JOURNÉE DU CLUB ERM

Paris

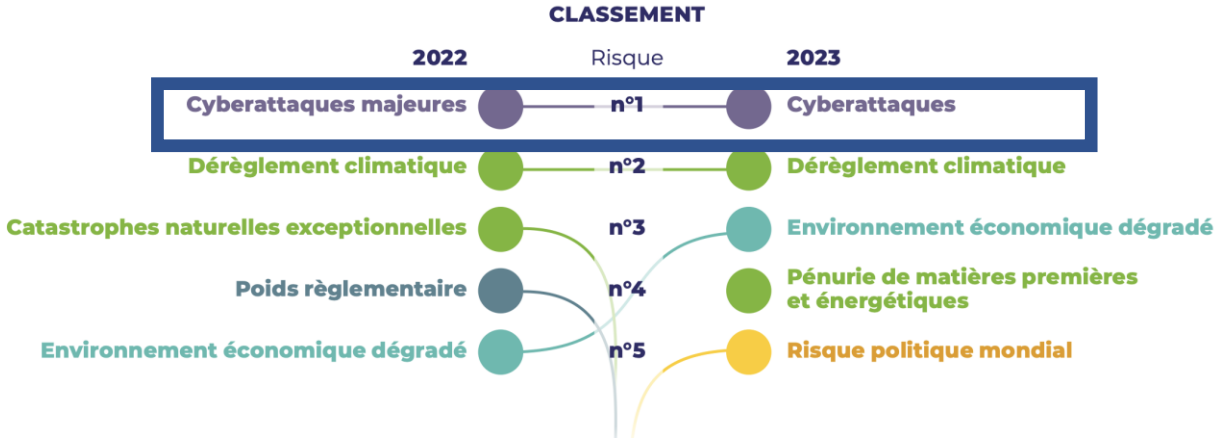
Le 20/06/2024

Risque de Digitalisation

SOMMAIRE

PERCEPTION ET RÉALISATION DU RISQUE CYBER

Le risque **Cyber** est en 1ère position du classement des risques à l'horizon 5 ans de France Assureur en 2023



Une préoccupation croissante des Conseils d'Administration car :

- la menace augmente,
- les dispositifs de prévention, de protection et de réponse représentent des investissements très importants (minimum 5% du budget de la DSI dans l'idéal selon le CIGREF),
- Risque avéré dans le secteur de l'Assurance : plusieurs compagnies d'assurance françaises ont été victimes d'attaque en ransomware,
- DORA entre en application le 17/01/2025.

UNE APPROCHE ÉMERGENTE DU RISQUE DE CYBER RÉSILIENCE

L'approche du risque de cyber résilience reste très succincte dans les rapports de Solvabilité en 2023

Communication vers le Régulateur
Rapport ORSA

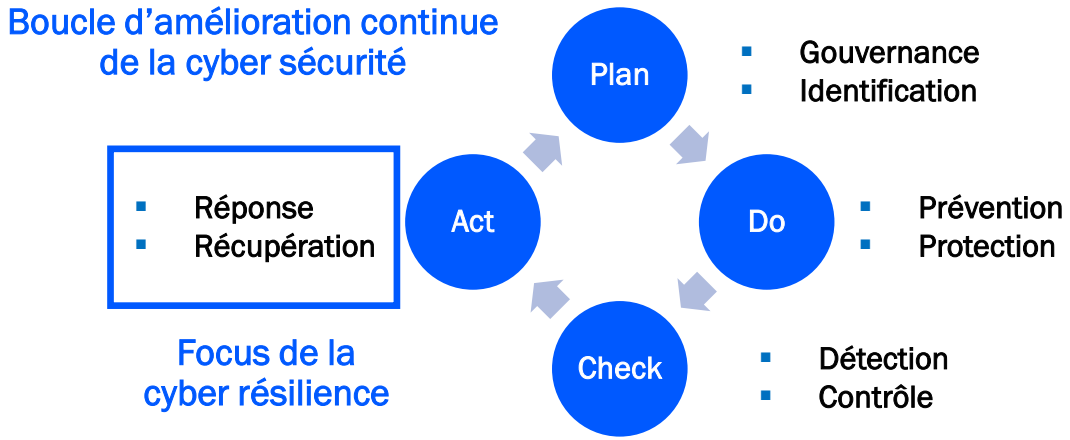
Communication vers le Public
Rapport SFCR

