La dynamique du post-marché

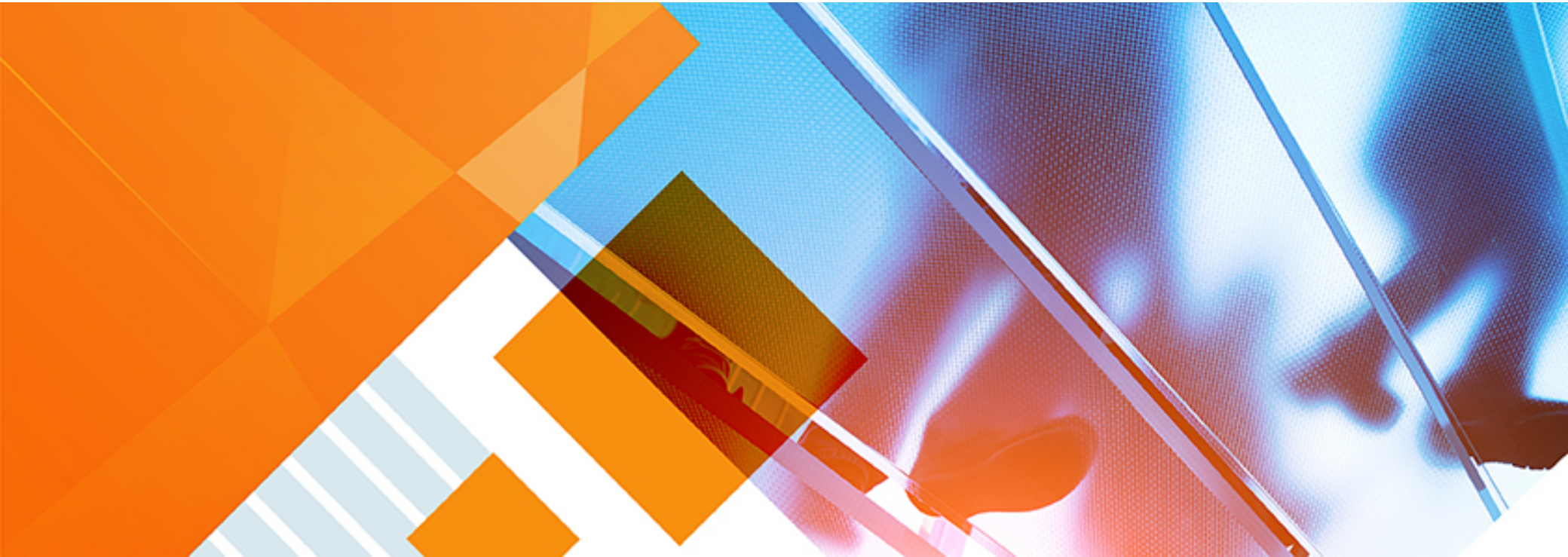
CONFÉRENCE AFTI

LES IMPACTS DE LA CYBERSECURITE SUR LES METIERS DU POST MARCHE

FÉDÉRATION BANCAIRE FRANÇAISE

Partenaire

JEUDI 14 OCTOBRE 2021



Programme

14h00 Introduction
Pierre Jond, Président AFTI
BNP Paribas Securities Services -Paris

14h05 **Sébastien Meunier**, Directeur Cybersécurité et Technologie
Chappuis Halder & Co - New-York

14h50 **Stephane Schatteman**, Responsable du pôle Robustesse et Cyber Résilience au sein du Service Résilience et Études des Infrastructures de Marché. En charge du Groupe de Place Robustesse
Banque de France - Paris

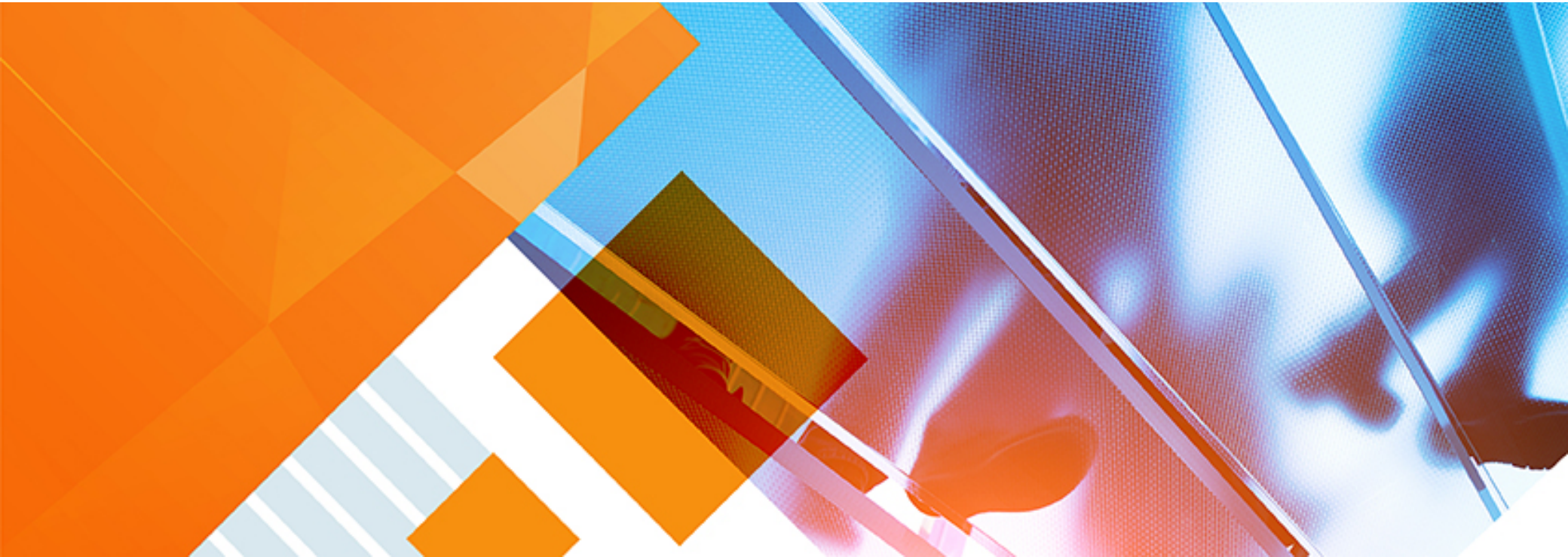
15h35 **Frédéric Rogé**, Expert en gestion et négociation de crise
Incertis - Nantes

