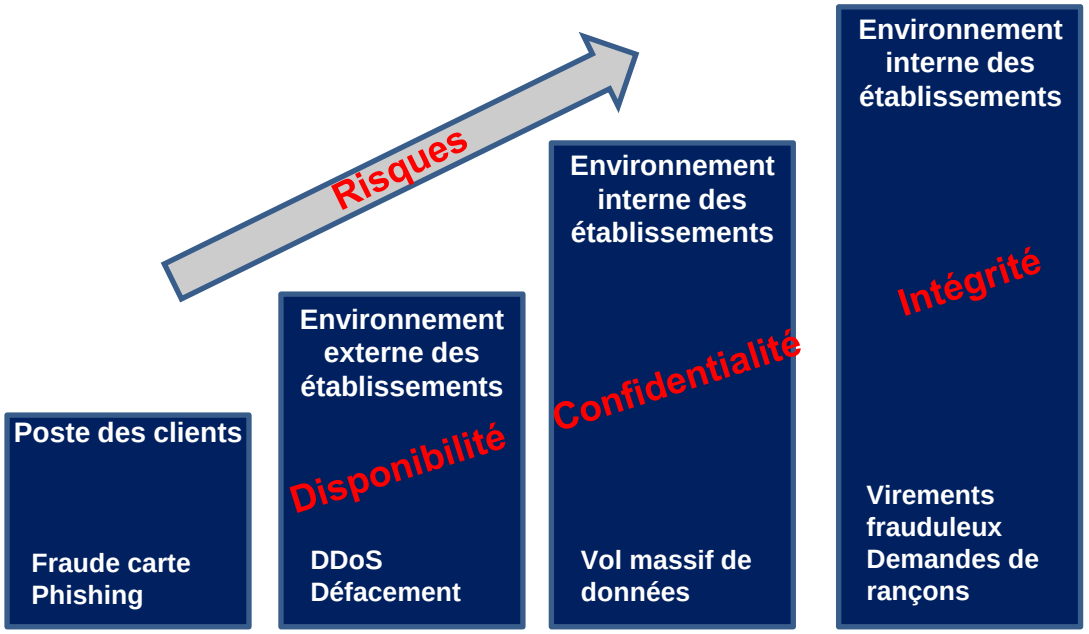
Les attentes de l'ACPR sur le risque informatique

Cybersécurité & Fraude :
un risque majeur pour l'industrie financière

Paris, le 12 février 2018 Frédéric VISNOVSKY Secrétaire général adjoint

1. - Un risque cyber qui renforce la nécessaire attention

- Les systèmes des établissements sont visés
- L'impact financier augmente
- Le risque de réputation est plus fort

