

Notes de synthèse

Vol. 5, Num. 6
2025

Cybersécurité et lutte contre la fraude: le rôle des centres de fusion dans la gestion des risques

Tom Verstichel, étudiant à la maîtrise en criminologie

Introduction

Dans un environnement financier de plus en plus numérisé, les institutions bancaires et financières sont confrontées à une menace croissante de fraudes et de cyberattaques sophistiquées. L'essor du numérique, la multiplication des transactions en ligne et l'évolution des techniques de cybercriminalité exposent les établissements financiers à des risques inédits. En effet, **le secteur financier serait la cible dans 18 % des attaques cybernétiques mondiales, souvent combinées à des tentatives de fraude ciblée, reflétant une tendance croissante à la convergence des menaces** [1, 2]. Cette convergence croissante entre cybermenaces et fraude financière souligne la nécessité d'une vigilance renforcée dans le secteur. Dans ce contexte se dessine une nouvelle approche de la gestion des risques fondée sur l'intégration opérationnelle et informationnelle des dispositifs de sécurité : **les Centres de fusion sur la cyberfraude (Cyber Fraud Fusion Centers)**. À l'instar des centres de coordination interagences nés dans le domaine du contre-terrorisme, **ces structures visent à créer des ponts entre les fonctions de sécurité, de détection de fraude, de conformité et de gestion des risques** [3].

Jusqu'à récemment, la cybersécurité et la lutte contre la fraude étaient traitées comme deux disciplines distinctes, opérant dans des silos organisationnels avec des outils et des appro-

ches méthodologiques différentes. Les équipes de cybersécurité se concentraient principalement sur la protection des infrastructures informatiques, la sécurisation des transactions et la détection des intrusions, tandis que les équipes de lutte contre la fraude étaient chargées de détecter les transactions suspectes, d'analyser les comportements frauduleux et de limiter les pertes financières liées aux fraudes internes et externes. **Cette fragmentation des responsabilités a souvent conduit à un manque de coordination, retardant la détection et la réponse aux menaces combinées.**

Or, avec l'évolution des attaques, les cybercriminels exploitent désormais des techniques hybrides mêlant intrusion informatique et fraude financière. Par exemple, des attaques de type « fraude au président » (*Business Email Compromise (BEC)* en anglais) consistent à infiltrer les systèmes d'une entreprise via des techniques d'hameçonnage ou d'ingénierie sociale, avant d'amorcer des transactions frauduleuses en usurpant l'identité de dirigeants ou d'employés. Dans ces cas, une approche cloisonnée où les services de cybersécurité et de lutte contre la fraude ne communiquent pas efficacement retarde la détection et accroît les pertes financières.

Cette note de synthèse vise à explorer les modè-

modèles de collaboration entre équipes de cybersécurité et de lutte contre la fraude dans les institutions financières, en mettant en lumière : 1) Les stratégies et modèles existants, du partage d'informations aux initiatives de coopération volontaire et aux cadres de gouvernance intégrés; 2) Les défis organisationnels, réglementaires et culturels, qui freinent encore une intégration efficace des services et 3) les recommandations stratégiques visant à renforcer cette coopération, notamment par l'intégration de technologies avancées et l'optimisation des mécanismes de partage d'informations.

L'émergence des Cyber Fraud Fusion Centers dans les institutions financières

Nés dans le champ militaire et de la sécurité nationale après les attentats du 11 septembre, les centres de fusion ont été adaptés au secteur privé pour répondre à des menaces transversales. Leur finalité est claire : **transformer l'information dispersée en connaissance exploitable en temps réel** [4].

Face à cette complexification des risques, il devient impératif de renforcer la synergie entre cybersécurité et lutte contre la fraude. **Une telle collaboration permettrait une meilleure détection des menaces grâce au croisement des données issues des systèmes de cybersécurité et des outils de lutte contre la fraude, de réduire les délais de réponse aux incidents, car les équipes travaillent en réseau et partagent les informations en temps réel.** Les institutions financières peuvent aussi optimiser la gestion des risques financiers et informatiques en unifiant leurs processus et en intégrant des solutions technologiques avancées, telles que l'intelligence artificielle (IA) et l'apprentissage machine (*machine learning*).

Bien que la littérature sur la coopération interinstitutionnelle soit abondante, peu d'études se penchent sur la collaboration effective entre équipes internes de cybersécurité et de lutte contre la fraude au sein des institu-

-tions financières. Cette lacune est d'autant plus frappante que **les retours d'expérience sur les centres de fusion sur la cyberfraude montrent les bénéfices concrets d'une telle convergence.** En effet, ces centres permettent de rassembler des analystes des technologies de l'information, de la fraude, de la conformité et des risques autour d'une même structure opérationnelle [3, 5]. Toutefois, la gouvernance, le leadership transversal et l'alignement des objectifs restent des freins majeurs à cette collaboration intra-institutionnelle, encore rarement étudiée de manière approfondie dans les travaux académiques récents.

