Cadre réservé à la correction

Note : 18/20

Signature :

87 EDD

Feuillet n° : 1 / 5

Question 1

Les institutions financières sont particulièrement exposées aux risques cyber, c'est à dire, selon la définition de Cebula et Young, aux risques opérationnels pouvant affecter : la confidentialité, l'intégrité ou la disponibilité des données ou systèmes d'information. L'intrusion, volontaire ou pas, et les incidents opérationnels divers affectant le numérique en sont les deux sources principales qui permettent de déduire deux catégories de risques cybers affectant les institutions financières.

La première catégorie de risque cyber est celle de la cyberattaque, soit l'intrusion de partis externes donnant accès aux logicielles ou données de l'organisation. Les intrusions peuvent être volontaires ou pas et peuvent prendre différentes formes. Il peut s'agir d'attaque visant directement le système informatique ou un logiciel via l'exploitation de vulnérabilités. Mais l'attaque peut aussi être indirecte en exploitant des tiers de l'Entreprise, notamment en visant des intervenants de la chaîne d'approvisionnement ou en ciblant les employés de l'organisation, par exemple via des campagnes d'hameçonnage. Ces intrusions peuvent avoir différents objectifs, vol d'argent, directement, vol de données pour leur valeur ou à des fins d'espionnage. Les institutions financières sont

alors des cibles privilégiées car détiennent de ces richesses (argent et données) en abondance. Par exemple, l'agence de notation Equifax avait fait l'objet d'un vol de données en 2017. Mais les institutions financières peuvent aussi être la cible d' "hacktivistes" ne cherchant pas à voler mais à destabiliser le système financier. Ainsi, Anonymous a déjà attaqué plusieurs places de bourse mondiales dans ce but.

La deuxième catégorie de risque concerne tout incident affectant les systèmes numériques de l'institution. Les incidents peuvent être dûs à des défaillance de procédure ou bien des incidents physiques. C'est ainsi que la pandémie de COVID s'est accompagnée d'une recrudescence des incidents cyber. Les entreprises ayant déployés le télétravail, elles étaient plus vulnérables aux attaques mais surtout à tout évènement plus courant. Par exemple, un bris de matériel ou un manquement dans les processus empêchant la connexion des collaborateurs. Le secteur financier est particulièrement concerné par la numérisation de son mode de travail ou de ses prestations, le rendant vulnérables et dépendants à son système d'information

Par ailleurs, les banques et autres institutions financières peuvent être impactés par des problèmes cyber affectant leurs clients ou même d'autres acteurs du système financier. Ainsi, les incidents cyber peuvent être un facteur de risque systémique.

Cadre réservé à la correction

Note : /20

Signature :

87 EDD

Feuillet n° : 2 / 5

Question 2

Pour mesurer le risque systémique, c'est à dire le risque de voir pouvant jouer atteinte à l'ensemble du secteur financier, engendré par des vulnérabilités cyber, il convient de mesurer l'importance du risque cyber puis son impact sur les institutions financières.

Tout d'abord, il s'agit de mesurer le niveau de risque cyber global afin de comprendre les probabilités d'occurrence et l'ampleur des effets dûs à des vulnérabilités cyber. Il n'existe pas encore d'indicateurs de référence en la matière. C'est pourquoi Lhuissier et Tripier propose par exemple un indice de tendance de risque cyber. Celui ci est construit grâce au nombre d'apparition de mots clés en lien avec le cyber dans les messages twitter d'acteurs économiques anglophones. A priori, plus ces mots sont mentionnés, plus il y a d'incidents ou plus ils ont d'ampleur. Ensuite, il est nécessaire de quantifier les pertes engendrés par les événements cyber. La Value at Risk est la méthode la plus répondue, permettant de mesurer les pertes probables d'un événement. Mais cette quantification des pertes est particulièrement complexes soit car tous les événements ne sont pas reportés, les données sont insuffisantes mais aussi car les incidents cyber peuvent avoir des effets sur

parties prenantes indirectes. Ainsi pour mesurer le niveau de risque cyber global il est particulièrement important d'identifier les interconnexions ces nœuds critiques source de propagation des incidents. En effet, une étude sur l'attaque de NotPetya de 2017 a montré que les pertes ou manques à gagner pour les entreprises indirectement impactées ont été de 7,3 milliards de dollars soit 4 fois plus que pour les entreprises directement touchées.

Ces données permettent ensuite d'établir des scenarios et de faire des modélisations pour mesurer l'impact pour le système financier de l'occurrence d'incidents cyber. Il s'agit alors d'établir plusieurs scenarios en fonction des différents incidents pouvant se matérialiser : atteinte des données, perturbation de fonctions critiques. A partir de ces scenarios, des stress test peuvent être menés pour mesurer la capacité des banques à absorber les pertes liées à un "cyberrisk". L'impact reste cependant dur à défendre. Ainsi Duffie et Younger ~~i~~ concluent dans leur étude de 2019 qu'une perte de confiance liée à un incident cyber ne poserait pas de problèmes aux plus grosses banques américaines car elles disposeraient suffisamment de liquidité. Alors qu'Eisenbach en 2020 analyse que si une des 5 plus importantes banques américaines était touchées alors l'impact serait systémique.