La documentation du risque de cyber résilience et les études d'impact de scénarios de crise doivent se renforcer pour refléter répondre aux exigences croissantes des régulateurs notamment dans le cadre de DORA

CYBER SÉCURITÉ VS CYBER RÉSILIENCE

Définition de la cyber sécurité :

- Technologies, Processus et Contrôles permettant de lutter contre la cybercriminalité
- Sous section de la sécurité de l'information



Définition de la cyber résilience :

- Discipline englobant la cyber sécurité, la gestion de la continuité d'activité et la gestion de crise
- Centrée sur l'objectif d'assurer la survie d'une entreprise suite à une attaque

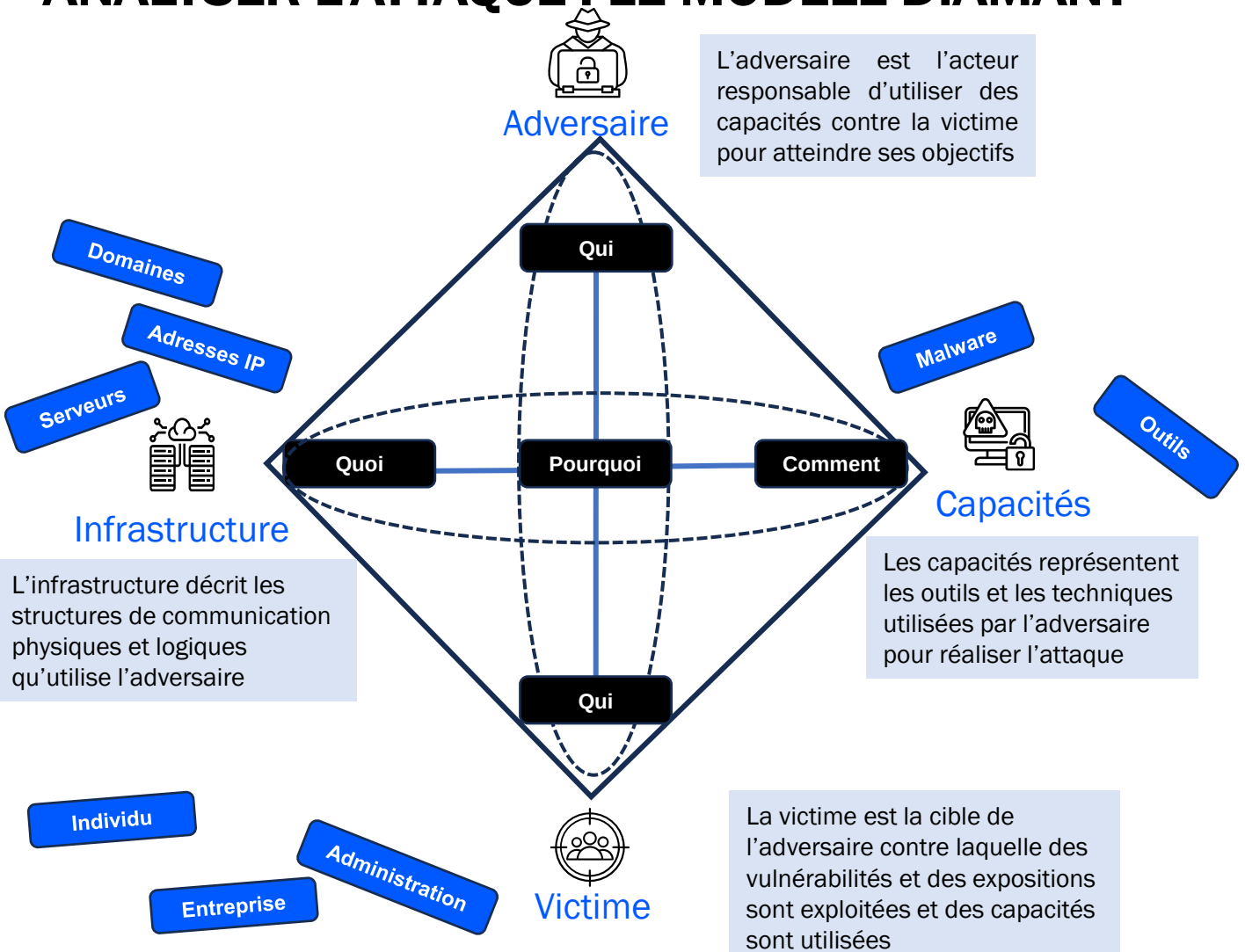
ANALYSER L'ÉTAT DE LA MENACE

Sources de risque	Objectifs visés
Les acteurs de l'Etat Nation lancent des attaques ciblées pour voler des données sensibles à des entreprises privées ou des gouvernements en vue de gagner un avantage économique, politique ou militaire.	Etat Nation — Géopolitique
