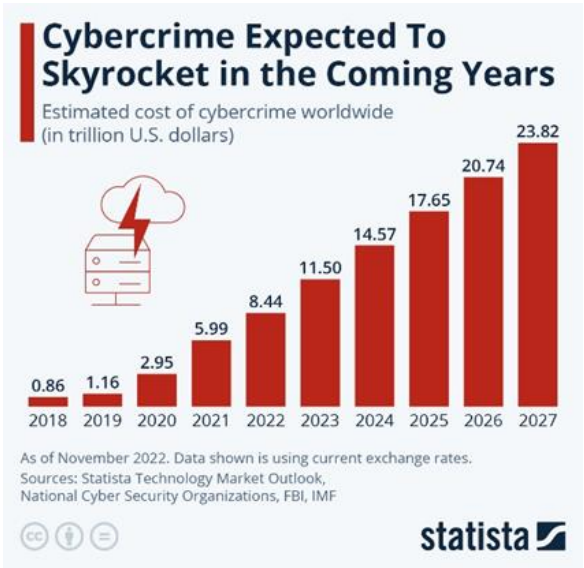
Crédit Mutuel Asset Management

N / 618

28 février 2024

Risque Cyber : le nouvel Hydre de Lerne

Présentée comme un puissant levier de croissance, la transformation digitale des entreprises s'appuie sur le déploiement d'infrastructures de communication plus performantes (fibre, 5G…). Alors que le futur de nombreuses industries semble désormais reposer sur les promesses de modèles d'affaires digitaux (intelligence artificielle, voitures autonomes, smart cities, e-commerce, cloud, internet des objets…) le risque cyber, qui leur est consubstantiel, reste encore largement sous-évalué alors que le coût estimé des crimes cyber dépasse déjà les 10 000 milliards de $, soit l'équivalent du 10e du PIB mondial.
D'ici à 2027, ce dernier devrait croître près de 4 fois plus vite que la croissance mondiale.



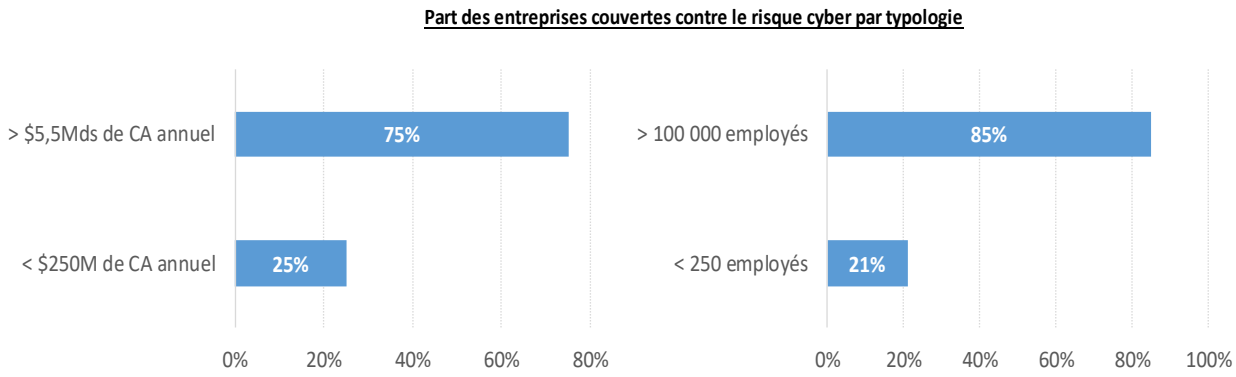
Bien qu'il reste encore le plus souvent évoqué sous un angle anecdotique, le risque cyber est devenu un risque systémique.

Selon le site du ministère de l'Économie des Finances et de la Souveraineté industrielle et numérique, celui-ci rassemble *« l'ensemble des risques liés à l'usage des technologies numériques et peut être défini comme un risque opérationnel portant sur la confidentialité, l'intégrité ou la disponibilité des données et systèmes d'information »*. Il se décline en 4 sous-catégories :

1. La cybercriminalité (i.e. rançongiciel, hameçonnage…)
2. L'atteinte à l'image (déni de service, modification de l'apparence ou du contenu de site internet)
3. L'espionnage
4. Le sabotage

Si la plupart des grandes entreprises identifient désormais ce risque comme une menace majeure pour leur organisation et communiquent également sur la façon dont elles travaillent à l'atténuer, celles de taille plus modeste semblent moins prendre la mesure de ce dernier.
Cette divergence croissante du niveau de protection des entreprises en fonction de leur taille est notamment mise en avant dans le Global Cybersecurity Outlook 2024, publié au terme du dernier Forum économique mondial.

Cet écart s'explique d'une part par l'ésotérisme des aspects techniques de la cybersécurité qui la rend moins facilement accessible aux entreprises de taille modeste, mais également par une « professionnalisation » des attaques qui, via leur complexification, tend à renchérir le coût des protections cyber. Ce fossé grandissant s'observe dans le recours différencié à des assurances cyber en fonction de la taille des entreprises.



