Dans un marché morose pour les valeurs de croissance, la cybersécurité pourrait générer de bons résultats futurs

Publié le 24 octobre 2022

Christopher Gannatti, CFA
Global Head of Research

Nous avons récemment effectué une tournée commerciale à Milan, Genève, Madrid, Londres et Paris durant laquelle nous avons abordé le thème de la cybersécurité avec les investisseurs. WisdomTree propose une large gamme de stratégies d'investissement thématique sachant que notre société a souvent noué pour chaque thème un partenariat avec des experts dans le domaine concerné. Dans le cadre de cette tournée commerciale, nous avons eu l'occasion de voyager avec Team8, la société qui fournit les données permettant de classifier de l'offre de cybersécurité des entreprises sous-jacentes.

Les attaques se sont poursuivies pendant notre tournée de présentation

Alors que nous étions en déplacement, une violation de certains des systèmes d'Uber a fait l'objet d'une forte médiatisation. La méthode a été particulièrement remarquée car l'attaque a visé à de nombreuses reprises un employé en lui envoyant une demande d'authentification à deux facteurs jusqu'à ce que l'employé finisse par l'accepter1. Cette approche nous rappelle à tous une vérité importante dans le domaine de la cybersécurité : généralement, le chemin le plus simple vers un système passe par un être humain, plus particulièrement si le hacker arrive à le décontenancer ou à le frustrer.

Depuis, l'article intéressant suivant a été publié : « Les marques revoient leurs politiques sur la protection des données après le règlement de 1,2 million de dollars de Sephora » (« Brands Review Data Privacy Policies After $1.2 Million Sephora Settlement »)2.

Nous étions en déplacement en Europe où chaque investisseur avait pleinement conscience de l'existence du règlement général sur la protection des données (RGPD). De nombreux résidents américains pourraient penser que les États-Unis ne disposent pas de telles lois. Or le California Consumer Privacy Act a été voté en 2018 et il est entré en vigueur en 2020. Dès le 1er janvier 2023 et l'entrée en vigueur du California Privacy Rights Act qui étend et amende la loi précédente, de nombreuses entreprises pourraient avoir droit à un réveil difficile.

Plus de 100 entreprises cotées et non cotées ont reçu des lettres du Procureur général de Californie M. Rob Bonta dans le cadre du coup de balais passé parmi les grands distributeurs qui a donné lieu au règlement Sephora, et de nombreuses lettres supplémentaires ont été envoyées depuis.

La protection des données est l'un de nos thèmes clés de cybersécurité et il est intéressant d'examiner toutes les lois qui élargissent le cercle au-delà du RGPD en Europe.

Distinguer le contexte macroéconomique de la mégatendance

Nombre des sociétés de cybersécurité les plus innovantes exercent à l'aide d'un modèle économique de Software-as-a-Service (SaaS) qui a été popularisé dans le secteur de l'informatique dans le cloud. La principale caractéristique de ces entreprises est la manière dont les clients souscrivent à un service durant une période donnée. Les entreprises SaaS couronnées de succès auront tendance à proposer des produits qui fidélisent, c'est-à-dire que les clients vont les souscrire et ne pas en changer rapidement en annulant leur abonnement.

Si l'on tient compte du fait que la durée de rétention moyenne d'un produit est de 5 à 7 ans, une entreprise SaaS peut proposer d'autres services. L'un de ses objectifs est de parvenir à un taux de rétention net supérieur à 100 %. Cela signifie que les clients prolongent non seulement leur service, mais dépensent davantage ou souscrivent des services différents de la gamme de la société. L'autre sujet souvent abordé est le coût d'acquisition des clients. Nous entendons souvent la phrase « ce qui compte avant tout, c'est la croissance ». S'il coûte environ 1 an de revenus tirés d'un client pour acquérir un client et si la durée de rétention moyenne est de 5 à 7 ans, alors il semble logique de dépenser ce montant afin d'accélérer la croissance. Si l'entreprise fonctionne, elle peut éviter cette dépense à l'avenir, une fois acquis plus de clients, et avoir une activité plus rentable.