Les cyber criminels cherchent à obtenir des gains financiers en se livrant à différents types d'activités illicites telles que le phishing, l'usurpation d'identité, les attaques en ransomware et d'autres types d'activités frauduleuses	Cybercriminels — Financier
Les activistes on des motivations sociales ou politiques qui utilisent leur compétences digitales pour mener des actions visant à sensibiliser le public et a protester contre ce qu'ils perçoivent comme des injustices	Hacktiviste — Politique ou social
Les groupes terroristes utilisent différentes techniques telles que le hacking ou le sabotage pour répandre la peur, accéder à données sensibles et diffuser leur idéologie par des actions de propagande	Terroriste — Idéologique

Institut des ACTUAIRES

2. Techniques d'analyse de la menace

ANALYSER L'ATTAQUE : LE MODÈLE DIAMANT



L'adversaire est l'acteur responsable d'utiliser des capacités contre la victime pour atteindre ses objectifs

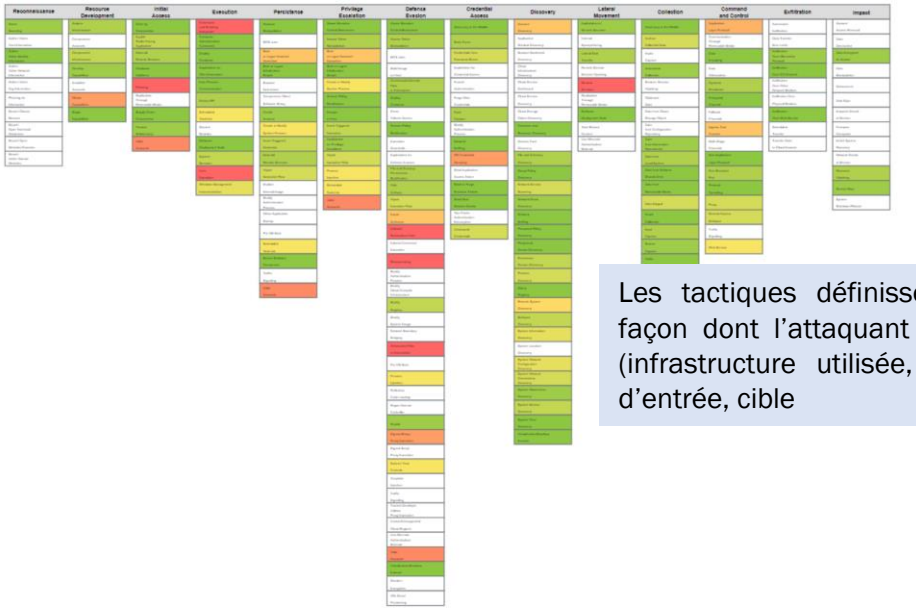
L'infrastructure décrit les structures de communication physiques et logiques qu'utilise l'adversaire

