ÉTUDE DE DOSSIER

Cadre de direction 2022

Le risque dit « cyber » est désormais considéré par les établissements financiers comme le principal risque pesant sur leur activité. La digitalisation progressive de la finance, le recours accru au télétravail depuis la crise sanitaire liée au Covid-19, et la guerre engagée par la Russie en Ukraine, ont augmenté la probabilité de matérialisation du risque et la vulnérabilité du secteur financier aux incidents « cyber » de toute nature.

À partir des documents ci-joints, vous répondrez aux questions suivantes :

1. Quels sont les différents risques cyber pesant sur les institutions financières ?
2. Comment évaluer le risque de crise systémique engendré par les vulnérabilités cyber ?
3. En quoi les compagnies d'assurance sont-elles particulièrement exposées au risque cyber ?
4. Quelles sont les avancées permises par le règlement DORA en vue de favoriser la résilience du secteur financier face aux risques cyber ? Est-ce que ce règlement permet de répondre aux enjeux selon vous ?
5. Based on your understanding of the documents, what are the main challenges in assessing and quantifying cyber risks? *(Réponse à rédiger en langue anglaise)*

Les questions sont indépendantes ; nous vous recommandons toutefois de les traiter dans l'ordre. Il n'est pas nécessaire de recopier l'intitulé des questions.

LISTE DES DOCUMENTS JOINTS

1. **Évaluation des risques du système financier français – Le risque cyber** (extrait)
   https://publications.banque-france.fr – Juin 2022 – 13 pages

2. **Le risque cyber dans le secteur financier**
   www.tresor.economie.gouv.fr – Décembre 2021 – 8 pages

3. **Cyber Risk of the Financial Sector: A Framework for Quantitative Assessment**
   www.imf.org – 22/06/2018 – 9 pages

4. **The drivers of cyber risk – Bank for International Settlements**
   www.bis.org – 20/05/2020 – 5 pages

5. **Covid-19 and cyber risks in the financial sector – BIS bulletin**
   www.bis.org – 14/01/2021 – 5 pages

6. **Finance numérique : accord provisoire concernant le règlement sur la résilience opérationnelle numérique**
   www.consilium.europa.eu – 11/05/2022 – 2 pages

7. **Cybersécurité : que fait l'Union européenne ?**
   www.touteleurope.eu – 16/05/2022 – 3 pages

8. **The EU's Digital Operational Resilience Act nearing the finish line: implications for financial services firms**
   https://ukfinancialservicesinsights.deloitte.com – 23/02/2022 – 4 pages

9. **The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict**
   https://hbr.org – 18/02/2022 – 2 pages

10. **Une mesure de l'évolution du risque cyber**
    https://blocnotesdeleco.banque-france.fr – 17/12/2021 – 5 pages

11. **Cyber risk for insurer – Challenges and opportunities**
    www.eiopa.europa.eu – September 2019 – 2 pages

12. **Cyber security insurance – how can insurers quantify the risk?**
    www.pwc.co.uk – 2 pages

(...) ## 2. Le risque cyber

Porté par une numérisation de l'économie et du système financier toujours plus prégnante, le risque cyber se détache de manière croissante comme un risque à haute probabilité et à fort impact potentiel. La crise sanitaire a renforcé le recours aux outils de travail à distance, accroissant la surface d'exposition à des attaques informatiques, tandis que la guerre russo-ukrainienne donne une nouvelle actualité à la menace. Si aucun incident critique n'a jusqu'ici été constaté dans le secteur financier français, le risque cyber doit plus que jamais faire l'objet d'une vigilance maximale.

Le risque cyber est un risque lié aux systèmes d'information au sein de la catégorie plus large du risque opérationnel. Il peut se définir comme tout risque de perte financière, d'interruption des activités ou d'atteinte à la réputation d'une entreprise en raison d'une défaillance des systèmes de technologies de l'information. Ces risques peuvent se matérialiser par une intrusion volontaire et non autorisée dans un système sécurisé, une intrusion involontaire ou accidentelle, ou un incident opérationnel découlant d'une défaillance de processus internes. Si les incidents cyber ne trouvent pas tous leur source dans des attaques malveillantes, ces dernières occasionnent de la majorité des incidents majeurs. L'intention potentiellement malveillante à son origine, la vitesse et l'ampleur de la propagation, distinguent le risque cyber d'autres risques opérationnels, même si celui-ci peut se traduire par des conséquences similaires.

La première partie de ce chapitre propose un panorama général du risque cyber, la deuxième évoque les aspects qui participent de la dimension systémique du risque cyber, tandis que la dernière présente les évolutions récentes ainsi que les réglementations amorcées pour répondre à ces enjeux.

2.1 Le risque cyber constitue une menace grandissante pour l'économie et le secteur financier

Le poids économique du risque cyber apparaît en hausse, même si la mesure du risque demeure difficile

Les mesures disponibles suggèrent globalement une fréquence accrue des cyberattaques et des coûts élevés en forte hausse ces dernières années.

Graphique 2.1 : Messages consacrés au risque cyber sur Twitter

x : axe temporel / y : (gauche : nombre d'évènements extrêmes), (droite : tendance du risque cyber)

Source : Lhuissier, Tripier, Measuring Cyber Risk, Août 2021.
Notes : L'histogramme indique le nombre annuel d'événements extrêmes liés au risque cybernétique entre 2011 et 2020 (échelle de gauche). La ligne rouge montre l'évolution quotidienne de l'indice de cyber-risque de janvier 2011 à mars 2021 (échelle de droite).

Ainsi, une analyse textuelle des transcriptions des conférences d'annonce de résultats financiers révèle une augmentation des références au risque cyber, associée à un sentiment de plus en plus négatif [29]. L'analyse des messages consacrés au risque cyber sur le réseau social Twitter peut également fournir un indicateur de suivi [30]. Depuis 2011, le nombre d'évènements extrêmes [31] mesurés par cette méthode augmente significativement, avec un pic en 2017 (cf. graphique 1.1). La tendance de long terme de l'indice purgée des évènements extrêmes atteste également d'une attention croissante pour la thématique, ravivée à partir de 2020 dans le contexte de la crise sanitaire. Dans une étude, l'assureur spécialisé Hiscox relève que la proportion d'entreprises ayant rapporté des attaques dans le panel étudié est passée de 38 % en 2020 à 43 % en 2021, et près d'un quart ont été visées plus de cinq fois au cours de l'année. Les conséquences en matière de coûts sont très variables, mais parmi les entreprises victimes d'une attaque, une sur six a déclaré que sa survie était menacée [32]. Si de nombreuses cyberattaques entraînent des pertes limitées, certaines sont très coûteuses pour les entreprises et quelques-unes ont eu des effets économiques importants. Une publication d'Accenture (2019) évalue le coût annuel moyen de

[29] Jamilov, Rey & Tahoun, *The Anatomy of Cyber Risk*, National Bureau of Economic Research, 2021.
[30] Lhuissier, Tripier, *Measuring Cyber Risk*, Août 2021.
[31] Un évènement extrême est caractérisé par un fort retentissement médiatique
[32] Hiscox Assurances, *Rapport 2021 sur la gestion des cyber-risques*, 2021.

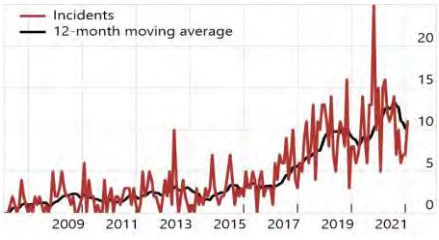
la cybercriminalité [33] pour une grande entreprise à 13 millions de dollars [34]. Par exemple, Sopra Steria, victime du rançongiciel Ryuk en octobre 2020, a estimé ses pertes à 50 millions d'euros [35]. La cyberattaque la plus destructrice à ce jour, l'attaque NotPetya [36] de 2017 dirigée initialement contre l'Ukraine, a infligé des dommages estimés à plus de 10 milliards de dollars, soit un peu plus de 10 % du PIB de l'Ukraine à l'époque [37]. En matière de pertes agrégées, une étude du Center for Strategic and International Studies et de l'éditeur en cybersécurité McAfee de 2020 [38] montre que le coût de la cybercriminalité aurait augmenté de plus de 50% en deux ans, pour représenter 1% du PIB mondial environ. Au total, la cybercriminalité engendrerait 945 milliards de dollars de pertes financières par an.

Aux coûts des incidents s'ajoutent les nécessaires dépenses en matière de cyber-sécurité qui participent au poids économique du risque cyber. Selon Gartner, les dépenses mondiales en matière de cybersécurité et gestion des risques excèderont 167 milliards de dollars en 2022. Pour autant, les budgets cyber ne représenteraient encore que 6 % du budget informatique des grandes entreprises françaises tous secteurs confondus selon une étude récente du cabinet Wavestone[39].

Concernant le secteur financier, selon une étude du Fonds monétaire international (FMI), les pertes moyennes annuelles dues aux cyberattaques seraient équivalentes à 9 % du résultat net des banques (soit 97 milliards de dollars) pour les pays de l'échantillon étudié. Le ratio monterait à 26 % (268 milliards de dollars) dans un scénario plus sévère où la fréquence des attaques est doublée par rapport à 2013, sans prise en compte des effets de contagion[40]. Une autre modélisation, tenant compte des effets de contagion et comparant trois modèles avec des hypothèses distinctes, met en évidence la forte sensibilité des résultats aux paramètres retenus. En effet, suivant l'hypothèse d'exposition utilisée (estimation de la Value at Risk par la Securities and Exchange Commission) et les paramètres du modèle (pays, expositions financières, type d'attaque), les coûts totaux en PIB s'échelonnent de 799 milliards à 22 500 milliards de dollars[41]. Ces coûts regroupent non seulement les coûts directs causés par l'attaque (vol de données) mais aussi les coûts indirects tels que la perte de confiance, la contagion à d'autres entreprises, la perte de données ou encore la mise en place de nouveaux systèmes de sécurité.

Graphique 2.2 : Nombre d'incidents cyber ciblant les institutions financières

x : axe temporel / y : nombre d'incidents



Source : Financial Stability Board

Ces diverses estimations permettent d'illustrer la hausse du risque ; toutefois, la fréquence et les coûts des incidents cyber demeurent particulièrement difficiles à estimer. En premier lieu, la notification des incidents et pertes associées est encore très partielle (notamment pour des questions de réputation et de sensibilité en matière de sécurité) et repose jusqu'à présent sur des obligations sectorielles (surtout pour les secteurs des télécoms et du médical). À cette différentiation sectorielle, s'ajoute la question du seuil de matérialité : aucune obligation ne contraint les entreprises du secteur financier à signaler les incidents dès lors qu'ils ne sont pas classés comme majeurs ou qu'ils n'ont pas de conséquence importante. Cette définition n'étant elle-même pas normée, il est alors difficile d'avoir une vue harmonisée de ces incidents, que ce soit au sein du secteur financier ou entre différents secteurs.

En outre, le véritable coût des cyberattaques doit, comme pour les autres risques opérationnels, intégrer les coûts indirects tels que le risque de réputation, la dépréciation de la valeur de la propriété intellectuelle ou encore l'impact sur les futures primes de cyber-assurance. Ce coût ne se manifeste que sur plusieurs années, ce qui complique l'estimation *ex ante* des coûts potentiels à long terme des incidents[42]. Ainsi, la prévalence et le coût

[33] Le terme « cybercriminalité » regroupe les attaquants cyber qui ont une visée lucrative et ne sont pas sponsorisés par un État
[34] Accenture, *Ninth annual cost of cybercrime study*, 2019.
[35] Sopra Steria expects €50 million loss after Ryuk ransomware attack (bleepingcomputer.com)
[36] Attaque par sabotage qui ciblait les systèmes d'information d'institutions et d'entreprises ukrainiennes et qui s'était propagée à d'autres pays.
[37] Walker, *The Economic Impact of Cyberattacks*, Goldman Sachs Economics Research, Mars 2022.
[38] https://www.csis.org/analysis/hidden-costs-cybercrime
Le CSIS est un *think tank* américain qui mène des études et des analyses stratégiques sur des questions politiques, économiques et de sécurité à travers le monde.
[39] www.wavestone.com/fr/communiques-de-presse/cybersecurite-ou-en-sont-les-grandes-organisations-francaises/
[40] Bouveret, IMF Working Paper, *Cyber risk for the financial sector: a framework for quantitative assessment*, 2018.
[41] Dreyer et al, *Estimating the global cost of cyber risk*, 2018.
[42] IMF Working Paper, *Cyber Risk, Market Failures and Financial Stability*, 2017.

des cyberattaques, bien qu'incertains, sont probablement sous-estimés. Compte tenu de la nature très évolutive des cyberattaques et du manque de données empiriques, le risque cyber ne peut pas être facilement modélisé ou mesuré sur la base des expériences passées, contrairement aux risques financiers [43]. En tout état de cause, ces estimations de coûts variables sont supérieures de plusieurs ordres de grandeur à la taille actuelle du marché de la cyber-assurance, les pertes cyber assurées mondiales restant inférieures à 5 milliards de dollars d'après Swiss Re[44].

Encadré 2.1 : L'assurance du risque cyber, un marché encore peu mature

Face à l'augmentation des cyberattaques, la cyber-assurance peut constituer un outil de couverture du risque. Le marché américain de la cyber-assurance apparaît plus développé que le marché européen, encore en pleine construction. En France, le rapport de mai 2021 de l'Association pour le management des risques et des assurances de l'entreprise (AMRAE) note en effet une augmentation du volume de primes de 49% en 2020 qui reste très inférieure à celle du montant des indemnisations versées (qui a été multiplié par trois)[45].

Le développement du marché se heurte notamment aux hésitations des assureurs qui craignent de s'exposer à des risques excessifs, ce qui s'explique en partie par l'absence de bases de données fiables et par la difficulté à modéliser le risque ainsi que par une faible capacité de mutualisation du risque. Aussi, les produits et couvertures de cyber-assurance sur le marché sont aujourd'hui très hétérogènes.

Des travaux en cours, aux niveaux tant national qu'européen, visent à développer une meilleure mesure du risque cyber et des expositions ainsi qu'à clarifier le périmètre de la couverture assurantielle, pour *in fine* faire émerger des offres françaises et européennes de cyber-assurance plus matures. L'enjeu est de taille puisque selon l'AMRAE, seules 8% des entreprises de taille intermédiaire auraient souscrit une cyber-assurance. Une offre plus étendue de cyber-assurance participerait d'un « cercle vertueux » : ces assurances procureraient des outils de prévention et de protection et un meilleur accompagnement aux assurés afin de les inciter à renforcer leurs pratiques et défenses en matière de cyber-sécurité.

En France, la question de la couverture du paiement de rançons à la suite d'une cyberattaque fait débat[46]. Un rapport parlementaire d'octobre 2021 propose d'inscrire dans la loi l'interdiction pour les assureurs de couvrir un tel paiement tandis que le Haut comité juridique de la place financière de Paris (HCJPP) estime que cette interdiction n'enrayerait pas la cybercriminalité et pourrait au contraire pénaliser les entreprises et les collectivités[47].

Parmi les autres enjeux relatifs à la cyber assurance figurent la problématique du risque de couverture implicite du risque cyber dans des assurances traditionnelles ainsi que la nécessité éventuelle de clarifier les exclusions possibles lorsque le fait générateur est constitutif d'un acte de cyberguerre.

Le secteur financier constitue une cible d'intérêt

La numérisation croissante de l'économie et des services financiers constitue une tendance structurelle qui contribue à l'augmentation du risque cyber. Le contexte de crise sanitaire n'a pas créé de nouveaux points d'entrée mais a considérablement agrandi la surface d'attaque en raison du recours plus large au télétravail, ainsi qu'à des procédures mises en place rapidement et destinées à assurer la continuité de l'activité. Il a notamment été nécessaire d'augmenter le nombre de services exposés sur Internet, de déployer dans l'urgence de nombreux postes de travail nomades et d'accroître rapidement les capacités d'accès à distance. Une forte corrélation entre la prévalence du travail à distance et l'incidence des cyberattaques a pu être observée entre février et juin 2020, le secteur financier occupant une position élevée sur les deux plans[48]. Par ailleurs, la présence d'actifs et de

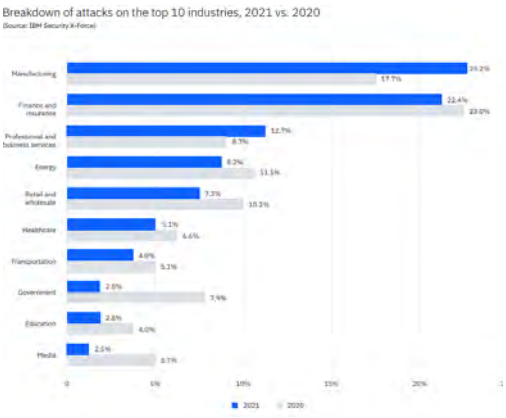
[43] Institute of International Finance, *Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system*, 2017.
[44] S&P Global, *Cyber risk in a new era: Insurers Can Be Part Of The Solution*, 2020.
[45] AMRAE, Lumière sur la cyber-assurance, 2021.
[46] Source : G. Poupard (ANSSI), rapport parlementaire de V. Faure-Muntian sur la cyber-assurance (octobre 2021), p. 8.
[47] Rapport parlementaire de V. Faure-Muntian sur la cyber-assurance, octobre 2021 ; Haut Comité Juridique de la Place financière de Paris, *Rapport sur l'assurabilité des risques cyber*, Janvier 2022.
[48] BRI, Bulletin No 37, *Covid-19 and cyber risk in the financial sector*, 2021.

données à haute valeur ajoutée concourt également à expliquer l'attrait du secteur financier pour les cybercriminels recherchant un gain financier.

Ainsi, IBM estime que le secteur financier mondial a subi 22% du total des cyberattaques et incidents observés en 2021, en deuxième position après le secteur manufacturier alors qu'il représente environ 8% du PIB. Parmi ces attaques, 70% ont visé des banques[49]. Selon une autre étude, le secteur financier est exposé à un plus grand nombre d'attaques mais subit des pertes inférieures en moyenne, grâce à des investissements proportionnellement plus importants dans la sécurité des systèmes d'information[50]. Les pertes associées au risque cyber ne constituent encore qu'une petite partie des pertes opérationnelles mais peuvent néanmoins représenter jusqu'à un tiers de la *Value-at-Risk* (VaR) opérationnelle totale d'après un papier de recherche de la Banque des Règlements Internationaux[51]. En Europe continentale, les demandes d'indemnisation des institutions financières en matière de cyber-assurance seraient les plus nombreuses (+ 29 % au cours de l'année 2020), bien que d'autres secteurs s'en approchent avec des taux d'incidence élevés[52].

Graphique 2.3 : Décomposition des attaques par industrie

x : Pourcentage / y : Industrie



Source : IBM X-Force Threat Intelligence

De nombreux acteurs traditionnels du secteur financier ont déjà subi des attaques abouties. En 2016, le piratage du terminal de paiement SWIFT de la banque centrale du Bangladesh afin d'émettre des messages de paiement frauduleux a abouti au vol de 81 millions de dollars. Le piratage du serveur des distributeurs automatiques de billets de Cosmos Bank en Inde en 2018 s'est soldé par le vol de 13,5 millions de dollars par le biais de transactions frauduleuses. En août 2020, les perturbations de la bourse néo-zélandaise provoquées par une série d'attaques ont conduit à interrompre des transactions en raison de préoccupations concernant l'intégrité du marché. D'autres types d'acteurs sont également concernés, tels que les prestataires de services en actifs numériques (vol en janvier 2022 de 80 millions de dollars chez Qubit Finance par exemple) ou les agences de notation de crédit (vol de données chez l'entreprise américaine Equifax en 2017).

Encadré 2.2 : Une attention croissante des agences de notation

En 2019, l'agence S&P a dégradé la note de la Bank of Valletta à la suite d'une cyberattaque ayant renforcé les inquiétudes relatives à la robustesse de son cadre de gestion des risques opérationnels. Cette attaque par campagne d'hameçonnage a usurpé des images de l'Autorité des marchés financiers (AMF) dans un objectif de vol par virements frauduleux. La banque maltaise a réussi à interrompre ces virements et à éviter le vol de près de 13 millions d'euros.

Si les cyberattaques n'ont eu jusqu'à présent qu'un effet limité sur les notations de crédit des institutions financières, la fréquence et la complexité croissantes des attaques pourraient se traduire à l'avenir par davantage d'actions de notation. La présence d'un cadre de cybersécurité robuste et de standards de gouvernance cyber sont désormais pris en compte par les agences dans leur évaluation de la notation de crédit, avant même tout incident. Les agences de notation indiquent explorer de nouvelles façons d'évaluer l'exposition des entités au risque cyber, en collaborant notamment avec des sociétés spécialisées en cybersécurité. Une analyse de Fitch Ratings souligne ainsi que les banques dont les notes de crédit sont les plus élevées affichent généralement de meilleurs scores en matière de cybersécurité mais que la taille financière n'est pas nécessairement un bon indicateur de la maturité cyber ; les grandes banques sont en effet plus susceptibles d'être dotées d'une infrastructure informatique historique et complexe.

[49] X-Force Threat Intelligence Index, 2022.
[50] Aldasoro, Gambacorta, Giudici, Leach, *The drivers of cyber risk*, BIS Working Papers, 2020.
[51] Aldasoro, Gambacorta, Giudici, Leach, *Operational and cyber risks in the financial sector*, BIS Working Papers, 2020.
[52] Marsh, CMS Law, Kivu, Microsoft, *The Changing Face of Cyber Claims*, Octobre 2021.

En cas de cyberattaque, une détection et une résolution rapides peuvent permettre d'éviter une dégradation du profil de crédit de l'entreprise. Les notations de crédit peuvent être sensibles aux incidents cyber qui ont des impacts marqués ou durables sur les opérations commerciales, nuisent à la réputation de l'émetteur ou à la confiance des clients, entrainent des amendes ou des règlements importants et affectent le profil financier d'un émetteur (rentabilité, liquidité ou levier)[53].

Une menace protéiforme et évolutive

Les vecteurs d'infection ouvrant l'accès au système d'information (SI) d'une entité, qu'elle soit financière ou non, sont variés. Les attaquants peuvent tout d'abord agir par opportunisme et pénétrer le SI d'entreprises par en exploitant des de vulnérabilités (protocolaires, logicielles, etc.) identifiées ou achetées sur des places de marché souterraines, en recourant à des campagnes d'hameçonnage massives, ou encore 'en achetant des d'accès à des SI préalablement compromis par d'autres. D'autres attaquants, aux méthodes réputées plus sophistiquées, pratiquent de la reconnaissance approfondie afin de compromettre des entités spécifiques. L'ingénierie sociale est en effet de plus en plus poussée, les attaquants allant parfois jusqu'à contacter directement des employés qu'ils ont repérés sur des réseaux sociaux dans le but de gagner leur confiance. Par exemple, entre 2018 et 2019, le mode opératoire du groupe d'attaquants[54] APT38, réputé lié à la Corée du Nord, a posté une fausse offre d'emploi sur LinkedIn, convaincant les candidats (des employés en informatique travaillant dans des institutions financières), de télécharger ce qui était un faux logiciel de soumission de candidature pour infecter leur poste. Le SI du réseau interbancaire chilien de distributeurs automatiques de billets (DAB) RedBanc a pu être compromis de la sorte[55].

Enfin, les attaques par chaîne d'approvisionnement (*supply-chain attack*) permettent de contourner les mesures de cybersécurité des cibles finales en infiltrant une ressource de confiance (tel qu'un logiciel) ou en rebondissant depuis le SI d'un sous-traitant auquel elles seraient interconnectées. Par exemple, en décembre 2020, des attaquants cybercriminels ont exploité plusieurs vulnérabilités de l'application de transferts de fichiers de l'éditeur de logiciels de sécurité Accellion afin d'y installer un code malveillant. À partir de janvier 2021, plusieurs entités clientes d'Accellion, dont la Banque centrale de Nouvelle-Zélande et Morgan Stanley, ont reçu des courriels menaçant de publier sur un site de divulgation les données exfiltrées depuis l'application compromise si une rançon n'était pas payée.

Quel que soit le vecteur d'infection utilisé, les attaquants susceptibles d'affecter le secteur financier ont principalement une motivation lucrative ou déstabilisatrice, ou encore, dans une moindre mesure, une visée d'espionnage. Sur l'aspect lucratif, le secteur financier peut être la cible d'attaquants réputés sponsorisés par des États[56]. Certains, comme le groupe cybercriminel Cobalt Gang ou le groupe APT38 (alias Bluenoroff), planifient pendant plusieurs mois des attaques ciblées dans le but de compromettre le système d'information de banques, d'atteindre leur système de gestion de DAB, leur système de gestion de cartes ou leur interface d'accès au service de messagerie interbancaire SWIFT, et de réaliser ainsi des retraits ou des virements frauduleux. Néanmoins, depuis quelques années et l'essor des plateformes d'échanges de cryptoactifs, certains modes opératoires des attaquants tendent à substituer leur compromission, réputée plus aisée et plus rentable que celle de systèmes d'information bancaires traditionnels. Les attaques à visée d'extorsion augmentent fortement depuis 2018, soutenues par l'industrialisation de l'écosystème cybercriminel [57], bien qu'elles ne concernent pas seulement le secteur financier. Les plus communes sont les exfiltrations de données, avec chiffrement des fichiers (rançongiciel) ou non, accompagnées d'une demande de rançon et de menaces de divulgation sur un site Internet dédié en cas de non-paiement.

[53] Voir par exemple S&P Global, *Cyber Risk in a New Era : The Increasing Credit Relevance Of Cybersecurity*, Juillet 2021 ; Moody's, Cyber risk 2022 Outlook – *Workplace shifts open new attack channels, while insurance costs rise and coverage narrows*, Novembre 2021; Fitch, *Bigger Not Always Better for Bank Cyber Risk Scores*, Avril 2021.

