# Quelle gouvernance pour un pilotage holistique et efficient de la cyber-résilience ?

Dans un environnement en constante mutation, les établissements sont confrontés à des risques émergents au premier rang desquels le risque cyber au cœur des préoccupations ; la cyber-résilience est un enjeu majeur pour le secteur financier, elle impose la révision régulière des stratégies de résilience pour la continuité d'exploitation et protéger les actifs stratégiques face au risque cyber.

**Nicolas Vetriak,**
**Président Fondateur**

## SUR L'AUTEUR

Fondateur de Novaminds, Nicolas est ingénieur et titulaire d'un MBA en finance internationale, diplômé de l'ENPC. Il dispose de vingt ans d'expérience dans le secteur financier, d'abord dans des fonctions à responsabilités opérationnelles en sécurité, résilience et *risk management* puis dans le conseil en stratégie et organisation auprès des principaux établissements, avec la donnée au cœur de ses interventions.

## LES POINTS CLÉS

La cyber-résilience est un enjeu clé pour le secteur financier pour la continuité d'exploitation et la protection.

- Une gouvernance holistique associant tous les acteurs, avec le métier au cœur des réflexions.
- Un dispositif unifié et transversal piloté par la direction selon les enjeux business et l'appétence aux risques.
- Une approche globale intégrant l'*outsourcing* et plus largement l'ensemble des partenaires.
- Une cyber-résilience agile avec une recherche permanente de l'efficacité à la hauteur des investissements réalisés.
- L'adoption d'un langage commun pour fédérer tous les acteurs.

Les cyber-attaques se jouent des frontières, elles touchent toutes les organisations et les conséquences peuvent être multiples avec des impacts localisés ou généralisés : indisponibilité du système d'information, violation de données, corruption de données, fraude, chantage, rançongiciel…

Le risque cyber constitue un risque systémique pouvant se propager au-delà d'une organisation, à l'ensemble du secteur financier du fait des fortes interconnexions ; l'intensité et l'échelle de la propagation varient selon la menace et la vulnérabilité des établissements.

Le cadre légal et réglementaire est en constante évolution pour appréhender ce risque en mutation permanente. De nouvelles réglementations ont vu le jour notamment sur le plan européen : les textes de l'Autorité bancaire européenne sur les risques ICT, le *cloud*, l'*outsourcing*, ou encore le Règlement européen sur la protection des données à caractère personnel (RGPD), la directive Network and Information Security... L'European Systemic Risk Board a publié récemment un rapport sur le risque systémique cyber.

Les établissements ont de ce fait lancé de vastes programmes visant à renforcer leur cyber-résilience.

### Vers une gouvernance holistique de la cyber-résilience ?

Un des enjeux essentiels se situe sur le plan organisationnel : les établissements doivent articuler les dispositifs existants (sécurité, sûreté continuité, risques, contrôle, conformité, data management…) pour bâtir le modèle unifié de cyber-résilience.

Le risque cyber est un risque transversal qui présente de fortes porosités avec d'autres risques opérationnels ayant trait à la fraude, aux dysfonctionnements de l'activité, des systèmes, des processus… Cela complexifie l'unité du schéma organisationnel et par là même sa constitution.

> « La cyber-résilience se doit dorénavant d'être agile et déployée selon une approche par les risques avec une recherche permanente de l'efficacité à la hauteur des investissements réalisés »

Une des principales difficultés réside dans l'organisation et le positionnement de la cyber-résilience tenant compte de l'orientation et de la déclinaison opérationnelle des dispositifs sous-jacents.

Cette organisation doit concilier le juste équilibre entre d'une part, la centralisation requise pour la gouvernance, le pilotage et le contrôle à l'échelle de l'établissement ; et d'autre part la décentralisation au niveau des parties prenantes à la manœuvre pour la construction et le fonctionnement optimal du dispositif.