Diversité des dispositifs de gestion des risques et défis organisationnels à leur mise en œuvre

Stratégies et modèles de collaboration en cybersécurité et lutte contre la fraude

Plusieurs institutions financières ont commencé à adopter des modèles de collaboration interservices pour anticiper les menaces émergentes et limiter l'impact des attaques combinées. L'exemple des Pays-Bas, où la *Dutch Payments Association* a instauré un cadre de coopération volontaire entre les banques et les organismes de paiement, illustre **comment une coordination renforcée entre les équipes de cybersécurité et de lutte contre la fraude a permis une réduction significative des fraudes bancaires** [6]. Grâce à l'intégration de systèmes d'analyse en temps réel, les banques peuvent bloquer rapidement des transactions suspectes avant qu'elles ne causent des pertes financières. De même, aux États-Unis, **les partenariats public-privé ont montré que le partage de renseignements sur les menaces entre les institutions financières et les agences gouvernementales renforce considérablement la protection du secteur bancaire** [7].

Un autre modèle intéressant est celui de **l'appropriation croisée** qui propose **une articulation renforcée entre les opérateurs de**

marché et les contrôleurs des risques, dans le but d'anticiper plus efficacement les fraudes internes et de renforcer la sécurité des infrastructures financières [8]. Concrètement, ce modèle peut se traduire par l'intégration d'analystes en gestion des risques au sein même des équipes de négociation, leur permettant de surveiller les opérations en temps réel et de détecter rapidement toute anomalie [8]. En favorisant une circulation immédiate de l'information entre les services, cette approche réduit significativement les délais de réaction face aux menaces.

Dans ces modèles, les outils de détection avancés, tels que **les logiciels d'analyse comportementale et les systèmes basés sur l'apprentissage machine, sont devenus essentiels**. Ils permettent non seulement d'identifier des comportements anormaux, mais aussi de prévenir les fraudes par usurpation d'identité, qui sont en forte augmentation dans le secteur bancaire.

L'intégration des enjeux de gouvernance et de régulation

Si la collaboration entre équipes de cybersécurité et de lutte contre la fraude s'est renforcée ces dernières années, **elle doit encore être pleinement intégrée aux cadres de gouvernance des institutions financières** [9]. En effet, les banques doivent s'aligner sur les normes internationales telles qu'ISO 27001, le Règlement Général sur la Protection des Données (RGPD) et la loi Sarbanes-Oxley pour assurer une protection optimale des données. Les normes ISO 27001, le RGPD européen et la loi américaine Sarbanes-Oxley (SOX) constituent des cadres clés en matière de sécurité et de conformité. L'ISO 27001 définit les exigences pour sécuriser les systèmes d'information, tandis que le RGPD encadre la protection des données personnelles au sein de l'Union européenne. La loi SOX, quant à elle, impose des règles strictes de transparence financière et de sécurité des systèmes d'information. Ces dispositifs convergent vers un objectif commun : renforcer

la gouvernance des données et la résilience des institutions face aux risques technologiques et juridiques.

Toutefois, ces réglementations, bien qu'essentielles pour la sécurité des transactions, peuvent parfois entraver la fluidité des collaborations. En effet, **les contraintes juridiques imposées par les lois sur la confidentialité comme le RGPD ne limitent pas seulement le partage d'informations entre institutions financières, mais peuvent également freiner les échanges de données sensibles au sein même d'une organisation**. Cela concerne notamment les interactions entre les départements de cybersécurité, de conformité et de lutte contre la fraude, qui doivent souvent composer avec des règles d'accès différenciées et des cloisonnements internes, réduisant ainsi l'efficacité des stratégies de détection et de réponse coordonnées.

Un levier prometteur pour surmonter les obstacles liés au cloisonnement réglementaire réside dans **l'adoption des technologies de conformité automatisée, également connues sous le nom de RegTech**. Ces solutions permettent aux institutions financières de **gérer plus efficacement leurs obligations réglementaires tout en sécurisant les échanges d'informations sensibles entre services** [10]. Concrètement, les outils RegTech offrent la possibilité de tracer les accès aux données sensibles, de définir des autorisations différenciées selon les rôles, d'automatiser les comptes rendus de conformité (notamment liés au RGPD ou à la loi Sarbanes-Oxley), ou encore de suivre en temps réel les changements législatifs grâce à des moteurs de règles adaptatifs. En facilitant à la fois la conformité et la collaboration, ces technologies apportent une réponse opérationnelle aux défis posés par le partage d'informations dans un environnement réglementaire complexe [10]. La RegTech joue un rôle stratégique dans la transformation des modèles de gouvernance des institutions financières, en renforçant la transparence, l'agilité et la maîtrise des risques [10].