16h30 Conclusion
Stéphanie Saint Pé, Déléguée Générale
AFTI - Paris

INTRODUCTION
Pierre Jond

Président de l'AFTI

BNP Paribas Securities Services, Paris

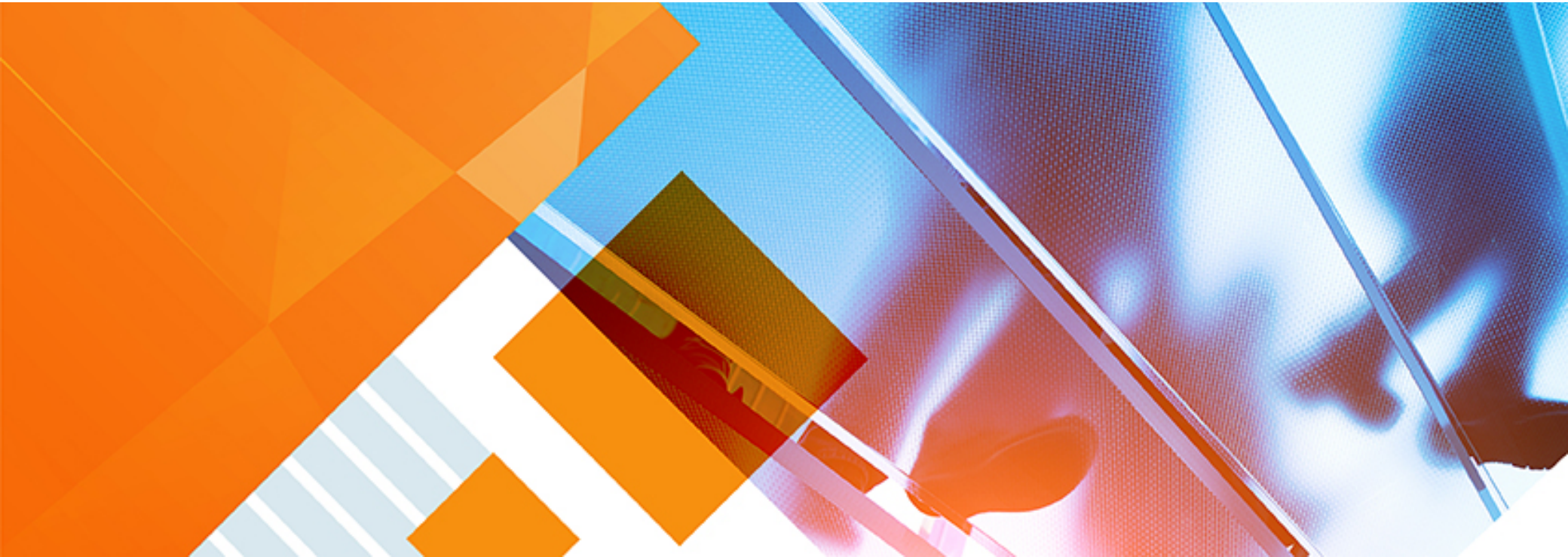


afti
La dynamique du post-marché

Retours d'expérience de projets de cybersécurité menés avec des institutions financières

Sébastien Meunier

Directeur Cybersécurité et Technologie
Chappuis Halder & Co, New-York



Retours d'expérience de projets de cybersécurité menés avec des institutions financières

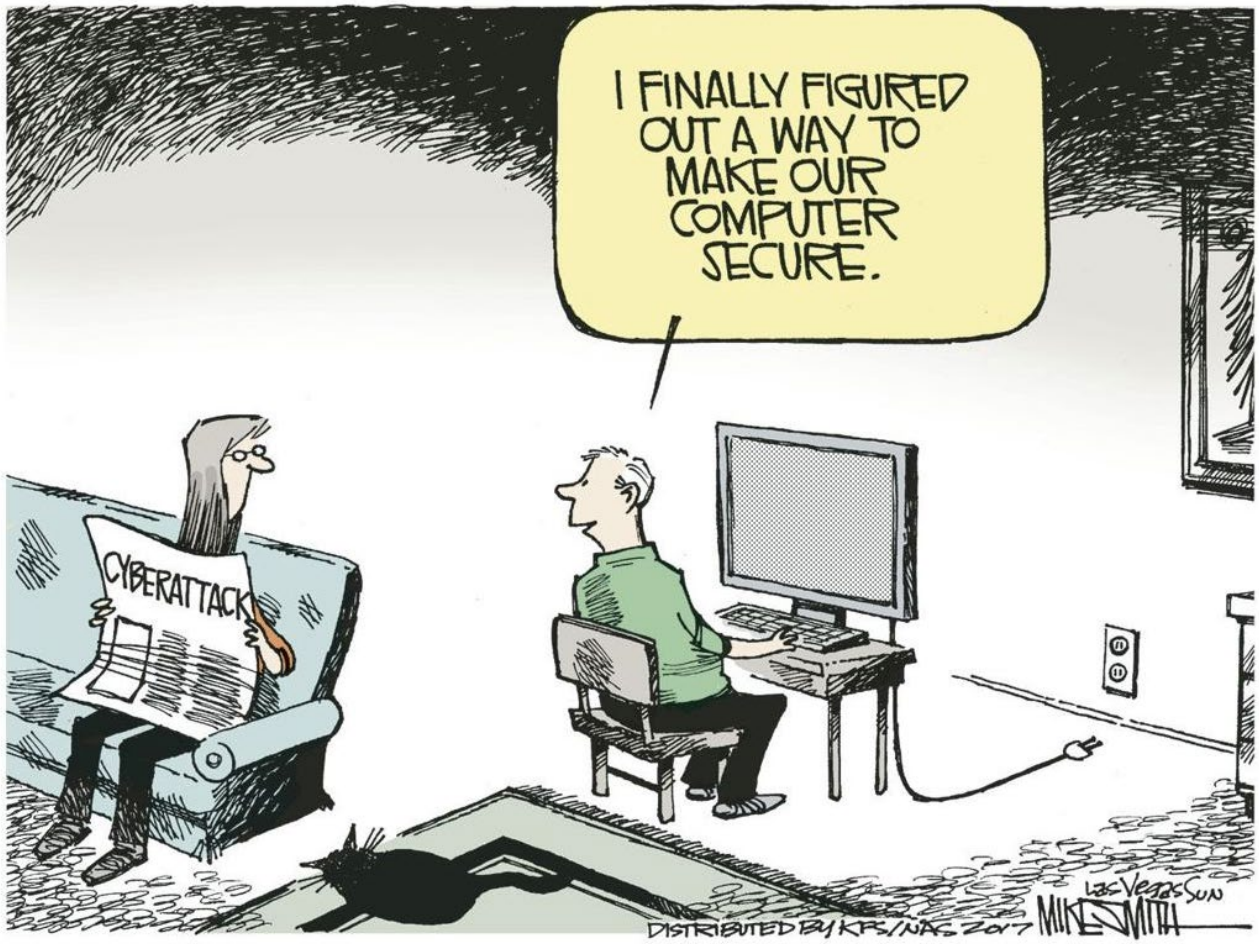
1. La gestion des risques de cybersécurité