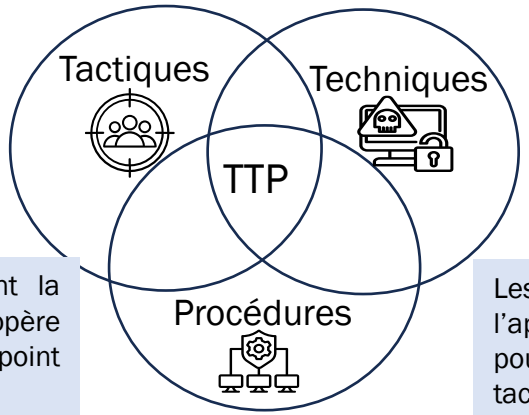
Les capacités représentent les outils et les techniques utilisées par l'adversaire pour réaliser l'attaque

La victime est la cible de l'adversaire contre laquelle des vulnérabilités et des expositions sont exploitées et des capacités sont utilisées

2. Techniques d'analyse de la menace

- MITRE ATT&CK® est base de connaissances accessible à l'échelle mondiale sur les tactiques et techniques des adversaires basée sur des cas réels
- MITRE ATT&CK® « Adversarial Tactics, Techniques and Common Knowledge » documente les Tactiques, les Techniques et les Procédures utilisées par les adversaires
- MITRE ATT&CK® organise les techniques en un ensemble de tactiques pour fournir du contexte à l'analyse. Il peut être utilisé pour profiler les étapes d'une cyberattaque
- Objectifs :
  - Comprendre les méthodes opératoires d'un attaquant
  - Identifier les techniques et les tactiques utilisées
  - Évaluer la couverture défensive de l'entreprise et identifier les gaps
  - Identifier les axes d'amélioration de la maîtrise des risques et définir une stratégie de gestion des risques numériques





Les tactiques définissent la façon dont l'attaquant opère (infrastructure utilisée, point d'entrée, cible

Les techniques représentent l'approche et les outils utilisés pour mettre en œuvre la tactique

Les procédures définissent la séquence d'actions utilisée par l'attaquant pour franchir chaque étape du cycle d'attaque

CYBER KILL CHAIN INSPIRÉE DU MODÈLE LOCKHEED MARTIN

1. **RECONNAISSANCE**
   Collecter des informations sur la cible pour planifier l'attaque
2. **ARMEMENT**
   Créer une charge utile malveillante à utiliser contre la cible.
3. **LIVRAISON**
   Transmettre la charge utile malveillante à la cible.
4. **EXPLOITATION**
   Exploiter une vulnérabilité pour exécuter du code malveillant sur la cible.
5. **INSTALLATION**
   Installer le malware sur le système cible pour maintenir un accès.
6. **COMMANDE ET CONTRÔLE**
   Contrôler le système compromis par un canal de communication
7. **ACTIONS SUR OBJECTIFS**
   Atteindre les objectifs finaux de l'attaque, comme le vol de données

Chaque étape de la kill chain peut être associée à plusieurs tactiques et techniques spécifiques décrites dans le framework MITRE ATT&CK, ce qui permet aux analystes de sécurité de mieux comprendre et de défendre contre les attaques sophistiquées.

PRINCIPES MÉTHODOLOGIQUES DES STRESS TESTS DE CYBER RÉSILIENCE DE L'EIOPA

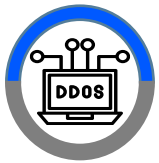
L'EIOPA a publié le 11 juin 2023 ses principes méthodologiques de construction des scénarios de stress tests cyber avec 2 composantes :

- L'application de stress tests à la cyber résilience
- L'application de stress tests à la souscription cyber

5 scénarios retenus pour la cyber résilience :

Perte d'un data center

Ransomware



Attaque en Déni de Service

Exfiltration de données

Perte d'alimentation électrique

Scénario Perte d'un Data Center

Causes

- Catastrophes naturelle ou d'origine humaine (crue, incendie,…)
- Erreur de configuration
- Sabotage

