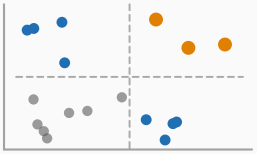
Risque opérationnel et résilience

Chapitre 8 : La cyber-résilience — panorama des pratiques



Jaouad Madkour

Faculté d'Économie et de Gestion de Tanger · 30 août 2026

Plan du chapitre

Avant de commencer

Pourquoi un rapport dédié

La cyber-résilience

Gérer, tester, répondre

Le partage d'information

Interconnexions et tiers

Synthèse

Avant de commencer

Pourquoi ce chapitre

Pourquoi ce chapitre ?

Après la gestion intégrée des risques (chapitre 7), le cours aborde une catégorie particulière du risque opérationnel — le risque cyber — devenue si centrale qu'elle a fait l'objet d'un rapport dédié du Comité de Bâle en 2018. Ce chapitre synthétise les pratiques observées, à travers le monde, en matière de gouvernance, de gestion, de test et de partage d'information sur la cyber-résilience.

Pourquoi un rapport dédié

Un périmètre élargi par la numérisation

La cyber-résilience selon le FSB

Le Comité de Bâle retient la définition du Conseil de stabilité financière (FSB) : la cyber-résilience est la capacité d'une organisation à poursuivre sa mission en anticipant et en s'adaptant aux cybermenaces, et en résistant, contenant et se rétablissant rapidement des incidents cyber. Une distinction est établie entre la gestion du **risque cyber** (vulnérabilités et menaces spécifiques) et la gestion du **risque informatique** au sens large, dont le périmètre dépasse ce rapport.

Un périmètre de risque qui s'étend au-delà du périmètre de l'organisation

L'automatisation croissante, le recours généralisé aux prestataires tiers et l'essor de l'informatique en nuage élargissent la surface d'attaque accessible aux cyber-adversaires et rendent le périmètre de la supervision partagé entre l'institution régulée et ses fournisseurs. Ce constat, posé en 2018 par le G20 puis approfondi par le Comité de Bâle, structure l'ensemble du rapport : gouvernance, gestion du risque, communication de l'information, et interconnexions avec les tiers.

La cyber-résilience

Stratégie attendue, mais rarement imposée

Un attendu de gouvernance plutôt qu'une obligation uniforme

La plupart des régulateurs n'imposent pas formellement l'adoption d'une stratégie de cybersécurité autonome, mais tous attendent des institutions régulées qu'elles disposent d'une stratégie de sécurité de l'information approuvée par le conseil d'administration, sous la responsabilité globale de la supervision technologique de ce dernier. Trois approches réglementaires coexistent : l'autorité impose des exigences sectorielles directement ; les établissements élaborent leur propre stratégie évaluée par le superviseur ; ou le superviseur vérifie simplement l'existence d'une stratégie informatique assortie de dispositions de sécurité.

Étude de cas 1 — les cadres réglementaires australien, allemand et américain

Trois initiatives illustrent la diversité des approches : la norme prudentielle australienne CPS 234 impose une gouvernance claire des rôles de sécurité de l'information et une notification obligatoire des incidents matériels à l'APRA ; les circulaires allemandes MaRisk et BAIT détaillent la stratégie et la gouvernance informatiques, la gestion des risques d'information, la gestion des accès et l'externalisation ; les régulateurs américains (Réserve fédérale, OCC, FDIC) ont proposé une réglementation cyber dédiée aux grandes institutions financières, couvrant la gouvernance du risque cyber, la gestion des dépendances internes et externes, et la réponse aux incidents.

Étude de cas 2 — le rattachement hiérarchique du RSSI

Le modèle des trois lignes de défense place typiquement le responsable de la sécurité de l'information (RSSI) sous l'autorité du directeur des risques (CRO) ou du directeur des systèmes d'information (CIO). Une tendance émergente considère toutefois ce rattachement au CRO comme sous-optimal : les deux fonctions ont des priorités potentiellement contradictoires, le CRO privilégiant la conformité quand le RSSI cherche à concilier innovation technologique et sécurité. Plusieurs grandes banques ont donc restructuré la fonction pour faire remonter le RSSI directement au directeur général ou au conseil d'administration.