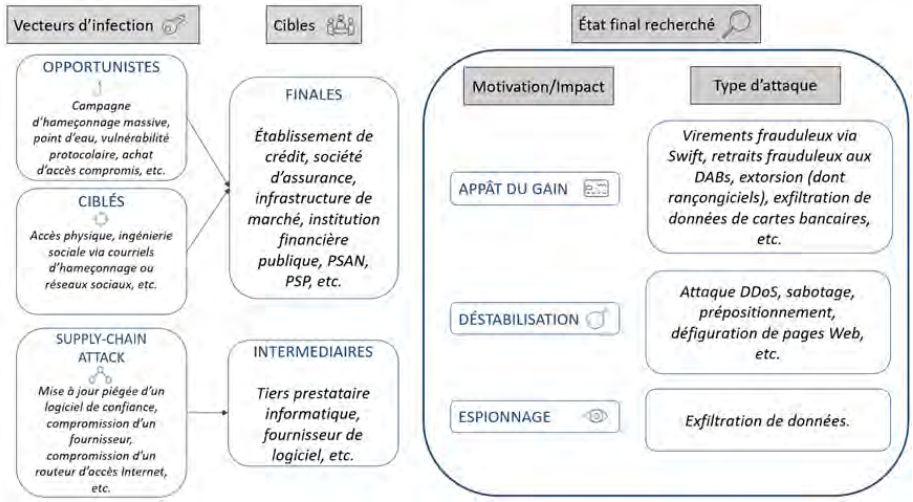
[54] D'après l'ANSSI, un groupe d'attaquants est un ensemble délimité, constitué d'individus identifiés ou identifiables revendiquant une appartenance à une organisation. Un groupe d'attaquants met en œuvre un ou plusieurs modes opératoires.

[55] INTEL, *Disclosure of Chilean Redbanc Intrusion Leads to Lazarus Ties,* 15 janvier 2019 (https://www.flashpoint-intel.com/blog/disclosure-chilean-redbanc-intrusion-lazarusties/).

[56] En particulier par la Corée du Nord dans un but de contournement des sanctions financières internationales à son égard (voir FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks | CISA).

[57] L'écosystème cybercriminel est constitué de vendeurs et d'acheteurs de biens (codes malveillants, accès compromis, données personnelles volées, etc.) et de services (location d'infrastructures de déni de service, d'anonymisation, etc.), permettant aux attaquants de sous-traiter une grande partie des ressources et outils nécessaires à la réalisation de leurs opérations malveillantes. Ces dernières sont ainsi facilitées.

Graphique 2.4 : Typologie des attaques



Notes : PSAN, prestataire de services sur actifs numériques ; PSP, prestataire de services de paiement ; attaque DDoS, attaque par déni de service distribué
Source : ACPR

Les attaques à visée déstabilisatrice, moins répandues que les attaques à visée lucrative, sont d'origine et de nature variées. Il peut s'agir d'attaques par déni de service distribué (DDoS)[58] conduites par des hacktivistes[59], comme cela a été le cas en juin 2016 lors de l'opération Icarus des collectifs Anonymous et Ghost Squad Hackers contre plusieurs bourses dont le NYSE Euronext[60]. Elles peuvent aussi émaner d'acteurs sponsorisés par un État, comme cela a semble-t-il été le cas en février 2022, en amont et au commencement de la guerre russo-ukrainienne, lorsque plusieurs banques publiques ukrainiennes ont été victimes d'attaques par DDoS[61]. Il peut également s'agir d'attaques par sabotage, comme celles subies par des institutions financières ukrainiennes en décembre 2016 lorsque des serveurs, des équipements réseau et des éléments du système de sauvegarde ont été endommagés.

En matière d'exfiltration de données à des fins d'espionnage, les assurances semblent être une cible privilégiée selon l'Agence nationale de sécurité des systèmes d'information (Anssi), car ces entreprises détiennent et manipulent une quantité importante de données variées, parmi lesquelles des données personnelles, des données financières ainsi que de la propriété intellectuelle. En 2014, les compagnies d'assurance américaines Anthem, Premera Carefirst et Excellus ont été compromises par des attaquants ayant supposément eu pour objectif de connaître les déplacements, la situation médicale, les fonctions et accès à des informations sensibles de divers responsables[62]. De plus, un nombre accru de sociétés d'assurance offrent des assurances cyber, et détiennent donc des données relatives aux dispositifs de cybersécurité des entreprises assurées : il apparaît que certaines compagnies d'assurance sont alors espionnées en tant que cible intermédiaire par des groupes cybercriminels[63] qui souhaiteraient s'informer sur la politique de sécurité du SI d'une entreprise cliente.

Dans le contexte de la guerre en Ukraine, le risque d'attaques à visée déstabilisatrice ou d'espionnage prend une acuité particulière. Si aucun incident majeur n'a été détecté jusqu'à présent, la menace contre les systèmes d'information européens reste élevée. En effet, cette menace est plurielle et englobe i) les attaques d'hacktivistes, ii) les acteurs offensifs indirectement liés aux belligérants qui ont déjà tenté d'exploiter la situation pour mener des activités ciblées d'hameçonnage, ii) une partie de l'écosystème cybercriminel qui s'est positionné dans le conflit en cours et serait en mesure dans un avenir proche de cibler des entités françaises à des fins de renseignement ou en représailles aux sanctions européennes. Ce contexte de conflit géopolitique et de multiplicité des menaces implique un haut niveau de vigilance des institutions financières ainsi qu'une certaine proactivité dans la mise en place de mesures défensives, qui doivent être maintenues[64].

[58] Attaque visant à rendre inaccessible un serveur afin de provoquer une panne ou un fonctionnement fortement dégradé du service.
[59] Attaquants informatiques aux intentions militantes.
[60] Daily Mail, *Hackers Attack the Stock Exchange: Cyber Criminals Take down Website*, 5 juin 2016
[61] Forbes, *Ukrainian Government And Banks Hit By New Wave Of Cyberattacks*, 23 février 2022.
[62] California Department of Insurance, *Investigation of Major Anthem Cyber Breach Reveals Foreign Nation behind Breach*, 6 janvier 2017.
[63] The Record, *"I Scrounged through the Trash Heaps… Now I'm a Millionaire :" An Interview with REvil's Unknown*, 16 mars 2021 (https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionairean-interview-with-revils-unknown/).
[64] Rapport Menaces et Incidents du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, 12 avril 2022.

2.2 Certains scénarios de matérialisation du risque cyber constitueraient une menace systémique pour le système financier

Au-delà des vulnérabilités propres à chaque entité, le risque cyber peut constituer un déclencheur d'instabilité à l'échelle du système financier. Si aucun incident cyber n'a eu à ce jour une répercussion systémique, les occurrences d'incidents de grande ampleur augmentent, mettant en lumière la diversité des cibles et des canaux potentiels de propagation.

De multiples événements déclencheurs et canaux de transmission pourraient conduire à un incident de portée systémique

Les cyberattaques peuvent constituer une menace pour la stabilité financière à travers leur impact sur une organisation donnée ou bien sur plusieurs composantes du système financier simultanément. Les perturbations occasionnées sont susceptibles de déclencher divers canaux de contagion financière et alimenter dans des scénarios extrêmes des boucles de rétroaction négatives. Le Comité européen du risque systémique (CERS) montre ainsi qu'un incident cyber pourrait évoluer d'une panne opérationnelle à une crise de liquidité[65], susceptible de provoquer à son tour une crise systémique, notamment en cas de pertes financières importantes (réelles ou anticipées) et de nette érosion de la confiance dans le système financier[66]. Les cibles affectées tout comme la nature des canaux de transmission sont déterminantes dans l'appréciation de l'ampleur potentielle d'un incident. Ainsi, une cyberattaque ayant l'intention délibérée de déstabiliser le système financier pourrait se traduire plus facilement par un choc de confiance qu'une attaque motivée par le simple gain financier.

Une perturbation majeure d'infrastructures ou de fonctions économiques critiques constitue une première famille de scénarios potentiels à fort impact. Parmi les services financiers critiques figurent les services de conservation des titres, de compensation centrale ou de paiement. Les systèmes de paiement de gros en temps réel (*real time gross settlement systems* – RTGS) et le système de messagerie SWIFT, par exemple, sont cruciaux pour les paiements et règlements en espèces et en titres, et sont considérés comme de potentiels « *points de défaillance uniques* » dans l'infrastructure de paiement mondiale[67]. Des perturbations des systèmes de paiement pourraient induire des incertitudes quant au caractère définitif des règlements liés aux obligations de paiement, ce qui aurait de larges répercussions sur les chaînes complexes de participants impliqués[68]. Selon une modélisation dite de « pre-mortem » de la Fed de New York, une cyberattaque sur le réseau de paiements de gros d'un des cinq plus grands participants du système de paiement américain affecterait en moyenne 38 % du réseau (en pourcentage d'actifs bancaires), tandis qu'un « scénario de cascade » dans lequel les institutions répondent cette fois stratégiquement à la dégradation de leurs soldes en cours de journée en renonçant à leurs paiements et en thésaurisant des liquidités, aboutirait à des abandons de paiements de l'ordre de 5 % à 35 % de la valeur totale des paiements quotidiens (soit 1 à 11 fois le PIB quotidien des États-Unis)[69]. Une étude estime que les institutions financières américaines d'importance systémique disposent de stocks suffisants d'actifs liquides de haute qualité pour couvrir les retraits des investisseurs de gros en cas de *cyber-run*[70] relativement important mais suggère que cela ne garantit pas pour autant que le système de paiement continuerait à traiter les paiements suffisamment rapidement pour éviter des dommages à l'économie réelle [71].

Une atteinte massive à l'intégrité des données représente un autre scénario potentiel pouvant causer de fortes perturbations pour les marchés financiers et l'économie réelle. Ainsi, une corruption simultanée de l'intégrité des données d'une banque dépositaire et de l'un des grands dépositaires centraux de titres rendrait difficile le recoupement ou la reconstruction des opérations communes entre ces entités, avec des effets négatifs sur le traitement et le prix des titres concernés, les échanges, et plus globalement sur la confiance[72]. De même, un

[65] Par exemple, le 27 juin 2014, la plus grande banque bulgare, la *First Investment Bank* (FIB), a connu une panique bancaire (ou course aux guichets) à la suite de courriels fallacieux et à une couverture sur les réseaux sociaux laissant entendre que la FIB rencontrait une pénurie de liquidités.
[66] CERS, *Systemic cyber risk*, 2020.
[67] World Economic Forum, *Understanding Systemic Cyber Risk*, 2016.
[68] Institute of International Finance, op.cit.
[69] Eisenbach, Kovner, and Lee, *Cyber Risk and the US financial System: a Pre-Mortem Analysis*, Fed Staff Report, 2020.
[70] Un « *cyber-run* » est un scénario dans lequel une cyberattaque provoque un « *bank run* » et une crise de liquidité.
[71] Hutchins Center Working Paper, Duffie and Younger, *Cyber runs*, 2019.
[72] Institute of International Finance, op.cit.

scénario hypothétique étudié par le CERS réside dans la manipulation simultanée des flux de prix de plusieurs marchés de matières premières et de marchés à terme, ainsi que des informations données par une chambre de compensation. L'incertitude quant à la fiabilité des prix et des positions conduirait à une baisse de la liquidité et des prix déclenchant une spirale négative de ventes forcées, source de pertes importantes pour de nombreux participants du marché[73]. De manière générale, la corruption de l'intégrité des données peut exiger des arbitrages délicats entre la nécessité d'opérer une récupération rapide des données et celle de garantir leur exactitude et leur sûreté afin d'éviter une propagation des risques dans le système[74].

En outre, une défaillance d'un composant technologique largement employé ou d'un prestataire de service dominant est susceptible d'affecter simultanément plusieurs parties importantes du système financier, ce qui pourrait engendrer de multiples réactions en chaîne. Alternativement, des failles de confidentialité ou des vols importants ou à fréquence élevée peuvent être également source d'instabilité financière s'ils entraînent une perte de confiance dans le système financier. Dans un scénario extrême, ce type d'incidents pourrait conduire à une forte volatilité des prix sur les marchés, une réduction des volumes échangés et des phénomènes de paniques bancaires (*runs*) induisant des enjeux de liquidité pour les institutions financières.

Enfin, un incident cyber affectant des infrastructures non financières sur lesquelles reposent le système financier, telles qu'un fournisseur d'électricité ou de télécommunications, peut également constituer une menace pour la stabilité financière. En fonction de l'étendue de l'attaque et de sa durée, les flux transitant par les institutions financières et les infrastructures de marché concernées pourraient s'en trouver considérablement retardés, voire arrêtés. À titre d'exemple, une étude de Lloyds estime qu'une attaque contre le réseau électrique du nord-est des États-Unis plongeant 15 États dans l'obscurité causerait entre 250 milliards et 1 000 milliards de dollars de dommages économiques[75].

Les interconnexions complexes entre les acteurs au sein et en dehors du système financier peuvent jouer un rôle amplificateur très important

Les vulnérabilités des systèmes d'information des entités financières engendrent des risques qui ne se limitent pas au périmètre des établissements considérés isolément. Les interdépendances opérationnelles favorisent potentiellement la propagation des attaques, une institution financière infectée pouvant devenir un « point d'entrée » pour l'ensemble des institutions qui lui sont liées. La complexité croissante du secteur financier élargit la surface d'attaque exploitable et le risque de contagion entre les acteurs du secteur, d'autant plus que tous les participants n'ont pas atteint le même niveau de maturité en matière de cybersécurité. Ces interconnexions sont également de nature financière, comme l'illustrent les scénarios évoqués plus haut. Or, l'identification des nœuds critiques au sein du système financier, c'est-à-dire des points névralgiques par lesquels passent les transactions et les fonctions les plus importantes entre les acteurs d'importance systémique, reste partielle.

Des études portant sur certains pans de ces interconnexions permettent d'illustrer l'ampleur potentielle de la contagion des incidents cyber. À travers les liens de la chaîne d'approvisionnement, une étude montre que les effets de l'attaque NotPetya en 2017 se sont propagées en « aval » aux clients des entreprises touchées par le code malveillant, affectant nettement leurs capacités productives et leurs bénéfices et les contraignant à utiliser leurs liquidités et augmenter leurs emprunts[76]. Les auteurs de cette étude estiment la chute des bénéfices pour les entreprises clientes concernées à 7,3 milliards de dollars, soit un montant quatre fois supérieur aux pertes signalées par les entreprises directement touchées par la cyberattaque. De même, un impact négatif des incidents cyber a pu être mis en évidence non seulement sur les rendements des actions des entreprises affectées mais également sur les entreprises non affectées d'un même secteur dans un même pays[77].

Le recours croissant à des prestataires de services tiers engendre de nouvelles interdépendances. Face à la complexification des technologies de l'information et aux investissements importants qui sont nécessaires pour

[73] CERS, op.cit.
[74] OFR, *Cybersecurity and Financial Stability: Risks and Resilience*, 2017.
[75] Lloyd's and the University of Cambridge's Centre for Risk Studies, *Business Blackout*, 2015.
[76] Crosigni *et al.*, *Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chain,* 2020.
[77] Jamilov et al, *The Anatomy of Cyber Risk*, 2020 ; Kamiya et al., *Risk management, firm reputation, and the impact of successful cyberattacks on target firms*, 2021.

les exploiter, de nombreuses entités du secteur financier font appel de plus en plus largement à des prestataires tiers de services informatiques. Les attaquants ciblent de manière croissante cette chaîne d'approvisionnement numérique, profitant de la confiance entre le fournisseur et le client et l'accès privilégié de nombreux fournisseurs aux systèmes d'information de leurs clients. Selon le dernier baromètre du Club des experts de la sécurité de l'information et du numérique (CESIN) sur la cyber-sécurité des entreprises en France, les attaques indirectes par rebond via un prestataire ont augmenté de 5 % pour concerner 21 % des entreprises répondantes en 2021[78].

Sur certains segments de marché, le nombre restreint de prestataires conduit à une situation de forte concentration : un nombre grandissant d'entités dépendent – y compris de plus en plus pour la fourniture de services qui sont essentiels à leur fonctionnement – de ces prestataires. La défaillance de l'un d'entre eux peut donc engendrer des dysfonctionnements simultanés dans une partie importante du secteur financier. Les attaques récentes dont l'origine était la compromission d'outils distribués par des prestataires informatiques à de très nombreux acteurs des secteurs financier et non financier (les éditeurs de logiciels de gestion informatique SolarWinds en décembre 2020 ou Kaseya en juillet 2021 par exemple) illustrent bien ce risque. Celui-ci est aggravé par le fait que ces points de concentration sont souvent mal ou pas identifiés ; nombre des clients de Solarwinds n'étaient même pas conscients d'être utilisateurs de ses logiciels[79]. En particulier, si les services d'informatique en nuage (le *cloud*) peuvent permettre de renforcer de manière importante la résilience des institutions considérées individuellement, la concentration potentielle de la fourniture de ces services pourrait entraîner des effets systémiques en cas de défaillance opérationnelle à grande échelle ou d'insolvabilité[80]. Quatre acteurs se partagent près des deux tiers du marché mondial de la fourniture des services de *cloud*[81]. Une étude de Lloyds estime qu'un incident cyber provoquant la mise hors ligne d'un des trois premiers fournisseurs de *cloud* aux États-Unis pendant trois à six jours entraînerait des pertes totales de l'ordre de 7 à 15 milliards de dollars[82]. À partir d'un modèle stylisé appliqué aux membres compensateurs d'une chambre de compensation centrale, une analyse de l'Autorité européenne des marchés financiers (AEMF) suggère que la forte concentration des fournisseurs de *cloud* pourrait créer des risques pour la stabilité financière si une panne chez l'un d'entre eux affecte nombre de ses clients, en augmentant la probabilité de pannes simultanées[83].

De nouveaux intermédiaires et de nouvelles technologies créent de potentielles zones d'exposition supplémentaires en lien avec les institutions financières. Le développement technologique rapide des fintech[84] s'accompagne d'une nouvelle gamme de services et de transactions financières, tels que les paiements mobiles sans contact. Un plus grand nombre d'entités distinctes peuvent être impliquées dans la fourniture d'un seul produit ou service, créant ainsi des réseaux complexes de dépendance opérationnelle[85]. De nouveaux services financiers fondés sur l'utilisation d'actifs numériques (ou « cryptoactifs ») ont également émergé. Or, les faibles garanties liées à la conservation des cryptoactifs les rendent vulnérables à des attaques cyber (par exemple les piratages de Mt. Gox en 2014 ou de Poly Network en 2021). Les plateformes centralisées ne sont pas les seules concernées puisque sur les 3,2 milliards de dollars de cryptoactifs volés en 2021 (près de 6 fois le montant volé en 2020), environ 2,3 milliards de dollars l'auraient été sur les plateformes DeFi[86] (« Decentralised Finance », cf. Banque de France, *Évaluation des risques du système financier français*, décembre 2021). Une étude souligne un coût moyen des incidents cyber liés aux cryptoactifs nettement plus élevé et l'existence d'une forte corrélation positive entre le prix du bitcoin et l'intensité des attaques sur les plateformes d'échanges de cryptoactifs[87]. Les cyberattaques contre des fournisseurs ont historiquement été suivis par des retraits importants de la part des clients, l'absence d'assurance des dépôts dans la DeFi renforçant la perception d'après laquelle tous les dépôts sont à risque[88]. La croissance du secteur de la DeFi pourrait conduire à une plus grande détention de ce type d'actifs, avec une hausse associée des effets de richesse, des expositions des institutions financières et des impacts sur la confiance en cas de matérialisation des vulnérabilités. Si les connexions directes entre les cryptoactifs, les

[78] www.cesin.fr/uploads/files/Barome%CC%80tre%20de%20la%20cyberse%CC%81curite%CC%81%20des%20entreprises%20vague%207-Opinionway-CESIN_Janv2022(1).pdf
[79] David E. Sanger, Nicole Perlroth, and Julian E. Barnes, *As Understanding of Russian Hacking Grows, So Does Alarm*, New York Times, 2 janvier 2021.
[80] Financial Stability Board, *Third-party dependencies in cloud services: Considerations on financial stability implications*, 2019.
[81] Feyen, Frost, Gambacorta, Natarajan and Saal, *Fintech and the digital transformation of financial services: implications for market structure and public policy*, BIS Papers, Juillet 2021.
[82] *Cloud Down*, 2018.
[83] Asensio, Bouveret, Harris, ESMA Report on Trends, Risks and Vulnerabilities, *Cloud outsourcing and financial stability risks*, 2021.
[84] FinTech, contraction de *Financial Technology* désigne des petites entreprises qui fournissent des services financiers grâce à des solutions innovantes.
[85] Feyen et al, op.cit.
[86] Chainalysis, *The 2022 Crypto Crime Report*, Février 2022.
[87] Aldasoro, Gambacorta, Giudici, Leach, *The drivers of cyber risk*, BIS Working Papers, 2020.
[88] IMF Blog, *Fast-Moving FinTech Poses Challenge for Regulators*, Avril 2022.

institutions financières d'importance systémique et les principaux marchés financiers demeurent pour l'heure limitées, elles sont néanmoins en croissance rapide et justifient un suivi attentif[89].

2.3 Les efforts menés pour renforcer la résilience opérationnelle du système financier doivent se poursuivre

Des évolutions réglementaires récentes ou programmées et la mise en place d'un cadre de supervision renforcent la résilience opérationnelle du secteur financier

La transformation numérique du secteur financier justifie un cadre réglementaire et de supervision permettant la maîtrise du risque cyber, au-delà des normes techniques existantes (comme par exemple le cadre de cybersécurité américain du National Institute of Standards and Technology– NIST). Les initiatives se sont donc multipliées depuis quelques années au niveau national, européen et international. Tout d'abord, des textes concernant le risque cyber et la résilience opérationnelle s'appliquent de manière transversale au-delà du secteur financier : la directive européenne NIS[90] (*Network and Information Security*) dont la révision est en cours, et la Loi de programmation militaire du 18 décembre 2013 définissent ainsi des règles de sécurité informatique pour les opérateurs de service essentiel (OSE) et les Opérateurs d'importance vitale (OIV) , parmi lesquels figurent certains acteurs du secteur financier.

Au niveau européen, les autorités européennes de surveillance (AES) ont publié entre 2019 et 2021 des orientations[91] concernant le risque informatique et la résilience opérationnelle. Ces textes de droit souple ont ouvert la voie au projet de règlement DORA (*Digital Operational Resilience Act*, cf. encadré 2.3) dont la négociation est en cours et l'entrée en vigueur serait pour fin 2022-début 2023. Ce règlement s'appliquera à la très grande majorité des acteurs du secteur financier et devrait permettre une plus grande harmonisation des règles de gestion du risque cyber. En France, l'ACPR s'est déclarée conforme aux orientations des AES concernant le risque informatique. Pour cela, le cadre réglementaire[92] a été ajusté, et l'ACPR a publié des Notices afin d'expliquer la réglementation et fournir à l'industrie des points de vigilance et des bonnes pratiques. En ce qui concerne les infrastructures de marché, la Banque de France étudie les modalités d'adoption du cadre européen TIBER-EU (*European framework for Threat Intelligence-based Ethical Red Teaming*) qui vise à harmoniser les pratiques d'exécution des tests de sécurité les plus avancés. Une réflexion est en cours afin de déterminer l'utilité de décliner ce cadre au niveau national pour la supervision par l'ACPR.

Encadré 2.3 : Le projet de règlement sur la résilience opérationnelle du numérique (DORA)

En avril 2019, sur demande de la Commission européenne, les autorités européennes de surveillance (AES) ont publié un avis conjoint sur la nécessité d'une avancée législative en matière d'exigences concernant la gestion, par le secteur financier européen, du risque lié aux technologies de l'information et de la communication par le secteur financier européen. La publication par la Commission européenne de la proposition de règlement DORA (*Digital Operational Resilience Act*) en septembre 2020 en a découlé. Le texte s'articule autour de quatre axes principaux :

- En ce qui concerne la gestion du risque informatique, le texte impose aux entités la formalisation de cartographies des actifs informatiques et des risques associés, ainsi qu'une gouvernance adaptée à la gestion du risque cyber. Tous les acteurs devront également mettre en œuvre des mesures de protection des systèmes et des données ainsi que des processus de détection d'anomalies ;

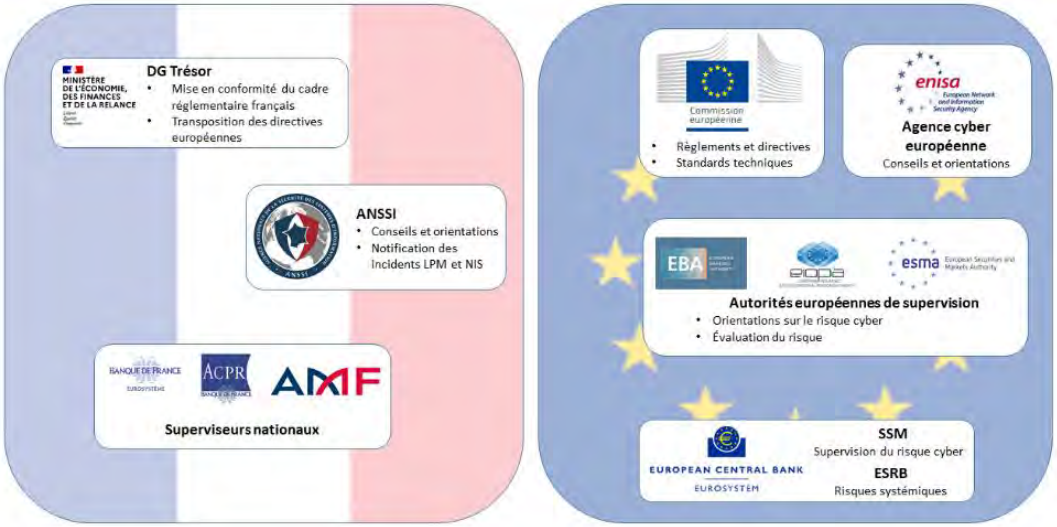
[89] Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-assets*, Février 2022.
[90] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016.
[91] Pour le secteur bancaire, les Orientations de l'Autorité bancaire européenne (ABE) sur la gestion du risque et de la sécurité informatique (EBA/GL/2019/04), sur la gouvernance interne (EBA/GL/2021/05) et sur l'externalisation (EBA/GL/2019/02). Pour le secteur de l'assurance, les orientations de l'Autorité européene des assurances et des pensions professionnelles (AEAPP) relatives à la sous-traitance à des prestataires en nuage (EIOPA-BoS-20-002).
[92] Pour le secteur bancaire, l'arrêté du 3 novembre 2014 sur le contrôle interne. Pour l'assurance, les articles L. 354-1 à L. 354-3 du Code des assurances.

- Les entités financières devront mettre en place des processus de gestion des incidents informatiques qui devront être catégorisés suivant des critères communs. DORA impose la notification au superviseur des incidents les plus importants dans un format harmonisé ;

- Le règlement impose la mise en œuvre d'une politique de tests de la résilience opérationnelle pour toutes les entités. En outre, pour les systèmes critiques, il définit les règles pour la conduite de test « avancés » (dits *threat-led penetration tests* - TLPT).

