Assurer l'avenir de la réglementation et du contrôle bancaires Novembre 2018

Atelier n °6
Cybersécurité et résilience opérationnelle

Présidence : Lyndon NELSON (Directeur général adjoint, *Prudential Regulation Authority*, et Directeur exécutif, *Regulatory Operations & Supervisory Risk Specialists*, Banque d'Angleterre)

Augmentation du cyberrisque et conséquences potentielles pour la stabilité financière

En mars 2017, le G20 des ministres des finances et des gouverneurs de banques centrales a déclaré que « l'utilisation malveillante des technologies de l'information et de la communication (TIC) pourrait perturber des services financiers essentiels aux systèmes financiers nationaux et internationaux, porter atteinte à la sécurité et à la confiance, et mettre en péril la stabilité financière »[1]. La propagation rapide du logiciel malveillant Wannacry et la découverte du vol d'informations personnelles affectant plus de 140 millions de comptes chez Equifax en mai 2017 ont exacerbé le sentiment d'urgence à l'égard d'une coordination des efforts internationaux visant à renforcer la résilience cybernétique à l'échelle systémique.

Si les cyberattaques de grande ampleur sous forme de déni de service distribué, vol de données, perte de propriété intellectuelle et cyberfraude existent depuis quinze ans déjà, leur fréquence et leur impact s'accroissent plus rapidement que la capacité des entreprises à les empêcher ou à les surmonter. Selon un récent rapport, la cybercriminalité coûte aux entreprises près de 600 milliards de dollars par an, contre 445 milliards en 2014, ce qui en fait le troisième fléau en valeur après la corruption gouvernementale et le trafic de stupéfiants[2]. Si les questions de cybersécurité concernent tous les secteurs et toutes les régions, les banques sont assurément une cible de choix pour les cybercriminels. Selon une enquête de 2017, un établissement financier typique fait face en moyenne à 85 cyberattaques chaque année, dont un tiers réussissent[3].

Cette accélération de tendance s'explique à la fois par l'évolution toujours plus rapide des technologies et par les interconnexions croissantes de l'écosystème dont font partie les banques. En outre, le secteur bancaire est fondé sur les données et les banques sont donc en concurrence avec les acteurs d'autres secteurs dépendants des données, sur tous les segments de leur chaîne de valeur. Dans un environnement où les réseaux sociaux fournissent des plateformes mondiales instantanées, la course aux

1 Voir le communiqué du G20, *G20 Finance Ministers and Central Bank Governors Meeting, Baden-Baden, Germany, 17-18 mars 2017*, http://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/g20-communique.pdf?__blob=publicationFile&v=3.

2 McAfee, en partenariat avec le Center for Strategic and International Studies (CSIS), février 2018, https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf

3 Accenture (2017), *High Performance Security Report 2016 https://www.accenture.com/us-en/insight-building-confidence-facing-cybersecurity-conundrum.*

clients est notamment déterminée par les délais de commercialisation et la qualité de l'expérience client, au risque de voir la sécurité et la solidité passer au second plan. Les banques suivent des stratégies d'automatisation et d'intégration qui nécessitent de stocker et traiter davantage de données hors des périmètres réglementés, tout en permettant à des prestataires de services comme les fintechs d'accéder à leurs environnements pour mettre en œuvre des processus commerciaux et technologiques. Une telle configuration est exposée à des attaques venant de toutes parts et incite les cyber-adversaires à accroître leurs ressources.

À l'échelle systémique, le Fonds monétaire international (FMI) considère les cybermenaces comme un risque pour la stabilité financière dans son *Rapport sur la stabilité financière dans le monde* d'octobre 2017[4], et les autorités nationales ont commencé à intégrer le cyberrisque dans leurs rapports périodiques sur la stabilité financière[5]. Au nombre des canaux de transmission potentiels évoqués dans ces rapports, l'interdépendance financière, les dépendances opérationnelles et l'impact sur la confiance reviennent le plus souvent, même si les établissements concernés tout comme le secteur officiel peinent à établir un ensemble comparable de paramètres significatifs pour quantifier et suivre le cyberrisque, et pour évaluer le niveau de résilience cybernétique des entreprises.

Q1. Quels sont les défis spécifiques que présente le cyberrisque, par opposition aux risques opérationnels classiques ?

Q2. Existe-t-il, au sein de l'écosystème actuel, une innovation ou une évolution technologique particulière qui suscite des préoccupations systémiques en matière de cybersécurité que les autorités de contrôle devraient surveiller de plus près ?