2. Les problématiques de gouvernance de la cybersécurité

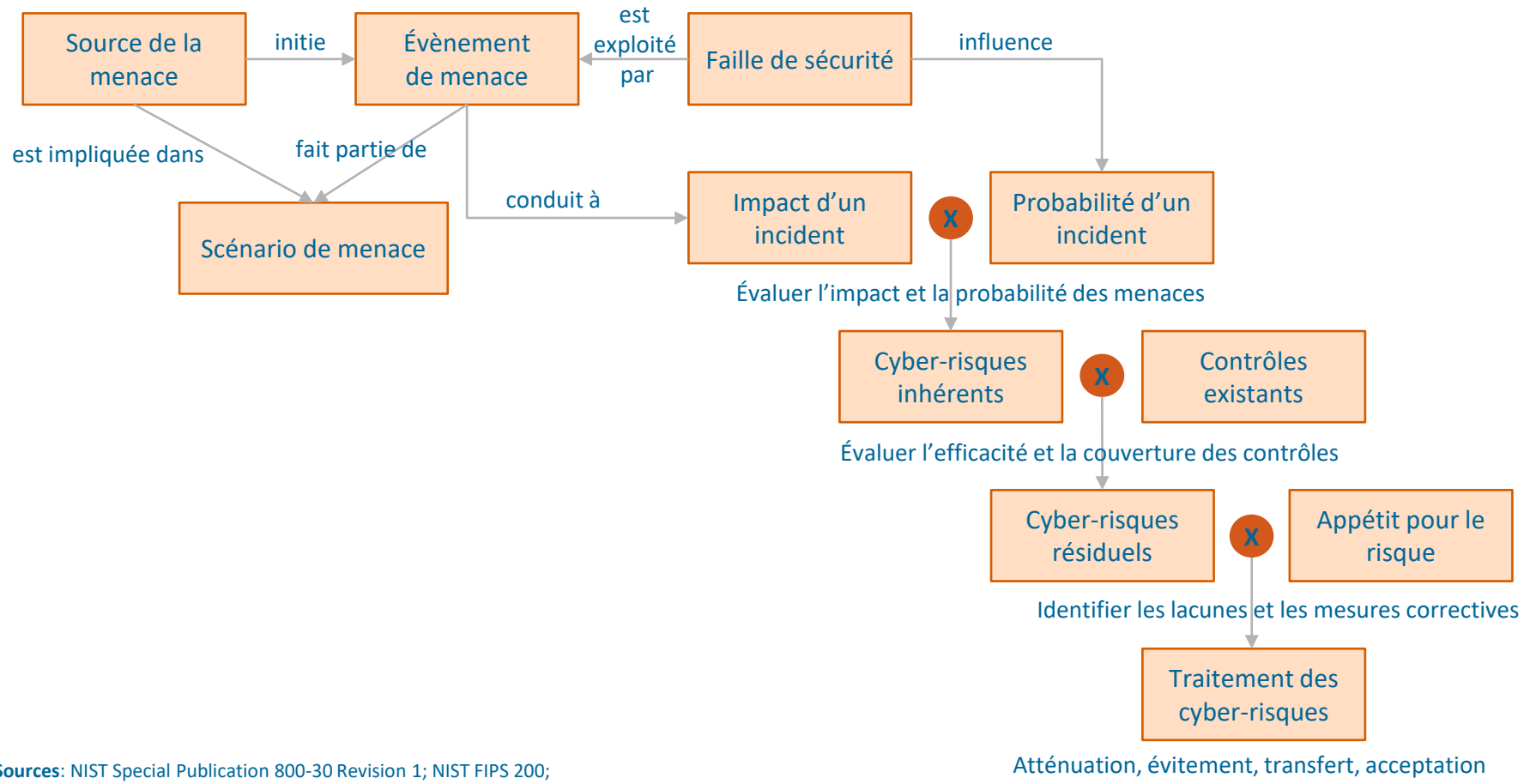
3. Les risques de cybersécurité liés aux nouvelles technologies
   - Cloud, intelligence artificielle, chaine de blocs

4. Le retour sur investissement de la cybersécurité
   - « Est-ce que l'on dépense trop, ou trop peu ? »

Comment éviter les incidents de cybersécurité

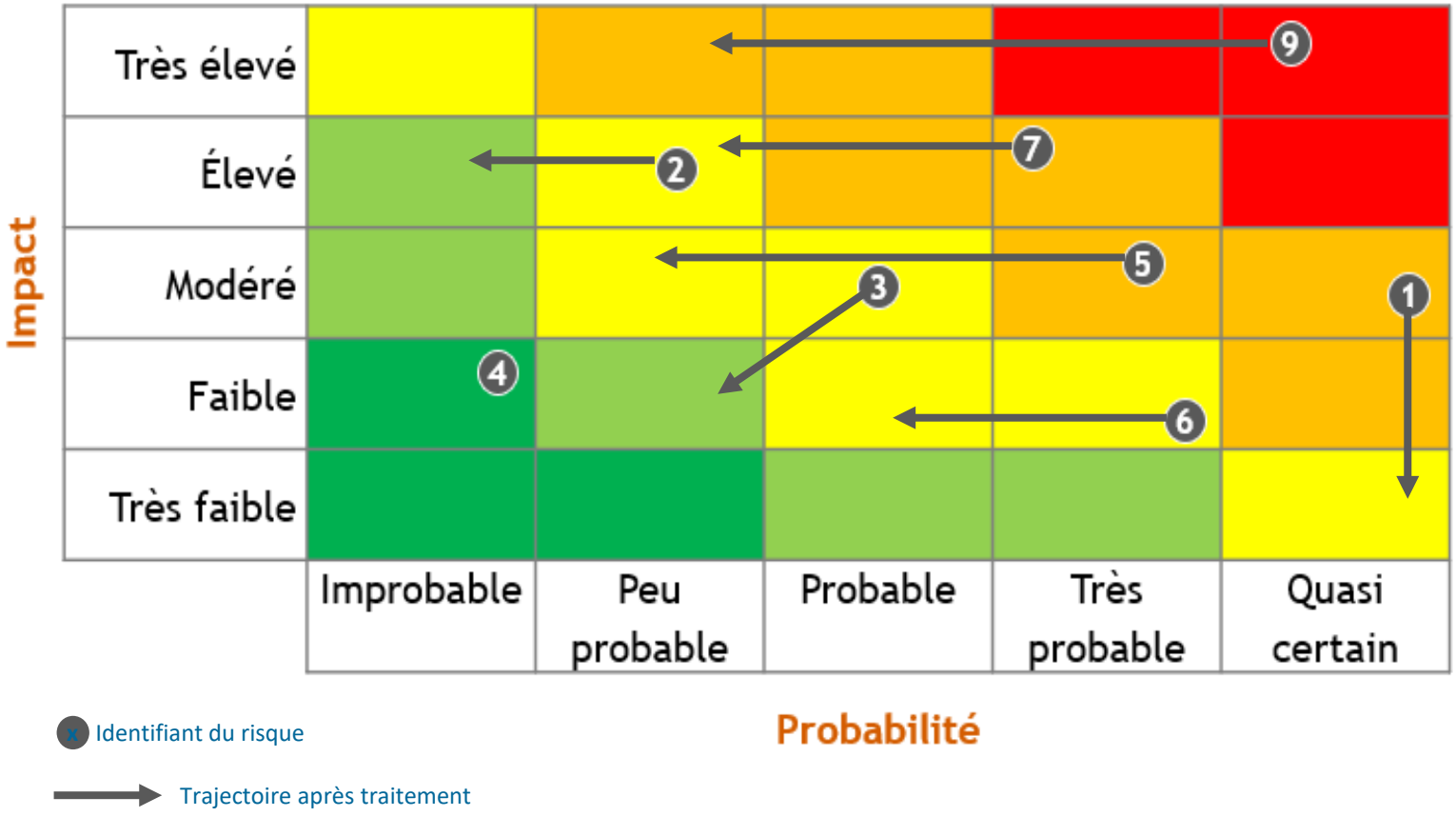


La gestion des risques de cybersécurité



Sources: NIST Special Publication 800-30 Revision 1; NIST FIPS 200;
MITRE Enhanced Cyber Threat Model for Financial Services Sector (FSS) Institutions