- En matière de gestion du risque de tiers et de surveillance des prestataires critiques, le texte édicte des exigences relatives à l'externalisation (notamment la mise en œuvre d'un registre des prestataires et des exigences relatives aux dispositions contractuelles) et instaure de manière novatrice une surveillance directe des prestataires informatiques identifiés comme critiques (*critical third party providers* – CTPP). Ce dernier axe prévoit notamment la mise en place d'un cadre de surveillance (*oversight framework*) sur le périmètre de leurs prestations de services informatiques aux entités du secteur financier de l'Union européenne.

Graphique 2.5 : Les principales autorités en matière de cybersécurité pour le secteur financier



Source : Banque de France

Les autorités de supervision financière et les autorités de sécurité de l'information coopèrent au niveau national et au niveau européen pour contrôler le risque cyber (cf. schéma supra). En France, l'ANSSI est chargée du risque cyber de tous les secteurs d'activité tandis que les superviseurs financiers intègrent le risque cyber à leurs contrôles et à leurs travaux, dans une optique de prévention mais également de gestion de crise. Au niveau européen, la BCE contrôle les banques les plus importantes dans le cadre du MSU, y compris pour le risque cyber. Les enjeux pour les superviseurs sont notamment de mieux connaître les incidents opérationnels, de pouvoir à terme surveiller les prestataires les plus critiques, et d'empêcher l'arbitrage réglementaire entre juridictions européennes. L'agence européenne de cybersécurité, l'ENISA, a pour rôle de favoriser la coopération et l'échange de bonnes pratiques entre autorités. Le CERS travaille sur les enjeux systémiques des crises cyber. Le sujet du risque cyber fait aussi l'objet de nombreux travaux internationaux, qui associent parfois l'industrie. À titre d'exemple, le Comité de Bâle a publié en mars 2021 des principes d'harmonisation pour la résilience opérationnelle et la gestion du risque opérationnel[93].

[93] *Principles for operational resilience ; Principles for the sound management of operational risk.*

L'adoption d'outils communs et le renforcement de la coordination figurent parmi les axes majeurs de travail pour renforcer la résilience du système dans son ensemble

Chaque entité du système financier dispose de sa propre organisation en matière de gestion des risques et constitue ainsi le premier maillon de la résilience face à un choc opérationnel majeur affectant le secteur financier. À ce titre, il est primordial que les dispositifs des institutions financières en matière de prévention, de réponse et de récupération après un incident continuent de se renforcer et de s'adapter. Toutefois, du fait des fortes interdépendances opérationnelles et financières entre acteurs, mais aussi de la forte interconnexion entre les différentes places financières, un cyber-incident, même ciblé, peut rapidement constituer une menace pour la stabilité du système financier dans son ensemble, ce qui justifie un renforcement de la capacité de prévention et de réponse collective.

Un premier moyen de faire face au risque cyber systémique est de travailler, aux niveaux européen et international, à l'adoption d'outils communs de mesure, de prévention et de gestion de crise. Tout d'abord, il apparaît aujourd'hui de plus en plus nécessaire – à la fois pour les entités financières et pour les superviseurs – de se doter d'outils communs pour affiner l'évaluation et l'appréciation des menaces et des incidents informatiques. L'aboutissement de projets concernant par exemple la systématisation des notifications des incidents graves aux autorités (règlement DORA) ou l'harmonisation des taxonomies d'incidents contribuera à pallier certaines difficultés de quantification du risque cyber. Une proposition de catégorisation commune des incidents informatiques, élaborée par l'ACPR et d'autres autorités du G7, a ainsi été publiée en avril 2021. Les travaux continuent sur ce sujet dans le cadre du Conseil de stabilité financière. L'adoption de ces outils permettrait d'évaluer plus finement le risque de chaque entité et favoriserait une meilleure comparabilité. Le Conseil de stabilité financière travaille également sur une révision du *Cyber Lexicon* de 2018[94] afin d'encourager l'emploi d'un vocabulaire commun et de permettre une meilleure identification des bonnes pratiques en matière de notification d'incidents cyber[95].

Pour mieux quantifier les risques qui pèsent sur le secteur financier, il sera également nécessaire de progresser dans l'identification des principales sources de risque cyber à l'échelle du système financier et dans l'analyse de leur impact potentiel sur la stabilité financière. À ce titre, les groupes de travail évoluant sous l'égide du Cyber Expert Group (CEG) du G-7 ont pu développer une première analyse sur les interdépendances opérationnelles entre acteurs financiers. Dans le même esprit, le CERS propose d'identifier les nœuds d'importance systémique sur les plans financier et opérationnel, y compris les fournisseurs tiers, afin de mieux comprendre les vulnérabilités existantes et les canaux de contagion au sein du système financier[96].

En matière de gestion de crise, le Conseil de stabilité financière a publié des bonnes pratiques en matière de réponse aux incidents cyber[97]. Le CEG du G7 se penche également sur des outils de réponse aux crises cyber, au risque de tiers, et aux rançongiciels. Plus largement, le CERS souligne la nécessité de renforcer la prise en compte du risque cyber dans les outils macroprudentiels, à travers une réflexion sur la notion de niveau acceptable d'interruption opérationnelle, la mise en œuvre de stress tests cyber systémiques, et le développement d'outils de gestion de crise propres au risque cyber systémique[98].

Outre ces outils, une coordination efficace entre acteurs privés et avec les autorités financières est propice à la création de relations de confiance dans le système financier, nécessaires au partage d'informations en temps normal comme en temps de crise majeure. Une coordination efficace requiert tout d'abord la mise en place de communautés de confiance, de canaux de communication sûrs et fiables ainsi que de processus bien définis entre entités pour garantir une forte réactivité en cas de crise. En France, banques, infrastructures de marché, autorités financières et services de l'État échangent dans le cadre organisé et sécurisé du groupe de place « Robustesse » (GPR) créé en 2005, dont le secrétariat est assuré par la Banque de France. Son objectif est de faciliter le partage d'informations et la coordination opérationnelle dans le cas d'un choc opérationnel majeur dont l'impact serait

[94] Ce lexique définit une cinquantaine de termes liés à la résilience et à la cybersécurité.
[95] *Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence* (octobre 2021)
[96] *Mitigating systemic cyber risk*, Janvier 2022.
[97] *Effective Practices for Cyber Incident Response and Recovery* (octobre 2020).
[98] *CERS, Mitigating systemic cyber risk, op.cit.*

systémique. Lors d'une crise, le GPR établit, à l'aide des informations collectées auprès de chacun des membres, un diagnostic complet de la situation de la Place, identifie les actions collectives possibles, fluidifie le dialogue des acteurs privés avec les services de l'État et les autorités et prépare l'après-crise.

La Banque de France et l'ACPR nouent également des liens de coopération bilatéraux en matière de cybersécurité avec des autorités financières étrangères. Un mémorandum d'entente (*Memorandum of Understanding* – MoU) a par exemple été signé avec l'Autorité monétaire de Singapour (MAS) en 2019 afin d'accroître la cyberrésilience des deux écosystèmes financiers, par le biais d'un partage d'informations sur les cyber-menaces et cyberincidents observés dans chaque juridiction. Au niveau européen, les échanges au sein de la plateforme CIISI-EU (*Cyber Information and Intelligence Sharing Initiative*), évoluant sous l'égide de l'ECRB (*Euro Cyber Resilience Board for pan-European Financial Infrastructures*), permettent à des acteurs publics et à des infrastructures de marché de partager des informations cyber stratégiques et opérationnelles au sein d'une instance de confiance et d'améliorer la connaissance collective sur le paysage des menaces cyber.

Pour renforcer le niveau de préparation des autorités financières en cas de crise cyber systémique, le CERS a émis en janvier 2022 une recommandation appelant à créer un cadre paneuropéen de coordination, nommé l'EU-SCICF (*pan-European Systemic Cyber Incident Coordination Framework*)[99]. Cette recommandation, vise à renforcer le partage d'informations et la communication de crise entre toutes les autorités financières de l'Union européenne et avec d'autres autorités au niveau international et favoriser une réponse collective cohérente et rapide. Le cadre EU-SCICF compléterait les dispositifs existants en matière de réaction aux incidents cyber, en prenant en compte la dimension systémique découlant du risque cyber.

Les exercices de simulation de crise, associant institutions financières et autorités publiques, sont également essentiels pour progresser dans la gestion individuelle et collective d'une crise cyber et limiter l'impact d'un potentiel incident systémique. Ainsi, pour renforcer son dispositif de gestion de crise, le Groupe de place Robustesse procède tous les ans à des exercices de place, au cours desquels ses membres s'entraînent à gérer les incidents et à assurer la continuité des services les plus critiques. Ces exercices sont conclus par une phase de retour d'expérience, pendant laquelle sont identifiés pour l'avenir des axes d'amélioration du dispositif de gestion de crise. Au niveau européen, l'Eurosystème a déjà organisé deux exercices, Titus (en 2015) et Unitas (en 2018), simulant une crise cyber affectant le système de paiement TARGET2 et la plateforme technique de règlement-livraison de titres T2S (TARGET2-Securities), en y associant les principales parties prenantes et utilisateurs de ces plateformes. Les autorités françaises participent également à des exercices de crise similaires organisés dans le cadre du G7, à l'instar de l'exercice de coordination transfrontralière (*cross border coordination exercise* – CBCE) piloté par la Banque de France lors de la Présidence française du G7 en 2019, qui a permis de valider un protocole de communication (le *Cyber Incident Response Protocol* ou G7 CIRP[100]) entre les 23 autorités financières du G7, mobilisable 24 h et 7j sur 7 en cas de crise cyber internationale.

(...)

[99] Recommendation of the European Systemic Risk Board of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities, 27 janvier 2022.
[100] Ce protocole définit notamment une liste de contacts et des modèles de documents pour recueillir l'information concernant un incident, afin de renforcer les capacités de réponse et de communication des autorités financières du G-7 en cas d'incident cyber affectant une ou plusieurs juridictions.

MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA RELANCE
*Liberté
Égalité
Fraternité*

Trésor-Éco

2

N° 295 • Décembre 2021

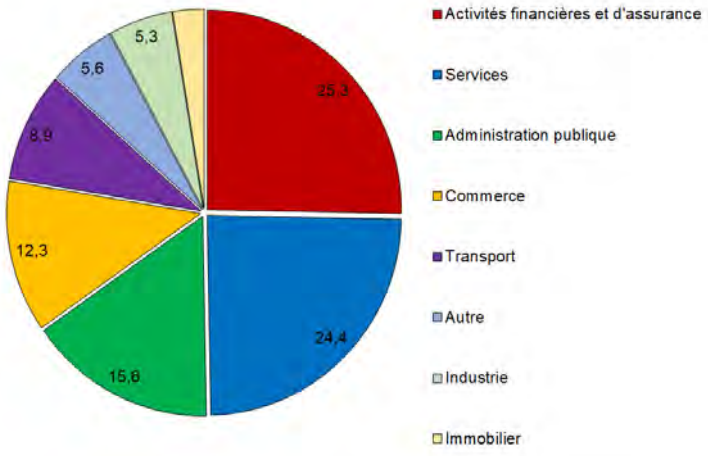
Direction générale du Trésor

Le risque cyber dans le secteur financier

Benjamin HADJIBEYLI, Adrien MOUTEL

- Le risque cyber désigne l'ensemble des risques liés à l'usage des technologies numériques et c'est aujourd'hui un des risques économiques majeurs. Il peut être défini comme un risque opérationnel portant sur la confidentialité, l'intégrité ou la disponibilité des données et systèmes d'information. Il recouvre à la fois les actes malveillants et les incidents non intentionnels issus d'erreurs humaines ou d'accidents.
- Le nombre d'incidents cyber est en forte augmentation, mais les coûts engendrés pour l'ensemble de l'économie restent difficiles à estimer. Ces coûts peuvent être directs ou indirects, affectant l'organisation qui subit l'incident mais également d'autres acteurs (entreprises partenaires, clients). Ils se chiffreraient en toute vraisemblance à plusieurs centaines de milliards d'euros par an pour l'économie mondiale.
- Le secteur financier est particulièrement ciblé par les cyberattaques en raison du potentiel de gains importants. Il est en outre fortement numérisé, ce qui accroît sa surface d'exposition. Le recours accru et soudain au télétravail en a fait un des secteurs les plus exposés durant la crise liée à la pandémie de Covid-19.
- Le secteur financier se caractérise également par de fortes interconnexions, accroissant les risques de propagation des chocs. Il repose sur la confiance des agents en son fonctionnement, confiance qui peut être remise en cause en cas d'incident. Même s'il n'a pas encore généré de crise systémique d'ampleur, le risque cyber est désormais identifié comme un des risques majeurs pour la stabilité financière.
- Les acteurs peuvent avoir tendance à sous-estimer le risque cyber et sous-investir en matière de cybersécurité. Pour assurer un niveau de sécurité suffisant, différents outils de politique publique peuvent être mobilisés : formation, réglementation, exercices de résilience, politique industrielle, cyber-assurance. Le projet de règlement européen DORA (*Digital Operational Resilience Act*) ou le groupe de travail sur la cyber-assurance lancé par la DG Trésor participent de cet effort.

Répartition des incidents cyber par secteur lors des six premiers mois de la pandémie de Covid-19 (mars-septembre 2020)



Note : Les données portent principalement sur les États-Unis.
Source : Aldasoro et al. (2021), "COVID-19 and cyber risk in the financial sector".

1. Le risque cyber couvre l'ensemble des risques provenant du monde numérique

1.1 Un risque dont le périmètre évolue

De façon générale, le risque cyber correspond à l'ensemble des risques liés au numérique. Il n'en existe pas de définition unique, étant donné son caractère relativement récent et son périmètre évolutif. On peut retenir la définition proposée par Cebula et Young (2010)[1], reprise depuis par d'autres travaux académiques et par les standards internationaux[2] : le risque cyber est un risque opérationnel pouvant affecter la confidentialité, l'intégrité ou la disponibilité des données ou systèmes d'information. D'autres propriétés, telles que l'authenticité, peuvent également être menacées[3]. La cybersécurité consiste en la protection de ces différentes propriétés par l'intermédiaire d'un dispositif de sécurité.

La définition du risque cyber englobe à la fois les actes malveillants et les risques ne relevant pas d'une intention de nuire : outre les actes de cybercriminalité, elle inclut la perturbation d'activités numériques par la matérialisation de risques physiques (incendie, coupure d'électricité) et les erreurs humaines (code informatique défectueux, mauvaise manipulation, négligence).

Parmi les différentes taxonomies qui ont été proposées, on peut retenir celle proposée par la Banque des règlements internationaux. Celle-ci classifie le risque cyber selon quatre dimensions :

- Les causes ou méthodes du risque cyber sont nombreuses et évoluent avec l'avancement de la technologie. Les causes de risque non intentionnelles sont relativement connues et évoluent peu, que ce soit les erreurs informatiques (code défectueux lors d'une mise à jour par exemple), la divulgation involontaire d'informations (*social engineering*) ou les risques physiques liés aux catastrophes naturelles. En revanche, les méthodes employées par des acteurs malveillants évoluent rapidement : logiciels malveillants (*malwares* – installation sans consentement d'un logiciel indésirable, comme les rançongiciels), hameçonnage (*phishing* – tentative de récupération d'informations confidentielles en se faisant passer pour une entité connue), déni de service (*DoS* – attaque visant à rendre indisponible un service), attaques *man-in-the-middle* (interception de communications, sur un réseau wifi public par exemple), failles *zero-day* (exploitation d'une vulnérabilité jusqu'alors non-corrigée présente dans un logiciel[4]).

- Le risque cyber peut provenir de différents acteurs. Il peut s'agir d'acteurs internes ou externes aux organisations visées. Parmi les acteurs externes, les États ou les groupes soutenus par des États ainsi que les groupes criminels sont une menace, mais le risque peut également provenir de hackers isolés. La mise à disposition d'outils et logiciels malveillants sur le web a engendré le développement d'un marché de « *crimeware as a service* », où des criminels peuvent acheter des outils perfectionnés.

- En termes d'intention, la principale distinction est le caractère malveillant (pour raisons financières ou politiques) ou non de l'incident cyber.

- Enfin, les conséquences peuvent êtres variées, et pas uniquement financières. Un incident cyber peut ainsi affecter durablement la réputation de l'organisme victime, et avoir des conséquences indirectes importantes au-delà de l'organisme visé[5] (par exemple en cas de fuite de données). L'ampleur des conséquences varie beaucoup : le risque cyber est à la fois un risque omniprésent, avec des occurrences dans le travail quotidien ou la vie privée qui n'ont qu'un impact limité (risque cyber « de tous les jours »), mais peut aussi donner lieu à des

(1) Cebula et Young (2010), "A Taxonomy of Operational Cyber Security Risks", Software Engineering Institute Technical Note CMU/SEI-2010-TN-028, Carnegie Mellon University.
(2) Voir par exemple Eling et Wirfs (2016), "Cyber risk: too big to insure? Risk transfer options for a mercurial risk class", *Université de Saint-Gallen*. Voir également le *Cyber Lexicon* du Conseil de stabilité financière.
(3) Par *confidentialité*, on entend la propriété selon laquelle les informations ne sont pas mises à la disposition de personnes, d'entités, processus ou systèmes non autorisés. Par *intégrité*, on entend l'exactitude et l'exhaustivité. Par *disponibilité*, on entend la capacité d'accéder et d'utiliser à la demande. Par *authenticité*, on entend la capacité à vérifier l'origine de l'information.
(4) Les failles *zero-day* sont des vulnérabilités n'ayant fait l'objet d'aucune publication ou de correctif connu : elles peuvent donc être utilisées par des hackers à l'insu des utilisateurs voire des créateurs du logiciel. En pratique, les attaques exploitent souvent des failles dites *one-day*, c'est-à-dire qui ont été divulguées mais dont le correctif n'a pas forcément été déployé ou installé pour tous les utilisateurs.
(5) On a par exemple observé des achats de panique avec l'afflux d'automobilistes américains dans les stations-services après l'attaque du Colonial Pipeline en mai 2021, ce qui a amené le président américain à déclarer l'état d'urgence.

incidents de type « cygne noir », à fréquence faible mais aux conséquences potentielles catastrophiques.

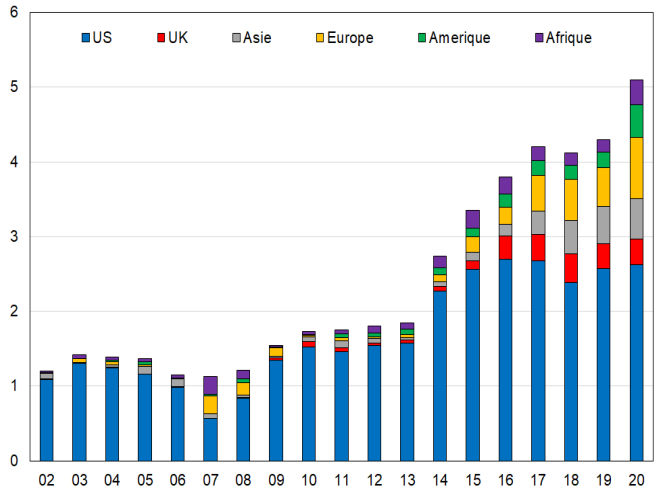
1.2 Un risque difficilement quantifiable mais vraisemblablement en hausse

Quantifier le risque cyber est difficile, à la fois en raison de son périmètre évolutif et de l'absence de transparence sur les incidents. Le mesurer suppose d'évaluer à la fois la fréquence d'occurrence du risque et son impact économique potentiel.

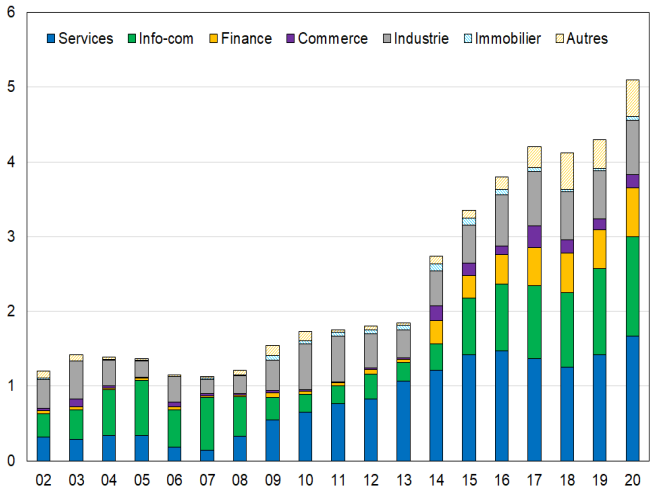
La forte augmentation du risque cyber depuis plusieurs années fait cependant consensus, et elle est documentée par des études académiques. Jamilov *et al.* (2021) montrent, à l'aide d'une analyse textuelle des transcriptions des conférences d'annonce de résultats financiers, que les références au risque cyber augmentent et correspondent à un sentiment de plus en plus négatif[6]. En analysant l'évolution du risque par zone géographique et par secteur, ils mettent en évidence que le risque s'est d'abord développé aux États-Unis, puis propagé aux autres régions du monde (*cf.* Graphique 1A), et qu'il se concentrerait particulièrement sur les secteurs des services aux entreprises (secteur qui inclut les fournisseurs de services de cybersécurité) et celui de l'information et de communication. Leurs travaux montrent également une forte augmentation de ce risque pour le secteur financier (*cf.* Graphique 1B). En examinant les causes et le coût des incidents cyber entre 2002 et 2018, Aldasoro *et al.* (2020) montrent la forte hausse du nombre d'incidents, même si le coût moyen reste faible. Le coût moyen et les causes d'incidents dépendent beaucoup du secteur. Par exemple, si le secteur financier est parmi les plus touchés, le coût moyen des incidents y est plus faible, ce qui peut s'expliquer selon les auteurs par un niveau d'investissement plus élevé en la matière[7].

Graphique 1 : Évolution du risque cyber

A. Par zone géographique



B. Par secteur d'activité



Note de lecture : Ces deux graphiques représentent la part des conférences de presse trimestrielles d'entreprises comportant une mention d'un ou plusieurs termes du champ lexical du risque cyber (en % du nombre total de conférences de presse comprises dans l'échantillon), agrégée par zone géographique et par secteur d'activité.
Source : Jamilov et al. (2021).

Le risque cyber affecte les organisations de différentes manières, à commencer par un impact direct d'ordre financier, comme le paiement d'une rançon ou le manque à gagner à la suite d'une interruption d'activité. Un incident cyber peut aussi avoir un impact indirect sur l'entreprise victime, par exemple en nuisant à sa réputation, dont l'ampleur est difficilement mesurable. Plusieurs études sur des entreprises cotées montrent ainsi que la révélation d'un incident cyber influe négativement sur le cours boursier de l'entreprise victime[8].

(6) Jamilov, Rey et Tahoun (2021), "The anatomy of cyber risk", *NBER working paper* n° 28906.
(7) Aldasoro, Gambacorta, Giudici et Leach (2020), "The drivers of cyber risk", *BIS Working Papers* 865.
(8) Voir Amir, Levi et Livne (2019), "Do firms underreport information on cyber-attacks? Evidence from capital markets", *Review of Accounting Studies*, et Tosun (2021), "Cyber Attacks and Stock Market Activity", *International Review of Financial Analysis* 76.

Un incident cyber peut également avoir un impact indirect sur des tiers, que ce soit par une perte de confiance affectant l'ensemble d'un secteur, la perte ou l'altération de données utilisées par plusieurs entreprises, l'impact d'une discontinuité de l'activité d'une entreprise sur l'ensemble de la chaîne de valeur, ou l'augmentation durable de l'aversion au risque.

Plusieurs études ont cherché à estimer l'impact agrégé résultant de ces effets directs et indirects, avec des ordres de grandeur qui varient substantiellement. En 2018, le Comité européen du risque systémique (CERS) recensait des estimations d'un coût annuel mondial allant de 50 Md$ à 650 Md$[9]. McAfee et le *think tank* Center for Strategic & International Studies l'estiment à près de 1 000 Md$ en 2020, soit plus de 1 % du PIB mondial[10].

Certains travaux cherchent par ailleurs à estimer la dispersion des impacts possibles, mobilisant le concept de *value-at-risk* : outre la perte moyenne anticipée, cette approche cherche à estimer une perte probable réaliste (atteignable avec une probabilité de 5 ou 10 %). Dreyer *et al.* (2018), dans un exercice méthodologique consistant à comparer plusieurs méthodes mises en œuvre dans la littérature, mettent en évidence la forte incertitude qui pèse sur ces estimations et la forte sensibilité aux paramètres retenus, obtenant des estimations de coût annuel moyen allant de 275 Md$ à 3 200 Md$ pour l'impact direct et de 800 Md$ à 10 100 Md$ pour l'impact global. Une méthode alternative mobilisant le concept de *value-at-risk* estime l'impact direct à 6 600 Md$ et l'impact total à 22 500 Md$, soit une *value-at-risk* à 5 % d'environ un tiers du PIB mondial pour la borne haute[11]. Dans le secteur financier, Bouveret (2018) estime que la perte moyenne annuelle liée aux cyberattaques représenterait environ 10 % du résultat net des banques au niveau mondial, soit environ 100 Md$, mais pourrait aller jusqu'à 30 % dans un scénario dégradé (doublement des cyberattaques par rapport à 2013)[12].

2. Le risque cyber touche particulièrement le secteur financier et est susceptible de remettre en cause la stabilité financière

2.1 Le secteur financier est particulièrement concerné

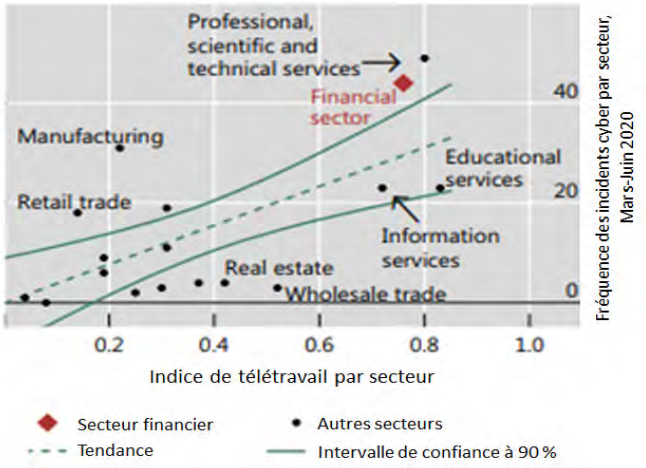
Selon le Boston Consulting Group, les entreprises du secteur financier seraient 300 fois plus susceptibles d'être ciblées que celles d'autres secteurs[13]. La plupart des études académiques identifient le secteur financier comme figurant parmi les secteurs les plus victimes d'incidents cyber. En raison d'un recours massif et soudain au télétravail, il aurait été particulièrement exposé lors de la pandémie de Covid-19 (*cf.* Graphique de la page de garde). Le secteur financier est d'autant plus concerné par le risque cyber qu'il est fortement numérisé[14], les principales infrastructures de marché (services de paiement, règlement, compensation, etc.) étant entièrement dématérialisées, ainsi qu'une grande partie des activités bancaires (échange de titres financiers, banque de détail). Si le secteur a subi quelques attaques d'ampleur ces dernières années, comme celle liée au *malware* Carbanak ou le cyberbraquage de la Banque centrale du Bangladesh[15], il n'a pas encore subi d'incident d'une ampleur systémique.