Défis organisationnels, réglementaires et culturels de l'intégration des services

L'un des principaux obstacles à l'intégration des services de cybersécurité et de lutte contre la fraude est la fragmentation organisationnelle. Les équipes de cybersécurité et celles de lutte contre la fraude travaillent souvent de manière isolée, avec peu de communication et des méthodologies différentes. Plusieurs facteurs limitent la collaboration, notamment des protocoles de signalement différents et des outils technologiques non interopérables [11]. **Cette absence de coordination entraîne des délais supplémentaires dans la gestion des incidents et expose les institutions à des pertes financières plus importantes.**

Un exemple de collaboration entre la cybersécurité et la lutte contre les fraude réside dans la prévention des menaces internes qui repose sur une approche multidimensionnelle, combinant des protocoles stricts de cybersécurité, une surveillance continue des accès et une formation des employés pour éviter les erreurs pouvant compromettre la sécurité des données [12]. Notamment, **les fraudes internes dans le secteur bancaire sont souvent facilitées par des accès non contrôlés aux informations sensibles, un manque de suivi des transactions suspectes et des politiques de cybersécurité peu adaptées aux risques internes** [12]. L'intégration de systèmes d'information centralisés et d'outils de gestion des incidents interconnectés est une solution clé pour surmonter ces obstacles. Effectivement, la mise en place de plateformes communes de détection des fraudes et des cyberattaques permettrait d'optimiser les ressources et d'accélérer la réaction face aux menaces [13].

Conclusion

La convergence entre cybersécurité et lutte contre la fraude est devenue un impératif stratégique pour les institutions financières, tant les menaces se multiplient et se sophistiquent. Les cybercriminels exploitent désormais des techniques hybrides, mêlant intrusions informatiques, ingénierie sociale et fraudes financières complexes. Face à cette évolution, **la séparation traditionnelle entre les services de cybersécurité et ceux chargés de la fraude n'est plus viable.** Une approche cloisonnée limite la rapidité et l'efficacité des réponses aux incidents, tandis qu'une collaboration interservices structurée permet de détecter et de contenir plus rapidement les menaces.

Plusieurs modèles de coopération, comme les partages d'informations interbancaires, les partenariats public-privé et l'intégration des systèmes de détection permettent d'améliorer significativement la sécurité des institutions financières. Pourtant, **de nombreux défis persistent, notamment les résistances organisationnelles, les barrières réglementaires et la fragmentation des outils technologiques.** C'est pourquoi l'interopérabilité des solutions, le partage sécurisé des renseignements et la formation continue des équipes apparaissent comme des leviers essentiels pour surmonter ces freins à la coopération. En effet, l'interopérabilité, telle que décrite dans le *Cyber Fusion Center Guide* [14], ne se limite pas à la simple compatibilité technique entre outils : elle implique également une harmonisation des processus, une architecture ouverte capable de faire dialoguer différents systèmes, ainsi qu'un alignement des flux de données entre services internes. Cette interopérabilité organisationnelle suppose des protocoles normalisés, un langage commun entre analystes et une plateforme centralisée de visualisation et de corrélation des alertes. Dans cette optique, **les centres de fusion favorisent une réponse collaborative aux menaces, en éliminant les silos techniques et humains et en renforçant la synergie entre cybersécurité**

et lutte contre la fraude [14].

L'objectif principal pour les banques et institutions financières est donc de **structurer une gouvernance intégrée, où cybersécurité et lutte contre la fraude ne sont plus considérées comme des entités indépendantes, mais comme des composantes essentielles d'un même système de gestion des risques**. Cette transformation ne peut être pleinement efficace sans l'adoption de technologies avancées, le développement de cadres de coopération formalisés et une évolution des politiques réglementaires permettant une flexibilité accrue dans le traitement des menaces financières et cybernétiques.

Recommandations

Développer des outils technologiques interconnectés et basés sur l'IA

L'un des défis majeurs de la collaboration entre cybersécurité et lutte contre la fraude réside dans l'hétérogénéité des outils et systèmes utilisés par ces deux domaines. **La mise en place de plateformes interconnectées et l'adoption de solutions basées sur l'intelligence artificielle et l'apprentissage machine permettraient d'améliorer la détection des menaces en temps réel.**

- **Développer des systèmes de surveillance intégrés**, combinant les données issues des équipes de cybersécurité (détection d'intrusion, surveillance des réseaux) avec celles des analystes en fraude (analyse comportementale, transactions suspectes).
- **Renforcer l'utilisation de l'IA pour identifier des modèles de fraude complexes** et limiter les faux positifs.
- **Automatiser les processus d'alerte et de réponse aux incidents**, afin de garantir une action rapide et coordonnée des équipes de sécurité et de lutte contre la fraude.