Visualisation du portefeuille de risques de cybersécurité

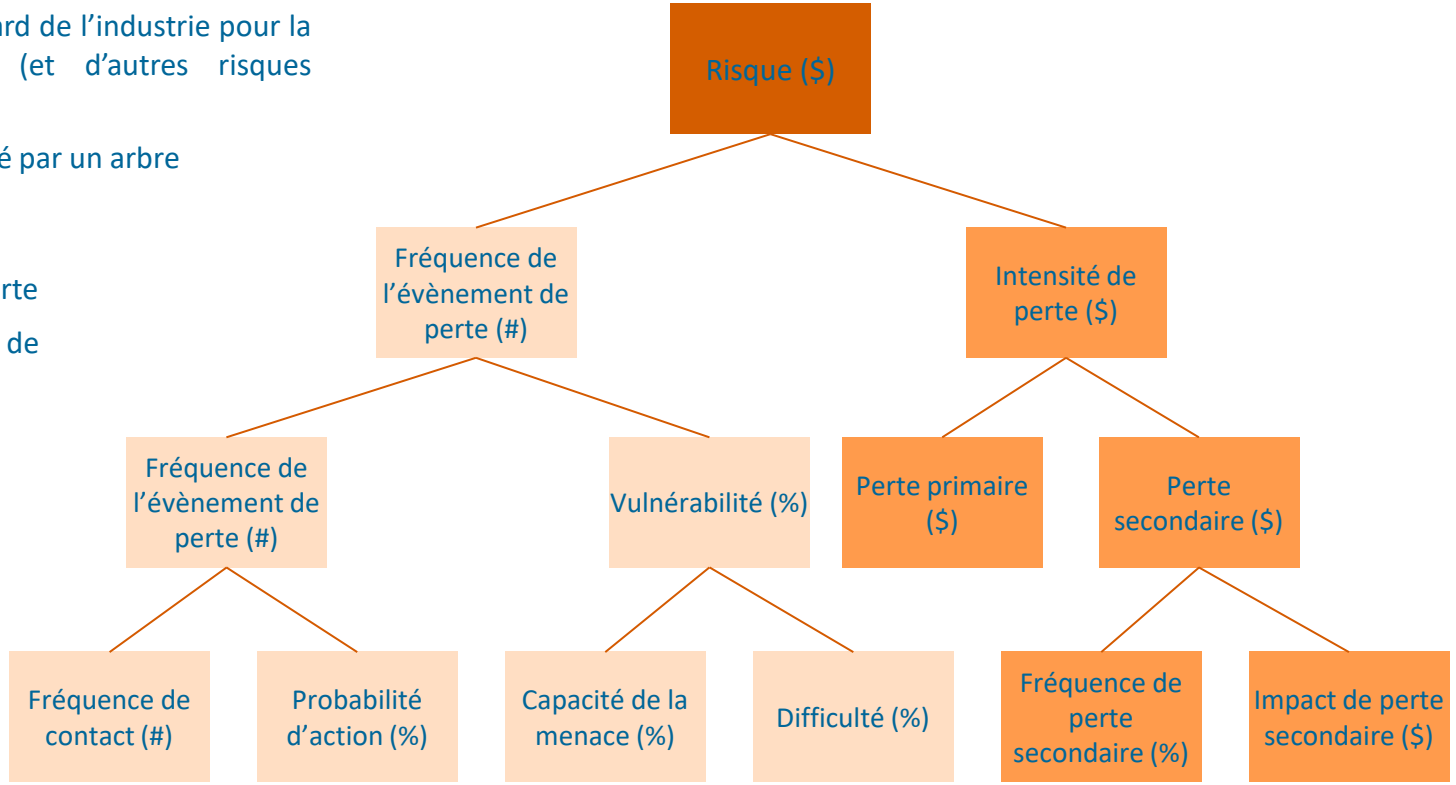


La quantification du risque de cybersécurité

La méthodologie FAIR est un standard de l'industrie pour la quantification du cyber risque (et d'autres risques opérationnels).

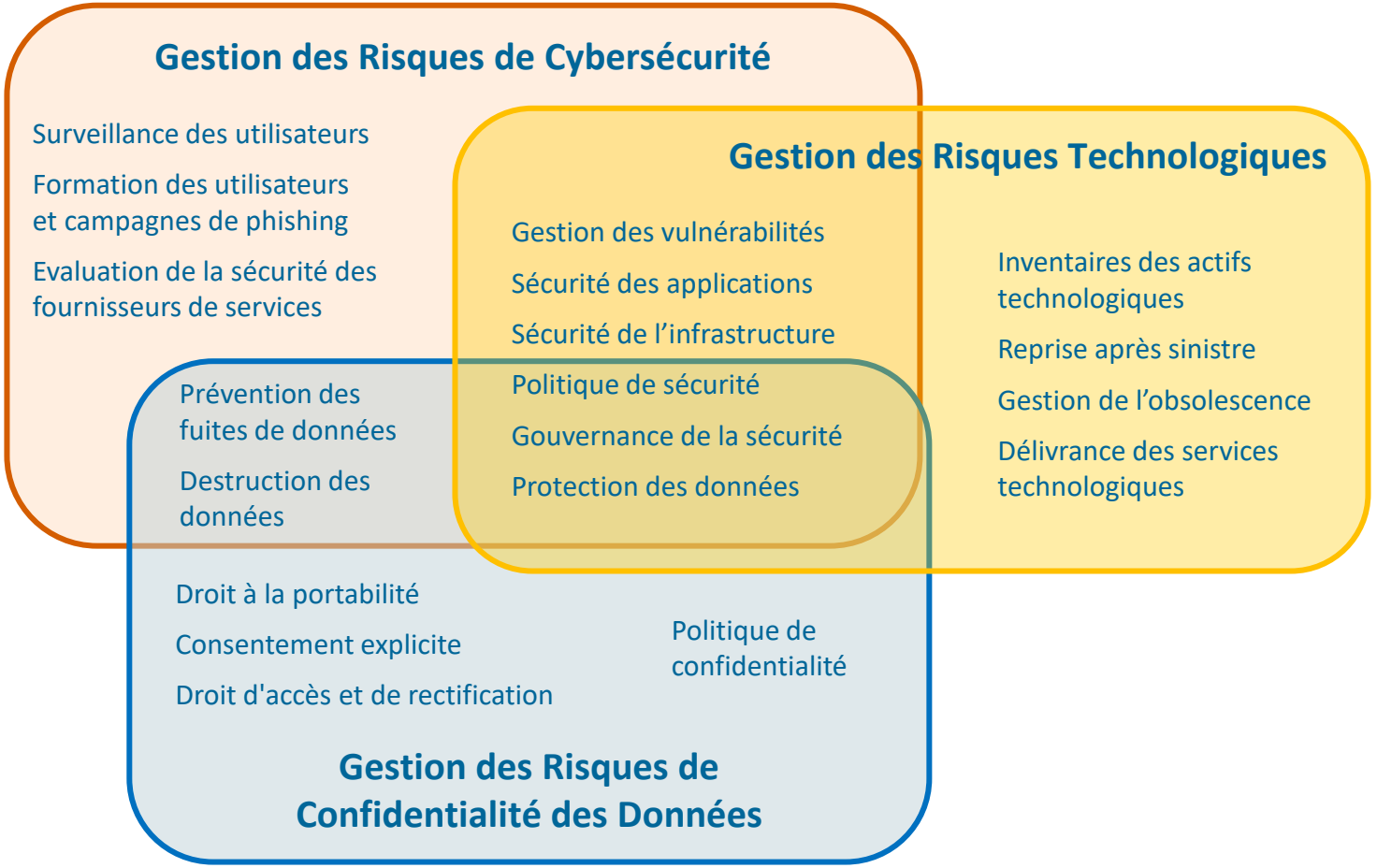
Le modèle FAIR peut être représenté par un arbre décomposable en 2 sous-arbres:

- La partie gauche traite de la probabilité de l'évènement de perte
- La partie droite traite de l'impact de l'évènement de perte



Source: FAIR Institute https://www.fairinstitute.org/

Recouvrement des périmètres de responsabilité



La difficulté du rôle de RSSI

Les RSSI tendent à perdre les leviers pour mener leur rôle à bien. Cela est dû à 4 facteurs:

1. Création de nouveaux **rôles fonctionnels** (tels que CDO, CPO, etc.)
2. **Réglementation** en matière de cybersécurité
3. Multiplication des **audits, revues et examens**
4. **Injonctions paradoxales**

La cybersécurité à travers les 3 lignes de défense

Première ligne

- Établir une politique et des procédures de gestion des risques cyber de 1ère ligne
- Evaluer les risques de cybersécurité (processus annuel)
- Définir et mettre à jour les processus de contrôle des risques de cybersécurité
- Tenir à jour l'inventaires des risques liés à la cybersécurité
- Effectuer une surveillance des risques de cybersécurité
- Communiquer des indicateurs liés aux risques de cybersécurité

Deuxième ligne

Département Risque

- Établir une politique et des procédures de gestion des risques cyber de 2ème ligne
- Challenger l'évaluation des risques de cybersécurité effectuée par la 1ère ligne
- Recommander à la 1ère ligne des méthodologies de calcul et d'agrégation des risques
- Établir des protocoles de gestion des exceptions aux politiques de risque cyber
- Communiquer des indicateurs liés aux exceptions aux politiques de risque cyber

Conformité

- Conseiller la 1ère ligne sur des sujets réglementaires liés à la cybersécurité

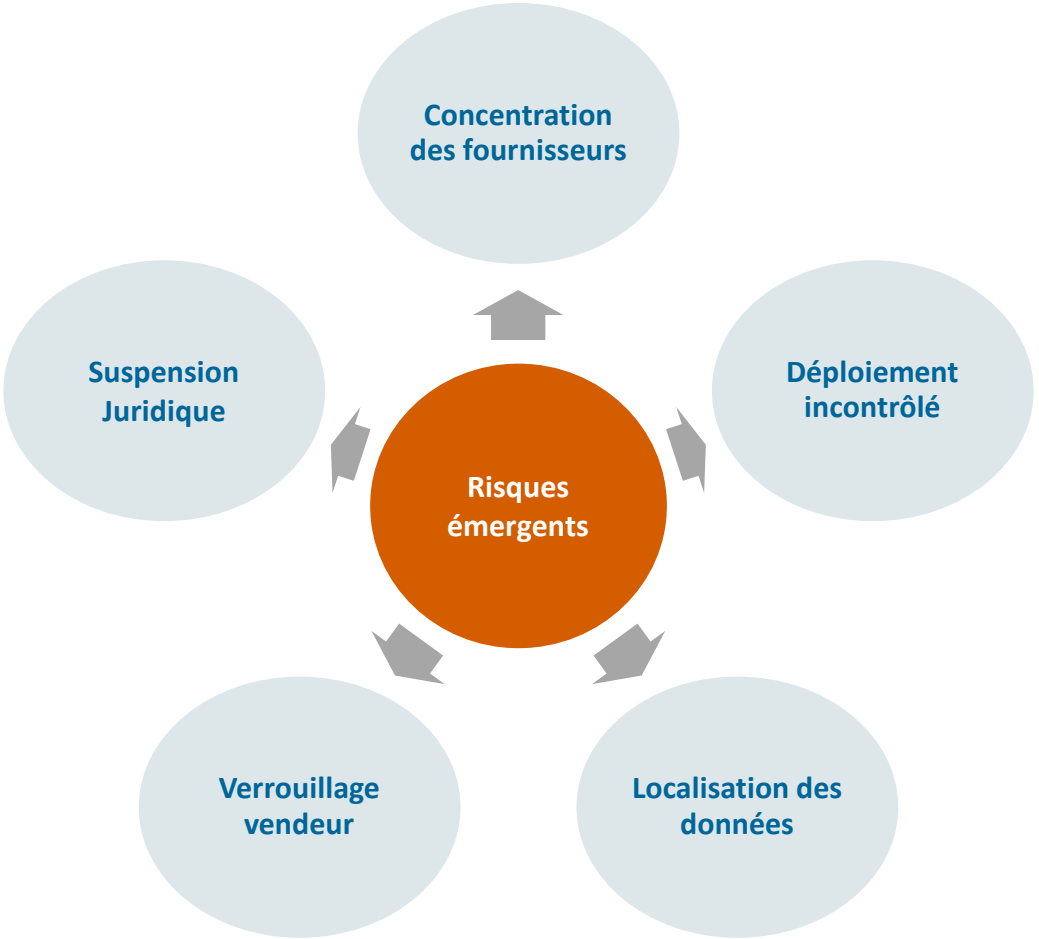
Troisième ligne

- Évaluer la pertinence et la conformité des politiques, procédures et contrôles de gestion des risques de cybersécurité de la 1ère et 2ème ligne
- Évalue l'efficacité globale de la gestion des risque de cybersécurité

Quelques recommandations

- Clarifier le **rôle de chaque ligne** de défense
- Revoir la gouvernance de la cybersécurité et ses **processus de décision**
  - Structure des comités
  - Acceptation des risques et gestion des exceptions
- Définir un **RACI de haut niveau** entre tous les acteurs, ainsi que des RACI détaillés pour les processus de cybersécurité transversaux tels que :
  - Gestion des vulnérabilités
  - Gestion des incidents de cybersécurité
  - Sécurité des applications
  - Sécurité du réseau
  - Protection des données

Les risques liés aux services infonuagiques

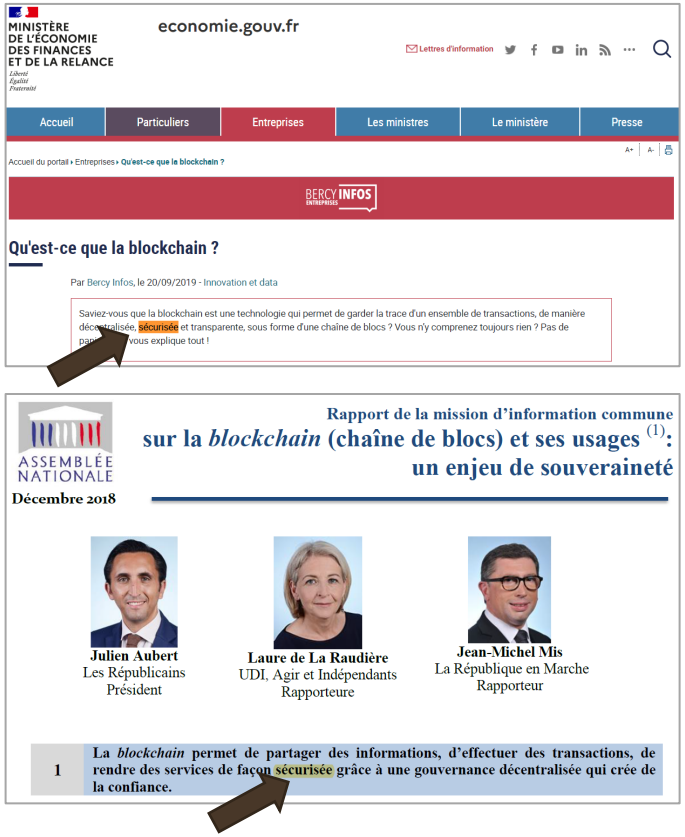


Les risques liés aux algorithmes d'apprentissage machine et d'intelligence artificielle