(9) European Systemic Risk Board (2020), "Systemic cyber risk", *ESRB Reports*.
(10) McAfee et Center for Strategic and International Studies (2020), "The Hidden Costs of Cybercrime".
(11) Dreyer *et al.* (2018), "Estimating the global cost of cyber risk", *Research Reports RR-2299-WFHF*, Rand Corporation.
(12) Bouveret (2018) "Cyber risk for the financial sector: a framework for quantitative assessment", IMF Working Papers 18/143.
(13) Zakrzewski et al. (2019), "Global Wealth 2019: Reigniting Radical Growth", Boston Consulting Group.
(14) À titre d'exemple, l'OCDE le classe parmi les secteurs à haute intensité numérique. Calvino (2018), "A taxonomy of digital intensive sectors", *OECD STI Working Paper* 2018/14.
(15) Le *malware* Carbanak a permis à des malfaiteurs de voler plus de 1 Md$ à une centaine de banques dans plus de 40 pays entre 2003 et 2018. En 2016, un groupe de hackers est parvenu à braquer la Banque centrale du Bangladesh en profitant de failles dans le réseau de paiement international SWIFT, récupérant ainsi près de 100 M$.

Encadré 1 : Un problème renforcé par la pandémie de Covid-19

Le fort développement du télétravail en lien avec la pandémie de Covid-19 a exacerbé les vulnérabilités au risque cyber en élargissant la surface d'exposition aux attaques. La numérisation accélérée des activités des entreprises en un temps réduit a rendu plus difficile le maintien des standards de cybersécurité. Une première adaptation au développement du télétravail a été le déploiement d'outils facilitant le travail à distance, à l'image des technologies d'accès au poste à distance (*remote desktop protocol*, RDP) et de réseau privé virtuel (*virtual private network*, VPN), qui ont néanmoins fait l'objet de multiples incidents. À cet égard, Aldasoro *et al.* (2021)[a] ont mis en évidence un lien fort entre le niveau de « télétravaillabilité » des postes par secteur et l'incidence des cyberattaques au T2 2020 (*cf.* Graphique 2). Ce risque devrait rester important à moyen terme en cas de pérennisation du télétravail.

Graphique 2 : Fréquence d'incidents cyber selon la part d'emploi permettant le télétravail, par secteur



Source : Aldasoro et al. (2021), "COVID-19 and cyber risk in the financial sector".

a. Aldasoro, Frost, Gambacorta et Whyte (2021), "COVID-19 and cyber risk in the financial sector", *BIS Bulletin* N° 37.

2.2 Le risque cyber peut devenir systémique

Le secteur financier est sujet à un risque de contagion en raison de sa forte interconnexion. En effet, le système financier contient des acteurs systémiques, principalement des banques et des assurances, qui concentrent une partie importante des actifs et des flux, et sont fortement reliés entre eux. Ainsi, un évènement isolé portant sur une unique entité du secteur financier peut se propager plus largement, dans un phénomène de contagion, et ce même au-delà des frontières.

Pour étudier l'impact potentiel d'un incident cyber sur le secteur financier, certaines études adoptent une approche similaire à celle des *stress tests*, c'est-à-dire qu'elles estiment la capacité financière des organisations à absorber un choc d'ampleur significative. Par exemple, Duffie et Younger (2019) montrent que les douze plus grandes banques américaines auraient suffisamment d'actifs liquides pour faire face à un incident cyber majeur[16]. Au contraire, Eisenbach *et al.* (2020) estiment qu'un incident cyber de grande ampleur, défini comme une interruption d'une journée entière des paiements d'une banque, pourrait avoir un impact critique sur l'ensemble du système financier s'il touche une des cinq plus grandes banques américaines[17].

Le secteur financier se distingue également par le fait qu'il repose fortement sur la confiance des acteurs en la sécurité du système. Le CERS a étudié comment un incident cyber pourrait remettre en cause la stabilité financière[18]. L'élément déclencheur d'une crise systémique pourrait prendre diverses formes (*cf.* Encadré 2). À titre illustratif, une attaque causant la destruction, l'altération ou le chiffrement irrémédiable de données d'une institution financière pourrait générer des pertes ou une discontinuité de l'activité suffisantes pour engendrer une érosion de la confiance des agents dans le système financier, entraînant des retraits massifs et simultanés des dépôts bancaires ou encore un gel de la liquidité sur le marché interbancaire.

(16) Défini comme une perte cumulée de 75 % des flux entrants de dépôts sur 30 jours. Voir Duffie et Younger (2019), "Cyber runs", *Hutchins Center Working Paper* n° 51.
(17) Eisenbach, Kovner et Lee (2020), "Cyber risk and the US financial system: a pre-mortem analysis", *Federal Reserve Bank of New York Staff Report* n° 909.
(18) European Systemic Risk Board (2020), Systemic cyber risk.

Encadré 2 : Exemples hypothétiques d'incidents cyber systémiques du CERS[a]

- Scénario 1 (accidentel) : une mise à jour provoque une interruption accidentelle du système de paiement d'une grande banque systémique, empêchant entreprises et particuliers d'accéder à leurs comptes et d'effectuer des transactions. L'incident est aggravé par l'apparition de rumeurs d'une cyberattaque sur les réseaux sociaux, menant à une perte de confiance généralisée dans le système de paiement.
- Scénario 2 (logiciel malveillant) : une cyberattaque lance simultanément une multitude de transactions sur les comptes tenus par une grande banque, altérant ainsi les soldes des comptes tenus ; les attaquants ayant pénétré depuis plusieurs mois le système d'information, les sauvegardes et procédures de restauration sont également affectées. La banque est ainsi dans l'incapacité de participer aux opérations financières pendant une longue période et la restauration des données n'est pas possible à court terme.
- Scénario 3 (attaque *man-in-the-middle*) : un logiciel malveillant affecte les informations transmises par des fournisseurs de données de marché et par une chambre de compensation centrale, menant à l'échec de transactions et à l'inexactitude des prix et positions affichés. Les acteurs de marché doutent progressivement des informations qu'ils reçoivent, ce qui mène à un assèchement du marché, un retour aux compensations bilatérales et finalement des ventes éclairs, les investisseurs cherchant à se défaire d'une position incertaine.

a. *Cf.* CERS (2020), "The making of a cyber crash".

L'étude de ces différents éléments suggère ainsi qu'un incident cyber alliant une intention malveillante à une propagation rapide et large pourrait être de nature systémique. La nature de la menace serait déterminante, une cyberattaque motivée par une intention de déstabiliser le système financier, au-delà du simple appât du gain, pourrait davantage conduire à un choc de confiance. Les fonctions touchées seraient aussi déterminantes, un évènement entraînant une perte d'intégrité permanente des données (ou apparaissant comme tel) étant plus susceptible de conduire à un évènement systémique. S'agissant des canaux de propagation, la probabilité qu'un évènement cyber ait un impact systémique serait fortement accrue si celui-ci s'accompagne d'une perte de confiance des agents. Enfin, une bonne préparation de la part des entreprises et des autorités réduirait la probabilité de survenance d'un évènement systémique. Pour toutes ces raisons, le Haut Conseil de stabilité financière a rappelé en septembre 2021 l'importance de mettre en œuvre des mesures adéquates de prévention et protection face à ce risque, et de conduire régulièrement des exercices de gestion de crise[19].

3. Des politiques publiques sont nécessaires afin que le secteur se protège correctement contre ce risque

3.1 Plusieurs défaillances de marché peuvent mener à un sous-investissement dans la cybersécurité

Plusieurs imperfections de marché peuvent justifier des mesures de politique publique[20]. Tout d'abord, il peut y avoir un désalignement des incitations entre les acteurs responsables de la cybersécurité et ceux qui en bénéficient. Ce désalignement concerne souvent les entreprises et leurs clients, les entreprises arbitrant entre la recherche de rendement (numérisation, réduction des coûts) et la sécurité des usagers. Par exemple, les banques encouragent leurs clients à utiliser les services en ligne afin de réduire les coûts opérationnels, mais elles n'encourent qu'une partie du coût des failles de sécurité.

La cybersécurité est également un domaine où il y a de fortes asymétries d'information. S'il peut être facile de mettre en évidence une faille de sécurité, il est impossible de prouver qu'un système est sécurisé. Une entreprise peut ainsi se montrer réticente à divulguer qu'elle a été victime d'une faille de sécurité, de peur de

(19) Communiqué de presse du HCSF du 14 septembre 2021.
(20) Voir Moore (2010), "The economics of cybersecurity: principles and policy options", *International Journal of Critical Infrastructure Protection*.

nuire à sa réputation. Il en résulte un marché où la qualité de l'offre des produits des fournisseurs de services de cybersécurité est difficilement observable, et donc peu différenciable par les clients.

Par ailleurs, la cybersécurité génère de nombreuses externalités. Ces externalités peuvent dans certains cas être bénéfiques. Les externalités engendrées par le risque cyber sont la plupart du temps négatives, soit par la propagation de la menace (par exemple via le recours à des sous-traitants[21]), soit par des canaux économiques de transmission (perte de réputation dans le secteur, discontinuation du service). De ce fait, la sécurisation des opérateurs d'importance vitale (OIV) limite les conséquences néfastes que la compromission d'une de ces entités pourrait avoir sur l'ensemble de la société. Il est donc légitime que la puissance publique s'assure de leur résilience.

Aldasoro *et al.* (2020)[22] trouvent qu'en moyenne les entreprises sous-investissent dans la cyber-sécurité, mais ce n'est pas le cas dans certains secteurs dont la finance. Toutefois, le modèle utilisé estime des dépenses optimales au niveau individuel[23] et ne prend pas en compte les externalités éventuelles.

En termes d'emploi, le secteur de la cybersécurité souffrirait en outre d'une pénurie mondiale de compétences. 70 % des professionnels du secteur déclarent un manque de spécialistes au sein de leur organisation, et 45 % d'entre eux indiquent que la situation se serait détériorée ces dernières années[24]. Outre les postes restant à pourvoir, il semble y avoir un désalignement des compétences au niveau des postes pourvus, les employés actuels du secteur provenant pour beaucoup d'autres corps de métier informatiques ou ayant un parcours professionnel dans le domaine datant de moins de 3 ans.

3.2 Plusieurs interventions publiques peuvent être mise en œuvre

Ces défaillances de marché impliquent que des politiques publiques peuvent être mobilisées pour en limiter les effets.

Premièrement, la réglementation peut agir pour rendre le marché de la cybersécurité plus efficient. Elle peut par exemple réaligner les incitations des entreprises et de leurs clients en imposant que l'entreprise soit garante de la sécurité des données de ses clients. Elle peut ensuite réduire les asymétries d'information en imposant aux entreprises de déclarer leurs incidents de cybersécurité[25]. Elle peut aussi développer des mécanismes de certification, tel le système introduit par le *Cybersecurity Act* au niveau européen, qui vise à harmoniser les méthodes d'évaluation du degré de protection conféré par les produits de cybersécurité afin d'en faciliter l'appréciation par les entreprises clientes. La proposition de règlement européen sur la résilience opérationnelle numérique du secteur financier (*Digital Operational Resilience Act*, ou DORA) va également dans ce sens, en renforçant les remontées d'incidents et les mesures prescriptives de protection, et en imposant des exigences de sécurité aux prestataires de services (*cloud* notamment) jugés critiques.

Deuxièmement, les autorités peuvent développer la capacité de réponse et de gestion de crise et la bonne appréciation des risques grâce à des tests de résilience (*stress tests*). Le projet DORA permettra également de renforcer les tests de résilience imposés aux acteurs. Elles peuvent également développer des systèmes de protection spécifiques pour les entités jugées systémiques d'un point de vue numérique, comme les opérateurs d'importance vitale. La résilience face au risque cyber passe aussi par les actions de sensibilisation, notamment de formation des salariés, le facteur humain étant une source majeure de vulnérabilité de la sécurité des systèmes d'information.

(21) Et notamment le recours à des prestataires de services de cloud, qui concentrent une partie importante du risque.
(22) Aldasoro, Gambacorta, Giudici et Leach (2020), "The drivers of cyber risks", *BIS Working Paper* 865.
(23) Le modèle consiste à calibrer l'investissement en sécurité informatique sur la base d'une analyse coût-bénéfice paramétrée à partir de données réelles d'incidents.
(24) Enterprise Strategy Group (2021), *The life and times of cybersecurity professionals in 2020*. Les professionnels nord-américains sont néanmoins surreprésentés dans l'échantillon de l'enquête (92 %), contre seulement 4 % d'entreprises domiciliées en Europe.
(25) *Cf.* Rapport d'octobre 2021 du FSB « Cyber incident reporting: existing approaches and next steps for broader convergence ».

Troisièmement, comme pour toute activité très innovante, le développement des capacités en cybersécurité génère des externalités positives pour l'ensemble de la société, que les fournisseurs de services de cybersécurité peuvent ne pas intérioriser, investissant alors en R&D de manière sous-optimale. Une politique industrielle incitant à la R&D peut dès lors être développée pour y remédier. Cette politique industrielle peut être complétée par le développement des compétences, essentielles dans une activité intensive en capital humain comme la cybersécurité, et où les difficultés de recrutement sont connues. C'est notamment l'un des objectifs du Plan cyber annoncé l'an dernier et l'une des priorités du plan d'investissement France 2030[26].

Enfin, des mécanismes d'assurance privée du risque cyber peuvent réduire ces failles de marché, en faisant internaliser le risque aux acteurs par le biais des prix de primes d'assurance et en imposant des normes de sécurité. Les mécanismes d'assurance du risque cyber sont recommandés depuis longtemps par les économistes, mais dans la pratique le marché reste peu développé[27]. Plusieurs facteurs peuvent expliquer ce manque de succès. Tout d'abord, la demande pour ce type d'assurance est limitée, la plupart des entreprises ne réalisant pas l'existence ou l'étendue du risque auquel elles font face. De l'autre côté, l'offre d'assurance est elle aussi peu développée, car le risque cyber est difficile à chiffrer pour les assureurs, qui disposent de données incomplètes, peu standardisées et avec un faible recul temporel. Ces caractéristiques, en particulier la forte asymétrie d'information entre assureurs et assurés, rendent le risque cyber difficilement assurable. Enfin, le risque cyber est caractérisé par une forte interdépendance des risques et une dépendance à de grands acteurs, ce qui rend ces risques très corrélés potentiellement très coûteux pour les assurances[28]. Pour approfondir la compréhension de ces difficultés et permettre le bon développement de ce marché, une concertation nationale sur l'assurance du risque cyber a été lancée en 2021 par la Direction générale du Trésor.

(26) Voir le dossier de presse de France Relance « Cybersécurité, faire face à la menace : la stratégie française ».
(27) MacColl, Nurse et Sullivan (2021), "Cyber Insurance and the Cyber Security Challenge", *Royal United Services Institute for Defence and Security Studies Occasional Paper*. Selon une étude récente de l'AMRAE, 8 % des ETI françaises auraient une assurance contre le risque cyber. *Cf.* « Lumière sur la cyberassurance », mai 2021.
(28) Voir par exemple Granato et Polacek (2019), "The growth and challenges of cyber insurance", *Chicago Fed Letter* n° 426, Federal Reserve Bank of Chicago.

Éditeur :

Ministère de l'Économie,
des Finances
et de la Relance
Direction générale du Trésor
139, rue de Bercy
75575 Paris CEDEX 12

Directeur de la Publication :

Agnès Bénassy-Quéré

Rédacteur en chef :

Jean-Luc Schneider
(01 44 87 18 51)
tresor-eco@dgtresor.gouv.fr

Mise en page :

Maryse Dos Santos
ISSN 1777-8050
eISSN 2417-9620

Derniers numéros parus

Décembre 2021

N° 294 Évaluations économiques des services rendus par la biodiversité
Vincent Bouchet, Clémence Bourcet, Eléonore Cécillon, Sophie Lavaud

Novembre 2021

N° 293 Discriminations sur le marché du travail : comment les mesurer, quel coût économique ?
Cyprien Batut, Chakir Rachiq

N° 292 Le positionnement de la Chine parmi les bailleurs en Afrique subsaharienne
Louis Bertrand, Sary Zoghely

https://www.tresor.economie.gouv.fr/Articles/tags/Tresor-Eco

Direction générale du Trésor

@DGTrésor

Pour s'abonner à *Trésor-Éco* : tresor-eco@dgtresor.gouv.fr

 WP/18/143

IMF Working Paper

Strategy, Policy & Review Department

Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

Prepared by Antoine Bouveret*

Authorized for distribution by Vikram Haksar

June 2018

Abstract

Cyber risk has emerged as a key threat to financial stability, following recent attacks on financial institutions. This paper presents a novel documentation of cyber risk around the world for financial institutions by analyzing the different types of cyber incidents (data breaches, fraud and business disruption) and identifying patterns using a variety of datasets. The other novel contribution that is outlined is a quantitative framework to assess cyber risk for the financial sector. The framework draws on a standard VaR type framework used to assess various types of stability risk and can be easily applied at the individual country level. The framework is applied in this paper to the available cross-country data and yields illustrative aggregated losses for the financial sector in the sample across a variety of scenarios ranging from 10 to 30 percent of net income.

JEL Classification Numbers: E44, G11, G21, G22

Keywords: Cyber risk, systemic risk, operational risk, risk management.

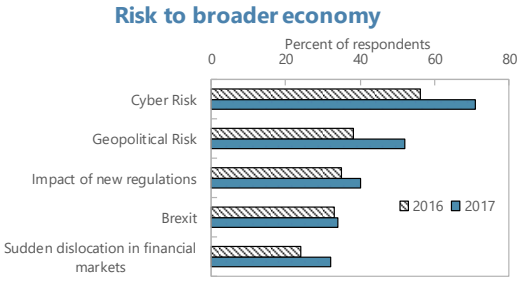
Author's E-Mail Address: abouveret@imf.org.

* Antoine Bouveret is an economist in the Macro-Financial Unit in the Strategy, Policy & Review Department. The author would like to thank Luke Carrivick from ORX, Sanjay Christo, Tamas Gaidosch,Vikram Haksar, Emmanuel Kopp, Rodolfo Maino, Manasa Patnam, Celine Rochon, Helene Poirson-Ward, Natalia Stetsenko, Aminata Touré, Andrew Tiffin, Christopher Wilson and Kevin Wiseman for helpful comments.

I. INTRODUCTION

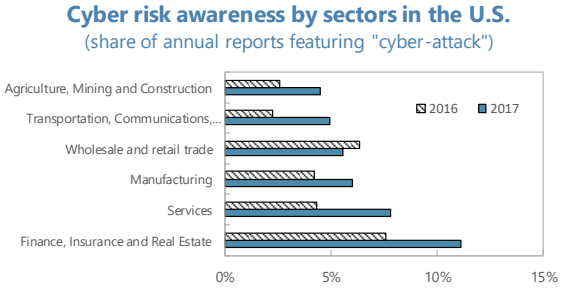
Cyber risk has emerged as a systemic risk concern, following recent cyber incidents (IIF (2017), IMF (2017b), OFR (2017)). Recent surveys point to cyber risk as a main concern among market participants ranked first in the DTCC Systemic Risk Barometer (Figure 1), and second in the 2017 H2 systemic risk survey by the Bank of England (Bank of England (2017)). Successful cyber-attacks such as Wannacry in May 2017 or NoPetya in June 2017 have shown that cyber-attack can lead to severe disruptions and major losses for the targeted firms.

Figure 1: Survey of risks to financial stability



Source: DTCC Systemic Risk barometer 2017Q1

Figure 2: Reporting of cyber risk



Sources: SEC form 10-K; and staff calculations.

Data on cyber incidents is scarce and there have been very few quantitative analyses of cyber risk.[1] Data on cyber risk is notoriously scarce, since there is no common standard to record them, and firms have no incentives to report them. For example, in the U.K. only 49 cyber-attacks were reported in 2017 to U.K. Financial Authorities, pointing to a material under reporting of successful cyber-attacks in the financial sector (Butler (2017)).[2] Moreover, international sharing of data reported to domestic regulators also has to take into account — beyond the typical privacy and other constraints— that there might be national security considerations in sharing and reporting of data.

In the U.S., the SEC released in 2011 guidance on disclosure of cyber risk for listed firms (SEC (2011)), which was revised in 2018 to provide additional details on how and when firms should disclose the information to investors (SEC (2018)). However, there is scope to provide a framework to report cyber-attacks, which could better address existing data gaps.

For example, among around 4,000 annual reports for U.S firms ('form 10-K') published in 2017, only 7 percent included a reference to cyber-risk, mainly in the finance and services sectors (Figure 2).

[1] Recent empirical work includes Biener et al. (2015) and Romanosky (2016).

[2] It is useful to make a distinction between cyber incidents and cyber-attacks. Incidents cover a broader category, while cyber-attacks cover malicious use of Information and Communication Technologies (ICT). This paper, and the data used, focus on cyber-attacks.

In the European Union, the General Data Protection Regulation (GDPR), which will enter into force in May 2018, requires firms to report breaches to the competent supervisory authority within 72 hours. Failure to comply with the reporting requirements could lead to fines up to EUR 20 Mn or 4 percent of global annual turnover (whichever is higher).

This paper provides a framework for assessing cyber risk for financial institutions complemented by a qualitative and quantitative overview. The financial sector is one of the most targeted sectors due to its reliance on information and its central role in the credit intermediation process (Kopp et al. (2017)). Moreover, due to regulatory requirements regarding operational risk, financial institutions are more likely to collect data on cyber incidents than non-financial corporates.

The objective of this paper is to shed light on cyber risk for financial institutions using publicly available data and commercial data sets, with potential use by regulators, supervisors and financial institutions. Section II provides an overview of recent cyber-attacks on financial institutions. Section III describes channels through which cyber risk can impact financial stability. Section IV provides an operational framework and methodology to assess aggregate losses for the financial sectors and some quantitative estimates.

II. AN OVERVIEW OF CYBER-ATTACKS TARGETED AT FINANCIAL INSTITUTIONS

A. Cyber risk and types of cyber-attacks

Cyber risk can be defined as "*operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems*" (Cebula and Young (2010)). Compared to risk categories covered by insurance, cyber risk shares characteristics with both property and liability risk, as well as catastrophic and operational risk (Eling and Wirfs (2016)). On the one hand, cyber risk can impact first (the target) and third parties (a counterpart to the target). On the other hand, losses due to cyber risk are frequently small and independent but they could also have a low frequency and a high impact ('blackout scenario'). Cyber risk can be unrelated to cyber-attacks: for example, software updates or natural disasters can lead to the crystallization of cyber risk through business disruptions without any nefarious intent, as outlined in the definition of cyber incidents (see footnote 2).

Cyber-attacks can impact firms through the three main aspects of information security: confidentiality, integrity and availability. Confidentiality issues arise when private information within a firm is disclosed to third parties as in the case of data breaches. Integrity issues relate to misuse of the systems, as is the case for fraud. [3] Finally, availability issues are linked to business disruptions. The three types of cyber-attacks have different direct impacts on the targets: Business disruptions prevent firms from operating, resulting in loss revenue; fraud leads to direct financial losses; while the effects of data breaches take more time to materialize, through reputational effects as well as litigation costs. More generally, the risk of

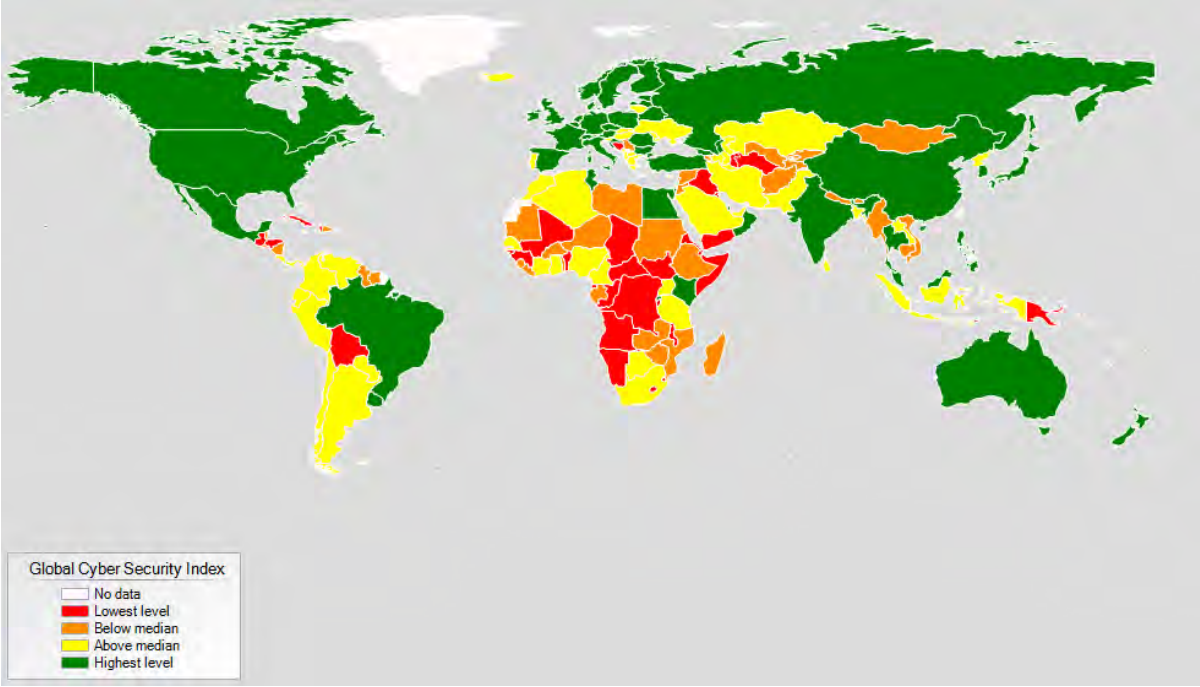
[3] We follow the taxonomy used by ORX, although other definitions exist. For example, the CRO forum (2016) considers data breaches, fraud, business disruptions and a fourth type of cyber-attack which occurs when the attacker is able to affect the integrity of the targeted institution by modifying its internal data. For simplicity, integrity attacks are included in the three main types of cyber-attacks referred above.

a loss of confidence following cyber-attacks could be high for the financial sector, given the reliance of financial institutions on the trust of their customers. Regarding the financial system, business disruptions are more likely to have direct short-term contagion effects than fraud or data breach, which tend to impact mainly the targeted firm in the short-term.