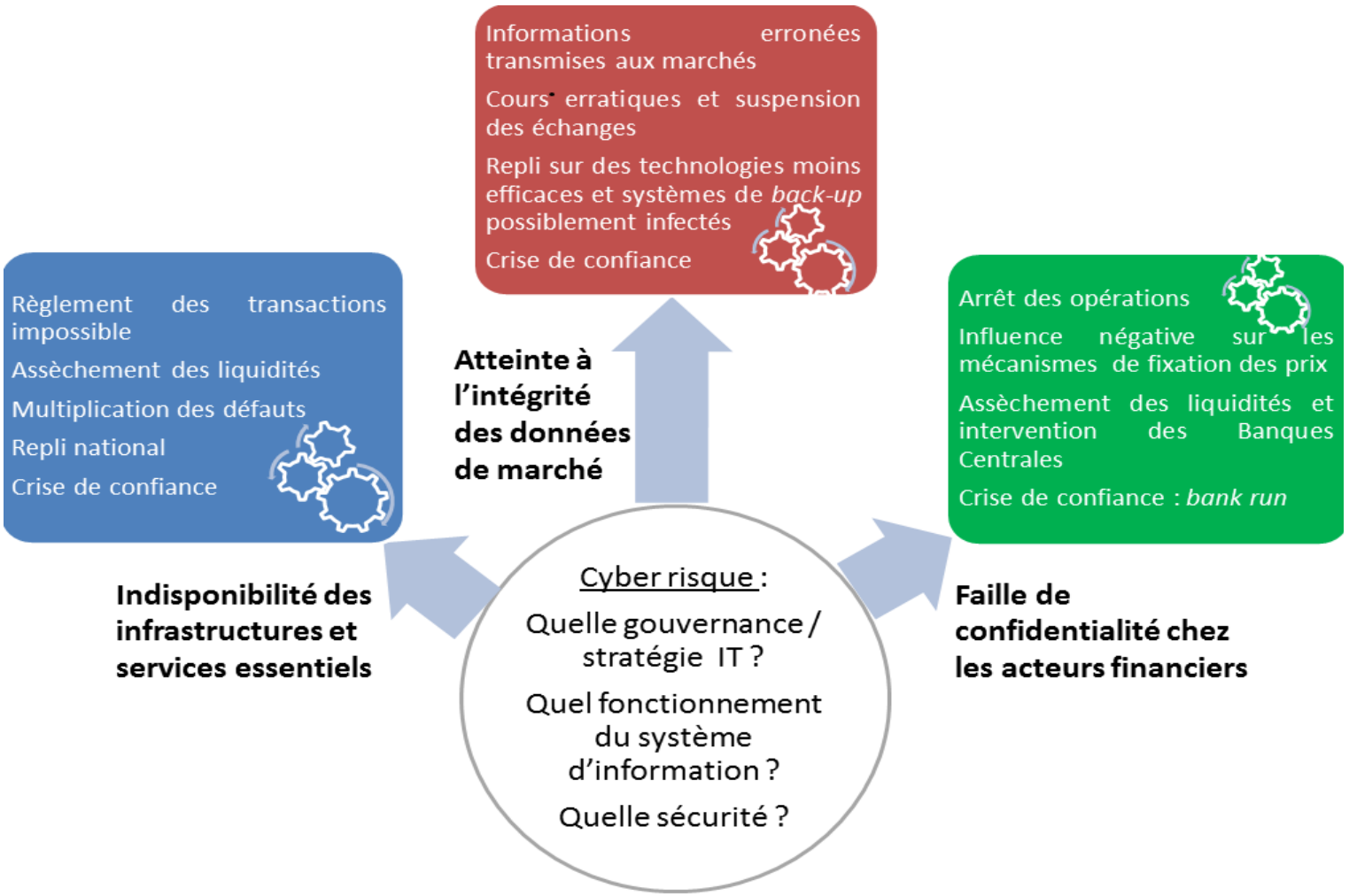


2. - Un risque potentiellement systémique

Évolution de la nature du risque	Interconnexions entre les systèmes d'information	Innovations technologiques et prépondérance des prestataires
• Des attaques qui visent les environnements informatiques des institutions (et plus seulement les équipements des clients) pour les voler et/ou pour les détruire • Des procédés qui eux-mêmes se complexifient : *Dark Net, social engineering, Exploit Kits*, puissance de calcul informatique plus forte, préparation inadéquate des employés en interne à l'utilisation des outils informatiques…	• Entre les acteurs : présence au sein d'un même groupe, relations interbancaires, (ré)assurance, externalisation, caractère intrinsèquement systémique de certains acteurs... • Nature transfrontalière des outils/ infrastructures utilisés (Internet, réseau SWIFT, chambres de compensation…) eux-mêmes systémiques	• Arrivée de nouveaux intermédiaires et technologies (FinTech ou GAFA/BATX), zones de fragilités supplémentaires possibles en lien avec les institutions financières • Croissance du recours à l'externalisation par des services de *Cloud Computing/Big Data*, impliquant des flux numérisés d'informations essentielles qui peuvent être interceptées et moins aisément contrôlables par les entités clientes souvent tributaires de leurs prestataires

Source : Banque de France - Évaluation des risques du système financier français • Décembre 2017

3. - Des canaux de transmission au système financier



Source : Banque de France - Évaluation des risques du système financier français • Décembre 2017

4. - De très nombreuses initiatives des autorités

Travaux internationaux

- G7 Expert group
- G20/ FSB
- CPMI/IOSCO
- IAIS
- Senior Supervisors Group
- EBA
- ECB

- **Renforcement des principes normatifs sur les risques cyber**
  - Autorité Bancaire Européenne :
    - Lignes directrices pour l'évaluation des risques informatiques (2017)
    - Recommandations sur l'usage du *Cloud computing* (décembre 2017)
    - Mise en chantier des « lignes directrices pour le risque informatique » (incluant la cybersécurité) en 2018
  - ACPR :
    - Recommandations sur l'usage du *Cloud computing* (Juillet 2013)
    - Élaboration d'un document de discussion sur les risques informatiques et leur maîtrise chez les banques et assurances (T1 2018)

- **Renforcement des actions de supervision depuis 2015**
  - BCE (Mécanisme de Supervision Unique) :
    - Enquête thématique début 2015
    - Lancement d'inspections sur place
    - Collecte des incidents de cybersécurité (démarrage en août 2017)
  - ACPR :
    - Questionnaire de maturité sur l'organisation et la maîtrise des risques informatiques dans les organismes d'assurance (2016)
    - Questionnaire d'auto-évaluation sur la cybersécurité (83 établissements de crédit « moins significatifs » interrogés en 2017)
    - Questionnaire sur la sécurité des SI dans les organismes d'assurance (2017)
    - Enquêtes sur place en banques et assurances
    - Accord de coopération renforcée entre l'ANSSI et l'ACPR (janvier 2018)