Risque	Contrôle	Taxonomie de l'évènement
Sélection d'hyperparamètres	Identifier les meilleurs hyperparamètres pour maximiser les performances tout en gardant le modèle simple	Un modèle complexe est plus susceptible d'être instable et de présenter des vulnérabilités supplémentaires aux attaques cyber
Ingénierie des facteurs	Vérifier la signification affaire des facteurs en tant que clusters de variables et d'observations	Une impasse d'interprétation ou une précision déficiente qui interviennent post-modélisation empêchent un traitement ciblé et efficace. Le risque cyber est accentué par le manque de clarté
Nouveauté des données	Identifier si les données changent	Un modèle ne fonctionnera pas bien sur les données non représentatives (avec des distributions différentes et des variables latentes). Les domaines d'application où les données changent en continue constituent des points d'entrées aux attaques cyber.
Dégradation du modèle	Identifier quand le modèle prédit moins précisément	Un modèle commence à sous-performer en perdant généralement de la précision (fonction de perte accrue). Ceci peut être la manifestation d'une attaque cyber.
Interprétation des prédictions	Déterminer si les nouvelles tendances ont une incidence sur le modèle	Un modèle sous-performe si les prédictions ne peuvent pas être interprétées de façon cohérente et constante.
Détection des biais éthiques	Identifier lorsqu'un biais est présent dans le modèle ou définir les contraintes ex ante au cœur du modèle	La présence de partialité peut entraîner de graves problèmes de réglementation et d'éthique. Ceci peut être la cible d'attaques cyber.

Les risques liés aux chaines de blocs

Le mythe

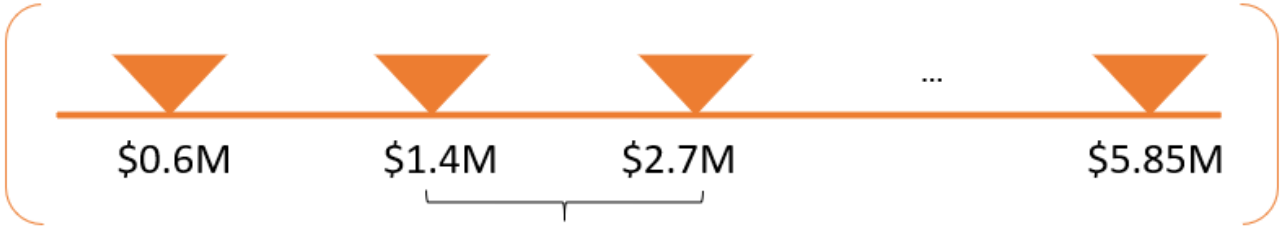


La réalité

Les blockchains sont piratées régulièrement. Ce ne sont ni des passoires ni des solutions miracles en matière de cybersécurité. **Il faut les considérer dans leur écosystème** et leur appliquer des méthodologies de sécurité classiques comme les standards du NIST, le FFIEC CAT ou l'ISO 27001:

- Le **code des « contrats intelligents »** doit faire l'objet de revues de sécurité minutieuses
- Les **utilisateurs** doivent être formés à la sécurité
- Les **clients physiques** (ordinateur personnel, smartphone) doivent être protégés par mot de passe, chiffrement du disque dur, antivirus, VPN, pare-feu logiciel et système de sauvegarde
- Les **clients logiciels** doivent être mis à jour régulièrement et utiliser une authentification multi-facteurs
- Les **connections internet** doivent être sécurisées (mot de passe réseau, configuration du navigateur, pare-feu physique, etc.)

Couts moyens des incidents de cybersécurité



Mean cost of all cyber incidents in Financial Services (**Hiscox / Forrester, 2019**)

5,400 respondents, firms of all sizes from 7 countries

Average financial impact of a data breach (**Kaspersky IT Security Economics 2019**), depending on type of incident

4,958 interviews, 355 firms of all sizes from 23 countries

Average total cost of a data breach in the Financial Industry, including loss of business (**IBM / Ponemon, 2020**)

3,200 interviews, 524 firms of all sizes from 17 countries

Quelques chiffres « connus »

Couts des incidents

Company	Year of Incident	Cost (USD)
Capital One	2019	Between 100 and 150 million
Desjardins	2019	108 million
Postbank	2019	58 million
EQUIFAX	2017	1.4 billion
BANGLADESH BANK Central Bank of Bangladesh	2016	81 million stolen through transfer

Amendes (OCC & NY DFS)

Company	Year of fine	Cost (USD)
RMS Residential Mortgage Services	2021	1.5 million
national a B. Riley Financial company	2021	3 million
Capital One	2020	80 million
citi	2020	400 million
Morgan Stanley	2020	60 million
USAA	2020	85 million

Coût interne de la cybersécurité

Average % of IT spend on security for financial institutions (**Gartner IT Key Metrics Data 2019**)	Cyber spend as a percentage of IT spend for large financial institutions (**FS-ISAC/Deloitte Cyber Risk Services CISO Survey 2019**)	Mean percentage of company's total IT budget represented by IT security (**2019 State of the CIO by CIO.com**)	Share of IT security in overall IT budget (**Kaspersky IT Security Economics 2020**)
	97 respondents	683 IT executives	5,266 interviews, firms of all sizes from 31 countries

Deux autres métriques utilisées:

- **Le cout moyen par employé**
  - **$2,162** par Gartner
  - **$2,700** par FS-ISAC/Deloitte
- **Le cout en % des revenus**
  - **0.56%** par Gartner
  - **0.4%** par FS-ISAC/Deloitte
  - **0.16%** par Protiviti

Company	Year	Cybersecurity Budget (USD)	Metric
BANK OF AMERICA	2018	660 to 680 million[13]	~$3,284 per employee
J.P.Morgan	2018	~600 million[14]	~$2,344 per employee[14]