B. Which countries are more exposed to cyber risk?

The financial sector is highly exposed to cyber risk, across all types of countries. The International Telecommunication Unit (ITU)— an agency of the United Nations— provides a global cybersecurity index for the world. Their index is based on a range of factors, including legal, technical and organizational arrangements as well as capacity building and cooperation (ITU (2017)). Figure 3 shows the cross-country heterogeneity regarding cybersecurity, with most Advanced Economies and Emerging Markets having a high value of the cybersecurity index (above the median), while middle income and low-income countries tend to have lower values.

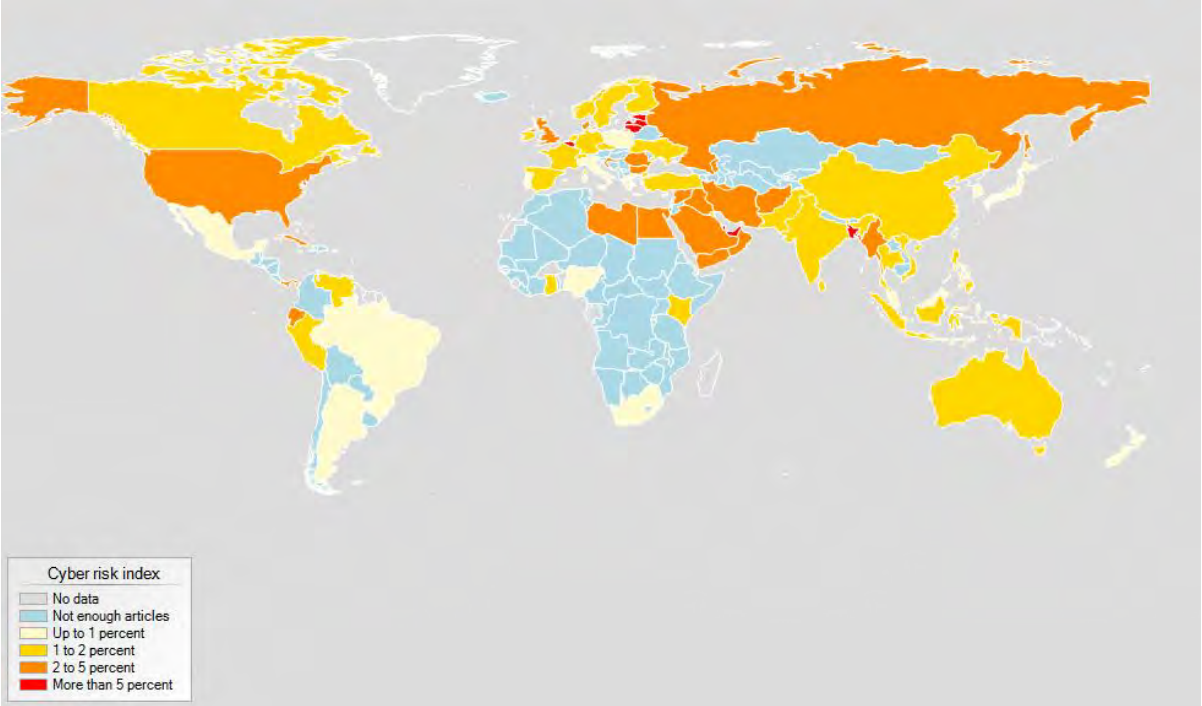
Figure 3: Global Cybersecurity Index



Source: ITU (2017).

Since there is no quantitative measure of cyber risk by country for the financial sector, we build an indirect measure using media coverage. An index is computed using the number of articles referring to cyber risk by country, divided by the number of articles referring to risk in the financial sector (Figure 4). As shown in the map, almost all countries are covered. The index is highest in countries that recently suffered from cyber-attacks such as Bangladesh and the Baltic states.

Figure 4: Measure of cyber risk for banks



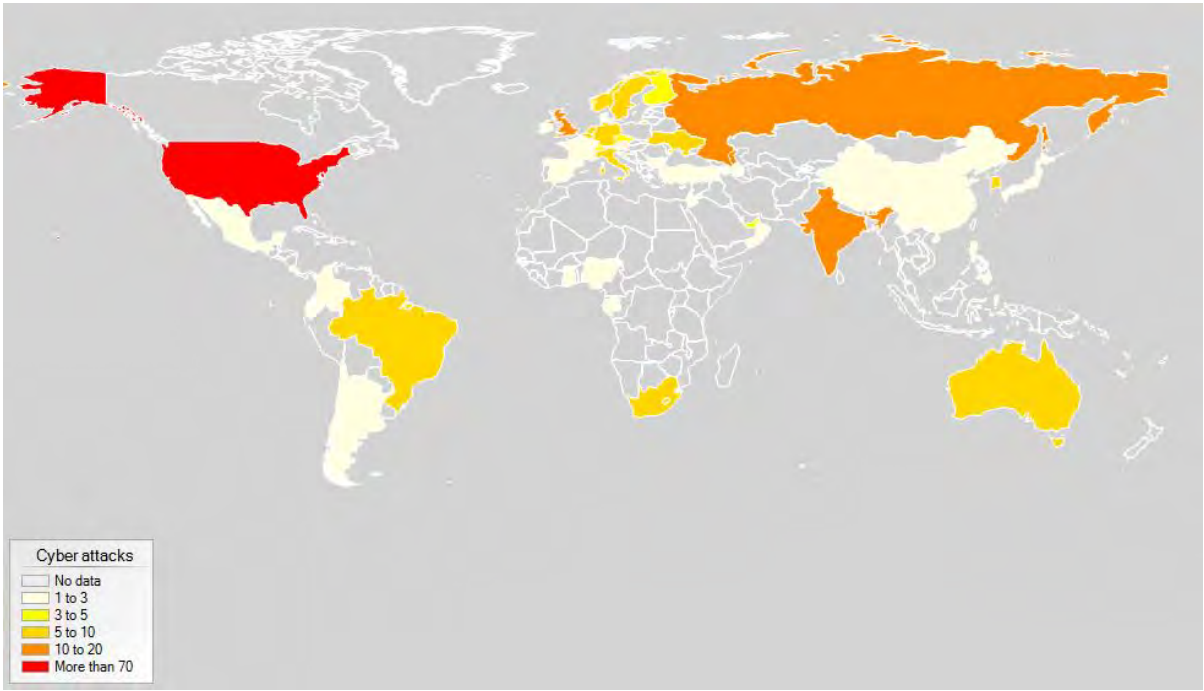
Note: Number of articles featuring "cyber-attack" or "hack" or "cyber risk" or "cyber security" and "banks" or "bank" and "risk" divided by the number of articles featuring "banks" or "bank" and "risk" by country. The index is not computed for countries with fewer than 25 articles on cyber risk (light blue). Only articles in English were included. Period range: Jan-2014-Sep. 2017. Sources: Factiva; and author's calculations.

Complete data on cyber-attacks is notoriously scarce. Available public and commercial datasets exist but they are incomplete, have different coverage and use different definitions of cyber-attacks, which makes the analysis of cyber losses difficult.[4] Moreover, data on losses are gathered from different sources and using different methods (actual costs, estimated costs etc.) making their comparability difficult. Among non-public datasets, two main types are available: commercial data and consortium data. Commercial data providers such as SAS or IBM collect data on operational risk events— which includes cyber events based on publicly available information. Niche providers such as Advisen cover 37,000 cyber events. Consortium data is provided by ORX, a consortium of financial institutions that gathers data on operational risk events. ORX members provide anonymized data covering around 600,000 risk events which is available to members only. ORX also provides a dataset based on publicly available data, ORX News, which covers around 6,000 events, including cyber events related to cyber-attacks. Data on losses includes only direct losses— although indirect losses (reputation, business recovery and remediation etc.) account for more than 90 percent of total losses (Deloitte (2016)).

[4] Private sector initiatives have been launched to foster the harmonization of data related to cyber-attacks, such as the proposal by the Chief Risk Officer Forum (see CRO (2016)).

ORX News data on cyber events is the main source used in this paper. The data cover 341 cyber risk events that impacted financial institutions and reported over 2009-2017. Around 1/3 of the events provide loss data which amounts to USD 6.5 billion overall.
Based on the limited dataset, advanced economies are the main targets of cyber-attacks but EM and developing economies are also exposed to cyber risk (Figure 5), based on data from ORX News.[5] AEs account for 80 percent of successful attacks, mainly in the U.S. (39 percent) and UK (7 percent) as shown in Figure 6. Among EMs, the BRICS account for most of the attacks (17 percent), mainly in Russia (6 percent), China (4 percent) and India (3 percent). Overall, financial institutions in more than 50 countries have been victims of cyber-attacks over the last few years according to reports in the public media.

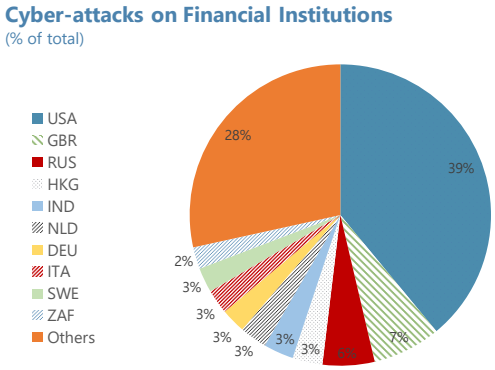
Figure 5: Number of cyber-attacks by country in the ORX database



Sources: ORX News; www.orx.org.

[5] The dataset is potentially biased towards Advanced Economies and English-speaking countries, given that the data is based on media reports in English, more likely to be available in countries with free press.

Figure 6: Share of cyber-attacks by country

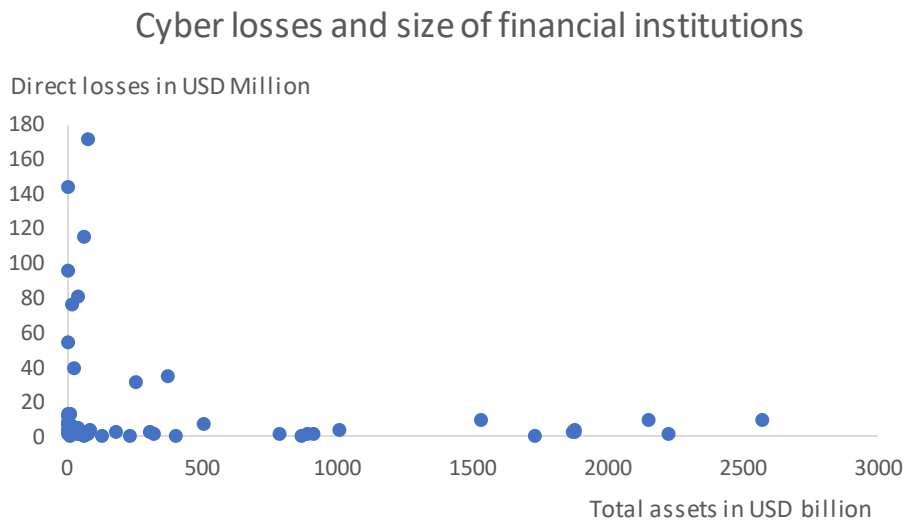


Sources: ORX News; IMF staff calculations

Among financial institutions, banks account for the bulk of the attacks (91 percent of the attacks), followed by insurance companies (7 percent). Among banks, retail banking activities (39 percent of the total) and credit cards services (25 percent) were the main business lines targeted.

Direct losses due to cyber-attack are generally unrelated to the size of the financial institution targeted (Figure 7). The largest losses recorded have been concentrated among smaller institutions, possibly due to lower absolute investment in IT security.

Figure 7: No relationship between size and losses due to cyber attacks



Sources: ORX News, SNL.

Central banks in AEs and EMs have also been the victims of cyber-attacks. In AEs, attacks were either data breaches (U.S., Italy) or business disruptions (Norway, Sweden), while in EMs, most attacks were related to fraud, resulting in losses of USD 117 million (Table 1).

Table 1: Recent cyber-attacks on central banks

Institution	Year	Type of attack	Details
Federal Reserve Bank of Cleveland	2010	Data breach	Theft of 122,000 credit cards
Federal Reserve Bank of New York	2012	Data breach	Theft of proprietary software code worth USD 9.5 Million
Sveriges Riksbank	2012	Business Disruption	Distributed Denial of Service (DDoS) attack left the website offline for 5 hours
Banco Central del Ecuador	2013	Fraud	USD 13.3 Million stolen from the account of the city of Riobamba at the central bank
Federal Reserve Bank of Saint Louis	2013	Data breach	Publication of credentials of 4,000 US bank executives by Anonymous
Central Bank of Swaziland	2014	Fraud	Theft of USD 688,000
ECB	2014	Data breach	20,000 email addresses and contact information compromised
Norges Bank	2014	Business Disruption	DDoS attack on seven large financial institutions, resulting in suspended services during a day.
Central Bank of Azerbaijan	2015	Data breach	Theft of thousands of bank customers' information
Bangladesh Bank	2016	Fraud	The SWIFT credentials of the Bangladesh central bank were used to transfer USD 81 Million from its account at the FRBNY. Hackers tried to steal USD 951 Million.
Bank of Russia	2016	Fraud	21 Cyber-attacks aimed at stealing USD 50 Million from correspondent bank accounts at the central bank, resulted in a loss of USD 22 Million.
Bank of Italy	2017	Data Breach	Hack of email accounts of two former executives.

Source: ORX News

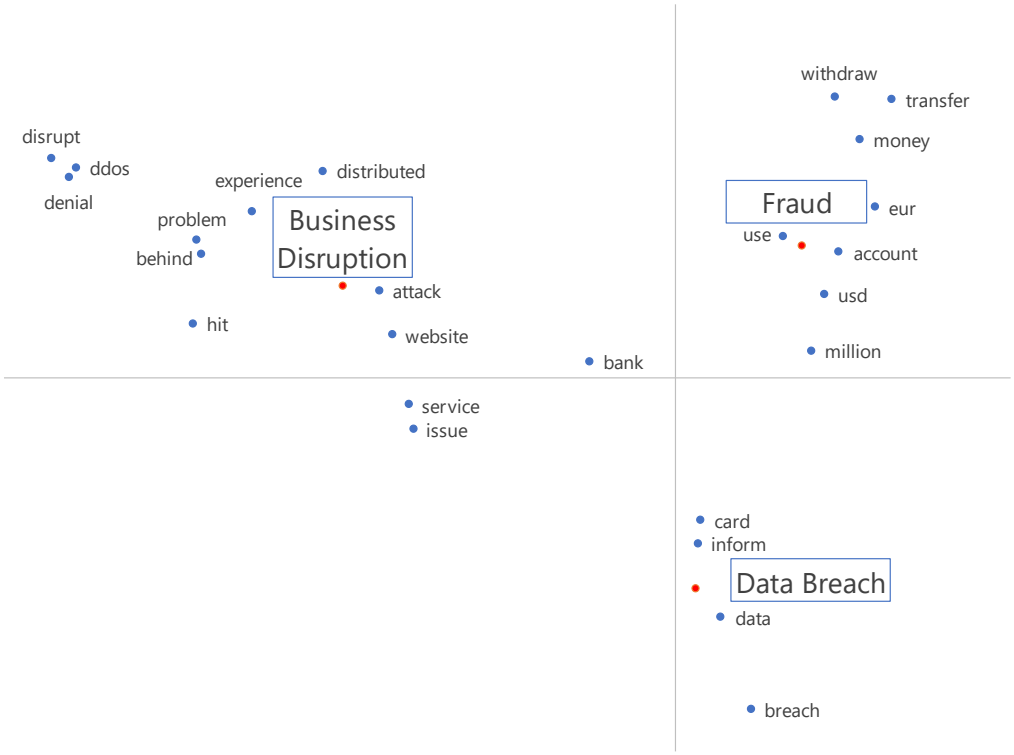
Among cyber-attacks, fraud and data breaches are more prevalent, yet business disruption is also significant. In the ORX News dataset, fraud accounts for 43 percent of events, data breaches 34 percent and disruption 23 percent. While business disruptions are known immediately, the other types of cyber-attacks can take place for months or years before being noticed and reported, which could lead to a downward bias in the dataset.

Patterns can be identified for each type of cyber-attacks using text-mining techniques (see Bholat et al. (2015) for an overview) applied to the ORX News dataset, which provides for each case background information in text form. More precisely, correspondence analysis — a statistical technique to provide a graphical representation of the structure of a dataset— is used to identify the words which tend to cluster around the three types of cyber-attacks (Figure 7).[6] Business disruption is associated with DDoS attacks which typically impact the website of the target— when a very large number of requests are sent to the targeted servers, overloading the system and making it unable to operate. Data breaches are linked with credit card information, and fraud is associated with money transfers, and a loss amount — since around 80 percent of the events with loss data are cyber-related fraud. The word "bank" is in the middle of the chart since banks are the main targets of all three types of attacks. The x-axis can be interpreted as a measure of the informational content regarding losses (with most

[6] Text-mining techniques are particularly useful when applied on very large datasets (thousands or millions of observations). The findings presented here are therefore limited by the small size of the sample.

events in the business disruption category having no loss information), while the y-axis measures whether the impact of the cyber-attack is immediate (business disruption or fraud) or takes more time to materialize, as in the case of data breaches.

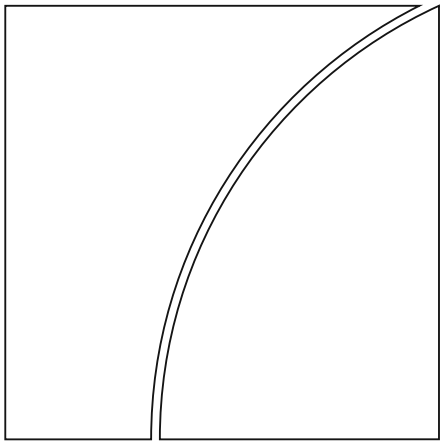
Figure 8: Correspondence analysis (terms contributing the most by types of attack)



Sources: ORX News, author's calculations

(...)

BANK FOR INTERNATIONAL SETTLEMENTS



BIS Working Papers
No 865

The drivers of cyber risk

by Iñaki Aldasoro, Leonardo Gambacorta, Paolo Giudici and Thomas Leach

Monetary and Economic Department

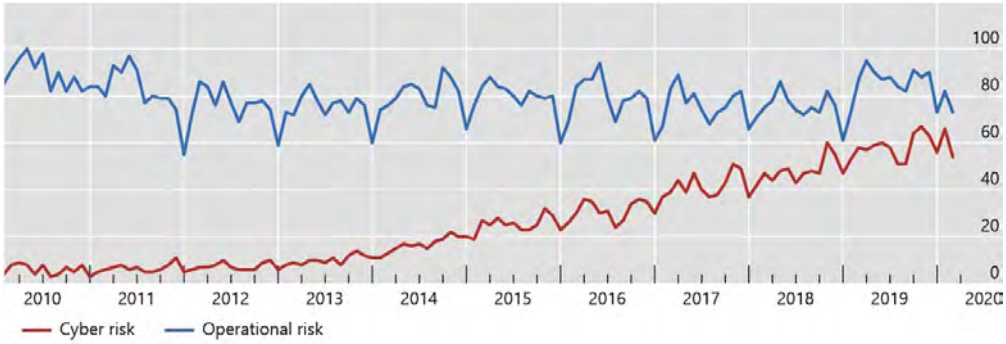
May 2020

JEL classification: D5, D62, D82, G2, H41.

Keywords: cyber risk, cloud services, financial institutions, bitcoin, cryptocurrencies, cyber cost, cyber regulation.

I. Introduction

Information technology (IT) has become a critical component of well-functioning economies, underpinning economic growth over the past decades. Organisations of all sizes in both the public and private sector are becoming ever more interconnected and reliant on IT products and services, such as cloud-based systems and artificial intelligence. Accordingly, there is a growing exposure to cyber risks. Cyber risk commonly refers to the risk of financial loss, disruption or reputational damage to an organisation resulting from the failure of its IT systems. These episodes include malicious cyber incidents (cyber attacks) where the threat actor intends to do harm (e.g. ransomware attacks, hacking incidents or data theft by employees). In the wake of recent high-profile cyber attacks such as the WannaCry incident in May 2017, public awareness of these threats is on the rise (see Figure 1).



Notes: Number of online searches for "cyber risk" and "operational risk" over the last decade. Worldwide search interest is relative to the highest point (=100). Data accessed on 7 Feb 2020.
Source: Google Trends.

Figure 1
Interest on cyber risk is on par with operational risk.

Firms actively manage cyber risk and invest in cyber security. However, cyber costs are difficult to quantify. In the financial sector, cyber risks are a key " known unknown" tail risk to the system and a potential major threat to financial stability.[1] More broadly, cyber risk in sectors that play a critical role in the economic infrastructure could have systemic implications and should be viewed as a matter of national security (Brenner, 2017). Despite the acknowledgement of such consequences, information concerning the costs, drivers and potential mitigating factors of cyber incidents is relatively scarce.

This paper seeks to help fill this gap. The analysis uses a detailed dataset of over 100,000 cyber events across all sectors of economic activity. We first document some stylised facts. The frequency of cyber incidents rose strongly in the decade to 2016, but has since receded somewhat. This reduction could reflect

[1] In March 2017, the G20 Finance Ministers and Central Bank Governors noted that "the malicious use of information and communication technologies could disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability".

increased investment in cyber security, but also delays in discovery or reporting.[2] The average cost of cyber events has been increasing constantly over the last decade. We find that certain economic sectors display a greater resilience to cyber incidents: for example, the financial sector has experienced a higher frequency of cyber incidents but these have been on average relatively less costly. Regarding the type of incident, privacy violations and phishing/skimming scams fraud in short are the most frequent but least costly. Data breaches, in turn, are both relatively frequent and costly, while business disruptions are quite infrequent but can have high costs.

The richness of the database also allows us to examine the relationship between firm, sector and event-specific characteristics and the relative cost of cyber events. The main empirical results can be summarised as follows.

First, we identify the key drivers contributing to the costs of cyber-related events. Firm size measured in terms of total revenues is positively correlated with the average cost of an event, implying that larger firms tend to incur larger costs. However, the elasticity is quite low: a 1% increase in total revenues is associated with a 0.2% increase in cyber costs. We also find that that cyber events which impact multiple firms at the same time (i.e. "connected" events) are also associated with higher costs. Cyber-related incidents can occur unintentionally by human error, e.g. a bug in some internally developed software; or can also be caused by an actor with malicious intent.[3] Malicious cyber attacks have, on average, lower costs, because most incidents simply reflect general discontent. However, some actors seek a profit or to inflict the largest possible losses and damage. Indeed, a quantile analysis reveals that at the tail of the sample distribution this relationship is reversed and in fact malicious incidents are associated with higher costs. This finding indicates that, while most attackers are stopped before they can do considerable harm, a successful attacker can go on to cause extensive damage. Incidents related to crypto exchanges, which are largely unregulated, produce higher losses.

We then look at the role of developing technological capabilities to reduce cyber costs. Many firms, especially if they are smaller, could lack the specific knowledge needed to make rational decisions about which software or cyber security provider to choose. Information asymmetries between firms can further exacerbate problems when investments in new technologies do not pan out as expected (Zhu and Weyant, 2003). How can firms mitigate these risks? We find that investment in technological skills pays off in terms

[2] This phenomena is widely recognised in the operational risk literature (see Aldasoro et al. (2020); Carrivick and Cope (2013). The dataset used in this analysis did not contain sufficient information concerning the dates of events, thus an "end-of-sample" bias could not be accurately estimated.

[3] The best known types of cyber attack are: man-in-the-middle attacks, cross-site scripting, denial-of-service attacks, password attacks, phishing, malware and zero-day exploits. Man-in-the-middle attacks occur when attackers insert themselves into a two-party transaction. Cross-site scripting is a web security vulnerability that allows attackers to compromise the interactions a victim has with a vulnerable application. Denial-of-service attacks flood servers with traffic to exhaust bandwidth or consume finite resources. Phishing is the practice of stealing sensitive data by sending fraudulent emails that appear to be from a trustworthy source. Malware (i.e. "malicious software") is a software designed to cause damage to IT devices and/or steal data (examples include so-called Trojans, spyware and ransomware). A zero-day exploit is an attack against a software or hardware vulnerability that has been discovered but not publicly disclosed. The discovery of a zero-day exploit can result in a situation where both the customers and vendors of the IT asset are now subject to cyber attacks for which no pre-defined detection signatures or remedial patches are available. Exacerbating this situation are commercial firms that conduct research to sell zero-day exploits on the open market. Some of these firms, such as Zerodium, pay large cash rewards (up to $2.5 million) for high-risk vulnerabilities.

of reducing the cost of cyber events. In particular, firms in sectors that employ more IT specialists, use more computers and provide more IT training to staff, are better equipped to mitigate the costs stemming from a cyber event. From a policy perspective, these findings can inform governments and cross-sector regulators regarding the mitigating steps that can be taken to reduce the cost of cyber incidents and which sectors are lacking in such areas.

Cybersecurity activities provided by third-party service providers are an alternative to risk transfer mechanisms. Rowe (2007) argues that, if multiple organisations share the same service provider, economies of scale and information-sharing can create positive externalities. Cloud technology can reduce IT costs, improve resilience and enable firms to scale better (Financial Stability Board, 2019). However, the technology strengthens interdependence across firms that have shared exposures to similar (or even the same) cloud service providers. For example, several cloud suppliers may use a common operating system so that, if the operating system has a vulnerability, it could create a correlated risk across all cloud suppliers. By analysing the cost-benefit trade-off, we find that the use of cloud services is associated with lower costs of cyber events. While this speaks to the resilience of cloud technology, it should be interpreted with caution. As firms' exposure to cloud services increases and cloud providers become systemically important, cloud dependence is likely to increase tail risks (Danielsson and Macrae, 2019).

Of particular concern is the exposure to cyber risk of financial institutions and infrastructures, given the critical services they provide (Kopp et al., 2017; Committee on Payments and Market Infrastructures, 2014). Following the financial crisis, banks in particular became a target for activists.[4] We interact a finance sector dummy variable with our baseline regressors to assess average costs of losses relative to other sectors. While the frequency of attacks in the financial sector is high relative to others, the sector is better at mitigating the cost of attacks. This could be the outcome of more proactive policy, regulation and investment in risk management and governance practices with respect to information technology.

