur financier vers des solutions de cryptographie post-quantique, et un second groupe réunissant les agences de sécurité nationale a, quant à lui, produit un document expliquant les mesures pratiques à prendre pour engager la migration post-quantique.

La coordination des efforts dans le domaine de la cybersécurité est rendue nécessaire par l'interconnexion des systèmes informatiques : les cyberattaquants s'introduisent via les points du réseau les moins protégés, qu'il s'agisse de logiciels vieillissants ou d'institutions ou de prestataires moins bien protégés. Aussi le groupe d'experts préconise-t-il d'adopter un calendrier commun pour le déploiement de la cryptographie post-quantique d'ici 2035 au plus tard, échéance aujourd'hui considérée comme la cible par les spécialistes du domaine, en donnant la priorité aux systèmes les plus exposés pour que ceux-ci puissent être couverts d'ici 2030 (cf. graphique).

Graphique. Calendrier de déploiement de la cryptographie post-quantique



Source : G7-CEG-Quantum-Roadmap.pdf

***

Alors que la coordination multilatérale fait face à d'importantes difficultés, il est intéressant de constater que, sur des sujets précis et techniques pour lesquels il existe un intérêt commun évident, la convergence reste possible et qu'elle produit des résultats. Face au risque cyber, tout le monde est effectivement sur le pont. L'arrivée sur le marché de nouvelles technologies permettant de contourner les protections des systèmes d'information, de multiplier les cyber-attaques et, enfin, de financer ceux qui les commettent, va nécessiter de renforcer les équipages et leur coordination internationale, malgré une mer tumultueuse qui pourrait les décourager.