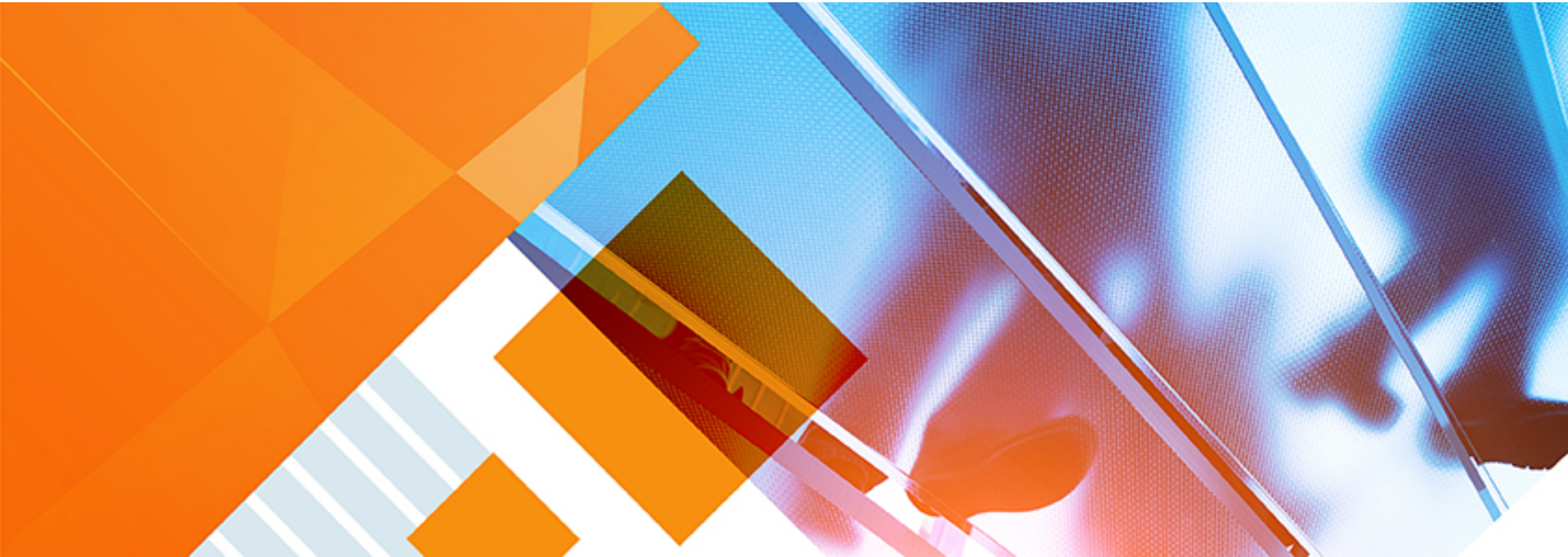
A retenir

- La cybersécurité, c'est avant tout de la gestion des risques
- L'écosystème technologique est en évolution constante, les risques de cybersécurité également
- Une bonne gouvernance de la cybersécurité est un facteur clef de réussite
- Un incident peut couter très cher. Le retour sur investissement de la cybersécurité se mesure en réduction du risque (et libération du capital de risque associé)

Stephane Schatteman

Responsable du pôle Robustesse et Cyber Résilience au sein du Service Résilience et Études des Infrastructures de Marché

En charge du Groupe de Place Robustesse - Banque de France, Paris



1. Le dispositif de gestion de crise nationale (le Groupe de Place Robustesse)

2. La préparation de la Place, s'exercer pour faire face aux impacts d'une crise Cyber

3. Retour sur les derniers exercices de Place

PREAMBULE

Le dispositif de gestion de crise nationale (le Groupe de Place Robustesse)

Le dispositif de gestion de crise nationale , le Groupe de Place Robustesse (GPR)

Depuis 2005 Le GPR, présidé et piloté par la Banque de France, a pour objectif de **contribuer à renforcer et garantir la stabilité financière de la Place de Paris** en la rendant plus robuste, plus résiliente, pour lui permettre d'affronter un choc ou une **crise opérationnelle majeure** dont l'origine serait exogène au système financier mais qui pourraient entraîner **des impacts systémiques**

L'origine de ces crises peut être diverse, voire conjuguée :

- Attaque terroriste
- Catastrophe naturelle
- Mouvement social majeur
- Pandémie
- Défaillance d'un prestataire critique
- Cyber attaque

Avec des effets pluridimensionnels sur :

- L'opérationnel, liés aux ressources humaines et aux sites physiques
- Les systèmes d'information
- Les activités financières critiques (gestion de liquidité, opérations de paiements, refinancement, etc.)

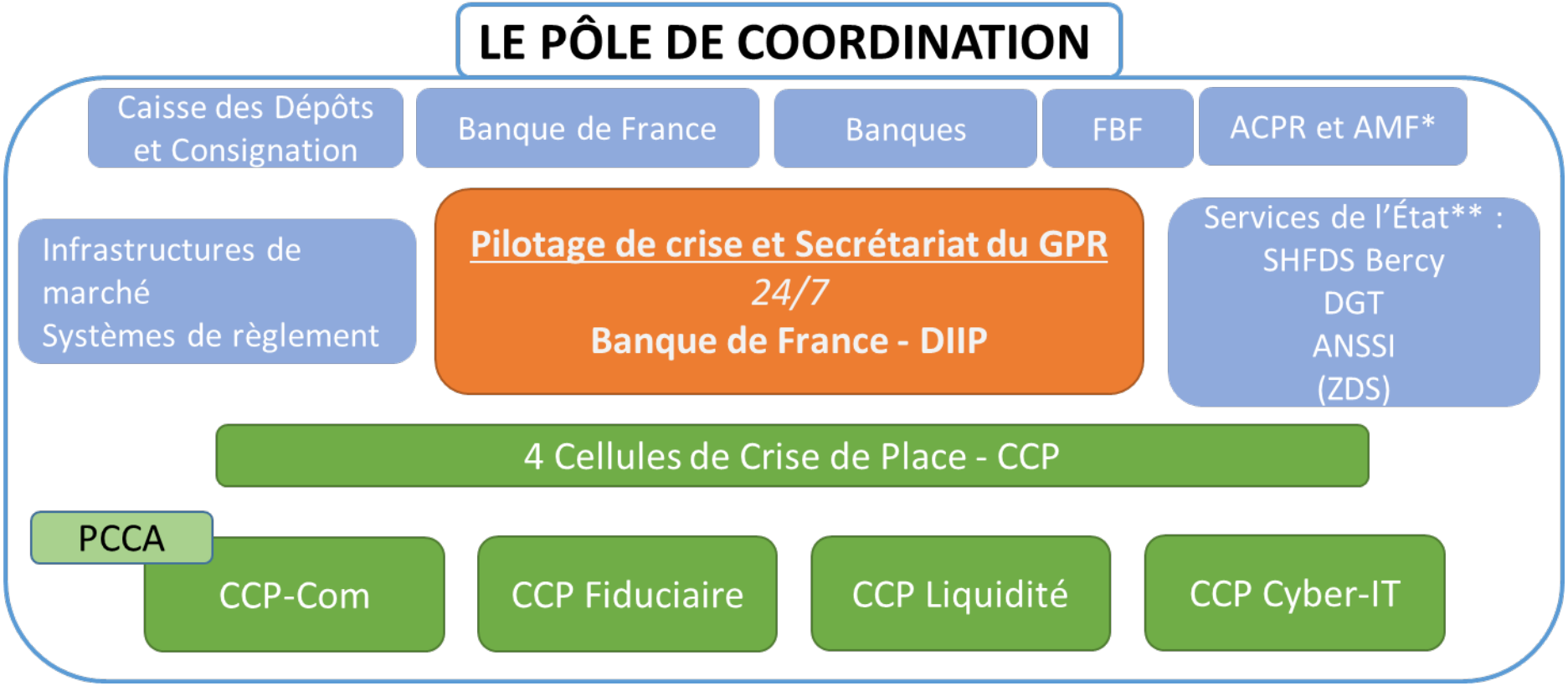
Le dispositif de gestion de crise nationale , le Groupe de Place Robustesse (GPR), une action en trois temps

Avant la crise

En crise

Après la crise

Le dispositif de gestion de crise nationale , le Groupe de Place Robustesse (GPR), la mobilisation en cas de crise



La préparation de la Place, s’exercer pour faire face aux impacts d’une crise Cyber

La préparation de la Place, s'exercer pour faire face aux impacts d'une crise Cyber, l'exercice annuel du GPR

Un **cadre général** qui doit permettre :

- **D'activer le Pôle de Coordination et les quatre cellules de crise de Place**
- **D'éprouver la capacité de la Place à maintenir ses processus critiques**
- **De renforcer la capacité de coordination du secteur financier**
- **D'exercer la communication interne et externe**

Une **stratégie Triennale** qui fixe des axes prioritaires

Un **trigger de crise** parmi les contextes de mobilisation du GPR

avec l'objectif de jouer à 2 niveau, individuel et collectif

A quoi sert, concrètement, un exercice ?
À s'exercer évidemment ! Mais à s'exercer à quoi ?