Cryptocurrencies have emerged as a challenge to established financial institutions and currencies. Despite initial claims of superior security, the cryptocurrency space has suffered numerous cyber attacks. This notoriety stems both from attacks on crypto-exchanges due to poor security standards and due diligence on internal controls,[5] as well as from the use of cryptocurrencies as ransomware that is difficult to trace, e.g. WannaCry (Kshetri and Voas, 2017). We find that the average cost of crypto-related events is significantly higher. These costs are not independent of the soaring price of cryptocurrencies in recent years. We document the existence of a strong positive correlation between the price of bitcoin and the intensity of attacks on crypto-exchanges. To quantify this relationship, we use a Probit model to show that an increase in the price of bitcoin increases the likelihood of future attacks on crypto-exchanges. However, the inverse relationship is not found to be significant, i.e. there is no price decrease following cyber incidents related to cryptocurrencies.

Finally, we use data on the level of IT spending across sectors to assess which sectors may be over- or

[4] For a list of attacks on banks see: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

[5] Analytics firm Chainalysis reported that approximately $1 billion worth of cryptocurrency was stolen from digital currency exchanges in 2018 (https://news.bitcoin.com/report-two-hacker-groups-stole-1-billion-from-crypto-exchanges/).

underspending on their IT security. This analysis can act as a helpful indicator to policymakers as to which sectors may be exposed due to underinvestment in IT systems. We find that, across all sectors, there is a deficit in IT-spending. This is concerning, as the threat of cyber-related incidents is likely to increase in the future. Some sectors, however, exhibit an adequate level of spending. Such is the case of the finance and insurance sector. The dividend of such investments is evident through our other analyses, whereby the observed cost of attacks for that sector is lower. This result does not provide a reason for firms in sectors that are in a spending surplus to cut back on their investments, as the threat landscape continues to evolve.

The rest of the paper is organised as follows. Section II discusses related literature. Section III contains a description of the data. Section IV discusses our baseline results. Section V looks at the impact of technological skills on cyber losses. Section VI explores whether exposure to cloud services affects the cost of cyber events. Section VII examines the relationship between the price of bitcoin and the hacking of crypto exchanges. Section VIII zooms in on the financial sector. Section IX analyses the optimal amount of IT spending across sectors. Finally, Section X summarises the main conclusions.

(...)

X. Conclusions

The digital revolution has increased the interconnectivity and complexity of the economic system. The use of technology and internet has improved firms' productivity, but also makes them vulnerable to the spread of viruses and malware. Moreover, the greater use of cloud services exposes further important eco-nomic sectors to common risks, especially in case of cyber attacks.

Despite the large and growing exposure to cyber risks, cyber costs are difficult to quantify. Using a unique database of more than 100,000 cyber events across sectors, we document the characteristics of cyber incidents and help quantify cyber risk. The average cost of cyber events has increased over the last decade. These costs are higher for larger firms and more connected events, and relatively lower for cyber events with malicious intent (cyber attacks), especially if the attack is not conducted on a large scale.

The financial sector experiences the highest number of cyber incidents (especially of a malicious type, privacy and lost data incidents). However, banks and insurance companies incur more limited losses relative to other sectors, likely due to the effects of regulation and higher investment in cyber security.

We document that developing technological skills helps firms mitigate the costs of cyber incidents, as does more reliance on cloud services. This last result should be taken with caution and qualified. As cloud connectivity increases and cloud providers become systemically important, cloud dependence is also likely to increase tail risks.

Crypto-related activities, which are largely unregulated, are associated with higher losses. We observe the existence of a positive correlation between the price of bitcoin and the intensity of crypto-related cyber events. With rising Bitcoin prices there is an increased incentive to attack exchanges, a vulnerable part of the cryptoasset ecosystem. Stronger regulation of the activities of intermediaries that operate in cryptoasset markets is likely necessary as the expected costs for cyber-related events are also significantly higher than for other events.

Finally, we do a first evaluation of over- or underspending on IT budgets by sector. While our analysis does not account for the systemic implications of failures in specific critical sectors, the results can inform policymakers as to where to direct their attention in order to improve the economy's overall cyber resilience.

Iñaki Aldasoro *inaki.aldasoro@bis.org*
Jon Frost *jon.frost@bis.org*
Leonardo Gambacorta *leonardo.gambacorta@bis.org*
David Whyte *david.whyte@bis.org*

Covid-19 and cyber risk in the financial sector

Key takeaways

- *The financial sector has been hit by hackers relatively more often than other sectors during the Covid-19 pandemic.*
- *While this has not yet led to significant disruptions or a systemic impact, there are substantial risks from cyber attacks for financial institutions, their staff and their customers going forward.*
- *Financial authorities are working to mitigate cyber risks, including through international cooperation.*

During the Covid-19 pandemic, financial institutions have been at the leading edge of the response to cyber risk. Their already large exposure to cyber risk has been further accentuated by the move towards more working from home (WFH) and other operational challenges. This Bulletin serves as a primer on cyber risk and presents initial findings on how the financial sector has met the challenges of the pandemic. We draw on new data to assess changes in the threat landscape for financial institutions in the pandemic.

Cyber risk: a taxonomy

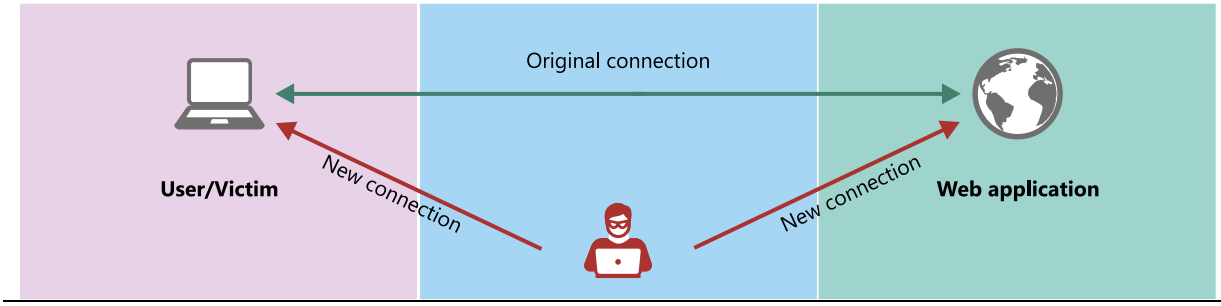
As the economy and financial system become more digitised, cyber risk is growing in importance. "Cyber risk" is an umbrella term encompassing a wide range of risks resulting from the failure or breach of IT systems. According to the FSB Cyber Lexicon (2019), cyber risk refers to "the combination of the probability of cyber incidents occurring and their impact". A "cyber incident", in turn, is "any observable occurrence in an information system that: (i) jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not". Cyber risk is one form of operational risk (Aldasoro et al (2020b), CPMI-IOSCO (2016)). Cyber risks can be classified based on their cause/method, actor, intent and consequence (Aldasoro et al (2020a), Curti et al (2019)).

The causes or methods vary, and include both unintended incidents and intentional attacks. Examples of the former are accidental data disclosure, and implementation, configuration and processing errors. Such incidents are frequent. Yet around 40% of cyber incidents are intentional and malicious, rather than accidental, ie they are cyber attacks (Aldasoro et al (2020c)).

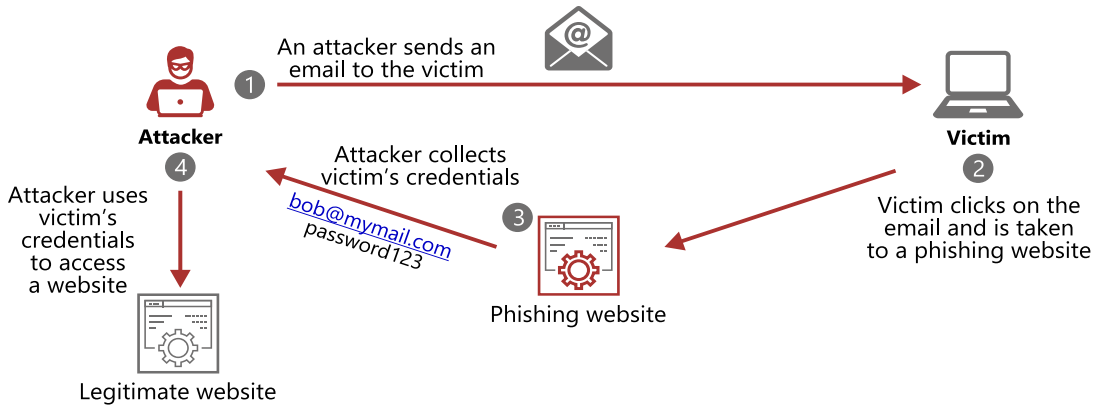
Some cyber attacks involve threat actors inserting themselves into a trusted data exchange. *Malware* (ie "malicious software") is software designed to cause damage to IT devices and/or steal data (for example, so-called Trojans, spyware and ransomware). *Man-in-the-middle attacks* occur when attackers insert themselves into a two-party transaction (Graph 1, first panel), accessing or manipulating data or transactions. *Cross-site scripting* is a web security vulnerability that allows attackers to compromise the interactions a victim has with a vulnerable application. *Phishing* is stealing sensitive data or installing malware with fraudulent emails that appear to be from a trustworthy source (Graph 1, second panel). To gain a victim's trust, phishing attacks may imitate trusted senders. After gaining entrance, these may help attackers to gain credentials and entry into a system. *Password cracking* is the process of recovering secret passwords stored in a computer system or transmitted over a network.

Selected causes of cyber attacks Graph 1

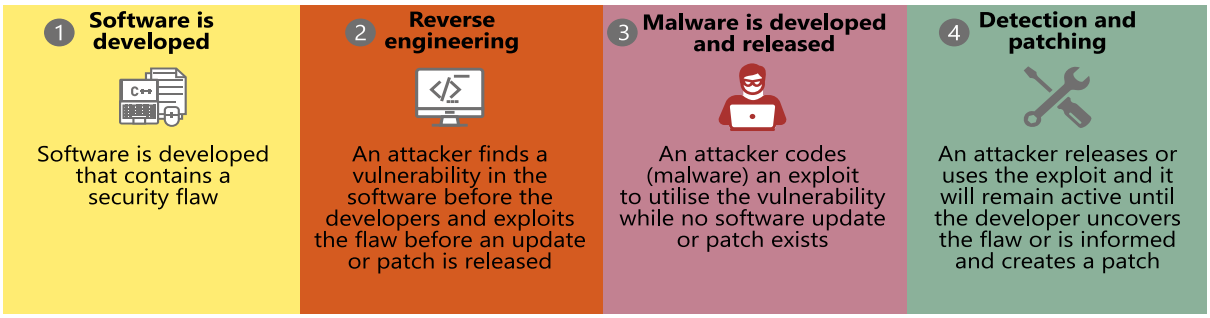
Man-in-the-middle



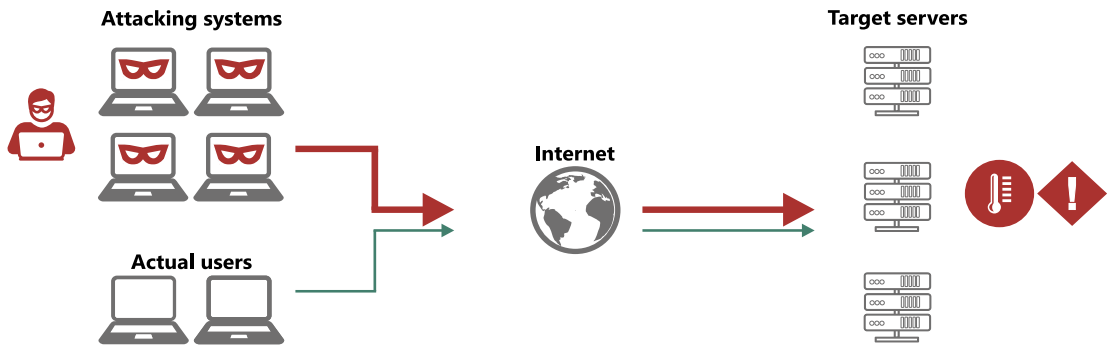
Phishing



Timeline of zero-day vulnerabilities



Distributed denial-of-service (DDoS) attack



Source: Authors' elaboration.

Some attacks involve professional tools and planning. *A zero-day exploit* is an attack against a software or hardware vulnerability that has been discovered but not publicly disclosed (Graph 1, third panel). The discovery of a zero-day exploit can result in a situation where both the customers and vendors

of the IT asset are now subject to cyber attacks for which no predefined detection signatures or remedial patches are available. Exacerbating this situation are commercial firms that conduct research to sell zero-day exploits on the open market. Some of these firms, such as Zerodium, pay large cash rewards (up to $2.5 million) for high-risk vulnerabilities. Finally, *distributed denial of service (DDoS) attacks* flood servers with traffic to exhaust bandwidth or consume finite resources (Graph 1, fourth panel). These attacks may require renting computing capacity, or hacking third-party devices, to participate in an attack.

Actors include outright criminal and terrorist organisations, industrial spies, "hacktivists", or state and state-sponsored players. The damage they can cause depends on their sophistication and resources. For example, in 2016, hackers associated with North Korea carried out a notable attack by breaching the systems of Bangladesh Bank and using the SWIFT network to send fraudulent money transfer orders (Bangladesh Bank-FRBNY (2019)). The attack highlighted rising cyber risks for payment systems and associated infrastructures.[1] The ultimate purpose can be for profit (eg ransomware, industrial spying), geopolitical (state-sponsored attacks on critical infrastructures) or general discontent (hacktivism).

The consequences of cyber attacks can be severe. Business disruptions and IT system failures can damage the integrity and availability of assets and services. Data breaches compromise the confidentiality of sensitive data, with financial and reputational losses. Fraud and theft include the loss of funds or any information (eg intellectual property) that may or may not be personally identifiable. In some circumstances, cyber attacks could have systemic implications and cause serious economic dislocations.

Covid-19, remote working and changes in the cyber threat landscape

Covid-19 has precipitated a move to working from home (WFH). Financial institutions – like other organisations – have temporarily shifted to remote working to protect their workers. Moving the majority of activities to the digital world could increase the risk of cyber attacks. For instance, the use of remote access technologies such as the remote desktop protocol (RDP) and virtual private network (VPN) increased by 41% and 33%, respectively, in the first two months of the Covid-19 outbreak (ZDNet (2020)). Unless well managed, this may allow new opportunities for threat actors to penetrate IT systems and carry out cyber attacks, along with other types of financial crime (Crisanto and Prenio (2020)). WFH may also challenge business continuity plans and the response to an operational or cyber incident.

The recent SolarWinds hack underscores risks from third-party vendors. In December 2020, it was reported that hackers had inserted malware into the company SolarWinds' product Orion, used by thousands of companies and government agencies around the world (FBI-CISA-ODNI (2020)). Software supply chain attacks are one of the hardest types of threat to mitigate, as they take advantage of established trust relationships and the machine-to-machine communications used to provide essential software updates. While the financial sector was not a primary target, the hackers gained access in March 2020 and remained undetected for many months. The full scale of the attack has not been fully disclosed.[2]

The financial sector has been hit relatively more often by cyber attacks than most other sectors since the pandemic started. Data on attacks can be obtained from Advisen, a for-profit organisation that collects information from reliable and publicly verifiable sources (mostly in the United States), covering date, actor, loss amount and other features. There is a strong link between the prevalence of WFH arrangements – as measured by the WFH index by sector from Dingel and Neiman (2020) – and the incidence of cyber attacks between the end of February and June 2020 (Graph 2, left-hand panel). The financial sector ranks high on both accounts (red square). Outside the health sector, the financial sector has the largest share of cyber events classified as Covid-19-related in recent months (right-hand panel). Examples are phishing attacks that explicitly use the uncertainty around Covid-19 to entice users to open fraudulent attachments or grant attackers access to networks.

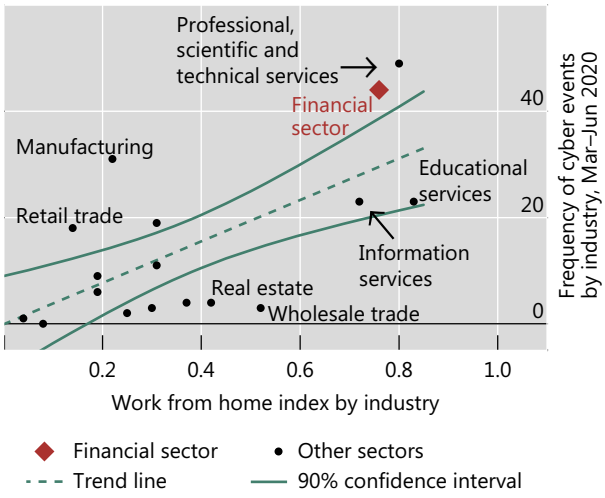
[1] In response to ever more sophisticated attacks, SWIFT launched a Customer Security Programme (CSP) in 2016 (SWIFT (2019)).

[2] Separately, in January 2021, the Reserve Bank of New Zealand (RBNZ) reported that a third-party file sharing service that the Bank used to share and store some sensitive information was illegally accessed (RBNZ (2021)).

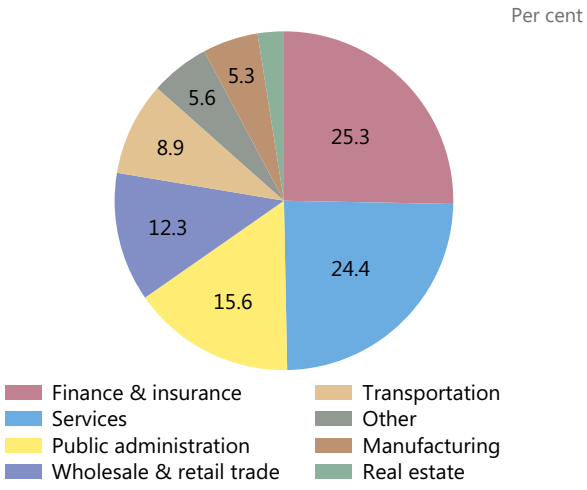
Payment firms, insurers and credit unions have been especially affected. A survey among financial institutions by the Financial Services Information Sharing and Analysis Center (FS-ISAC) finds a substantial rise in phishing, suspicious scanning and malicious activity against webpages for WFH staff to access the network. Payment firms, insurance companies and credit unions have seen the strongest increase in hacks (Graph 3, left-hand panel). Covid-19-related attacks grew with the spread of the pandemic, from fewer than 5,000 per week in February to more than 200,000 per week in late April. They rose further by around one third in May and June compared with March and April (Check Point Research (2020)). The survey highlighted that, in 45% of cases, staff WFH overwhelmed virtual desktop infrastructure (VDI)/VPN processes. In one third of cases, business continuity IT plans were not prepared for a long-term at-home work force (right-hand panel). One fifth of the financial firms reported that their network operation activities were interrupted during the pandemic.

The financial sector has been hit by cyber attacks during the pandemic — Graph 2

WFH index versus cyber events during Covid-19[1]



Covid-19-related cyber events by sector[2]



[1] Excludes the health sector. [2] Based on cases classified by Advisen as Covid-19-related. Includes data up to 9 September 2020. The sample in the graph excludes the health sector (57 Covid-related cases) and affecting health-related items of the manufacturing sector (163 cases).

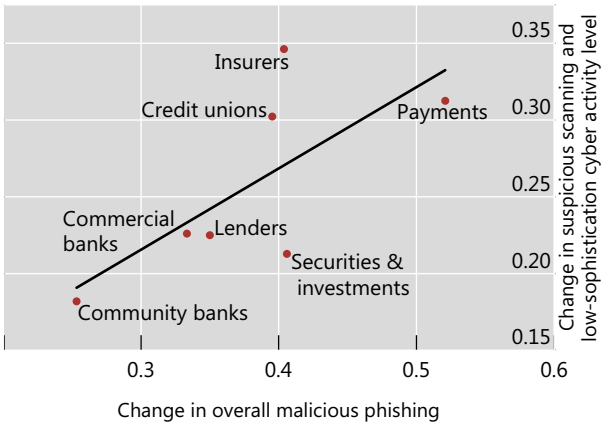
Sources: Dingel and Neiman (2020); Advisen; authors' calculations.

Mass migration to WFH can make financial institutions' staff more vulnerable. As staff work from home through firm-issued and private devices and networks, new risks may arise. In a household, multiple family members could be logging on to the same network, potentially exposing devices to malware that could then enter a firm's enterprise environment. Some videoconferencing facilities have been shown to have suboptimal security standards. Trader surveillance may also be subject to unintended consequences. Regulatory rules require that traders' calls are recorded and monitored, but traders have been working from home and calls may go unrecorded. Another factor at play is the expansion of the range of self-service options available to customers online – for wealth management trades, mortgage, loan applications, etc. Ensuring robust security controls becomes even more essential.

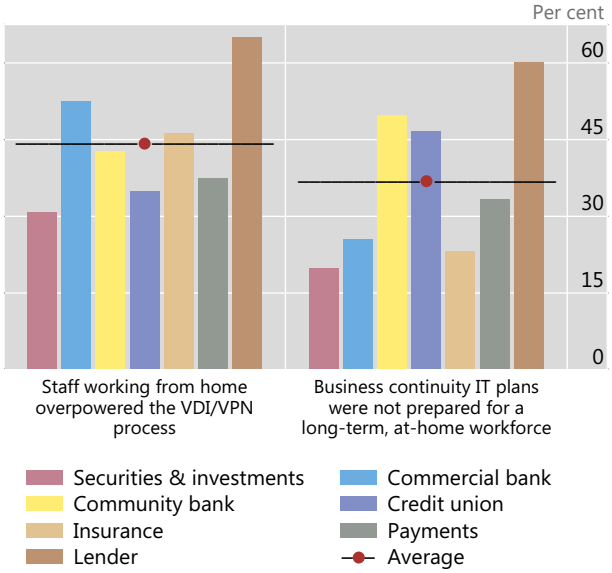
Evidence so far suggests the same threat actors, intent and methods as before the pandemic, but new opportunities given Covid-19-related uncertainty. Phishing ploys are not new, but the volume of such attempts has spiked. A recent report found that a quarter of cyber incidents responded to in the United Kingdom over August 2019–August 2020 involved criminals and hostile states exploiting the Covid-19 pandemic (NCSC (2020)). In the European Union (EU), threat actors compromised the VPN services of EU institutions that allow staff to work from home (CERT-EU (2020)). In other cases, threat actors imitated trusted sources such as the World Health Organization to get users to open malicious links and files (Microsoft (2020)). In one case, a DDoS attack was able to disrupt trading at a major stock exchange for four consecutive days (Hope (2020)), underscoring the risks of hacking to critical infrastructures.

Working from home (WFH) opens up new possibilities for cyber attacks[1] Graph 3

Cyber attacks increased during the Covid-19 period, with differences across financial firm types[2]



WFH overpowers VDI/VPN processes and business continuity plans[3]



[1] The graphs report the results of a survey by FS-ISAC among financial institutions in April 2020. [2] The first question (results reported on the horizontal axis) is: "During the past few months, has your firm experienced a change in overall malicious phishing levels?". The second question (results reported on the vertical axis) is: "During the past few months, has your firm experienced a change in overall suspicious scanning or other low-sophistication cyber activity levels?". The results of the survey are summarised by a Covid-19 cyber attack diffusion index, which aggregates answers. Financial institutions that answered "considerably" are given a weight of 1; those that answered "somewhat" receive a score of 0.5. The index ranges between –1 and 1. A positive value indicates an increase in cyber attacks. [3] The first question (results reported on the left) is: "Did staff working from home overpower your VDI/VPN process?". The second question (results reported on the right) is: "Were business continuity IT plans prepared for a long-term, at-home workforce?". The panel gives the share of firms that answered "yes".

Source: FS-ISAC (2020).

Policies to reduce risks to financial stability

Policy must take account of two near-term trends. First, remote work is likely to remain higher than in the pre-Covid-19 period. Business continuity plans designed for short-term disruptions may need to adapt to WFH over longer periods, and business processes may need to adapt to the "new normal". Second, financial institutions are likely to continue to move parts of their IT operations to public cloud environments. As the market for cloud services is highly concentrated, there are warnings about increased homogeneity in the financial sector and single points of failure (Danielson and Macrae (2019)). A recent survey indicates that 82% of companies increased cloud usage as a result of the coronavirus pandemic and 91% are planning a more strategic use of cloud in the near future (Snow (2020)). Through shared software, hardware and vendors, incidents could, in principle, spread more quickly, leading to higher losses for financial institutions and stress in the financial system (Welburn and Strong (2019)).

Policymakers and businesses are actively working together to mitigate cyber risks and their systemic implications. For instance, many private and public sector organisations are strengthening their operational resilience, and many have engaged in "war games" or simulations of cyber attacks. These exercises can help to identify vulnerabilities and enhance preparedness and line of communication. Moreover, financial supervisors and overseers are leveraging national or international standards or guidance to promote cyber resilience.[3] In addition to global initiatives, there are several regional groups and cooperation forums. The BIS will continue supporting international cooperation in this area, recognising that cyber resilience is fundamentally a global public good (Cœuré (2019), Carstens (2019)).

[3] For relevant standards and practices, see CPMI-IOSCO (2016), IAIS (2016), FSB (2017) and BCBS (2018) among others.

Council of the EU

PRESS
FR

COMMUNIQUÉ DE PRESSE
433/22
11/05/2022

Finance numérique: accord provisoire concernant le règlement sur la résilience opérationnelle numérique

Compte tenu des risques toujours plus importants de cyberattaques, l'UE renforce la sécurité informatique des entités financières telles que les banques, les compagnies d'assurance et les entreprises d'investissement. Hier soir, la présidence du Conseil et le Parlement européen sont parvenus à un accord provisoire en ce qui concerne le **règlement sur la résilience opérationnelle numérique (règlement DORA)**, qui doit permettre au secteur financier européen de maintenir des opérations résilientes en cas de perturbation opérationnelle grave.

Le règlement DORA fixe des exigences uniformes pour la sécurité des réseaux et des systèmes d'information des entreprises et des organisations actives dans le secteur financier ainsi que des tiers critiques qui leur fournissent des services liés aux technologies de l'information et de la communication (TIC), tels que des plateformes d'informatique en nuage ou des services d'analyse de données. Le règlement DORA crée un cadre réglementaire sur la résilience opérationnelle numérique en vertu duquel **toutes les entreprises doivent veiller à pouvoir résister à tous les types de perturbations et de menaces liées aux TIC, y répondre et s'en remettre**. Ces exigences sont homogènes dans tous les États membres de l'UE. L'objectif principal est de prévenir et d'atténuer les cybermenaces.

En vertu de l'accord provisoire, la nouvelle réglementation constituera **un cadre très solide qui favorisera la sécurité informatique du secteur financier**. Les efforts demandés aux entités financières seront proportionnels aux risques potentiels.