Maîtrise des risques

- Plan de continuité d'activité
- Plan de secours informatique

Impacts

- Indisponibilité prolongée des infrastructures
- Arrêt d'activités métier critiques
- Perte définitive de données et coûts de reconstruction des données

Description du scénario

- Perte de tout ou partie de l'infrastructure (serveurs, applications, bases de données supportant des activités métiers) due à une atteinte physique aux infrastructures (incendie, phénomène climatique, sabotage etc.)
- Possibilité de perte simultanée du site primaire et du site de back-up
- Possibilité de perte définitive de données

Justification et limites du scénario

- Objectif : tester le plan de continuité d'activité informatique de l'entreprise
- Scénario qui s'est déjà produit : cas OVH
- Dans les fait compte-tenu des dispositifs de secours en place (site de back-up et dispositifs de sauvegarde indépendants) le scénario aurait des impacts modérés
- La probabilité que le site principal et le site de back-up soient atteints simultanément est extrêmement faible sauf si les deux sites sont proches
- Les hypothèses sur la perte de données sont complexes à formuler et les impacts de la perte de données sont difficiles à évaluer.

Scénario Attaque en Déni de Service (DDOS)

Causes

- Attaque DDOS : envoi de requêtes multiples sur un site

Maîtrise des risques

- Dispositif de prévention anti-DDOS

Impacts

- Indisponibilité de plusieurs heures des sites web de l'entreprise
- Arrêt des activités en ligne de l'entreprise (Souscription, Gestion de la Relation Clients etc.)

Description du scénario

- Attaque coordonnées contre les principaux acteurs du secteur financier impliquant l'indisponibilité de bases entières de données clients ainsi que des sites d'accès aux services des clients,
- Scénario alternatif : Malware exploitant une vulnérabilité d'un équipement réseau d'un fournisseur majeur de composants réseau comme CISCO
- L'attaque peut ou non toucher directement l'assureur, le choix du scénario doit considérer un évènement extrême

Justification et limites du scénario

- Schéma d'attaque des Hacktivistes pour attirer l'attention et protester contre des situations considérées comme inacceptable
- Scénario plausible notamment en cas d'action de l'entreprise jugée critiquable par des groupes d'opinion
- Exemple attaque DDOS lancée contre des universités au UK pour protester contre le soutien du gouvernement britanique aux actions militaires d'Israël à Gaza

Scénario Ransomware

Causes

- Catastrophes naturelle ou d'origine humaine (crue, incendie,…)
- Erreur de configuration
- Sabotage

Maîtrise des risques

- Dispositif de sécurité (prévention)
- Dispositif de sauvegarde et restauration et de résilience opérationnelle numérique (réponse)

Impacts

- Indisponibilité prolongée des infrastructures
- Arrêt d'activités métier critiques
- Perte définitive de données et coûts de reconstruction des données
- Coûts de rattrapage des tâches non réalisées (perte de jours/personne)

Description du scénario

- Attaque ciblant un employé via phishing ou le data center directement en exploitant une vulnérabilité (par exemple du site web de l'institution,
- Propagation du ransomware et chiffrement des données déclenchant la coupure du SI
- Données chiffrées considérées comme détruites
- Cette attaque peut impliquer la menace de communiquer des informations sensibles telles que des données clients avec un impact RGPD potentiel

Justification et limites du scénario

- Objectifs : tester le dispositif de sauvegarde et restauration et de réponse à incident
- Type d'attaque produisant une indisponibilité prolongée du système d'information (jusqu'à plusieurs semaines)
- Scénario très représentatif de l'évènement redouté extrême pour un assureur

Scénario Exfiltration de données

Causes

- Facteur humain (malveillance/malhonnêteté d'un employé, erreur humaine)
- Attaque cyber

Maîtrise des risques

- Dispositif de lutte contre la fuite de données
- Dispositif de contrôle d'accès

