

POINT DE VUE POUR LES INVESTISSEURS

Cybersécurité : la gouvernance est importante

Le cyberrisque est maintenant une préoccupation omniprésente pour la majorité des sociétés que nous évaluons dans l'ensemble des secteurs et des régions. Les atteintes – lorsqu'elles se produisent – peuvent perturber considérablement les activités, être coûteuses et nécessiter une attention considérable de la part de la direction.

Sommaire d'information

Le cyberrisque est maintenant une préoccupation omniprésente pour la majorité des sociétés que nous évaluons dans l'ensemble des secteurs et des régions. Les atteintes – lorsqu'elles se produisent – peuvent perturber considérablement les activités, être coûteuses et nécessiter une attention considérable de la part de la direction. Elles peuvent aussi causer de graves dommages à la réputation, ce qui peut ébranler la confiance des consommateurs et, par conséquent, influencer sur les évaluations. Pour les investisseurs, ces événements peuvent devenir importants sur le plan financier, selon divers facteurs.

Reprise plus rapide ou plus lente

Les sociétés qui subissent une atteinte à leur cybersécurité en ressortent à des rythmes différents, souvent en fonction de facteurs semblables.

Reprise plus rapide

- Réponse transparente et immédiate de la direction
- Contrôles et gouvernance préexistants solides
- Perturbations opérationnelles limitées découlant de l'atteinte

Reprise plus lente

- Faible gouvernance avant l'incident
- Divulcation ou réponse publique tardive
- Forte participation des organismes de réglementation
- Modèle d'affaires déjà fragile

AUTEURS

**POOJA DAFTARY**

Analyste de recherche
sur les actions

**DAN POPIELARSKI**

Stratège, Stratégie
des clients en matière
d'investissement durable

La gouvernance est un important facteur de différenciation

Comme le cyberrisque est omniprésent, les investisseurs doivent comprendre comment les sociétés le gèrent.

Les atteintes ne sont pas toutes également préoccupantes; les conséquences divergent considérablement en fonction de quelques caractéristiques sous-jacentes. À une extrémité du spectre se trouvent les incidents dont l'effet sur le plan opérationnel est limité, soit parce que le temps d'arrêt n'a pas de conséquence importante sur les clients, soit parce que les structures de gouvernance et de gestion du risque de la société ont permis de repérer l'atteinte plus rapidement, soit parce que les données exposées ne sont pas très sensibles. Dans de tels cas, la perturbation est limitée dans le temps, les systèmes sont rapidement rétablis et les effets d'entraînement sont limités. De plus, l'incidence sur le plan financier est habituellement limitée à des coûts ponctuels, avec une normalisation relativement rapide des activités et de l'humeur du marché à l'égard de la société.

À l'autre extrémité du spectre se trouvent les incidents dont la reprise est plus lente et dont les conséquences vont au-delà de l'événement initial. Selon notre expérience, la gouvernance dans ces situations est souvent plus faible ou les contrôles ne sont pas appliqués de façon uniforme. Cela entraîne un retard dans la détection d'une atteinte, faisant en sorte que la communication est réactive plutôt que proactive. La surveillance réglementaire pourrait également être plus élevée en raison de ce qui a été considéré par la suite comme des lacunes évidentes dans la gestion du risque, prolongeant ainsi la préoccupation. Dans les cas les plus extrêmes, la fragilité préexistante du modèle d'affaires peut considérablement bousculer la société. Dans ces cas, l'incidence des éléments de la première atteinte s'aggrave, les coûts directs n'étant qu'une partie de l'histoire : les perturbations opérationnelles durent plus longtemps, les clients sont plus touchés et l'attention de la direction est détournée de la mise en œuvre quotidienne de la stratégie. Le marché a tendance à traiter ces cas comme des défis structurels plutôt que comme des problèmes temporaires, ce qui crée un important risque de surévaluation.