En résumé, même si le discours actuel porte exclusivement sur la rentabilité plutôt que la croissance, cette dernière demeure importante sur le segment SaaS. En examinant les spécificités de ces activités sous-jacentes, il est clair qu'elles possèdent beaucoup de forces qui peuvent être masquées par un manque actuel de rentabilité.

Les entreprises vont-elles continuer de dépenser ?

Il a été assez facile de convaincre les personnes avec lesquelles nous avons parlé que tout le monde, particuliers ou entreprises, nécessite une cyber-stratégie.

Une statistique très discutée parmi les Directeurs informatiques et de la sécurité des informations est qu'environ 7 à 10 % des dépenses informatiques devraient être consacrées à la cybersécurité3. Ainsi, si nous estimons que les dépenses informatiques générales vont augmenter sur une période donnée, alors les dépenses dans la cybersécurité devraient également suivre cette tendance.

Toutefois, un autre angle de discussion porte sur le nombre de catégories différentes de dépenses informatiques qui peuvent augmenter ou diminuer à différents moments. Il ressort de la situation actuelle que l'environnement des menaces dans le domaine de la cybersécurité est assez important. Les Directeurs de la sécurité informatique de certaines des plus grandes entreprises au monde en ont conscience et agissent en conséquence. La réflexion porte avant tout sur la défense et la protection et sur les dépenses nécessaires afin de les garantir. Ainsi, il peut arriver que dans un environnement marqué par exemple par

la crise entre la Russie et l'Ukraine, les budgets de cybersécurité augmentent davantage que les dépenses informatiques générales.

Les thèmes qui sont l'avenir de la cybersécurité

WisdomTree cible sept thèmes clés dans le domaine de la cybersécurité qui représentent les domaines les plus prioritaires à l'avenir. Il est important de réfléchir à ce qui fonctionnera à l'avenir plutôt que ce qui a fonctionné par le passé. Ces thèmes sont les suivants :

1. Sécurité du cloud
2. Sécurité plus intelligente
3. Résilience et reprise
4. Sécurité des objets
5. Monde sans périmètre
6. Sécurité des données
7. « Shift-Left » (tests logiciels et tests système effectués plus tôt dans le cycle de vie)

L'une des parties les plus intéressantes de toute discussion sur la cybersécurité est d'examiner comment ces thèmes sont en lien avec le monde dans lequel nous vivons. À titre d'exemple, le concept « Shift-Left » peut donner l'impression que nous avons oublié des mots dans cette expression. Or il s'agit d'une expression utilisée dans le développement de logiciels qui signifie qu'il convient d'envisager la sécurité plus tôt dans le processus de développement des logiciels. Il peut s'agir d'une manière de réduire le risque d'utilisation d'un code non sécurisé qui peut entraîner des « attaques de la chaîne logistique » comme nous avons pu le constater dans le cas de Solar Winds il y a quelques années. Ces attaques informatiques sont pernicieuses car le hacker obtient un accès à une partie du logiciel utilisé par de nombreux clients.

Une autre caractéristique de ces thèmes est que chacun peut avoir son propre échéancier. La sécurité du cloud continue de croître rapidement et elle reste très nécessaire, mais à une certaine date future, nous pourrions constater que tout le monde a déjà opté pour le cloud. Une fois que tout le monde est dans le cloud et doté d'une configuration efficace, il est peut-être temps de se préoccuper d'un autre domaine. La sécurité des données pourrait débuter uniquement lorsque différents pays situés en dehors du continent européen commencent à voter des lois plus strictes concernant la protection des données. Fréquemment, c'est le risque de responsabilité qui conditionne les changements de comportements.