Presque toutes les entités financières seront soumises à la nouvelle réglementation. Au titre de l'accord provisoire, les **auditeurs** ne seront pas soumis au règlement DORA, mais feront partie d'un futur réexamen du règlement, dans le cadre duquel une éventuelle révision des règles pourrait être envisagée.

Les prestataires critiques établis dans un pays tiers qui fournissent des services informatiques aux entités financières dans l'UE seront tenus d'établir une filiale dans l'UE, afin que la supervision puisse être correctement mise en œuvre.

En ce qui concerne le cadre de **supervision**, les colégislateurs sont convenus d'opter pour un réseau de supervision commun supplémentaire, qui renforcera la coordination entre les autorités européennes de surveillance sur ce sujet transsectoriel.

En vertu de l'accord provisoire, des **tests de pénétration** seront effectués en mode fonctionnel et il sera possible d'inclure les autorités de plusieurs États membres dans les procédures de test. Le recours à des auditeurs internes ne sera possible que dans un certain nombre de circonstances strictement limitées, sous réserve de conditions de sauvegarde.

En ce qui concerne l'interaction du règlement DORA avec la **directive sur la sécurité des réseaux et des systèmes d'information (directive SRI)**, en vertu de l'accord provisoire, les entités financières sauront très clairement les différentes règles qu'elles doivent respecter en matière de résilience opérationnelle numérique, en particulier pour les entités financières détenant plusieurs agréments et opérant sur différents marchés au sein de l'UE. La directive SRI continue de s'appliquer. Le règlement DORA s'appuie sur la directive SRI et supprime d'éventuels chevauchements au travers d'une exemption dite de lex specialis.

L'accord provisoire conclu hier soir doit être approuvé par le Conseil et le Parlement européen avant de faire l'objet de la procédure d'adoption formelle.

Une fois que la proposition de règlement aura été formellement adoptée, elle sera intégrée à la législation de chaque État membre de l'UE. Les autorités européennes de surveillance (AES) concernées, telles que l'Autorité bancaire européenne (ABE), l'Autorité européenne des marchés financiers (AEMF) et l'Autorité européenne des assurances et des pensions professionnelles (AEAPP), élaboreront ensuite des normes techniques que tous les établissements de services financiers devront respecter, qu'ils soient chargés d'opérations bancaires, de produits d'assurance ou de la gestion d'actifs. Les autorités nationales compétentes seront chargées de la surveillance de la conformité et feront respecter le règlement en tant que de besoin.

Contexte

La Commission a présenté la proposition de règlement DORA le 24 septembre 2020. Celle-ci s'inscrit dans le cadre plus large du train de mesures sur la finance numérique, qui vise à mettre au point une approche européenne favorisant le développement technologique et assurant la stabilité financière et la protection des consommateurs. Outre la proposition de règlement DORA, ce train de mesures contient une stratégie en matière de finance numérique, une proposition sur les marchés de crypto-actifs (MiCA) et une proposition sur la technologie des registres distribués (DLT).

Il comble une lacune dans la législation existante de l'UE en permettant de s'assurer que le cadre juridique actuel ne fasse pas obstacle à l'utilisation de nouveaux instruments financiers numériques. Dans le même temps, il s'agit de veiller à ce que ces nouvelles technologies et nouveaux produits entrent dans le champ d'application de la réglementation financière et des dispositifs de gestion des risques opérationnels des entreprises actives au sein de l'UE. Le paquet vise donc à soutenir l'innovation et l'adoption de nouvelles technologies financières tout en assurant un niveau approprié de protection des consommateurs et des investisseurs.

Le Conseil a adopté son mandat de négociation sur le règlement DORA le 24 novembre 2021. Les trilogues entre les colégislateurs ont débuté le 25 janvier 2022 et se sont terminés par l'accord provisoire intervenu hier.

Press office - General Secretariat of the Council
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press

Cybersécurité : que fait l'Union européenne ?

Nos données personnelles, l'économie ou encore les services publics sont de plus en plus numérisés. Vulnérables, les systèmes informatiques peuvent toutefois faire l'objet d'attaques malveillantes. Quelles sont les politiques européennes mises en place pour y faire face ?

En septembre 2021, l'Assistance Publique-Hôpitaux de Paris (AP-HP) porte plainte. Le motif ? Le vol des données personnelles d'environ 1,4 million de personnes qui avaient passé un test PCR en Île-de-France. Cette attaque concernait un service de partage de fichiers, utilisé ponctuellement en 2020 pour transmettre des informations à l'Assurance maladie et aux agences régionales de santé (ARS). Quelques semaines plus tard, un étudiant opposé au pass sanitaire reconnaît être à l'origine du piratage, qui visait selon lui à montrer les failles informatiques des hôpitaux parisiens.

Ce genre d'attaque, qui fait fi des frontières, devrait se multiplier dans les années à venir. C'est pourquoi l'Union européenne cherche à assurer un haut niveau de cybersécurité.

Qu'est-ce que la cybersécurité ?

La cybersécurité consiste à protéger les systèmes informatiques contre les attaques malveillantes ou l'espionnage. Elle englobe toutes les techniques et les outils mis en œuvre pour protéger les infrastructures mais aussi la confidentialité, l'intégrité et la disponibilité des données qui sont stockées ou échangées dans le monde numérique.

Plus largement, l'UE définit que la cybersécurité recouvre "*les activités nécessaires pour protéger les réseaux et les systèmes d'information ainsi que les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces*".

Selon une information reprise par le Conseil de l'UE, la valeur du marché européen de la cybersécurité est estimée à plus de 130 milliards d'euros et progresse à un rythme de 17 % par an.

Quelles sont les menaces ?

Les menaces qui peuplent l'espace virtuel sont relativement nouvelles et touchent les citoyens mais aussi les administrations et les entreprises. "*Le cyberespace est devenu un domaine de concurrence stratégique, dans une période de dépendance croissante à l'égard des technologies numériques*", explique l'UE dans sa "boussole stratégique", un document définissant les grandes orientations européennes en matière de sécurité.

L'Agence de l'Union européenne pour la cybersécurité (ENISA, voir plus bas) identifie 9 menaces principales :

- les **logiciels rançonneurs**, ou "*ransomware*", consistent à attaquer un système informatique et à demander une rançon pour en rétablir le bon fonctionnement,
- les **logiciels malveillants**, afin d'endommager ou d'accéder à un appareil sans autorisation,
- le **minage clandestin**, qui infiltre un ordinateur ou un téléphone afin de produire de la cryptomonnaie à l'insu du propriétaire de l'appareil,
- les attaques par **e-mail**, avec les spams ou l'hameçonnage,

- les menaces sur **les données**, surtout concernant le vol et la divulgation d'informations personnelles,
- les attaques par **déni de service**, qui empêchent les internautes d'accéder à un réseau ou à un système, en bombardant par exemple un serveur web de sollicitations,
- la **désinformation,**
- les **attaques sur la chaîne d'approvisionnement**, c'est-à-dire ciblées sur un fournisseur de logiciels pour infester d'autres entités,
- les incidents qui ne proviennent pas d'intentions malveillantes, liés à l'erreur humaine ou à de mauvaises configurations informatiques.

Si tout internaute peut être la cible de ces menaces, les entreprises sont aussi concernées par des actes de malveillance, et pas seulement les plus grandes d'entre elles. Selon un Eurobaromètre, 28 % des PME européennes ont connu une cyberattaque en 2021. Un chiffre qui grimpe jusqu'à 41 % en Grèce et 48 % au Portugal. Les petites et moyennes entreprises sont particulièrement touchées par les virus informatiques et les logiciels espions ou malveillants. "*Moins armées que les grandes entreprises face à cette menace, elles constituent des cibles privilégiées pour les acteurs malveillants*", explique la CNIL dans un rapport.

De nombreuses administrations sont également la cible de cyberattaques. La mairie de Saint-Cloud, dans les Hauts-de-Seine, a par exemple subi récemment une paralysie de ses systèmes informatiques, avec une demande de rançon de la part de ces malfaiteurs des temps modernes.

Certaines attaques de grande ampleur peuvent entraîner des conséquences beaucoup plus graves, touchant notamment les infrastructures de base. Mi-avril, l'Ukraine a affirmé avoir déjoué une opération informatique russe visant un fournisseur d'électricité, qui aurait pu plonger dans le noir des "*millions d'Ukrainiens*".

D'où viennent ces menaces ?

De fait, les attaques cyber semblent être l'apanage de certains États. Mais les failles de cybersécurité peuvent aussi être exploitées par des individus isolés ou des groupes ne dépendant pas d'un pays en particulier. Des organisations terroristes sont par exemple amenées à utiliser internet pour transférer des fonds, ou à se servir de monnaies virtuelles afin de contourner les circuits bancaires traditionnels.

Dans le cadre de la coopération structurée permanente, une équipe composée d'experts d'États de l'UE aide l'Ukraine à repousser les cyberattaques provenant de son voisin russe.

Que dit le droit européen en vigueur ?

Consciente de ces menaces et de leur nature transnationale, l'Union européenne a mis en place une Agence de l'UE pour la cybersécurité (ENISA). Créée dès 2004 et renforcée en 2019, elle produit des schémas de certification de cybersécurité et coopère avec les États membres ainsi qu'avec les organes européens, afin de maintenir et de renforcer la sécurité numérique sur le Vieux Continent. Ce cadre défini en 2019 englobe des exigences techniques, des normes et des procédures.

Un centre européen spécialisé dans la lutte contre la cybercriminalité a par ailleurs été créé au sein d'Europol. Il se concentre sur les crimes perpétrés en ligne, la pédocriminalité et la fraude financière.

Avant le règlement de 2019 redéfinissant l'ENISA, la première initiative européenne en matière de cybersécurité s'était concrétisée par la directive "NIS" (ou SRI, pour "sécurité des réseaux et des systèmes d'information"). Celle-ci a établi des obligations en matière de sécurité pour les opérateurs dans des secteurs stratégiques comme les transports, l'énergie, la santé ou la finance, incluant par exemple une obligation de notifier des incidents à l'autorité nationale compétente lorsqu'ils se produisent.

Comment l'Union européenne prévoit-elle d'aller plus loin ?

La Commission européenne a souhaité réviser cette législation, proposant la directive "NIS 2" en décembre 2020. Celle-ci doit couvrir un plus grand nombre de secteurs, comme les messageries des administrations publiques ou les services de gestion des déchets et des eaux usées. Un réseau européen pour la préparation et la gestion des crises numériques (UE-CyCLONe) a été installé. Son objectif est d'améliorer la coordination lors d'incidents de cybersécurité à grande échelle. La directive vise aussi à renforcer les obligations des entreprises et à introduire des mesures de surveillance plus strictes pour les autorités nationales. Le Parlement et le Conseil ont réussi à s'accorder en mai 2022 sur un texte provisoire, plus d'un an après la proposition de l'exécutif européen.

Le 10 mai dernier, le Parlement et le Conseil ont trouvé un terrain d'entente à propos d'un autre règlement. Sobrement intitulé "DORA" (pour le moins sobre "*Digital Operational Resilience Act*", ou "résilience opérationnelle du numérique" en français), il s'attaque à la question de la sécurité des systèmes numérique du secteur de la finance. Cela concerne aussi bien les banques que les compagnies d'assurance ou les producteurs de cryptomonnaie. Les entreprises devront s'assurer de pouvoir résister à des cyberattaques. Il impose aussi des tests approfondis pour vérifier si les entreprises et les institutions financières sont bien préparées aux incidents informatiques.

L'UE prévoit également d'installer des "centres opérationnels de sécurité" (SOC), associés à de l'intelligence artificielle et qui pourraient s'apparenter à des "policiers" du monde numérique.

L'exécutif veut par ailleurs mettre en œuvre une "connectivité spatiale sécurisée". En d'autres termes, c'est une nouvelle constellation de plusieurs centaines (voire milliers) de satellites en orbite basse afin d'améliorer la connectivité et l'accès à internet. Un dispositif destiné à assurer la poursuite du service en cas de cyberattaque, pour un coût total estimé à 6 milliards d'euros.

Enfin, la Commission européenne devrait proposer un "*European Cyber Resilience Act*" au second semestre 2022. Avec l'objectif de fixer des règles communes en matière de cybersécurité tout au long de la vie des produits vendus, en particulier des objets connectés. Une consultation publique est ouverte jusqu'au 25 mai.

Dans le cadre du budget pluriannuel 2021-2027 et de son programme pour une Europe numérique, l'UE compte investir 1,6 milliard d'euros dans ce domaine et sur cette période. Elle souhaite notamment financer des infrastructures et des outils de cybersécurité sur l'ensemble de son territoire.

Arthur Olivier

The EU's Digital Operational Resilience Act nearing the finish line: implications for financial services firms

The European Parliament (EP) and European Council have reached their respective positions on the DORA package and have begun inter-institutional negotiations called "trilogues," which are the final stage of talks necessary before the file can become law. This aims to align the positions of the EP and Council where they currently differ. We expect these talks to conclude by mid-2022.

When will firms have to implement the DORA?

The European Commission's original proposal was for a 12-month implementation period for most of the DORA's requirements and a 36-month period for resilience testing requirements. Both the EP and the Council want to extend the general implementation period to 24 months. However, the EP and Council disagree on the implementation timeline for resilience testing requirements. The EP wants to keep the original 36-month implementation period, while the Council wants it reduced to 24 months. A shorter timeframe here could be difficult for mid-size firms that have not run tests such as Threat-Led-Penetration-Testing (TLPTs) before. While timeframes can still change, the Council's text is likely to strongly influence the outcome. As a result, we believe that firms should use a working assumption of a 24 month implementation period for all the DORA's requirements, running from H2 2022 to H2 2024.

What is the state of play in key components of the DORA?

We see several important takeaways from our analysis of where the Council and EP are aligned on the DORA, and where they differ. These are:

- **ICT risk management requirements:** The Council and the EP's positions on ICT risk management and governance are mostly aligned. Both have a similar approach on proportionality and agree that smaller and less-complex FS firms should implement a simpler set of rules. Crucially, both delegate much of the detailed rulemaking for ICT risk management to the European Supervisory Authorities[i] (ESAs) to produce in Regulatory Technical Standards (RTS). These RTS are likely to be an evolution of existing Guidelines on ICT Risk Management published by some of the ESAs. Some significant differences between the two include the EP pushing for firms to disclose a record of all ICT-related incidents in an annual public report and the Council using more specific language to require firms to conduct business impact analyses of their exposure to severe disruptions.

- **ICT incident reporting requirements:** The introduction of a harmonised reporting requirement for major ICT-related disruptions is maintained in both texts, as well as instructions to the ESAs to develop important RTSs to further specify the materiality threshold for reporting disruptions as well as the information and timing required of these reports. These reporting requirements will supersede equivalent ones in other EU regulations such as the Network Information Security Directive (NISD) and are likely to broaden the reporting requirements most firms will face. Firms also may be asked to report significant cyber threats to competent authorities, but the EP has set this on a voluntary basis whereas the Council is seeking for it to be mandatory. However, the outcome here is likely to be aligned with requirements in the reviewed NISD, which is also in legislative negotiations due to conclude this year.

- **Resilience testing requirements:** The DORA will introduce a requirement for firms to regularly carry out several different tests of their operational resilience, with certain firms being subject to "advanced" testing, including TLPTs. The TLPT requirement will more consistently roll-out a "red-team" testing framework that has so far only been adopted for FS firms in some EU countries. The EP and Council are agreed on this but need to align on the scope of firms included and the required frequency of TLPTs. The EP is seeking a three year frequency, while the Council wants to delegate the decision to authorities. The ESAs will elaborate advanced testing methodologies in an RTS, but we believe firms can use the ECB's Threat Intelligence-Based Ethical Red-Teaming (TIBER-EU) framework as a guide before the RTS is available.

- **ICT third party risk management:** Both the EP and Council maintain most of the DORA's proposed requirements for firms that use third party providers (TPPs) to support critical or important functions, including the introduction of key contractual provisions. However, the EP also wants to add some additional requirements, namely: contractual provisions requiring TPPs to agree to provide FS firms with higher levels of assurance, through allowing audits and ongoing monitoring of their performance. The EP is also seeking to ensure that contracts with third country TPPs are governed by the law of an EU Member State. Overall these are new requirements for firms and will require significant work both in terms of mapping but also negotiating contractual provisions and gathering the necessary assurance required from TPPs.

- **CTTP oversight:** the EP and Council agree that certain ICT TPPs that are designated as "critical" should come under the direct oversight of EU financial authorities. Both have maintained the Commission's initial proposal designating one of the ESAs to act as a "Lead Overseer" of the CTTP and to have powers to inspect and require changes to the CTTPs practices. The EP and Council have also both made similar amendments requiring a CTTP to have a legal subsidiary in the EU if it is to offer services to FS firms. There are differences between the EP and Council on the institutional design of the oversight mechanism, with the EP proposing a more complex "Joint Oversight Forum" of authorities that would assist the Lead Overseer. This requirement will bring new non-FS firms/ TPPs into the FS regulatory perimeter. This will be a significant step change for in-scope non-FS TPPs whose risk and resilience frameworks have not historically been subject to FS supervisory oversight and scrutiny.

- **Cryptoassets:** The DORA makes a series of amendments to existing EU Directives to align them with the new operational resilience framework that is being proposed. One of these is an amendment to include DLT-enabled products in the MiFID2 definition of a financial instrument. This will help to reduce scope for arbitrage in the regulatory treatment of certain cryptoassets (security tokens) across Member States. The EP and Council's positions are aligned on this.

Level 2 rulemaking will be an important part of new requirements

The DORA package delegates significant decision-making authority to the ESAs to write technical standards specifying the rules that firms will have to follow. The RTS on ICT risk management will set out more detailed rules for the governance, security policies and event detection procedures firms will need to put in place as well as more detail on the required content of their business continuity plans. Further RTSs on reporting major ICT-related incidents, the approach and methodology for TLPT testing and on third party risk management and registers

will all be crucial for firms to understand the full spectrum of requirements they will face from the DORA.

The ESAs will only begin to draft these RTSs once the DORA is finalised later this year, and timelines for secondary rulemaking vary. The Council is asking for all RTSs to be produced by 18 months after the entry-into-force of the DORA, while the EP sets different timelines for each. All RTS, however, are due to be finished before the likely 24-month implementation period ends. This will nevertheless limit the clarity firms have as they prepare for the DORA's implementation, and any delays in producing the RTSs (which are not uncommon) will exacerbate this. This underlines the need for firms to assess and identify no-regret actions they can begin to take to prepare for the new rules, including when implementing technological/ infrastructure upgrades or negotiating new TPP contracts.

The ESAs will also have to conduct a feasibility study on the establishment of a centralised solution for EU ICT incident reporting. This will become part of important preparatory work for the introduction of a pan-European Systemic Cyber Incident Coordination Framework (EU-SCICF) which the ESAs publicly committed to working towards in a January statement.[ii] This initiative will primarily drive supervisory efficiency across the EU. However, any indirect benefit for firms will only become apparent over time.

International regulatory alignment cannot be ignored

Firms operating cross-border business models – e.g., operating in both the EU and UK – will need to consider how the DORA's requirements will fit in with work they are doing in other jurisdictions. One notable difference is that the DORA addresses operational resilience as a detailed set of legislative requirements whereas operational resilience is being handled as a principles-and-outcomes-based initiative by supervisors in the UK and elsewhere. The DORA also focuses on digital and ICT risks, whereas the UK and other frameworks consider operational resilience more broadly. This may contribute to a greater emphasis in the EU on cyber threat and other technology-related risk scenarios.

There are, however, a set of outcomes in the DORA's requirements that are common with the UK supervisory framework and, for banks, the Basel Committee's 2021 Principles on Operational Resilience. Both frameworks require the identification of critical parts of the business (i.e., important business services in the UK, critical or important functions in the DORA), and the alignment between jurisdictions here will be a key area for supervisors to determine. The Council's amendment requiring firms to conduct business impact analyses of their exposure to severe disruptions also brings the DORA closer to the UK and BCBS's introduction of testing resilience against "severe but plausible scenarios."

Our view is that cross-border firms will gain efficiencies when they adopt a consistent approach to operational resilience group-wide and modify it in each jurisdiction as far as necessary to meet specific requirements. There are clear opportunities for the DORA to be compatible with such an approach, but much will depend on the Level 2 work done by the ESAs and the supervisory approach taken by authorities, the ECB chief among them. The 2020 ECB, US, and UK authorities' statements committing to deliver a joined-up approach to the supervision of operational resilience demonstrates encouraging cooperation.[iii]

Early implementation actions need to be identified

It is important for firms to identify actions they can take now, before the primary legislation is finalised and Level 2 standards from the ESAs are available. In our experience of working with UK firms, where the regulatory initiative on FS operational resilience is at a more advanced stage, preparing for the initial implementation of the new rules has taken more time and resources than many firms anticipated.

In a recent executive survey we conducted for our 2022 Regulatory Outlook, UK firms highlighted the identification and management of TPP vulnerabilities as the most important challenge they faced in implementing operational resilience requirements.[iv] EU firms will likely face a similar challenge with the DORA as well.

In our view, several "no regret" actions firms should be considering include:

- **On ICT risk management:** conducting a gap analysis of existing ICT risk management and governance practices, specifically through a critical function lens, will be a worthwhile exercise. Additionally, increasing resources dedicated to threat and incident detection and improving firm-wide ICT security awareness training programmes with a special focus on awareness of management bodies will be beneficial.
- **On incident reporting:** running an incident management and reporting maturity evaluation to understand the firm's current-state capabilities and evaluate the firm's awareness of the multiple ICT incident reporting requirements that apply in the FS sector.
- **On resilience testing:** understanding the skills and capabilities required to shape and run resilience testing, including training sessions for board members on resilience testing methods (including TLPTs if likely to be in scope of advanced testing requirements), and the implications for remediation.
- **On TPP risk management:** focusing on improving mapping of TPP contracts and connections, documenting and reviewing third party vulnerabilities to help inform the development of a risk containment strategy.

As the DORA moves towards finalisation, firms need to be mindful of the scale of the challenge that implementation will bring. A two-year implementation period will be a short window of time to get things right. Firms can stay on the front foot by taking a proactive approach to assessing the impact of the requirements to develop a realistic and achievable implementation plan.

Endnotes

[i] As the DORA is cross-sectoral, Level 2 rulemaking will be done jointly by the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA), often working in their Joint Forum composition.

[ii] European Supervisory Authorities, Public statement, ESAs welcome ESRB Recommendation on a pan-European systemic cyber incident coordination framework for relevant authorities.

[iii] European Central Bank, Banking Supervision, Statement regarding supervisory cooperation on operational resilience

[iv] Deloitte, EMEA Centre for Regulatory Strategy, 2022 Financial Markets Regulatory Outlook

The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict

As warnings of an imminent Russian attack on Ukraine proliferate, news networks and social media have featured clips of Russian armed forces training, exercising, and preparing to fight. Less visible are Russia's formidable cyber forces that would be preparing to unleash a new wave of cyber-attacks on Ukrainian and western energy, finance, and communications infrastructure. Whether an invasion occurs now or not, tensions will remain high, and the cyber threat will likely wax, not wane.

The implications for business of conflict in Ukraine — whether conventional, cyber, or hybrid — will be felt far beyond the region's borders. As a business leader, you've likely already assessed whether you have people at risk, operations that might be affected, or supply chains that might be interrupted. The White House recently warned of the supply-chain vulnerabilities stemming from the U.S. chip industry's reliance on Ukrainian-sourced neon. And Russia also exports a number of elements critical to the manufacturing of semiconductors, jet engines, automobiles, agriculture, and medicines, as detailed in a Twitter thread by former Crowdstrike CTO, Dmitri Alperovitch. Given the existing pressure on U.S. supply chains from the Covid-19 pandemic, adding further shock to the system is worrisome.

But if you are just now evaluating your cyber posture, you are probably too late. Effective cyber defense is a long game requiring sustained strategic investment, not a last-minute bolt on.

Conflict in Ukraine presents perhaps the most acute cyber risk U.S. and western corporations have ever faced. Invasion by Russia would lead to the most comprehensive and dramatic sanctions ever imposed on Russia, which views such measures as economic warfare. Russia will not stand by, but will instead respond asymmetrically using its considerable cyber capability.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) recently issued a warning of the risk of Russian cyberattacks spilling over onto U.S. networks, which follows previous CISA warnings on the risks posed by Russian cyberattacks for U.S. critical infrastructure. The European Central Bank (ECB) has warned European financial institutions of the risk of retaliatory Russian cyber-attacks in the event of sanctions and related market disruptions.

Early cyber skirmishing has already begun, with Ukrainian government systems and banks attacked in the past week, and vigilant U.S. companies noting a dramatic increase in cyber probing. Rob Lee, CEO of the cybersecurity firm Dragos told us, "We have observed threat groups that have been attributed to the Russian government by U.S. government agencies performing reconnaissance against U.S. industrial infrastructure, including key electric and natural gas sites in recent months."

The security and intelligence teams at several major multinationals indicated to us that they are anticipating Russian cyberattacks and assessing the potential for second and third-order effects on their operations. Some companies noted that they are anticipating an increase in attacks and scams in conjunction with the Ukraine crisis, with risk assessments typically contingent on whether the company has direct links to Ukrainian national banks or other critical infrastructure. One corporate intelligence manager observed that their cyber team "doesn't think we're a likely target," but has been following CISA guidance. Another similarly indicated that their company was not concerned with direct threats to their data, because they have no presence in Ukraine or Russia, but were watching for indirect impacts on their customers and business partners in the region.

So, if it is too late to improve your cyber defense and conflict appears imminent, what can leaders do besides throw up your arms?

The first rule is that a cyber or IT problem quickly becomes a business problem. The primary step firms should be taking right now is pulling out, dusting off, and exercising business continuity plans. What would it mean to work in an analog world, or a pencil-and-paper world, for days, weeks, or months? When Saudi Aramco was hit by a cyberattack, 30,000 corporate laptops were turned into paper weights in the span of seconds. Take out your pen knife and poke under the crisis response paint. Ask: “If my IT systems go down, how am I going to track my inventory, manage my accounts, or communicate with my offices and plants?”

Second, closely examine your supply chain. Your firm may face the risk of hidden dependence upon Ukrainian-based software engineers, code writers, or hosted services. Ukraine’s Ministry of Foreign Affairs reports that more than 100 of the world’s Fortune 500 companies rely at least partially on Ukrainian IT services, with several Ukrainian IT firms being among the top 100 outsourcing options for IT services globally.

Third, connecting with peer networks, vendors, and the FBI can dramatically improve your odds of identifying and mitigating cyber intrusions. Empower your teams to reach out to cyber and intelligence teams at peer companies, and to federal and local government partners who are closely watching the same threats. Ensure that your teams know their regional CISA representatives and local FBI field office and that they’re on their mailing lists to stay on top of alerts and warnings. Share anomalous or malicious cyber activity with federal and local partners for greater awareness to help build a collective defense.