Réponses apportées jusqu'à présent par le secteur officiel

Lors de la Conférence internationale des autorités de contrôle bancaire (ICBS) en novembre 2016, la question de la cybersécurité avait été abordée dans le cadre d'un atelier portant sur « l'amélioration des bonnes pratiques dans le secteur bancaire ». Les risques que les attaques cybernétiques pourraient faire courir au système financier dans son ensemble avaient alors été évoqués, en particulier l'importance du facteur humain (depuis la méconnaissance des risques et le manque de compétences, tant au sein du personnel que de la direction des établissements, jusqu'aux difficultés de recrutement et de rétention des experts adéquats) – au-delà des aspects techniques propres à la maintenance de logiciels et matériels informatiques. Il y a deux ans, de nombreuses juridictions voyaient dans la législation sur la cybersécurité et la protection des consommateurs le moyen d'asseoir « certains éléments de gouvernance et d'adhésion à certaines normes en matière technologique ».

Moins d'un an plus tard, les préoccupations en termes de cybersécurité arrivaient en tête de l'agenda réglementaire international, monopolisant l'attention de la plupart des instances de normalisation mondiales, au-delà du seul secteur financier. Parallèlement, les banques ont renforcé et étoffé leurs ressources face à l'apparition de nouvelles menaces. Le Conseil de stabilité financière (CSF) a publié en octobre 2017 un rapport récapitulant les réglementations, recommandations et pratiques de contrôle existantes en matière de cybersécurité tant au plan national qu'à l'échelle internationale. Il a conclu que le secteur bancaire était le seul, dans les services financiers, pour lequel toutes ses juridictions membres avaient fait état d'au moins une réglementation, recommandation ou pratique de contrôle ; en

[4] Voir FMI (2017), *Rapport sur la stabilité financière dans le monde*, octobre. https://www.imf.org/en/Publications/GFSR/Issues/2017/09/27/global-financial-stability-report-october-2017

[5] Voir par exemple les récents rapports sur la stabilité financière publiés en Afrique du Sud, au Canada, en Inde et aux Pays-Bas, celui de la BCE et ceux du *Financial Stability Oversight Council* et de l'*Office of Financial Research* aux États-Unis.

outre, trois quarts des sondés (juridictions membres et organes internationaux confondus) avaient déclaré qu'ils comptaient publier des documents « dans l'année ». En outre, les juridictions membres du CSF ont indiqué qu'elles s'appuyaient sur un petit corpus de recommandations ou de normes nationales ou internationales existantes, provenant d'autorités publiques ou d'organismes privés, pour élaborer leurs dispositifs de réglementation et de contrôle de la cybersécurité (il s'agissait essentiellement des recommandations conjointes sur la résilience cybernétique des infrastructures de marché financier publiées en juin 2016 par le Comité sur les paiements et les infrastructures de marché (CPIM) et l'Organisation internationale des commissions de valeurs (OICV), du dispositif de cybersécurité du NIST[6] aux États-Unis et de la série de normes ISO 27000). Parmi les autres initiatives internationales mentionnées par les juridictions membres figuraient les éléments fondamentaux de cybersécurité pour le secteur financier[7] du G7 et, s'agissant de l'Union européenne, du Plan d'action pour les fintechs de la Commission européenne, qui invite les autorités de contrôle européennes à réfléchir à la publication de recommandations pour assurer leur convergence en matière de risques TIC[8].

Cependant, même si les banques et les autorités réglementaires s'accordent à dire que les recommandations existantes peuvent servir de base à des principes de haut niveau visant au renforcement de la cybersécurité, les acteurs du secteur déplorent souvent de devoir consacrer trop de temps et de ressources à « cocher des cases » ou effectuer des exercices de conformité au regard de réglementations parfois redondantes ou contradictoires, plutôt que de travailler effectivement à la constitution et à l'entretien de leurs capacités de résilience[9]. Du point de vue du secteur officiel, la diversité des dispositifs institutionnels nationaux en termes de cybersécurité, de même que le degré variable de maturité des initiatives sectorielles, posent problème dans la conception de politiques efficaces, sachant que la solidité du système s'arrête à son maillon le plus faible.

Q3. Existe-t-il des exemples concrets de fragmentation réglementaire (géographique, sectorielle) où l'addition des exigences aboutit en fait à un affaiblissement de la position des institutions ? Comment pourrait-on y remédier ?

De la cybersécurité à la résilience opérationnelle

À mesure que les attaques cybernétiques ont augmenté en nombre, en sophistication et en impact disruptif, le secteur financier a de son côté gagné en maturité, tirant les enseignements des expériences vécues. Parmi les principales leçons faisant consensus et guidant l'action actuelle des banques et des autorités réglementaires, citons les suivantes :

- Dans la grande majorité des cas, la réussite d'une cyberattaque est due à l'inobservation de principes de base d'hygiène cybernétique. Autrement dit, des investissements massifs dans des ressources et technologies de haut niveau ne garantissent pas nécessairement une meilleure protection s'il existe encore des failles dans la gestion des mots de passe, accès et correctifs. Les cybercriminels étudient les systèmes qu'ils ciblent à la recherche de fragilités potentielles, à commencer par les brèches les plus évidentes (souvent, en envoyant un email de hameçonnage

[6] National Institute of Standards and Technology.