Impacts

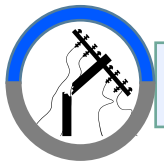
- Coûts de forensic, de récupération et de communication
- Coûts de procédures et d'indemnisation des clients
- Sanction financière
- Atteinte à la réputation : perte de clientèle impact le plus sévère particulièrement en cas d'atteinte aux données de santé

Description du scénario

- Des acteurs malveillants ont infiltré le réseau de l'organisation ou celui d'un prestataire critique et ont réussi à extraire des données sensibles
- Les données peuvent être vendues, rendues publiques, ou être utilisées comme levier pour commettre des actions d'extorsion contre l'organisation et toucher des tiers notamment des clients
- Vol de données personnelles de clients tels que numéros de Sécurité Sociale, coordonnées de carte bancaire utilisables pour commettre des usurpations d'identité et des fraudes

Justification et limites du scénario

- Objectif : les dispositifs de lutte contre la fuite de données
- Scénario relativement plausible et dont les conséquences peuvent être critiques notamment en termes de sanction mais aussi d'impact sur la réputation



Scénario Perte d'alimentation électrique

Causes

- Dommage Physique (Crue…)
- Atteinte aux infrastructures électriques de la part d'un acteur de menace d'origine étatique

Maîtrise des risques

- Dispositif de secours par Groupe Electrogène

Impacts

- Indisponibilité prolongée des infrastructures électriques
- Arrêt d'activités métiers critiques

Description du scénario

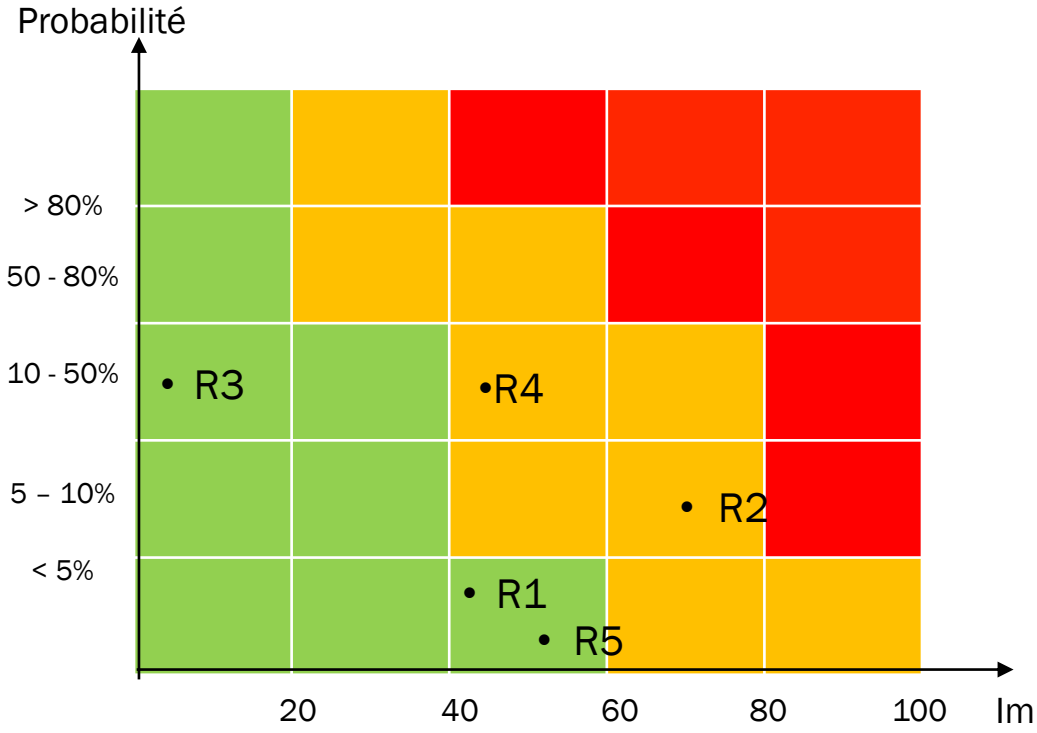
- Coupure de courant durable due à une attaque cyber du prestataire ou à un phénomène climatique
- Interruption d'activité majeure pendant la durée de la panne paralysant, la plupart des processus opérationnels,
- Une fois le courant rétabli, récupération rapide. peu de dommages permanents à l'infrastructure et aux systèmes de TIC attendus

