LES CYBERRISQUES, UNE PRÉOCCUPATION CROISSANTE POUR LA STABILITÉ MACROFINANCIÈRE

Dans un contexte d'accélération de la transition numérique, d'évolution des technologies et d'exacerbation des tensions géopolitiques, les incidents liés à la cybersécurité, notamment ceux guidés par des intentions malveillantes, sont devenus de plus en plus fréquents au cours des deux dernières décennies, plus particulièrement depuis 2020. De graves incidents survenant dans des institutions financières importantes pourraient mettre en grand péril la stabilité macrofinancière, ce qui se traduirait par une perte de confiance, par la perturbation de services essentiels et, du fait de l'interconnexion technologique et financière, par des répercussions sur d'autres institutions.

S'il dresse le constat qu'aucun cyberincident n'a pris une ampleur systémique à ce jour, ce chapitre souligne une augmentation du risque de voir des sociétés subir des pertes directes extrêmes — au moins 2,5 milliards de dollars — à la suite de tel incidents. De plus, les pertes indirectes provoquées par les cyberincidents sont elles aussi considérables et elles ont tendance à être bien plus importantes que les pertes directes communiquées au niveau des sociétés.

Pour mettre au point des politiques et stratégies de cybersécurité robustes, il est primordial de comprendre les facteurs qui contribuent à la survenance ou à la prévention des cyberincidents. L'analyse contenue dans ce chapitre laisse apparaître que le passage au numérique et les tensions géopolitiques ont considérablement accentué le risque de cyberincidents. Elle montre aussi qu'une législation plus étoffée en matière de cybersécurité et l'amélioration de la gouvernance au niveau des sociétés pourraient contribuer à atténuer ces risques.

Le secteur financier est fortement exposé aux cyberrisques puisque près d'un cinquième des incidents concernent des sociétés financières. Compte tenu de la forte concentration du marché et du faible degré de substituabilité, en particulier pour des services essentiels comme les paiements et les comptes de garde, des cyberincidents touchant des sociétés financières pourraient entraîner des perturbations considérables, ce qui souligne l'importance de renforcer la cybersécurité et la résilience opérationnelle. Dans leur fonctionnement, les sociétés financières sous-traitent souvent les activités informatiques à des prestataires tiers communs, ce qui augmente aussi le risque de chocs combinés et de contagion.

Un cyberincident de grande ampleur dans une institution financière pourrait miner la confiance accordée au système financier et, dans des cas extrêmes, provoquer des cessions d'actifs massives sur les marchés ou des ruées sur les dépôts bancaires. Bien que l'on ne recense à ce jour aucun mouvement de panique majeur à la suite d'un cyberincident, une analyse empirique montre qu'une cyberattaque a donné lieu à des retraits de dépôts modérés mais persistants dans les banques américaines de petite taille.

La cybersécurité du système financier mondial étant exposée à des risques considérables et croissants, les dispositifs d'action publique et de gouvernance doivent évoluer en conséquence. Pourtant, il ressort d'une enquête menée auprès des banques centrales et des autorités de contrôle dans les pays émergents et les pays en développement que les dispositifs des pouvoirs publics en matière de cybersécurité restent souvent insuffisants.

La résistance du secteur financier face aux risques pour la cybersécurité doit être renforcée en mettant au point une stratégie nationale pertinente en matière de cybersécurité ainsi que des dispositifs de réglementation et de contrôle adaptés, en formant le personnel à la cybersécurité, et en créant des conventions nationales et internationales de

partage d'informations. Pour un suivi plus efficace des risques de cybersécurité, il convient d'améliorer le signalement des cyberincidents. Les organes de contrôle doivent engager la responsabilité des administrateurs s'agissant de la gestion de la cybersécurité des sociétés financières et de la promotion d'une culture du risque avisée, de bonnes pratiques, et de formations et sensibilisations à la cybersécurité. Afin de limiter les perturbations pouvant être engendrées par les cyberincidents, les sociétés financières devraient mettre au point et tester des procédures de riposte et de retour à la normale. Les autorités nationales devraient élaborer des protocoles de riposte et des dispositifs de gestion de crise efficaces.

Le FMI s'emploie à aider les pays membres à renforcer leurs dispositifs de cybersécurité à l'aide des programmes d'évaluation du secteur financier et d'initiatives en matière de développement des capacités On trouvera la totalité de ce rapport, en anglais, à l'adresse : http://IMF.org/GFSR-April2024