

Bâtir une résilience numérique: le rôle de la cyberassurance

Pascal Clerc | Conférence BIM 2024, SwissTech Convention Center
Lausanne, 14.11.2024



BAUEN DIGITAL SCHWEIZ
BÂTIR DIGITAL SUISSE
COSTRUZIONE DIGITALE SVIZZERA
CONSTRUIR DIGITAL SVIZRA

Home of



Les cyberrisques

Cyberrisques = Hacking

Il s'agit d'attaques en provenance d'**Internet** et de **réseaux comparables** qui visent l'**intégrité**, la **disponibilité** et la **confidentialité** de l'**infrastructure technologique**, notamment en ce qui concerne les **données et systèmes IT critiques et/ou sensibles**.

Source: Cyberrisques et threat intelligence, 2019 FINMA

Les cyberrisques

Cyberrisques = Hacking

Il s'agit d'attaques en provenance d'**Internet** et de **réseaux comparables** qui visent **l'intégrité**, la **disponibilité** et la **confidentialité** de l'**infrastructure technologique**, notamment en ce qui concerne les **données et systèmes IT critiques et/ou sensibles**.

Source: Cyberrisques et threat intelligence, 2019 FINMA

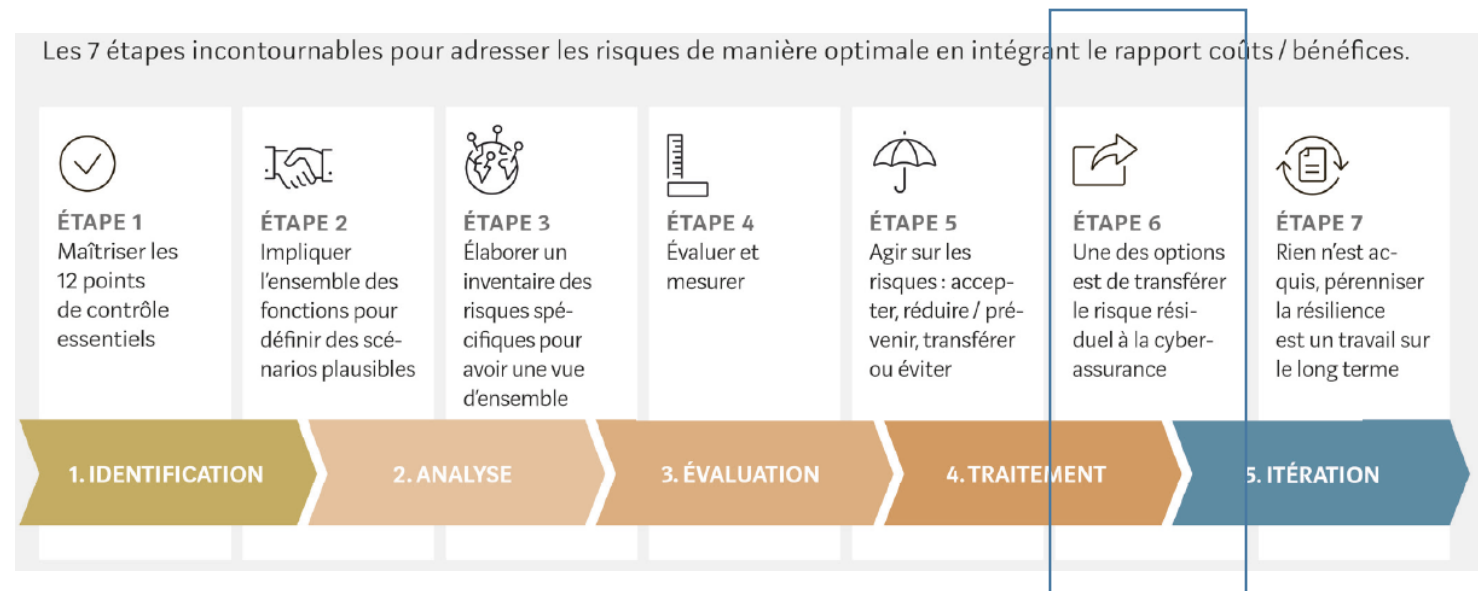
Les risques encourus sont, notamment, **le vol ou la perte de données, les intrusions volontaires ou involontaires sur un réseau, les virus informatiques, les fraudes informatiques, le cyberterrorisme, les erreurs humaines, les interruptions ou la dégradation de services**, ainsi que **les dommages matériels ou immatériels** qui peuvent affecter négativement **la réputation, les activités ou les finances**, par exemple, d'un individu ou d'une entreprise.

Source: https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?ld_Fiche=26543833

Processus de gestion des risques cybernétiques



Cyber resilience is a journey, not a destination.