5. - Un enjeu majeur de supervision (1/7)

Les points d'attention identifiés

- Besoin de renforcer l'implication du management
- Inventaires à actualiser des logiciels et réseaux
- Système IT hétérogènes et inter connectés
- Obsolescence et complexité des systèmes IT

- La gestion des droits d'accès est un élément majeur
- Meilleure identification des environnements et informations sensibles

- Qualité des capteurs
- Détection dans l'ensemble des systèmes IT

- Dispositifs de réaction et de rétablissement pas nécessairement adaptés aux cyber attaques

5. - Un enjeu majeur de supervision (2/7)

Un prochain document de discussion de l'ACPR sur les attentes en matière IT

Principaux messages du document

- Le risque informatique est une **préoccupation majeure** des autorités de supervision :
  - toute l'activité des établissements est dépendante de leur IT et ces environnements sont devenus très complexes à gérer
  - les dommages informatiques peuvent avoir des conséquences particulièrement graves (pannes, cyberattaques)

- Les travaux des **instances internationales** sur le risque informatique se sont intensifiés depuis 2015 mais l'ancrage du risque informatique dans le risque opérationnel reste à clarifier.

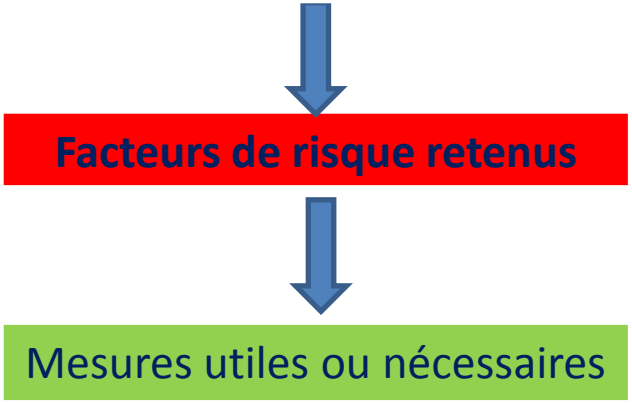
- Une **définition du risque informatique** : Le « risque informatique » (ou « risque des technologies de l'information et de la communication - TIC », ou « risque du système d'information ») correspond au risque de perte résultant d'une organisation inadéquate, d'un défaut de fonctionnement, ou d'une insuffisante sécurité du système d'information, entendu comme l'ensemble des équipements systèmes et réseaux et des moyens humains destinés au traitement de l'information de l'institution.

5. - Un enjeu majeur de supervision (3/7)

Une catégorisation du risque informatique en trois grands domaines

Organisation du système d'information et de sa sécurité	Fonctionnement du système d'information	Sécurité du système d'information

Pour chaque processus



5. - Un enjeu majeur de supervision (4/7)

Organisation du système d'information et de sa sécurité

Facteurs principaux du risque informatique :

- Implication des instances dirigeantes
- Alignement de la stratégie informatique avec la stratégie métier
- Pilotage budgétaire
- Rôles et responsabilités des fonctions informatique et sécurité de l'information
- Rationalisation du système d'information
- Nécessaire maîtrise de l'externalisation
- Respect des lois et règlements
- Gestion des risques

Mauvaise perception des enjeux
Décisions inappropriées
Pilotage insuffisant

exemple

\+

facteurs secondaires

5. - Un enjeu majeur de supervision (5/7)

Fonctionnement du système d'information

Facteurs principaux du risque informatique :

- Gestion de l'exploitation (systèmes et réseaux)
- Gestion de la continuité d'exploitation
- Gestion des changements (projets, évolutions, corrections)
- Qualité des données

\+

facteurs secondaires

5. - Un enjeu majeur de supervision (6/7)

Sécurité du système d'information

Facteurs principaux du risque informatique :

- Protection physique des installations
- Identification des actifs
- Protection logique des actifs
- Détection des attaques
- Dispositif de réaction aux attaques

\+ facteurs secondaires

5. - Un enjeu majeur de supervision (7/7)

Quel usage de cette définition et de cette catégorisation par les établissements ?

1. Les établissements sont libres d'utiliser leur propre catégorisation ou de choisir celle indiquée par l'ACPR.
2. Il convient en tout état de cause qu'ils couvrent l'entièreté du champ des risques identifiés, sauf à ce que leur organisation ou leur modèle d'affaire ne le justifie pas.
3. Lorsque tout ou partie du système d'information d'un établissement est sous-traité, cela ne signifie pas que l'établissement n'est plus exposé à ces risques informatiques. Il doit en conséquence continuer à les identifier et les maîtriser dans le cadre de sa gestion du risque opérationnel et de son dispositif de contrôle interne

Plus de détail à venir dans le document de discussion à publier

Merci de votre attention
et retrouvez les analyses de l'ACPR sur notre site internet : www.acpr.banque-france.fr