Question 3.

Les compagnies d'assurance sont à la fois des cibles privilégiées des attaques cyber et impactées dans leur modèle d'affaires par le développement des risques cyber.

D'abord, les compagnies d'assurance sont directement exposées au risque cyber puisqu'elles détiennent notamment d'importantes quantités de données pouvant être particulièrement confidentielles. Elles sont alors la cible privilégiée des attaques pour espionnage. C'est d'ailleurs la raison qui aurait poussé au vol de données en 2014 des compagnies américaines Anthem, Premera Carfirst et Excellus. Elles peuvent aussi faire l'objet de piratage cyber. En effet, en détenant des données sur la qualité des systèmes d'information de leurs clients, elles possèdent une source de renseignement particulièrement intéressante afin que les hackers puissent mieux identifier leurs victimes.

Mais, par ailleurs, les compagnies d'assurance sont exposées aux risques cyber au travers de leurs prestations. D'ores et déjà, les assurances constatent une multiplication des incidents pouvant requérir un remboursement de leur part. Même lorsqu'elles ne couvrent pas encore le risque cyber ouvertement, la

hausse des incidents opérationnels qu'ils provoquent amènent les assurances à questionner leurs modèles de couverture. De plus les assurances anticipent qu'elles devront permettre la couverture de risques cyber. L'assureur Hiscox a interrogé un panel de clients entreprises sur l'occurence d'attaques cyber : 38% d'entre elles furent attaquées en 2020 et 43% en 2021 dont plus d'un quart furent visées au moins cinq fois dans l'année. Les assurances visent à mettre en place des couvertures cyber mais les difficultés pour la mesures rendent le développement de telles offres très risqué. En effet, la bonne compréhension du risque et sa quantification sont primordiales pour les modélisations des assurances. L'autorité européenne des assurances EIOPA assure que pour le moment la compréhension du risque cyber insuffisant et doit donc être au coeur des préoccupation des acteurs et régulateurs.

Question 4.

Le règlement DORA (Digital Operational Resilience Act) de la Commission Européenne devrait permettre de répondre à la plupart des enjeux du secteur financier liés aux risques cybers en Europe. En effet, il propose notamment d'améliorer la connaissance de ce risque en définissant un cadre de référence commun et impose aux différents acteurs du secteur de mettre en place de bonnes pratiques.

Premièrement, l'un des défis de la cyber sécurité est la quantification du risque.

DORA permettra d'améliorer l'identification des risques en imposant aux banques l'établissement d'une cartographie de leurs actifs informatiques et des risques liés, en définissant un vocabulaire commun et en demandant la mise en place de procédure de détection des incidents.

Deuxièmement, DORA promet la mise en place et le développement de bonnes pratiques en matière de gestion des risques cyber. Même les plus petits établissements bancaires devront mettre en place des tests de pénétration. De plus, ils seront tenus de prévoir un cadre de gouvernance et de gestion des risques couvrant le risque cyber.

Enfin, le règlement s'attaque au problème des effets dominos entre les banques et leurs tiers. Notamment il prévoit une surveillance renforcée des prestataires critiques de services informatiques. En outre, il impose aux prestataires critiques situés dans des pays tiers de créer des filiales en UE pour garantir une meilleure supervision.

Ainsi le règlement DORA propose de nombreuses solutions aux enjeux cyber, d'autant plus qu'il n'est qu'une composante d'un package règlementaire européen sur le sujet qui vise d'autres aspects tels que les monnaies

crypto via le règlement Mica. Mais étant donné le caractère systémique et global des risques cyber, une couverture seulement européenne peut rester insuffisante.

Question 5.

It is challenging to assess and quantify the cyber risks given the difficulties to obtain the related data and the lack of a common framework.

The lack of information is a major obstacles to the measurement of the risk. The companies victims of cyber risk are reluctant to report incidents because they are afraid for their reputation or even because they have not identified the problem. Then, the modelisation and quantifying of losses is very sensible. For instance, the IMF reports that depending on the assumptions, a systemic impact of cyber risk could entail between $ 799 bn and $ 22,500bn of losses. The models are very sensible to very uncertain information. For instance, it is impossible to conclude wether an IT system is fully secured.

This lack of information is also the result of missing regulatory or commun framework. For instance banks must report significant incidents but the definition of significant is unclear.

That is why using a common vocabulary becomes paramount. The financial authorities can play a major role by introducing clear definition, common measurements and best practices, to improve the assessment of cyber risks and thus their understanding, to avoid any major incidents