Au niveau des Entités

Au niveau du GPR, des Cellules de Crise de Place (CCP)

Comment parvenir à ce résultat?

Par une préparation très lourde du scénario

Par une préparation, réelle, des joueurs

Car il ne s'agit pas de piéger les joueurs, les équipes ou les entités face à une situation extrême décrite par notre scénario, non, il s'agit de progresser ensemble !

Malgré tout, ne jamais oublier Les limites d'un exercice…

Tirer des enseignements de ce moment, de cet effort, individuel et collectif

Un exercice, qui se déroule sans accrocs… est un exercice qui a manqué sa cible

Tous les participants (jusqu'aux animateurs) doivent pouvoir tirer enseignements de ces exercices!

Un exercice c'est l'occasion, à chaud, puis à froid de :

- Déceler, nos forces, nos faiblesses, nos manques
- De valoriser et de partager nos bonnes pratiques
- De consolider notre relationnel
- De faire émerger des pistes de travail, des préconisations,
- En bref, de se poser des questions et de construire nos réponses, nos plans d'actions…

Que nous éprouverons… lors de l'exercice suivant

Et tout cela sans juger

Retour sur les derniers exercices de Place

Retour sur les derniers exercices, l'évolution depuis 2019

En 2019, le premier exercice G7 lié au Cyber Expert Group G7 a été organisé et joué par le GPR : un véritable changement de dimension…

Un scénario exceptionnel…

des enseignements

15 juin 2021, premier exercice de la stratégie 2021-2023

Le contexte

Participation et sollicitations

Le scénario général

15 juin 2021, premier exercice de la stratégie 2021-2023

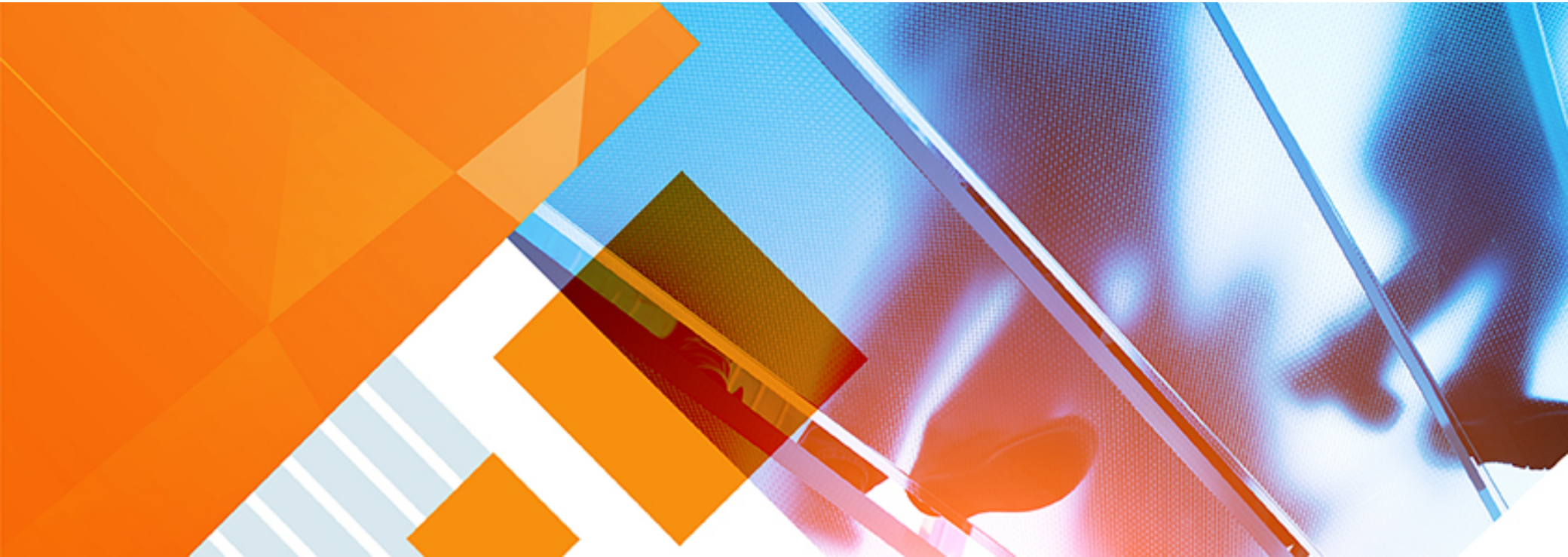
Les évènements Cyber/IT	Les impacts métiers projetés	scénario
Attaques DDOS, massives et répétées	Paralysie des sites, impact public et retail	R
Anomalies sur les limites des opérations de marché	Incertitude sur les outils utilisés par les opérateurs	ML
Effets de la *Supply chain attack* contre les usines de paiement de 3 établissements	Émission massive de virements non justifiés et non référencés dans le SI de l'établissement	R
	Blocage des flux, entrée / sortie des usines de paiement	R
Effets de la *Supply chain attack* contre les logiciels de gestion de flux	Nombreuses tentatives erronées de pré-matching sur produits OTC (swap de taux, de devises), défauts de règlements à des contreparties (actés dans votre SI)	ML
	Interruption de la capacité nominale d'émission de message SWIFT (marché et liquidité)	ML
Tentative de destruction des bases de données liées – destruction des Index des Bases Usines de Paiement / liquidités, marchés	Interruption de la capacité nominale prolongée et mode secours en temps long	MLR
Qualification de la supply chain attack usine de paiement / liquidité marchés	Préparation du retour à la normale (sous 48h a minima) mode secours long confirmé	MLR
Révélation par les attaquant de la réussite de leurs actions	Impacts d'image, marchés, clientèle	MLR

En conclusion…

Pas de conclusion… mais…

Frédéric Rogé

Expert en gestion et négociation de crise – Incertis, Nantes



1. Une organisation humaine qui en rançonne une autre
    - Une menace en augmentation
    - Un cap passé dans les attaques

2. Une volonté d'affaiblir l'organisation visée
    - La recherche de vulnérabilité par l'humain
    - Fishing et biais cognitifs
    - La compromission interne
    - Axes d'améliorations

3. La crise cyber : un test de résilience
    - Une réponse à la menace parfois sous-estimée
    - Les mécanismes de pression et l'incertitude
    - Une crise de leadership et de communication

CONCLUSION

Stéphanie Saint Pé

Déléguée Générale – AFTI, Paris