Prioriser le partage d'informations et renforcer les partenariats public-privé

Le partage d'informations est un élément fondamental pour anticiper et répondre efficacement aux cyberattaques et aux fraudes. Toutefois, les banques sont souvent réticentes à partager des données sensibles, notamment en raison de contraintes réglementaires et de la crainte de nuire à leur réputation en cas d'incident majeur.

- **Faciliter les accords de coopération entre institutions financières en mettant en place des cadres sécurisés pour l'échange d'informations sensibles**, conformes aux normes de protection des données.
- **Développer des partenariats publics-privés** avec les agences gouvernementales et les entreprises spécialisées en cybersécurité afin d'accéder à des renseignements enrichis sur les menaces émergentes.

Intégrer les équipes et mutualiser les outils pour une réponse unifiée aux menaces hybrides

Face à la convergence croissante des cybermenaces et des fraudes, il ne suffit plus de coordonner les efforts entre équipes, il faut également penser à une **intégration organisationnelle et technologique plus poussée**.

Structuration d'équipes fusionnées

Plusieurs institutions financières ont amorcé la mise en place de centre de fusion sur la cyberfraude, qui regroupent des analystes cybersécurité, des spécialistes de la fraude, de la conformité et du renseignement dans une même cellule. **Cette approche permet une meilleure circulation de l'information, une corrélation plus fine des signaux faibles et une réponse coordonnée face aux menaces hybrides** [5, 14, 15].

Interopérabilité des outils de sécurité et de surveillance

Au-delà de l'intégration humaine, **la mutualisation des plateformes technologiques est essentielle**. L'utilisation conjointe de solutions comme les systèmes SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response) et UBA (User Behavior Analytics) permettent une vision globale des risques et une détection en temps réel des anomalies comportementales, tant techniques que transactionnelles [14].

Alignement des processus et gouvernance transverse

Pour que cette convergence soit réellement opérationnelle, elle doit s'appuyer sur des processus harmonisés (détection, investigation, remédiation) **et des indicateurs de performance communs**. La mise en place d'un cadre de gouvernance partagé - avec des responsabilités croisées et des objectifs alignés - constitue un facteur clé de succès documenté dans plusieurs retours d'expérience internationaux [5, 12].

Références

- [1] IBM Security. (2023). X-Force Threat Intelligence Index 2023. IBM Corporation.
- [2] European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape for the Finance Sector January 2023 to June 2024. ENISA. .
- [3] Gundert, L., et Alforov, S. (2024, novembre). The Need for Cyber Fraud Fusion Centers. *Recorded Future*.
- [4] Fooshée, T. (2023). Fraud organizational structures: Progressing toward a holistic financial crime corporate strategy. *Datos Insights*.
- [5] PwC. (2023). *Cyber and fraud fusion comes of age*. PricewaterhouseCoopers.
- [6] Doeland, R. (2017). The Dutch Payments Association: Coordinated action against payment fraud. *European Payments Review*, 4(1), 33-38.
- [7] Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O. et Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, 14(3), 01-16.
- [8] Dufour, F. et Laffort, J. (2016). Appropriation croisée et sécurité des systèmes financiers. *Revue Banque & Stratégie*, 348, 42-47.
- [9] Raoui, A. et El Gnaoui, L. (2023). Gouvernance financière des banques et lutte contre la criminalité financière à l'ère du digital. *International Journal of Economic Studies Manga*, 3(4), 101-115.
- [10] Deloitte. (2022). *The rise of RegTech: Transforming compliance and risk management*. Deloitte Insights.
- [11] Dagorn, N. (2009). Identifying Security Elements For Cooperative Information Systems. *International Conference on Security and Cryptography*, 1, 319-324.
- [12] Deloitte. (2024). *Fusion centers: Uniting forces against financial crime*. Deloitte Insights.
- [13] Boitan, I. A. (2019). Enhancing fraud detection in banking using artificial intelligence techniques. *Journal of Financial Crime*, 26(2), 585-596.
- [14] Cyware. (2023). *Cyber Fusion Center Guide VI: Boost threat response with better collaboration between security teams*.
- [15] VIPSS. (2024). *Session 2: Fusion Centre Presentation*. VIPSS Conference.