Processus de gestion des risques cybernétiques



Authentification multifactorielle (MFA) pour l'accès à distance et l'accès des administrateurs privilégiés



Sauvegardes sécurisées, cryptées et testées



Filtrage du courrier électronique et sécurité du web



Détection et réponse des points finaux (EDR)



Gestion des accès privilégiés (PAM)



Remplacement ou protection des systèmes en fin de vie (EOL)



Plans de réponse aux incidents



Sensibilisation à la cybersécurité et tests d'hameçonnage



Protocole de bureau à distance (RDP) et autres techniques de durcissement



Gestion des cyberrisques de la chaîne d'approvisionnement numérique

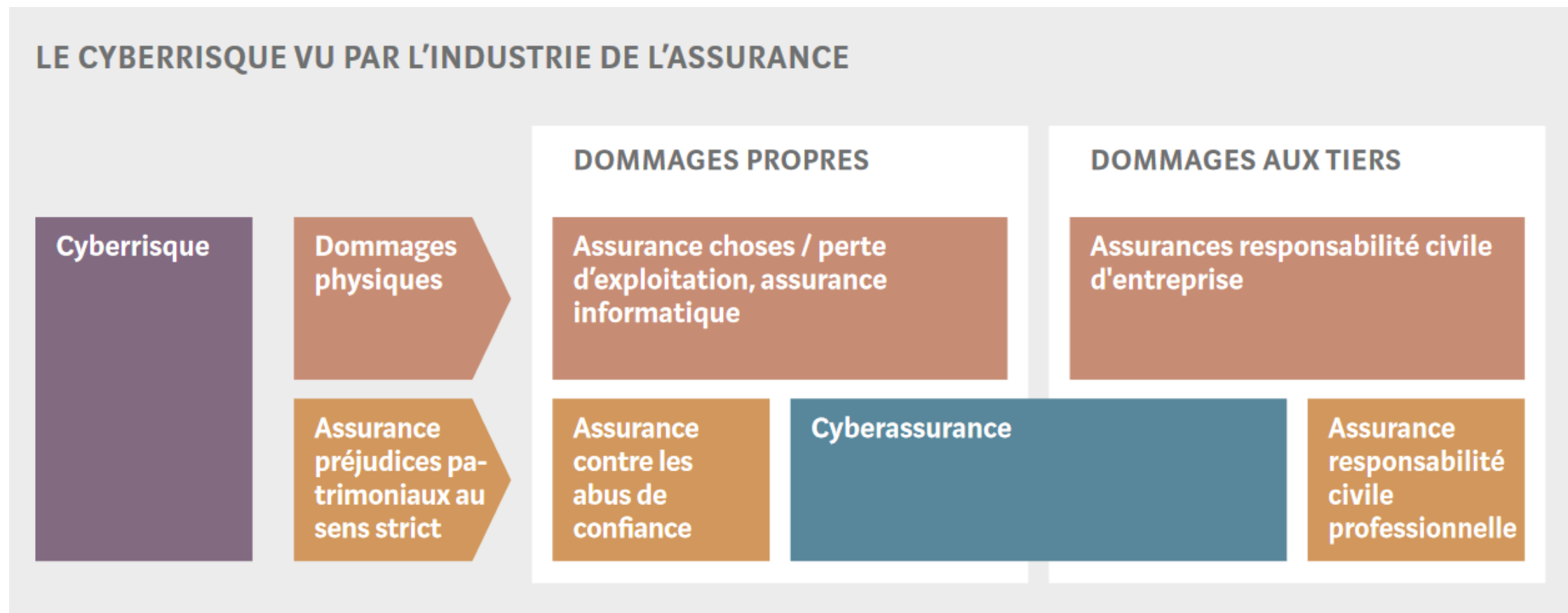


Gestion des correctifs et des vulnérabilités



Journalisation et surveillance

Transfert du risque résiduel



Optimisation des coûts des risques



Gestion de crise

Assistance de l'assureur /
Prestataires externes

Couverture des frais de
gestion de crise



Dommmages propres

Perte d'exploitation
Reconstitution des données
Menace et extorsion
(ransomware)
Criminalité informatique /
Ingénierie sociale



Dommmages aux tiers

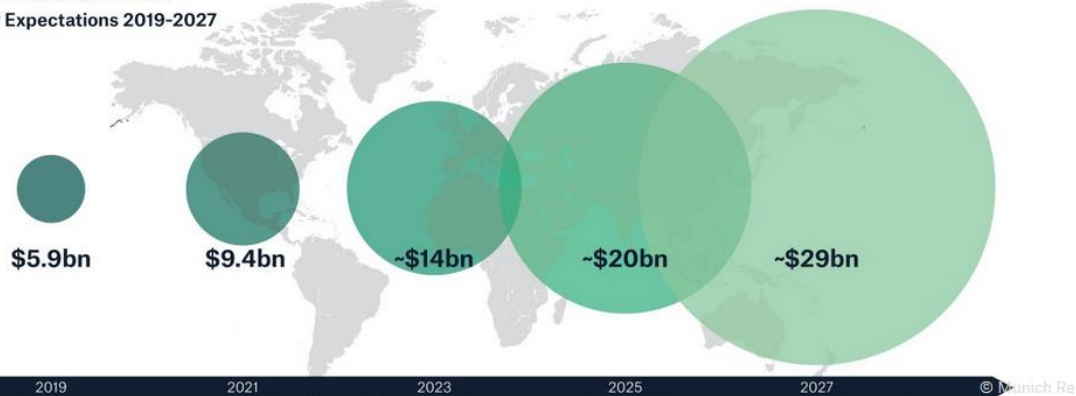
Violation de la
protection/sécurité
des données
Protection juridique passive

