# ANTICIPER ET GÉRER *les cyber risques* LIÉS À L'IA EN TANT QUE CEO

**Avec Brice Augras**
**Président et chercheur en cybersécurité BZHunt**

**L'IA est partout et s'immisce à une vitesse grandissante dans nos vies et nos entreprises. Si elle fascine, autant qu'elle effraie, elle nous ferait presque oublier, par moments, qu'elle aussi comporte son lot de cyber risques et ouvre d'importantes failles de sécurité. Cette omniprésence s'accompagne d'une recrudescence des cybermenaces, générant des enjeux de sécurité inédits et posant de nouveaux défis complexes pour les organisations. Des menaces qui viennent accentuer la pression sur les dirigeants, dans un contexte d'incertitude économique complexe. L'enjeu est de comprendre et de savoir gérer les risques financiers et réputationnels qui en découlent, car le constat est simple et sans appel : la cybersécurité est indispensable, et il en va de la responsabilité de chaque CEO.**

Conférence d'ouverture animée par

**Charlotte Bricard**
**Journaliste**

## La complexe réalité des cybermenaces

L'essor de l'IA modifie le paysage des cybermenaces, en particulier dans le secteur du e-commerce. Les cyberattaques deviennent plus sophistiquées, l'IA permettant aux cybercriminels de perfectionner leurs techniques, ne serait-ce qu'en améliorant la qualité du phishing (par la réduction des fautes d'orthographe), en allant jusqu'à usurper des identités par des synthèses vocale et visuelle. L'exposition accrue des entreprises due au télétravail a également accentué leur vulnérabilité.

**L'IA peut être utilisée comme un "agent allié" par les hackeurs, leur offrant un accès facilité à divers services internes.**

Dans ce contexte, il est difficile, voire impossible, de donner quelques chiffres clefs. Malgré les obligations légales, avec le fameux RGPD qui oblige toute entreprise à déclarer un incident de cybersécurité dans un délai de 72 heures, dans la réalité, c'est plutôt la loi du silence. Pour des raisons diverses et variées, notamment d'image de marque, les entreprises préfèrent prendre le risque de payer la rançon pour espérer récupérer potentiellement leurs données. Cette absence de transparence ne permet pas d'évaluer à juste titre l'ampleur des cyberattaques.


## Identification et cartographie des risques

Bien que les techniques de cyberattaques se multiplient, renforcées par l'IA, les tests d'intrusion et simulations de cyberattaques ciblées continuent de démontrer que **7 fois sur 10, le point d'entrée demeure l'humain** : le classique email de phishing ouvert malencontreusement le lundi matin...

Parmi les cas concrets les plus effrayants : il suffit à un hackeur de récupérer 30 secondes de voix pour usurper et simuler la voix d'une personne que nous connaissons, ou même de simuler le visage d'un proche ou d'un collègue, au travers d'une visioconférence...

Comment remédier à ces nouvelles problématiques sécuritaires ? Les réponses sont aujourd'hui encore assez pauvres, liées à l'émergence et l'accélération de cette nouvelle technologie.

**Le référentiel Mitre Atlas liste toutefois l'ensemble des vecteurs d'attaques qu'il est possible de réaliser** à l'encontre des LLM et d'IA plus ou moins sécurisés. Ces attaques peuvent compromettre la disponibilité, l'intégrité et la confidentialité des données traitées par l'IA, ainsi que leur comportement. L'IA peut être utilisée comme un "agent allié" par les hackeurs, leur offrant un accès facilité à divers services internes. A noter que le nombre de techniques d'attaque référencées augmente rapidement (50è en septembre 2024, 74 en mars 2025).

**Bonnes pratiques et pièges à éviter**

**Une prudence particulière doit être exercée face à l'intégration précipitée de l'IA : cette accélération provoque actuellement un retour 10 ans en arrière en matière de cybersécurité.**

Dans cette euphorie, cette course à l'innovation et au « time-to-market », les entreprises doivent impérativement intégrer une dimension sécuritaire dans leurs choix technologiques. Une prudence particulière doit être exercée face à l'intégration précipitée de l'IA : cette accélération provoque actuellement un retour 10 ans en arrière en matière de cybersécurité.

Dans un monde idéal, il faudrait minimiser la dépendance à l'utilisation des LLM et produits proposés en format cloud. Bien que ce soit assez coûteux, les entreprises qui le peuvent, doivent réfléchir à internaliser leur puissance de calcul afin de garantir un contrôle optimal des données et ainsi limiter leur exposition à des vulnérabilités externes.

**Une autre erreur serait d'avoir un LLM unique à disposition de tous les services de l'entreprise** : il est très important, voire même crucial, de cloisonner la donnée. Un modèle ne doit avoir accès qu'à la donnée qu'il est supposé servir, dans un cas d'usage, un cadre opérationnel et un métier bien spécifique, et cantonné uniquement aux personnes qui sont censées avoir accès à ces données. Faute de quoi, les progrès de l'IA pourraient paradoxalement ramener les entreprises dix ans en arrière sur le plan sécuritaire.

**Enjeux et vulnérabilité des e-commerçants**

Les périodes commerciales stratégiques, telles que le Black Friday, exacerbent la vulnérabilité des e-commerçants avec une recrudescence d'attaques visant l'indisponibilité des services ou la multiplication des fraudes financières.

**En e-commerce, près de 80 % des failles concernent spécifiquement les tunnels d'achat, où manipulations de prix, de codes discounts et fraudes financières prospèrent.**

Pour répondre à ces nombreux défis, le secteur doit réussir à créer des vocations pour faire face à l'actuelle pénurie de compétences, sans oublier que nous devons tous être responsables de notre cybersécurité.