[7] Voir G7, *Fundamental Elements of Cybersecurity for the Financial Sector,* octobre 2016.

[8] L'Autorité européenne des marchés financiers (ESMA), l'Autorité bancaire européenne (EBA) et l'Autorité européenne des assurances et des pensions professionnelles (EIOPA), collectivement regroupées sous le nom d'« autorités de contrôle européennes ».

[9] Voir FSI Insight n °2 sur les approches réglementaires du renforcement des dispositifs bancaires de cybersécurité, https://www.bis.org/fsi/publ/insights2.pdf, août 2017.

à un employé). Les entreprises et autorités doivent faire en sorte que les interventions de l'ensemble des employés, processus et technologies nécessaires à un fonctionnement en continu soient conformes aux principes de base de sécurité des outils et pratiques informatiques.

- En ce qui concerne les incidents cybernétiques, la question n'est pas de savoir s'ils se produiront, mais quand ils se produiront. La menace peut provenir de sources extérieures aussi bien qu'intérieures, et des failles ou défaillances peuvent passer inaperçues pendant plusieurs mois, ce qui signifie que les établissements pourraient avoir un faux sentiment de sécurité les rendant en fin de compte plus vulnérables. Des entreprises pourraient même être les victimes collatérales d'attaques non dirigées contre elles (voir par exemple l'infection de Maersk par NotPetya) ; elles doivent donc se préparer à l'inattendu et prêter attention à ce qui se passe dans d'autres pays et secteurs.
- La cybersécurité a un impact à la fois opérationnel et commercial. La cybersécurité ne concerne plus seulement les technologies et systèmes d'information et de communication. Chaque fonction, service ou produit conçu et exploité par les entreprises présente un profil de cyberrisque particulier qui, à son tour, a un certain type d'impact sur l'activité. Aucune mesure en matière de fonds propres ou de liquidité ne peut garantir une protection si une fonction ou un service critique est compromis, perturbant ou interrompant des activités essentielles. En conséquence, la dimension cybernétique devrait non seulement faire partie des stratégies opérationnelles décidées au niveau des conseils d'administration, mais également être intégrée aux activités quotidiennes des entreprises, afin que les processus, services et produits soient conçus pour être sûrs.

Ces constatations simples ont conduit les acteurs du secteur privé et du secteur officiel à aborder la gestion du cyberrisque dans une perspective stratégique et opérationnelle élargie, plutôt que de la limiter à une discipline purement technique, centrée sur la sécurité[10]. Dans le cadre d'une vision globale, la dimension cybernétique peut être considérée comme un élément important de la résilience opérationnelle. Comme il faut s'attendre à ce qu'une faille apparaisse quel que soit le niveau de protection, la gestion des risques ne devrait pas seulement consister à vérifier que les contrôles et mécanismes d'atténuation des risques sont en place, mais également porter sur la manière de réagir à cette faille, de la surmonter et d'en tirer les leçons. Ce type de plan d'urgence et de poursuite des activités implique que les systèmes d'une entreprise soient présentés en fonction de leur degré d'importance, et qu'un degré d'appétit pour le risque soit défini pour les actifs et activités de l'entreprise, au regard des paramètres pertinents. Une telle approche s'applique aussi aux perturbations d'activité dont l'origine n'est pas une cyberattaque (par exemple, une catastrophe naturelle ou la défaillance d'un prestataire de services tiers essentiel à la banque).

Travaux du Comité de Bâle sur la résilience opérationnelle

Dans ce contexte, le Comité de Bâle sur le contrôle bancaire a reconnu les mérites d'une approche de la résilience opérationnelle dépassant la gestion du risque opérationnel et les exigences minimales de fonds propres, et établi début 2018 un Groupe de travail sur la résilience opérationnelle (ORG) dans l'intention de contribuer, entre autres, à l'effort international sur la gestion du cyberrisque.