Justification et limites du scénario

- Objectif : tester le dispositif de secours par groupe électrogène
- Deux cas de panne électrique répertoriés récemment l'un dû à une cyber attaque d'un fournisseur d'électricité, l'autre dû à un phénomène climatique,
- En cas de Crue de la Seine ce scénario pourrait se matérialiser avec un impact d'autant plus fort qu'il y aurait des difficultés à acheminer du carburant pour les groupes électrogènes
- Impact dépendant de la durée du phénomène qui devrait être courte
- Impact simultané sur plusieurs sociétés

4. Choix des scénarios à utiliser pour les stress tests

ÉVALUATION QUALITATIVE DE LA PROBABILITÉ ET DE L'IMPACT DES SCÉNARIOS DE STRESS EIOPA



R1 Perte d'un Data Center : scénario de probabilité très faible qui aurait un faible impact en termes d'interruption d'activité avec des coûts de reconstruction d'infrastructure principalement

R2 Ransomware : scénario de probabilité faible (peu d'attaques réussies, mais d'impact potentiel majeur pour le business (plusieurs semaines d'interruption d'activité)

R3 Attaque en Déni de Service : scénario plausible d'impact faible

R4 Exfiltration de données : scénario plausible d'impact élevé notamment de dommage à la réputation en fonction du volume de DCP exfiltrées

R5 Perte d'alimentation électrique : scénario de probabilité faible mais d'impact potentiel élevé selon la durée d'interruption d'activité

Les scénarios R2 et R4 sont sauf cas particuliers les plus adaptés pour les stress tests car ils sont plausibles et peuvent générer des impact très forts. Le scénario de ransomware touchant un prestataire critique est également à considérer

5. Facteurs de risque à prendre en compte

- Tous les métiers ne sont pas équivalents en termes d'exposition au risque cyber
- L'exposition au risque d'exfiltration de données dépend des facteurs suivants :
  - Nombre (ou % sur une population de clients données) de personnes susceptibles d'être concernées par le scénario d'exfiltration de données à caractère personnel
  - Niveau de sensibilité des données (Données de santé, données de paiement…)
- L'exposition au risque d'interruption d'activité dépend des facteurs suivants:
  - Nombre de collaborateurs impacté**s par l'interruption d'activité**
  - **% de collaborateurs dont il faut rattraper la charge de travail (backlog)**
  - Nombre ou % de clients touchés
  - Solutions de contournement
  - Périmètre du chiffre d'affaires en production nouvelle qui serait arrêté
- Les paramètres de durée d'arrêt d'activité dépendent du temps que mettrait la DSI à restaurer les applications critiques impactées dans le scénario central et dans un scénario extrême (exemple 5 et 20 jours ouvrés)

IMPACTS POTENTIELS D'UNE INDISPONIBILITÉ PROLONGÉE DU SYSTÈME D'INFORMATION

1 Perte de Chiffre d'Affaires (affaires nouvelles)

- L'**arrêt du développement commercial** pendant une période prolongée aboutit à une perte d'affaires nouvelles au profit de la concurrence
- Seuls les **distributeurs non reliés au SI** poursuivent leurs activités

2 Augmentation de l'attrition clients

- La **baisse de la qualité de service** liée à l'indisponibilité du SI augmente le risque de résiliation infra-annuelle
- La **compromission directe de DCP Clients** peut entrainer la fuite massive de clients vers la concurrence

3 Indemnisation Clients & pertes dues au non respect de contraintes contractuelles

- Le **non respects de contraintes contractuelles** peut entrainer des pertes directes (exemple contraintes d'exécution de rachats)
- Les clients peuvent exiger l'**indemnisation du préjudice en cas de compromission de données**

