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

Trésor-Éco

N° 295 • Décembre 2021

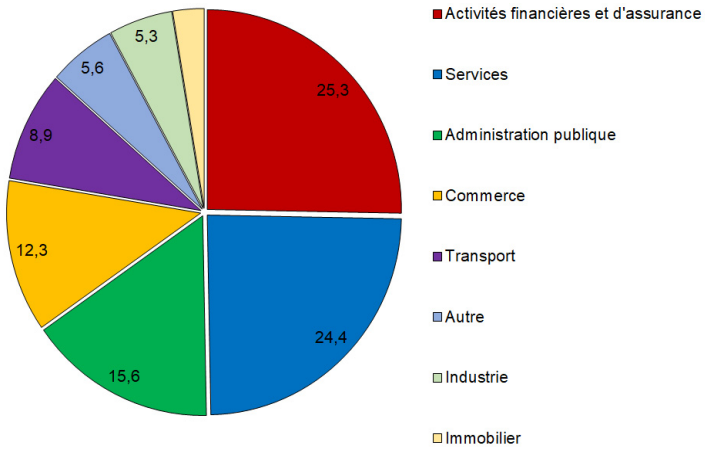
Direction générale du Trésor

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.

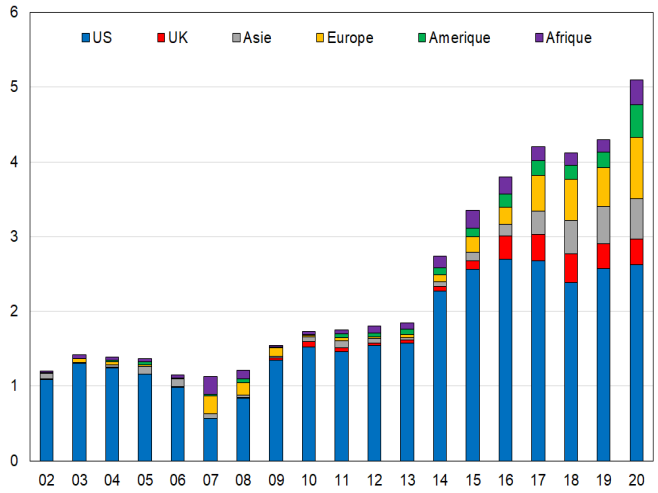
1.2 Un risque difficilement quantifiable mais vraisemblablement en hausse

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.

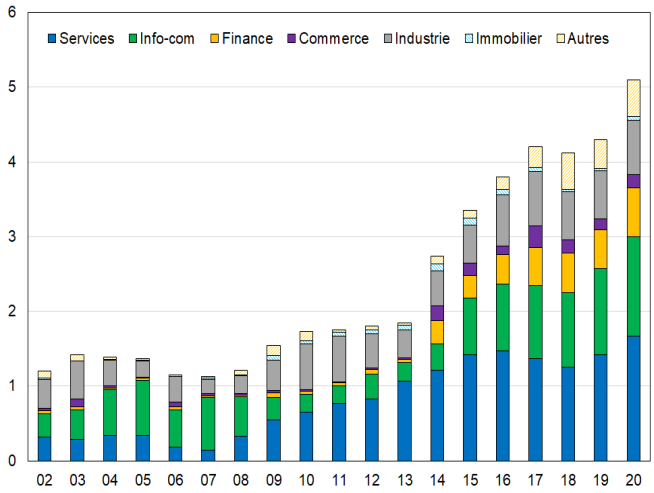
La forte augmentation du risque cyber depuis plusieurs années fait cependant consensus, et elle est documentée par des études académiques. Jamilov *et al.* (2021) montrent, à l'aide d'une analyse textuelle des transcriptions des conférences d'annonce de résultats financiers, que les références au risque 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

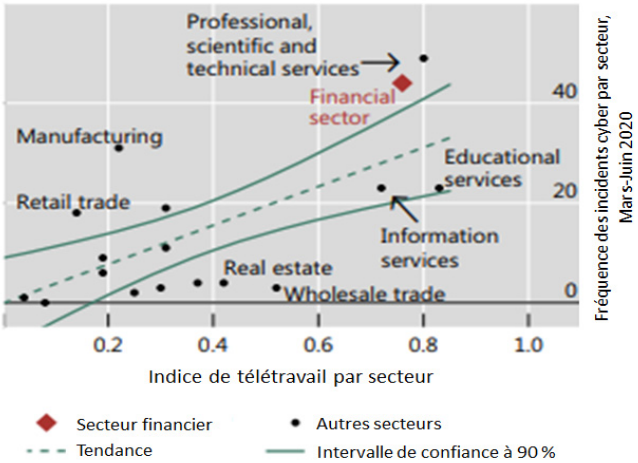
Selon le Boston Consulting Group, les entreprises du secteur financier seraient 300 fois plus susceptibles d'être ciblées que celles d'autres secteurs[13]. La plupart des études académiques identifient le secteur financier comme figurant parmi les secteurs les plus victimes d'incidents cyber. En raison 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