Une compétence humaine autant que technique

La plupart des régulateurs encouragent le développement d'une culture commune de sensibilisation au risque cyber, condition d'une gestion efficace. Certaines juridictions imposent une formation de sensibilisation à chaque étape du parcours d'un salarié, du recrutement au départ, et des clauses de confidentialité assorties de vérifications d'antécédents pour limiter les menaces internes.

Étude de cas 3 — les cadres de formation professionnelle et de certification

Le Japon (FISC, 1984) et la Corée du Sud (FSI, 2015) illustrent des partenariats public-privé anciens pour la formation des professionnels de la cybersécurité, tandis que la Banque d'Angleterre (accréditation CBEST) et l'Autorité monétaire de Singapour imposent des programmes de formation dédiés au conseil d'administration lui-même — reconnaissant que la gouvernance cyber ne peut se réduire à la seule fonction technique.

Gérer, tester, répondre

Des pratiques de supervision alignées sur les standards de l'industrie

Les spécialistes des risques s'appuient sur des preuves documentaires, des inspections physiques, des rapports d'incidents et des enquêtes pour évaluer l'adéquation des contrôles, en cohérence avec des référentiels tels que COBIT et NIST. La cartographie et la classification des services d'affaires critiques constituent un préalable à tout dispositif de test et d'assurance robuste.

Un cadre paneuropéen de tests d'intrusion ciblés

La Banque centrale européenne a publié en mai 2018 le cadre européen TIBER-EU (Threat Intelligence-based Ethical Red Teaming), premier dispositif transfrontalier de tests d'intrusion ciblés et réalistes contre les institutions financières. Ces tests, réalisés par des prestataires spécialisés en renseignement de la menace, ne donnent pas lieu à un résultat pass/fail mais fournissent à l'entité testée une évaluation de ses forces et faiblesses pour progresser en maturité cyber.

Étude de cas 4 — l'exercice « Resilient Shield »

En 2015, le Royaume-Uni et les États-Unis ont mené un exercice conjoint public-privé, « Resilient Shield », destiné à renforcer la coordination et la compréhension mutuelle des processus de partage d'information et de réponse aux incidents entre gouvernements et secteur financier. L'exercice ne testait ni des firmes individuelles ni les systèmes financiers eux-mêmes, mais les mécanismes de communication et de coordination entre autorités.

Des métriques de résilience encore peu matures

Des indicateurs rétrospectifs à compléter par des indicateurs prospectifs

La plupart des juridictions se concentrent encore sur des indicateurs rétrospectifs (incidents déjà survenus, résultats de tests passés), pertinents lorsque l'environnement est stable — ce qui n'est pas le cas face à des adversaires cyber qui adaptent continuellement leurs tactiques. Un indicateur emblématique, le vieillissement des correctifs de sécurité (patch ageing), illustre la nécessité de développer des indicateurs prospectifs de résilience, encore peu harmonisés d'une juridiction à l'autre.

Le partage d’information

Cinq catégories de flux d'information

Entre banques, des banques vers les régulateurs, entre régulateurs, des régulateurs vers les banques, avec les agences de sécurité

Le rapport distingue cinq types de partage d'information de cybersécurité : entre banques, des banques vers leurs régulateurs, entre régulateurs, des régulateurs vers les banques, et avec les agences de sécurité nationales. Le partage entre banques et avec les agences de sécurité est le plus répandu ; le partage entre régulateurs reste le moins observé, en partie du fait de sa nature souvent informelle et bilatérale.

Le partage entre banques : le modèle FS-ISAC

Étude de cas 5 — le Financial Services Information Sharing and Analysis Center

Le FS-ISAC, organisation à but non lucratif créée en 1999 aux États-Unis, collecte et diffuse en temps réel, via son système propriétaire CINS, des alertes de vulnérabilités et de menaces cyber entre ses membres — banques, assureurs, régulateurs financiers. Les informations partagées sont anonymisées pour ne jamais permettre de remonter à la source, un principe de confidentialité jugé essentiel pour encourager la participation volontaire des membres.