Fourth, instill a security mindset in your employees. Enabling multifactor authentication (which, according to CISA Director Jen Easterly makes you 99% less likely to get hacked), patching those old vulnerabilities, ensuring passwords are strong, and remembering that phishing is still the number one attack vector, even for sophisticated adversaries — all of these can contribute to better overall security.

Finally, recognize cyber security as closely connected to overall business security and risk. In face of cyber threats, corporate leadership too often turns to IT for a solution, but IT security and geopolitical risk assessments must go hand in hand.

Teams looking at cyber security, geopolitical risk, and physical security should be working closely together, not in silos. In one case, a corporate intelligence manager told us that he had produced a joint assessment with his cyber intelligence team on Russia-Ukraine — the first time they had ever cooperated in that way. In this case, the crisis built on pre-existing relationships and prompted new levels of cooperation.

If you’re building relationships in crisis, it may be too late. It’s far better to build communication and cooperation before disaster strikes. Be wary of risk assessments that assign too much weight to proximity or presence. In a cyber war, innocent bystanders far afield can be hit by stray cyber bullets or precise cyber sniper fire.

In a crisis, corporate resilience and business continuity plans become paramount, and these require whole of company attention and solutions. With the threat of war in Europe looming, which will certainly include cyber, it is time to pull out those contingency plans and test if they are current, realistic, and fit for purpose.

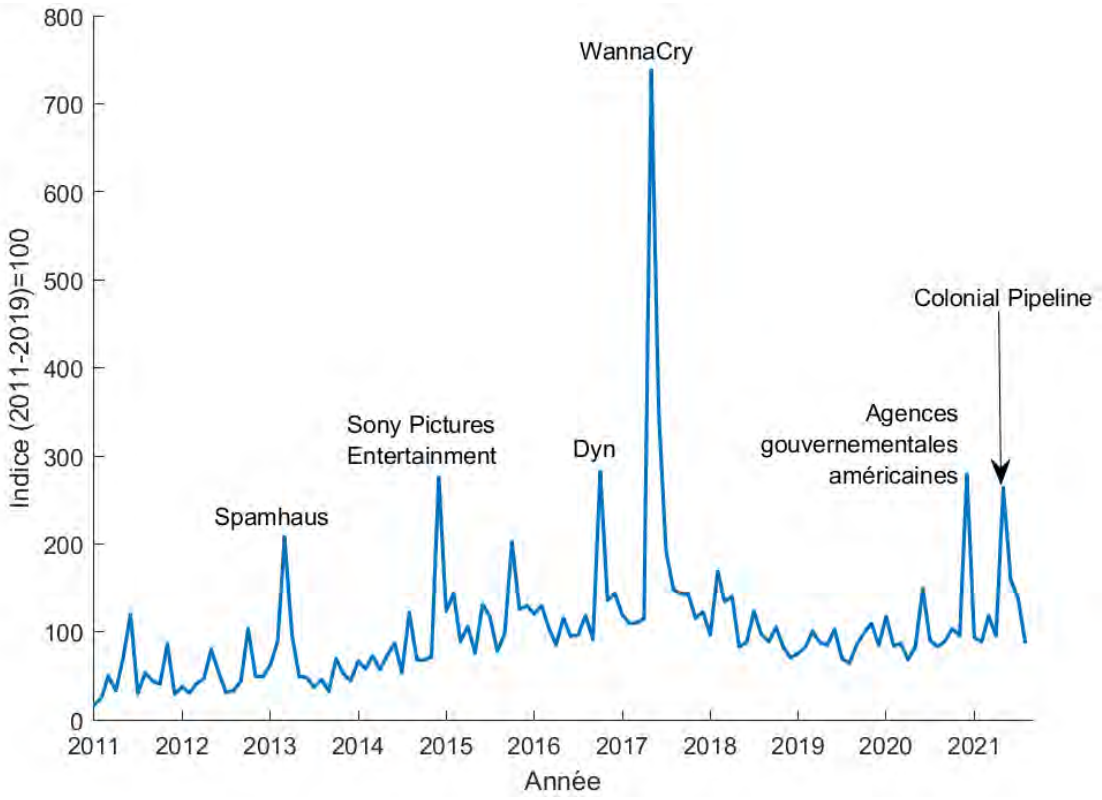
Paul R. Kolbe
Maria Robson Morrow
Lauren Zabierek

Une mesure de l'évolution du risque cyber

Par Stéphane Lhuissier et Fabien Tripier

Après la crise financière de 2008, la crise sanitaire de 2020, la prochaine crise économique mondiale sera-t-elle cyber ? Le risque cyber constitue une réelle menace pour l'économie face à laquelle les autorités sont mobilisées. Ce billet présente un indicateur permettant de suivre quotidiennement l'évolution de ce risque à partir des échanges sur le réseau social Twitter.

Graphique 1 – Évolution du risque cyber au cours de la dernière décennie



Source : Twitter et calcul des auteurs.

Avec la digitalisation et la transformation du système économique et financier, le risque d'une crise majeure émanant du cyberespace est à prendre au sérieux. C'est ce que suggèrent Christine Lagarde, la Présidente de la Banque Centrale Européenne, dans son discours du 5 février 2020, ainsi que Jerome Powell, le Président de la Réserve fédérale des États-Unis le 12 avril 2021. Ce dernier déclarait « *Les chances que nous ayons un effondrement qui ressemble de près ou de loin à celui [de 2008] (…) sont très, très faibles. (…) Le monde évolue. Et les risques changent également. Et je dirais que le risque que nous surveillons le plus actuellement est le risque cyber. (…)* ». Dans une enquête sur le risque

systémique menée en 2019 par la Banque d'Angleterre, 61% des participants ont d'ailleurs exprimé leurs inquiétudes quant à l'impact sur le système financier de cyberattaques si elles devaient se matérialiser, plaçant ainsi le risque cyber devant le risque géopolitique et le risque d'un ralentissement économique mondial.

Bien que les considérations de risque cyber aient été progressivement intégrées dans le cadre de la gouvernance et de la gestion des risques des autorités monétaires et financières (Kashyap et Wetherilt, 2019), la disponibilité d'outils de suivi du risque cyber reste cependant très limitée (une exception est l'étude de Jamilov, Rey et Tahoun., 2021, qui propose une mise en perspective historique de l'évolution de ce risque à travers le monde et au sein des principaux secteurs d'activité économique).

Un outil de suivi quotidien et en temps réel du risque cyber

Dans Lhuissier et Tripier (2021), nous construisons un nouvel indicateur du risque cyber depuis 2011. La finalité de l'indicateur est de permettre un suivi à haute fréquence, quotidien, du risque cyber et une analyse des différents secteurs de l'économie concernés.

Le risque cyber se définit comme la combinaison de la probabilité de survenance des incidents cyber (incidents malveillants ou non qui mettent en péril la cybersécurité d'un système d'information ou enfreignent les procédures et règles de sécurité) et de leur impact. Pour en mesurer son évolution, nous avons calculé la part des messages consacrés au risque cyber sur le réseau social Twitter depuis dix ans. Plus précisément, notre indicateur reflète la fréquence de tweets, émis par les utilisateurs anglophones, qui contiennent le duo de mots suivant : « cyber » et « risque », « attaque », ou « menace ». Les avantages de notre méthodologie sont multiples : elle permet 1) d'englober tous les évènements qui se sont réalisés au niveau mondial et ont donné lieu à des échanges en anglais sur ce réseau social, 2) de pondérer l'importance d'un évènement par rapport à un autre (un évènement majeur se verra naturellement attribuer plus de tweets qu'un évènement dérisoire), et 3) de suivre de manière quotidienne et en temps réel le développement du risque cyber. Il faut néanmoins garder à l'esprit les limites de cet indicateur. Il ne couvre que les acteurs de l'économie présent sur ce réseau, et qui plus est anglophones. De plus, nous ne mesurons que la fréquence de l'occurrence des mots clefs liés au risque cyber, sans analyser le contenu des messages ni les interactions des émetteurs de ces messages.

Le graphique 1 affiche l'évolution de notre indicateur de risque cyber de janvier 2011 à août 2021. La plus forte occurrence des messages liés à la cybersécurité sur Twitter que nous mesurons a eu lieu en mai 2017 lors de l'attaque WannaCry, un logiciel malveillant qui a frappé des centaines de milliers d'ordinateurs dans des centaines de pays. L'évènement majeur le plus récent que nous identifions est l'attaque en mai 2021 de la société Colonial Pipeline (gestionnaire d'un oléoduc entre Houston et New York) qui a eu des répercussions politiques importantes (dont la réunion sur la cybersécurité organisée le 25 août dernier par le Président Joe Biden).

Certains évènements se répercutent sur les marchés financiers. À titre d'exemple, en décembre 2020, le piratage de SolarWinds, éditeur de logiciels de gestion informatique et fournisseur d'agences fédérales et de sociétés américaines, a paralysé jusqu'à 18 000 clients et plus d'une centaine de sociétés américaines. L'action SolarWinds Corp a chuté d'environ

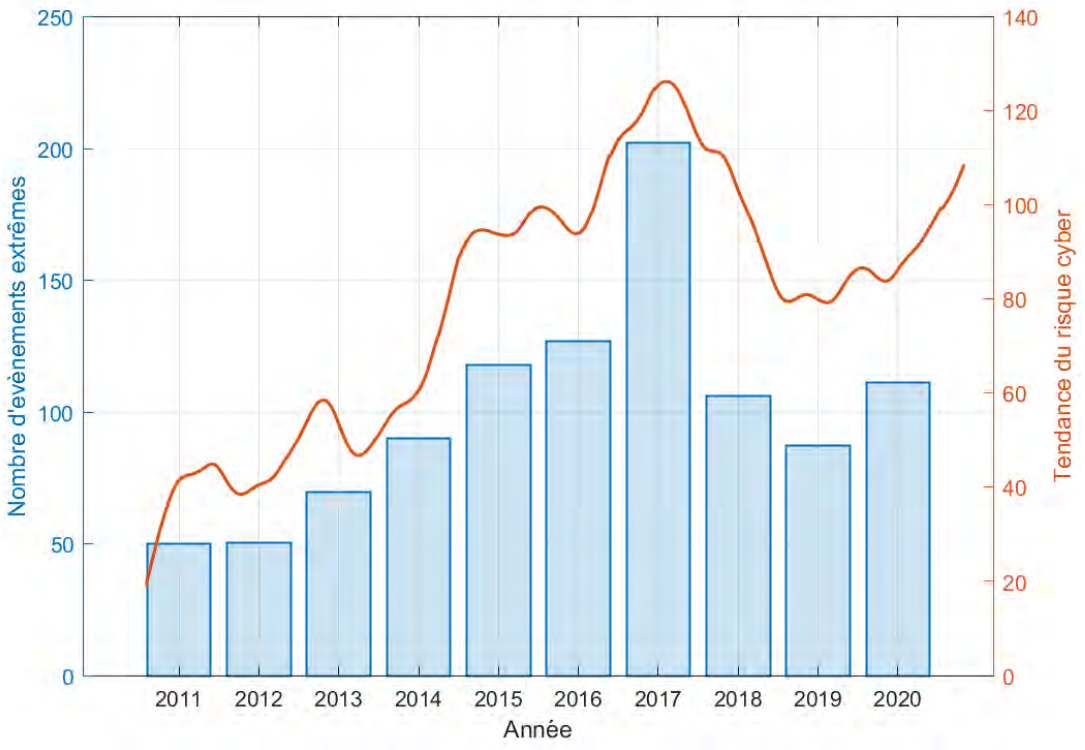
40% en seulement quelques jours à la suite de l'attaque. Bien que ses effets n'aient pas provoqué d'incidents majeurs dans le secteur financier, on pourrait tout à fait imaginer qu'un tel scénario se produise dans le futur. La très forte digitalisation et interconnexion du secteur financier en fait un secteur particulièrement exposé au risque systémique, c'est-à-dire que les conséquences de l'incident cyber se transmettent bien au-delà de l'entité initialement impactée causant des dommages au système économique et financier dans son ensemble.

Une décomposition tendance-cycle du risque cyber

L'indicateur fournit une mesure du risque cyber à haute fréquence, quotidienne. Cependant, il ne permet pas d'avoir une vision claire de ses tendances. Afin de mieux appréhender la tendance du risque cyber, le graphique 2 affiche le nombre d'évènements extrêmes par année, définis ici comme les valeurs de l'indice les plus élevées (top 5%), ainsi que la tendance à long-terme de l'indice purgée des évènements extrêmes.

Entre 2011 et 2017, le nombre d'évènements extrêmes augmente de manière constante, avant de chuter en 2018 et 2019, et de rebondir en 2020. Cette évolution du risque cyber s'observe également à travers sa tendance de long terme. En effet, la tendance montre une attention croissante pour la cybersécurité jusqu'en 2017, puis ravivée à partir de 2020 dans le contexte de la crise sanitaire de la COVID-19. Ces évolutions s'expliquent logiquement par l'usage croissant des technologies de l'information et les transformations de l'organisation du travail et de la production, de plus en plus à distance et connectée.

Graphique 2 – Une recrudescence inquiétante du risque cyber depuis la crise sanitaire

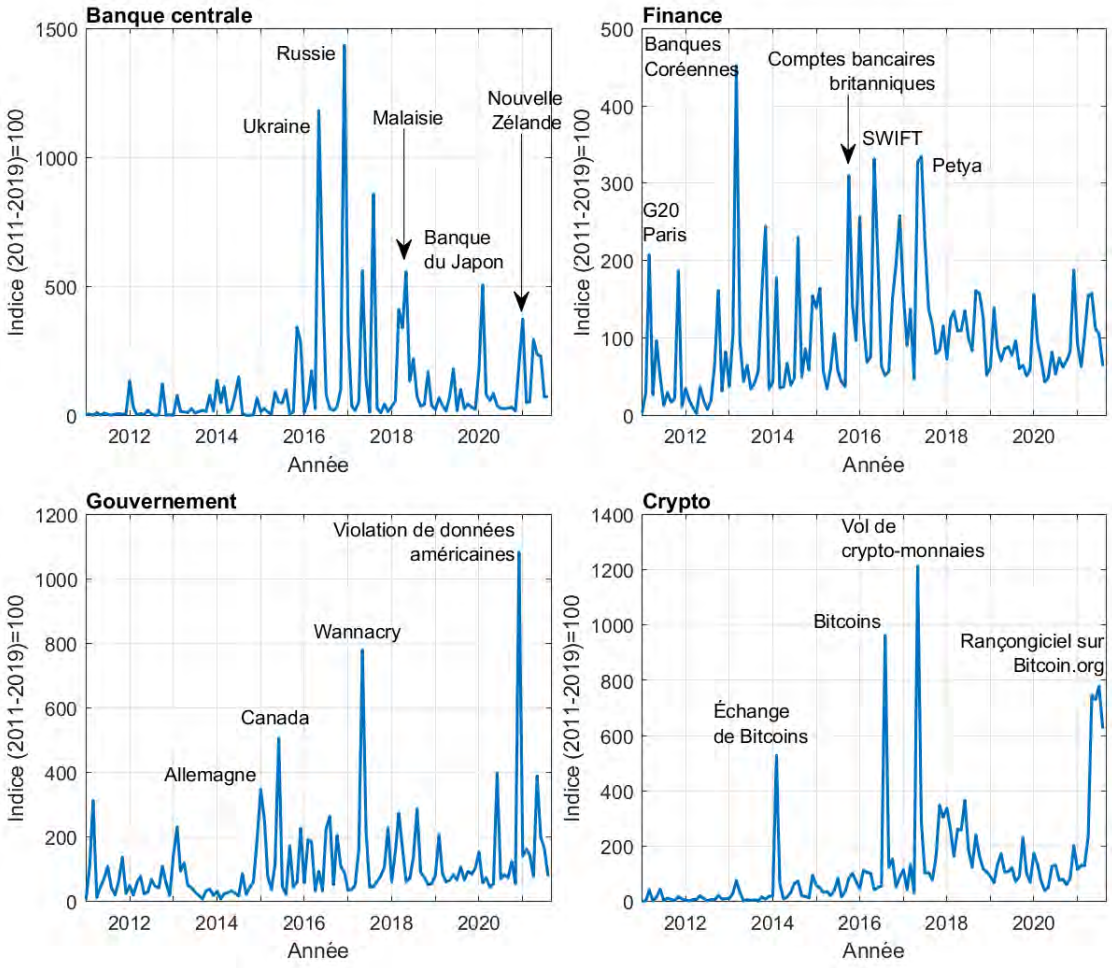


Source : Twitter et calcul des auteurs.

Des indicateurs sectoriels du risque cyber

En complément de notre indicateur de référence, nous développons des indices au niveau des secteurs les plus exposés aux cyber attaques en imposant des critères plus restrictifs lors des recherches de tweets. Par exemple, pour un indice spécifiquement lié au secteur financier, nous recherchons les mots supplémentaires suivants : « banque », « obligation », « marché financier », « pénurie de crédit », « monnaie », « dette », « dividende », « titres », et « finance ».

Graphique 3 – Indicateurs sectoriels du risque cyber



Source : Twitter et calcul des auteurs.

Le graphique 3 présente un exemple de sous-indicateurs étudiés dans notre analyse : banque centrale, finance, agences gouvernementales, et crypto-monnaie. Chacun de ces secteurs sont des cibles populaires pour les cyber criminels comme ils détiennent de nombreuses informations confidentielles et personnelles. À titre d'illustration, le risque cyber auquel sont exposées les banques centrales a atteint son plus haut niveau avec l'attaque de la banque centrale Russe en 2016, où des hackers ont volé plus de 2 milliards de roubles (24 millions d'euros) à partir de comptes de correspondant. Cependant, les pics ne sont pas nécessairement liés à la réalisation de cyber attaques. Par exemple, l'indicateur a

connu une forte progression en janvier 2020 lorsque la Banque du Japon s'inquiéta des risques de cyber-attaques avant le coup d'envoi des Jeux Olympiques. Autre exemple, le risque cyber auquel sont exposés les marchés financiers a connu une progression significative durant des évènements majeurs tels que l'attaque du sommet du G20 à Paris ou celui du réseau SWIFT, ou bien encore le rançongiciel Petya en 2017. Le graphique 3 montre également une recrudescence particulièrement inquiétante du risque cyber concernant les cryptoactifs (cet indicateur est construit en limitant les tweets de notre indicateur de référence à ceux liés aux cryptomonnaies). Les plateformes d'échange de cryptoactifs font effectivement l'objet d'un nombre croissant de cyber attaques (par exemple, la plateforme Bitcoin.org en juillet 2021).

Bien que les attaques informatiques n'aient pas engendré pour l'instant de crise économique et financière globale, certains cyber incidents pourraient toutefois affecter nos économies à l'avenir comme dans les scénarios étudiés par le comité européen du risque systémique (rapport de février 2020). Ainsi, le risque cyber n'est pas seulement un enjeu de sécurité informatique, il est donc important de l'intégrer et l'analyser dans le cadre de surveillance des risques macroéconomiques et financiers.

EXECUTIVE SUMMARY

In August 2018, EIOPA published the report "Understanding Cyber Insurance - A Structured Dialogue with Insurance Groups". The key finding was that the need for a deeper understanding of cyber risk presents the core challenge for the European cyber insurance industry.

In line with these findings and with EIOPA's mandate to safeguard financial stability, this report aims at further enhancing our understanding of cyber risks for the insurance sector. While the first report was based on a qualitative survey focusing on cyber underwriting only, this report covers both cybersecurity challenges and cyber underwriting practices of insurers.

As cyber threats have become more prominent in recent years, they are increasingly considered as a top global risk for the financial sector and the economy as a whole. The increasing frequency and sophistication of cyber attacks, the fast digital transformation and the increased use of big data and cloud computing make insurers increasingly susceptible to cyber threats. Insurance groups also form a natural target for cyber attacks, as they possess substantial amounts of confidential policyholder information. On the other hand, the digital economy and the advance of technology also offer opportunities to cyber underwriters. A well-developed cyber insurance market can play a key role in enabling the transformation to the digital economy, by raising awareness of cyber risks, sharing knowledge on good cyber risk management practices and facilitating responses to and recovery from cyber attacks.

Overall, this report provides new information about cyber risk for the European insurance sector, both from an operational risk management perspective and an underwriting perspective, based on the responses of 41 large (re)insurance groups across 12 European countries representing a market coverage of around 75% of total consolidated assets. The findings reflect the need for a sound cyber resilience framework for insurers as well as the challenges faced by the cyber underwriters. The main conclusions can be summarized as follows:

Cyber risk as an element of the insurer's own operational risk profile

- Having clear, comprehensive and common requirements on governance of cybersecurity as part of operational resilience would help ensure the safe provision of insurance services. This includes a consistent set of definitions and terminology on cyber risks to enable a more structured and focused dialogue between the industry, supervisors and policymakers, which could further enhance the cyber resilience of the insurance sector.
- The most common cyber incidents affecting insurers are phishing mail, malware infections (ransomware), data exfiltration and denial of service attacks. The main consequences suffered by insurers following these cyber incidents are business interruption and material costs for policyholders and third parties.

- Overall, the results indicate that the industry is aware of the potential cyber threats and have incorporated cyber risk explicitly in their risk management frameworks.
- Further actions to strengthen the resilience of the insurance sector against cyber vulnerabilities are essential, in particular considering the dynamic nature of cyber threats. This would include streamlining of the cyber incident reporting frameworks across the insurance and financial sector, to avoid inconsistencies in the reported information and ultimately enhance operational resilience.

Cyber insurance market

- Although still small in size, the European cyber insurance industry is growing rapidly, with an increase of 72% in 2018 in terms of gross written premium for the insurers in the sample, amounting to EUR 295 million in 2018 compared to EUR 172 million in 2017. The increasing frequency of cyber attacks, changes in regulation as well as continued technological developments are all expected to increase demand for cyber insurance in the near future.
- Non-affirmative cyber exposures remain a source of concern. While common efforts to assess and address non-affirmative cyber risks are under way, the lack of quantitative approaches, explicit cyber exclusions and action plans to address non-affirmative cyber exposures suggest insurers are currently not fully aware of the potential exposures to cyber risk.
- Some groups have adopted a 'wait-and-see' approach to address non-affirmative cyber risk, where the implementation of actions plans to address non-affirmative exposure depends on the materialization of future events. This approach in dealing with cyber risks can be particularly problematic, as insurers may suffer substantial unforeseen losses in traditional polices if a cyber incident materializes.
- The lack of transparency in non-affirmative exposures also creates uncertainty for policyholders, as it is often not clear whether their cyber claims would be covered within their insurance polices. Further effort is therefore needed to properly tackle non-affirmative cyber exposures to address the issue of potential accumulation risk and provide clarity to policyholders.
- It is essential for the industry to further improve its assessments and data collection, so that cyber risks can be adequately measured, monitored and managed. Ultimately, having common and harmonized standards for both cyber risk measurement and reporting purposes could greatly facilitate the understanding of cyber risk underwriting. To this end, creating a European-wide cyber incident reporting database, based on a common taxonomy, could be considered as well.

Cyber security insurance – how can insurers quantify the risk?

Cyber insurance is said to be one of the few areas of growth and innovation in the insurance market these days.

It is identified as one of the biggest risks facing the financial system, and the demand for insurance against it is growing. As pressure is being put on organisations to demonstrate that cyber risk is being managed or mitigated, many protection buyers get cover for the first time. As attacks become more malicious and costly, the demand is bound to increase.

Methods to assess this risk are at their infancy and in consequence the management of cyber risk against risk appetite is not an easy job to carry out. We ran a survey among specialist insurance companies to understand how they are getting on with this task, what their growth strategy is, and what investments they are making in this area. The PwC cyber risk management survey was carried out across 14 companies in the London market in Summer 2016.

Is cyber security risk insurable?

Lloyd's has pioneered the development in this class, but according to our survey the attitude towards cyber seems to have split the market in half. Approximately half of survey respondents already sell cyber policies, or see this as an area of growth. The other half do not actively pursue cyber, often believing this risk to be borderline insurable. The scepticism is due to limited experience of cyber losses standing in the way of confident underwriting.

On the other hand, even in the group that embraces cyber, insurers still trade carefully and tend to limit the amount of cover offered under each policy, despite the fact that there is appetite for more cover. Breach costs are constantly rising and the limited protection available doesn't even come near to what the cost of a truly damaging cyber attack would be to a large business.

The issue with silent cyber

Lloyd's and other regulators are questioning (re)insurers on how well they understand their exposure to cyber. While exposure to the so called "affirmative" cyber (arising from selling cyber policies) is to a certain extent possible to control, all insurers and reinsurers, regardless of their views on the insurability of cyber, will have exposure to "silent" cyber.

These losses come as a result of a cyber-attack, but not under a dedicated cyber policy but rather from other contracts which, while not designed to protect from cyber, do not exclude this type of risk either. For example: an attack on a common billing or payroll system could result in the loss of personal data and in financial loss, which could in consequence lead to a high number of claims under Professional Indemnity policies.

The PwC survey queried companies in the London market about parts of their book that are most exposed to silent cyber and professional liability, property and aviation lines were cited as most likely to be affected.

How do insurers quantify cyber risk?

The main challenge emerging is how to design a market leading but pragmatic approach to managing cyber risk. The issue is not only due to data available being scarce, but also because any models are at risk of quickly becoming obsolete due to the rapid change of the cyber risk landscape as cyber weaponry progresses.

While 85% of respondents claim to have a loss estimation methodology in place, the majority use simplistic exposure and factor based methods which have in the past shown to underestimate the risk (as we have seen with unmodelled events like the Thai Floods). This is contradicted by the fact that 70% of respondents believe their method to be overly conservative.

Insurtech and cyber scenarios

While a flurry of new software and data products has recently entered the market to help with this issue, only 25% of respondents use external tools, and the majority within that group uses technology mainly to supplement assumptions and data applied in simple exposure management based methods – the prevailing view is that the tools available need further development to be suitable to manage insurance portfolios.

The job of understanding accumulations of this risk has in most cases been given to exposure management teams, and while parallels can be seen between early years of catastrophe models and cyber, management of this risk requires some unique consideration and analysis.

It is worth bringing stakeholders together and use extreme scenarios to test the interconnectedness of exposures, as well as seek to understand how policies that are silent to cyber might respond. While those scenarios may be unlikely to occur, firms have been finding them helpful in understanding possible causes of losses and levels of coverage affected.

And as it is the case with natural catastrophes, we are likely to be very surprised (but learn a lot) when the next significant event occurs.