Source : Global Cybersecurity Outlook 2024, World Economic Forum

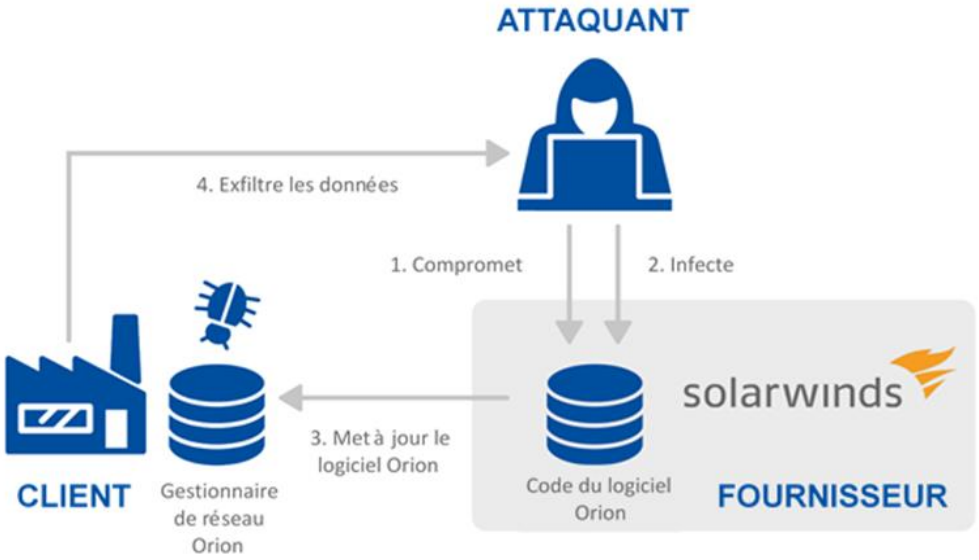
Dans la mesure où, comme les lions dans la savane, les cybercriminels focalisaient leurs attaques sur les dispositifs de protection des plus faibles, les grandes entreprises pouvaient, jusqu'à récemment, se sentir à l'abri de cette menace et se satisfaire de cet état de fait. **Or, selon le *Global Cybersecurity Outlook 2024*, 41 % des entreprises ayant été affectées par un incident de cybersécurité matériel au cours des 12 derniers mois l'ont été par la faute d'un tiers**.

En effet, comme toute chaîne, une chaîne logistique n'est jamais plus solide que le plus faible maillon qui la compose.

Les attaques contre la chaîne d'approvisionnement (*supply chain attack*), identifiées par l'agence de l'UE pour la cybersécurité (ENISA) comme l'un des 10 principaux risques cyber à l'horizon 2030, visent la relation entre une entreprise et ses fournisseurs.

Si, de par sa nature, elle implique un double niveau d'attaque (fournisseur + client), les modes opératoires sont multiformes. L'attaque de *supply chain* la plus connue est celle qui a touché le groupe américain de logiciels SolarWinds en 2020. Alors qu'un logiciel de gestion de réseau informatique qu'il développe avait été corrompu, SolarWinds a poussé une mise à jour vers ses 18 000 clients (dont les principales institutions fédérales américaines), les exposant à une porte dérobée qui a été exploitée par les cybercriminels pendant plus de 9 mois sous différentes formes (espionnage, vol et altération de données…).

En effet, la détection de ces attaques est rendue compliquée par la complexité même des chaînes d'approvisionnement.



Source : Rapport de l'ENISA concernant le paysage des menaces dans le cadre des attaques de la chaîne d'approvisionnement (europa.eu), juillet 2021.

Vécue des 2 côtés de l'Atlantique de façon traumatique par les autorités en charge de la cybersécurité, cette attaque a débouché sur l'adoption, fin 2023, de la loi de l'UE sur la cyberrésilience (*Cyber Resilience Act*).

Celle-ci vise à protéger les matériels contenant des composants numériques et les logiciels tout au long de leur cycle de vie en faisant peser la responsabilité de leur cybersécurité sur leurs fabricants.

Ces dispositions seront applicables 36 mois après l'entrée en vigueur de la loi, prévue courant 2024.

Si ce dispositif s'avère efficace contre les attaques de la chaîne logistique, le risque cyber comme l'Hydre de Lerne possède plusieurs têtes. En voici 9 autres…

Source : ENISA Threat Landscape 2023

Cette imagination sans limite des cybercriminels et la diversité de leurs modes opératoires rendent de plus en plus illusoire le seul bouclier technique offert par les services informatiques (quel que soit leur qualité). En effet, il semble aujourd'hui globalement admis que toute entreprise est ou sera la cible de cyberattaques. Compte tenu de cette forme d'inéluctabilité et des dégâts (financiers, réputationnels, opérationnels…) causés par ces dernières, **la thématique de la cybersécurité s'inscrit naturellement au cœur du modèle de gouvernance des entreprises**. Les investisseurs doivent donc veiller à ce que leur Conseil d'Administration dispose des compétences nécessaires à comprendre les risques cyber et les minimiser.

Vincent Goussard
Pôle Finance Responsable et Durable

Achevé de rédiger le 22/02/2024

Édité par Crédit Mutuel Asset Management – 4, rue Gaillon 75002 Paris. Société de gestion d'actifs agréée par l'AMF sous le numéro GP 97-138. Société Anonyme au capital de 3 871 680 euros immatriculée au RCS de Nanterre sous le numéro 388 555 021 - Code APE 6630Z. TVA Intracommunautaire : FR 70 388 555 021. Crédit Mutuel Asset Management est une entité de Crédit Mutuel Alliance Fédérale.