Le partage entre régulateurs : un exemple bilatéral

Étude de cas 6 — l'accord bilatéral Hong Kong–Singapour

La Hong Kong Monetary Authority et l'Autorité monétaire de Singapour ont établi en 2018 un cadre bilatéral de partage d'information de cybersécurité fondé sur cinq principes : rapidité (partage sous 24 heures en cas de risque de propagation transfrontalière), caractère volontaire (sans obligation légale), confidentialité, efficacité (partage non limité aux seules institutions présentes dans les deux juridictions) et usage d'un protocole de classification standardisé (Traffic Light Protocol) et d'une taxonomie commune (STIX).

Étude de cas 7 — les équipes de réponse aux incidents dans l'UE

La directive européenne NIS (Network and Information Security, effective depuis mai 2018) impose l'établissement, dans chaque État membre, d'une ou plusieurs équipes de réponse aux incidents de sécurité informatique (CSIRT), reliées par un réseau européen dédié. La notification d'incidents à ces CSIRT est obligatoire pour les opérateurs de services essentiels, catégorie qui inclut certaines banques selon les juridictions.

Interconnexions et tiers

Un périmètre élargi de la notion de « tiers »

Externalisation, produits standards et contreparties interconnectées

Pour ce rapport, la notion de « tiers » couvre l'ensemble des formes d'externalisation (y compris l'informatique en nuage), les produits et services standardisés habituellement non considérés comme de l'externalisation (alimentation électrique, télécommunications), et les contreparties interconnectées telles que les infrastructures de marché (systèmes de paiement et de règlement, plateformes de négociation, dépositaires centraux).

La gouvernance des interconnexions tierces

Un cadre contractuel et un droit d'audit largement attendus

Les régulateurs attendent des institutions qu'elles se dotent d'un cadre d'externalisation approuvé par le conseil, incluant l'analyse préalable des risques (stratégique, de conformité, de sécurité, de continuité d'activité, de dépendance au prestataire, de concentration) et des clauses contractuelles garantissant un droit d'inspection et d'audit — parfois étendu directement aux autorités de supervision, comme en France, en Suisse et à Singapour.

Étude de cas 8 — le régime luxembourgeois des prestataires de services financiers

Le Luxembourg soumet les « professionnels du secteur financier » (PSF) fournissant des services spécialisés aux institutions financières au même régime d'agrément et de supervision continue que les institutions elles-mêmes. La circulaire CSSF 17/654 impose des obligations spécifiques pour l'externalisation vers l'informatique en nuage, incluant la désignation d'un responsable des ressources en nuage et, selon la matérialité de l'activité externalisée, une autorisation ou une simple notification préalable.

Étude de cas 9 — les sommets réglementaires organisés par les fournisseurs de cloud

Certains grands fournisseurs de services en nuage organisent des « sommets réglementaires » réunissant plusieurs autorités de supervision pour discuter collectivement des risques liés au cloud, dans un format proche du modèle du « collège de superviseurs » habituellement réservé aux grandes institutions bancaires internationales — une réponse pragmatique à la difficulté, pour un régulateur national isolé, d'exercer une supervision effective sur un fournisseur mondial.

Synthèse

Ce qu'il faut retenir

Synthèse du chapitre

La cyber-résilience prolonge le risque opérationnel dans un domaine où la surface d'attaque s'étend au-delà du périmètre de l'organisation, sous l'effet de la numérisation et de l'externalisation. Les pratiques observées convergent sur l'importance d'une gouvernance portée par le conseil d'administration, d'un positionnement indépendant du RSSI, de tests d'intrusion réalistes tels que TIBER-EU, et d'un partage d'information structuré autour de cinq catégories de flux — dont le modèle FS-ISAC illustre les bénéfices d'une plateforme sectorielle de confiance. Les interconnexions avec les tiers, en particulier les fournisseurs de cloud, imposent un cadre contractuel et un droit d'audit dont l'application reste hétérogène d'une juridiction à l'autre — un chantier encore en construction que le chapitre suivant illustrera à travers le cas Equifax.