Pour les établissements à dimension internationale, l'organisation doit de surcroît concilier les exigences groupe et locales et permettre la consolidation aux différents niveaux de l'organisation - selon des axes fonctionnels et géographiques - pour permettre un pilotage adéquat et le reporting à la gouvernance et aux autorités.

La cyber-résilience doit appréhender les activités de l'entreprise dans leur globalité y compris l'*outsourcing*. Cela suppose une parfaite connaissance des chaînes de traitement, de leurs interdépendances et des services externalisés dont il convient de veiller au parfait alignement dans le dispositif de cyber-résilience. Outre le nécessaire respect des exigences afférentes à l'*outsourcing*, l'externalisation doit être encadrée, contrôlée et régulièrement révisée pour s'assurer de (i) sa bonne insertion dans le dispositif de cyber-résilience et (ii) de son opérationnalité.

### La nécessité d'un pilotage par la direction selon les enjeux business et l'appétence aux risques

La direction et les métiers doivent être positionnés au cœur de l'organisation et des réflexions pour la cyber-résilience, afin de lutter contre les altérations durables du fonctionnement et de la création de valeur, outre l'image.

De ce fait, l'organisation adoptée doit être en mesure - de par son positionnement et ses moyens - d'appréhender les enjeux des métiers, d'identifier - tout en les priorisant - les actifs stratégiques à préserver en toute circonstance.

Mais l'organisation pour la cyber-résilience repose sur les dispositifs existants le plus souvent organisés en « silo », avec peu de transversalité.

Une dimension supplémentaire vient donc s'ajouter, à savoir l'alignement des parties prenantes autour des enjeux business, d'un langage commun pour une réponse coordonnée pour la cyber-résilience.

L'objectif est double : d'une part déployer un dispositif harmonisé, proportionné et agile pour la cyber-résilience et, d'autre part, permettre un pilotage transversal par la direction par une communication adaptée avec les indicateurs clés ; ces indicateurs permettent à la fois une prise de décision éclairée des dirigeants selon l'appétence aux risques, de s'assurer de l'efficacité du dispositif, et d'arbitrer les solutions à déployer ou à faire évoluer.

### Comment concilier les exigences, l'efficacité et le ROI pour la cyber-résilience ?

Alors que les investissements pour la sécurité, la protection de la donnée et la conformité ont connu une forte inflation ces dernières années, il s'agit désormais d'organiser la cyber-résilience dans le contexte de renforcement permanent des exigences des autorités et dans le même temps, de rationalisation des coûts.

La réponse n'est pas de créer *ex nihilo* une nouvelle filière (supplémentaire) mais bel et bien de capitaliser sur l'existant et les programmes en cours, cela sera clé pour la recherche de l'optimisation et de l'efficacité. Cela passe également par la mutualisation entre les dispositifs existants. Cela est aussi l'opportunité de requestionner plus globalement les organisations et missions de ces dispositifs, l'alignement des objectifs, le dimensionnement, les adhérences et les synergies possibles.

L'efficacité passe également par l'intégration en amont des besoins métiers et des exigences pour des solutions pragmatiques, rationnelles et optimales ; cet alignement est clé pour éviter toute rupture dans les chaînes de traitement ; le non-alignement outre l'inefficacité, pouvant être source de risque par la non-couverture de certaines menaces.

Les lignes de défense sont également un levier important en tant que garant de l'efficacité du dispositif dans son ensemble au regard des besoins et des exigences. Mais ces lignes de défense doivent être organisées et dimensionnées de manière pragmatique et rationnelle en veillant à leur indépendance, sans alourdir outre mesure le poids du contrôle.

L'efficacité passe aussi par un apport d'expertises à tous les échelons de l'organisation avec des compétences régulièrement actualisées à l'instar du dispositif de cyber-résilience selon l'évolution des menaces.

La cyber-résilience se doit dorénavant d'être agile et déployée selon une approche par les risques avec une recherche permanente de l'efficacité à la hauteur des investissements réalisés. ◆