[10] Par exemple, la Banque d'Angleterre a publié un document de discussion visant à « entamer un dialogue avec le secteur des services financiers en vue d'assurer un changement progressif dans la résilience opérationnelle des entreprises et des IMF ». Voir « Building the UK financial sector operational resilience », juillet 2018, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A

La première tâche de l'ORG a été d'identifier l'étendue des pratiques existantes en matière de résilience cybernétique, et d'évaluer les lacunes et les mesures susceptibles de renforcer à l'avenir la résilience opérationnelle des banques au sens large. En lançant cette initiative, le Comité de Bâle a reconnu la nécessité que l'ORG tienne dûment compte des divers dispositifs nationaux et internationaux existants ou en cours d'élaboration. La participation des membres de l'ORG aux groupes de travail pertinents du CPIM, du CSF et des autorités régionales, ainsi qu'aux initiatives du G7 sur la cybersécurité, témoigne de l'importance accordée par le Comité à une surveillance étroite et à une coordination internationale à travers le secteur financier. Au seul niveau du Comité de Bâle, des Principes liés à la gestion des risques pour les activités bancaires électroniques[11] et du risque opérationnel[12] ont été publiés dès 2003 et 2011. Le Comité a en outre publié, conjointement avec l'OICV et l'AICA (dans le cadre de l'Instance conjointe), des recommandations sur la sous-traitance dans les services financiers en 2005[13], et des principes de haut niveau pour la continuité opérationnelle en 2006[14]. Certains aspects de ces recommandations et principes de haut niveau demeurent valables et devraient servir de base aux mesures à venir, tandis que d'autres, obsolètes ou redondants, pourraient être revisités. De manière générale, la majeure partie des initiatives internationales passées et actuelles traitent des sujets suivants, qui couvrent les principales préoccupations des autorités de contrôle en matière de résilience opérationnelle :

- Dispositifs de gouvernance, y compris les rôles du Conseil d'administration et du Responsable de la sécurité des systèmes d'information ;
- Analyse et évaluation des cyberrisques ;
- Sécurité de l'information, confidentialité comprise ;
- Contrôles de sécurité et prévention des incidents ;
- Compétences, formation et sensibilisation au sens large dans le domaine de la gestion et du traitement des risques ;
- Suivi, tests et/ou audit des contrôles, y compris au moyen de tests par *red teaming* ou *purple teaming* ;
- Réaction aux incidents et reprise après incident pour comprendre, gérer, contenir les incidents et les surmonter ;
- Communication et partage d'informations avec les parties prenantes intérieures et extérieures, publiques et privées, à travers les secteurs et les pays ;
- Relations de sous-traitance et, plus généralement, dépendance à l'égard de tierces parties : le périmètre d'intérêt des autorités réglementaires du secteur financier s'est agrandi, et l'utilisation croissante des services d'informatique en nuage signifie que ce périmètre est désormais partagé ; et
- Apprentissage continu en vue de réévaluer, tester et améliorer la résilience de manière permanente, y compris au moyen d'exercices et de coopération public-privé.

En ce qui concerne l'évaluation de l'étendue des pratiques existantes, les autorités de contrôle partagent leurs expériences et connaissances directes de façon à permettre une compréhension plus concrète et spécifique des principales tendances, avancées et lacunes de la résilience cybernétique dans

11 Comité de Bâle sur le contrôle bancaire, *Principles for Electronic Banking*, juillet 2003, www.bis.org/publ/bcbs98.pdf

12 Comité de Bâle sur le contrôle bancaire, *Principles for the Sound Management of Operational Risk*, juillet 2011, www.bis.org/publ/bcbs195.pdf

13 Instance conjointe, février 2005, https://www.bis.org/publ/joint12.pdf

14 Instance conjointe, août 2006, https://www.bis.org/publ/joint17.pdf

le secteur bancaire. Le Comité de Bâle sur le contrôle bancaire s'engage aussi à maintenir un dialogue constant avec un vaste ensemble de parties prenantes, y compris au-delà du secteur bancaire, de manière à ce que ses travaux puissent concourir à des mesures de politique publique visant à renforcer la résilience opérationnelle, au sens large, des banques dans les années à venir.

Q4. Quels paramètres ou indicateurs pourraient être utilisés par les banques dans l'évaluation et la comparaison des niveaux de résilience opérationnelle de leurs prestataires de services tiers, et par les autorités de contrôle dans l'évaluation et la comparaison des banques ?

Q5. Quelles pratiques ont été jugées efficaces pour l'élaboration et la mise en œuvre d'un dispositif solide de résilience opérationnelle ? Quelles sont certaines des pratiques émergentes dans ce domaine ?

Q6. De quelle manière peut-on améliorer l'efficacité du partage d'informations entre banques et autorités réglementaires à travers les secteurs et les pays ?

Q6. Quelle pourrait être la meilleure manière de relever le défi des compétences cybernétiques auquel font face les organisations ?

Q7. Quels sont les enjeux pratiques de l'interaction avec les prestataires de services tiers ? Quels sont les difficultés rencontrées par les tierces parties dans le respect des exigences bancaires existantes ?

Q8. Existe-t-il des problèmes de mise en œuvre liés aux différences structurelles et régionales qui justifieraient un examen plus approfondi par le Comité de Bâle ? Dans quel domaine la normalisation apporterait-elle le plus d'avantages ?