Les enjeux liés au monde de la cyberassurance

Le marché suisse

- Une assurance jeune
- Des assureurs à appétit variable
- Une maturité du risque exigée
- Nombre de sinistres en baisse

Cyber Insurance Market:
GWP Expectations 2019-2027



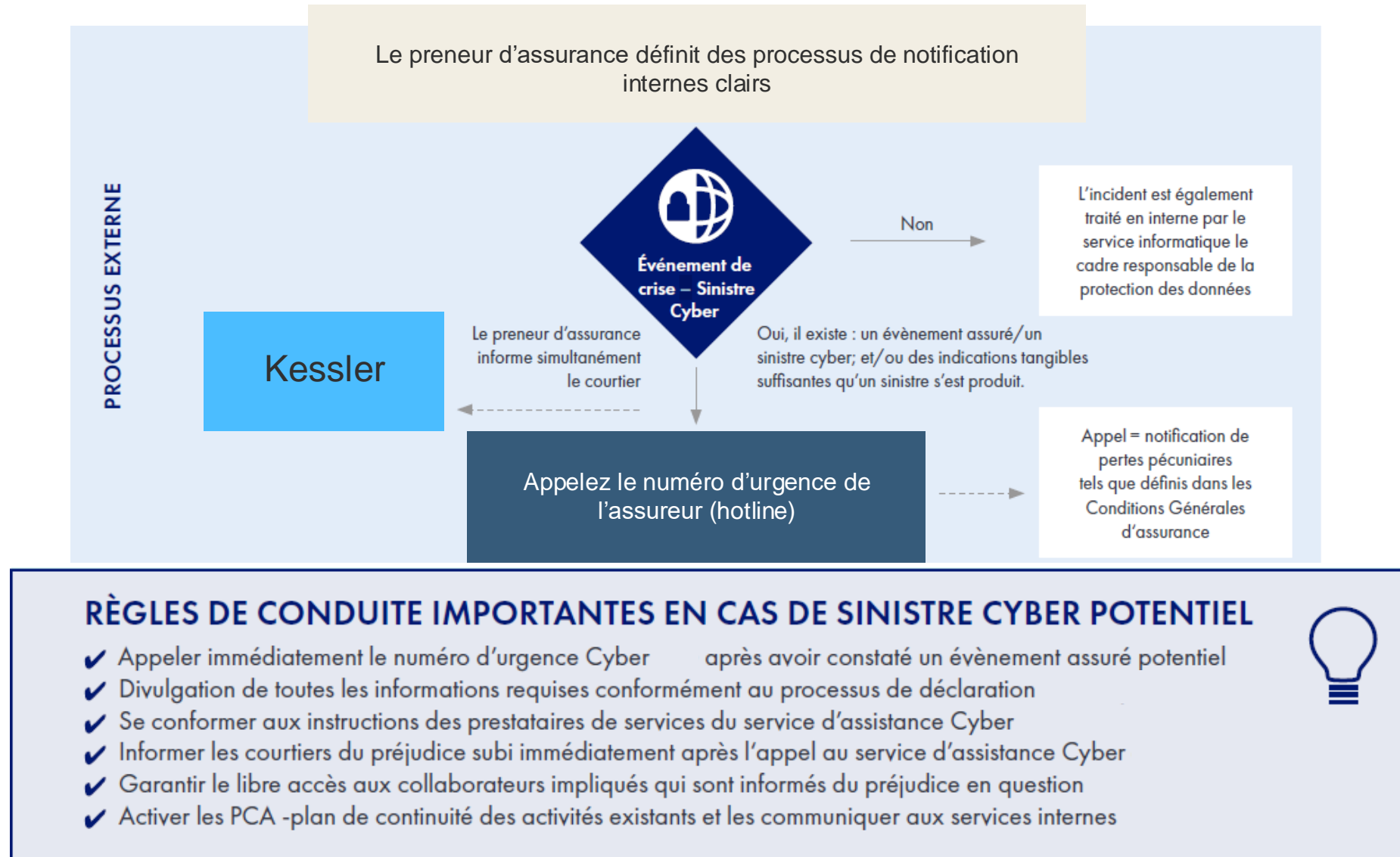
Munich Re Cyber Risk and Insurance Survey 2024

Outlook

- Le recours aux outils technologiques (assureurs)
- L'envolée du nombre de «Supply chain attacks»
- Le risque systémique ne découle pas forcément d'une attaque
- L'intégration de services additionnels
- L'introduction de termes dynamiques

Et l'intelligence artificielle dans tout ça?

Processus en cas de cyberincident (exemple)



Merci de votre attention !

KESSLER & CO SA
Avenue de la Gare 44
Case postale 950
CH-1001 Lausanne

T +41 21 321 60 30

www.kessler.ch