Conclusion : ne laissez pas la performance à court terme vous éloigner de la cybersécurité

2022 a été une année difficile pour la performance de nombreuses valeurs de sociétés Software-as-a-Service et celles spécialisées dans la cybersécurité n'ont pas fait exception. À notre avis, le recul des valorisations observé depuis un an pourrait constituer un point d'entrée plus intéressant pour un investisseur qui a une thèse d'investissement à long terme sur ce thème essentiel.

1 Source : Davey Winder. « Uber Hack Update: Was Sensitive User Data Stolen & Did 2FA Open Door To Hacker? » Forbes. Le 18 septembre 2022.

2 Source : Patrick Coffee. « Brands Review Data Privacy Policies After $1.2 Million Sephora Settlement. » Wall Street Journal. Le 27 septembre 2022.

3 Source : Bob Violino. « How much should you spend on security? » CSO. Le 20 août 2019.

Blogs associés

+ La politique des banques centrales a donné naissance à une opportunité de valorisation dans le secteur des logiciels

+ Why has the Ukraine war put a spotlight on cybersecurity and the energy transition?

Important Risks Related to this Article

Informations importantes

Communications commerciales publiées dans l¼Espace économique européen (« EEE ») Ce document est publié et approuvé par WisdomTree Ireland Limited, une société autorisée et réglementée par la Central Bank of Ireland.

Communications commerciales émises dans des juridictions en dehors de l¼EEE Ce document est publié et approuvé par WisdomTree UK Limited, une société autorisée et réglementée par la Financial Conduct Authority du Royaume-Uni.

WisdomTree Ireland Limited et WisdomTree UK Limited sont toutes les deux désignées comme « WisdomTree » (le cas échéant). Notre Politique sur les conflits d¼intérêts et notre Inventaire sont disponibles sur demande.

Réservé aux clients professionnels uniquement. Les informations figurant dans ce document sont fournies à titre informatif et ne constituent pas une ore de vente, ou une sollicitation d¼ore d¼achat de titres ou d¼actions. Ce document ne doit pas être utilisé comme fondement d¼une décision d¼investissement. La valeur des investissements peut fluctuer et vous êtes susceptible de perte tout ou partie du montant investi. La performance passée ne constitue pas nécessairement une indication des performances futures. Toute décision d¼investissement doit être fondée sur les informations figurant dans le prospectus approprié et sur des conseils indépendants en matière d¼investissement, fiscaux et juridiques.

L¼application des réglementations et lois fiscales peut souvent conduire à des interprétations diérentes. Tous les points de vue ou opinions exprimés dans cette communication représentent les points de vue de WisdomTree et ne doivent pas être interprétés comme des conseils réglementaires, fiscaux ou juridiques. WisdomTree ne donne aucune garantie ou représentation quant à l'exactitude des vues ou opinions exprimées dans cette communication. Toute décision d'investissement doit être fondée sur les informations contenues dans le prospectus approprié et après avoir sollicité des conseils indépendants en matière d'investissement, fiscaux et juridiques. Ce document n¼est pas et ne doit en aucun cas être interprété comme une publicité ou une ore publique d¼actions ou de titres aux États-Unis ou dans toute province ou tout territoire des États-Unis. L¼introduction, la transmission et la distribution (directes ou indirectes) de l¼original ou d¼une copie de ce document sont interdites aux États-Unis.

Bien que WisdomTree s¼eorce d¼assurer l¼exactitude du contenu de ce document, WisdomTree ne peut en garantir l¼exactitude. Les fournisseurs de données tiers sollicités pour obtenir les informations contenues dans le présent document ne donnent aucune garantie ou représentation de quelque sorte en rapport avec ces données. Lorsque WisdomTree exprime ses propres opinions concernant le produit ou l¼activité du marché, ces opinions sont susceptibles de changer. WisdomTree, ses ailiés et leurs dirigeants, directeurs, partenaires ou employés respectifs déclinent toute responsabilité pour toute perte directe ou indirecte découlant de l¼utilisation de ce document ou de son contenu.