4 Sanction pour non respect de contraintes réglementaire

- Le **non respect de contraintes de délais réglementaires** peut entrainer des sanctions,
- La compromission de DCP clients peut entrainer une sanction pour **non respect du RGPD** et défaut de protection des données

5 Coûts de rattrapage (Force de Travail Variable)

- Le **rattrapage des tâches non effectuées** pendant l'interruption d'activité entraine le recours à des ressources externes (consultants, travail temporaire) et / ou à des heures supplémentaires

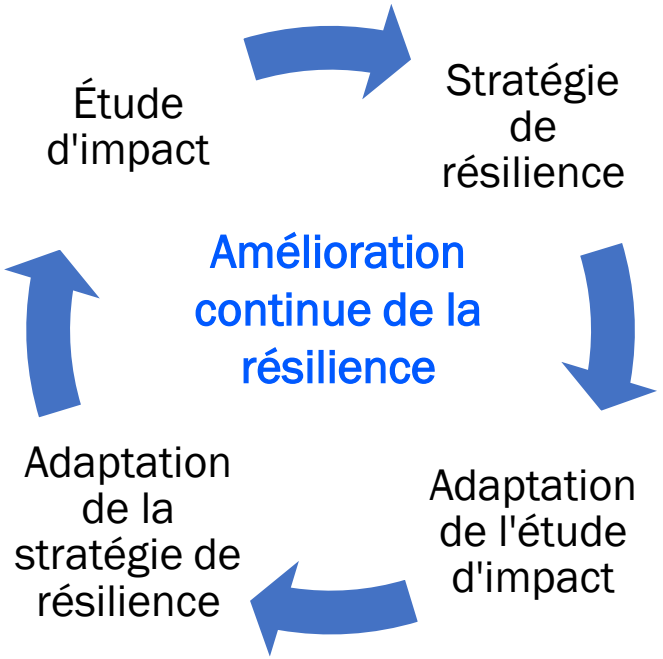
6 Coûts de communication et de rétablissement

- Pour minimiser l'impact d'une crise un dispositif d'**assistance clients et** de **communication** peut être mise en place
- Des coûts de **reprise et de restauration des données**, voire de reconstruction des réseaux des serveurs et des postes de travail peuvent être engagés

STRATÉGIE DE RÉSILIENCE BASÉE SUR L'ÉTUDE D'IMPACT

L'étude d'impact d'un scénario d'arrêt d'activité prolongé va permettre, en lien avec les métiers, de définir une organisation de crise et une stratégie de cyber résilience « métier » basée sur les piliers suivants :

- Mise en œuvre de solutions de poursuite d'activité sans IT exemples :
  - Procédure de passage d'ordres à la voix
  - Roll automatique des positions de couverture
  - Augmentation des seuils de délégation de gestion de sinistres aux courtiers
  - Orientation des clients sur les partenaires agréés (gestion de sinistres) etc.
- Priorisation de la communication de crise et de la gestion de la relation clients en fonction de leur exposition au risque d'attrition
- Définition du plan de reprise et de restauration en fonction des priorités métiers
- Adaptation de la police d'assurance cyber



RENFORCER L'ACCOMPAGNEMENT DES MÉTIERS DANS L'ÉVALUATION DES RISQUES CYBER

Compte-tenu des enjeux économiques de la lutte contre le risque cyber, la Direction des Risques doit renforcer son accompagnement des métiers dans l'identification et l'évaluation de ce risque pour répondre à des objectifs de :

- Communication sur le risque auprès du public et des régulateurs alignée par rapport aux enjeux
- Partage des enjeux de la maîtrise des risques avec le Conseil d'Administration
- Formation et sensibilisation des métiers à l'élaboration des Plans de Continuité et de Reprise d'Activité dédiés à des crises cyber
- Définition de la stratégie de renforcement de la Sécurité du SI et budget SSI
- Adaptation du transfert de risque à l'assurance