Nous estimons que la majorité des sociétés se situent quelque part dans ce spectre, mais les différences sur le plan de la préparation et des interventions expliquent pourquoi certains incidents de cybersécurité sont des problèmes de bénéfices à court terme, tandis que d'autres deviennent des préoccupations liées à l'évaluation sur plusieurs années.

Cyberrisque et émergence de l'IA

L'émergence de l'intelligence artificielle fait de la cybersécurité un risque encore plus important à gérer pour les sociétés, car elle accroît la taille et la complexité de leurs vulnérabilités numériques potentielles. Les modèles d'IA utilisent de grandes quantités de données sensibles et sont connectés à de nombreux systèmes et de nombreux tiers. Les cyberattaques disposent ainsi plus que jamais davantage de points d'entrée. Parallèlement, les cybercriminels utilisent également l'IA pour améliorer leurs méthodes. Ils peuvent maintenant automatiser l'hameçonnage, la fraude et la recherche des faiblesses du système, ce qui rend les attaques plus rapides et plus évoluées.

L'IA elle-même peut également engendrer des risques liés à la cybersécurité : un dénonciateur a découvert que le Fable 5 d'Anthropic pourrait être débridé d'une manière qui pourrait, compte tenu de ses capacités avancées, causer un risque lié à la cybersécurité important pour un nombre important de sociétés et de personnes partout dans le monde. Le modèle a été en mesure de repérer par lui-même des milliers de vulnérabilités critiques jusque-là inconnues des logiciels. Par conséquent, le modèle a été interdit jusqu'au 1^{er} juillet, date à laquelle il a été démontré que d'autres modèles moins performants pouvaient être manipulés de la même façon, ce qui signifie que cette vulnérabilité n'était pas propre à Fable et rendant le risque encore plus généralisé.

Cela accroît l'incidence potentielle des cyberincidents, surtout à mesure que l'IA devient plus intégrée aux activités courantes des entreprises. Du point de vue de la gouvernance et des placements, la cybersécurité est maintenant un signe important de la façon dont une société gère le risque. Les sociétés ont besoin d'une surveillance plus étroite, d'une meilleure protection des données et de plans d'intervention clairement définis. De plus, la surveillance ne devrait pas être seulement la responsabilité de la direction; les sociétés qui gèrent réellement le cyberrisque ont également un conseil d'administration dédié à la surveillance. Les sociétés doivent également gérer les nouveaux risques, comme la manipulation des modèles d'IA et les fuites de données. Maintenant plus que jamais, la cybersécurité est un élément clé de la gestion du risque d'entreprise et de l'utilisation responsable de l'IA.

Cadre d'évaluation du cyberrisque

Nous avons élaboré le cadre suivant pour guider notre évaluation de l'importance sur le plan financier des incidents de cybersécurité et de la prise de connaissance de la culture d'entreprise, du risque opérationnel et des évaluations. Ce cadre repose sur quatre piliers :

1 GOUVERNANCE ET RESPONSABILITÉ	2 EXPOSITION À DES TIERS	3 CONFIDENTIALITÉ	4 PRÉPARATION ET REPRISE APRÈS INCIDENT
Une surveillance claire de la cybersécurité doit être assurée au niveau de la direction et du conseil d'administration, ce qui nécessite des personnes ayant une expérience et une formation appropriées dans ce domaine. Cela influe sur la rapidité avec laquelle les problèmes sont repérés, transmis à un échelon supérieur et traités. Lorsque ce pilier est faible, la détection est plus lente, les interventions sont moins coordonnées et les résultats ont tendance à être pires.	Le cyberrisque a souvent une incidence sur une société par le biais de logiciels de tiers ou de l'utilisation de systèmes par des entrepreneurs et des personnes non membres du personnel. Certaines sociétés qui exercent leurs activités dans des écosystèmes complexes ou qui font l'objet d'une forte impartition ont tendance à avoir plus de points de vulnérabilité, ce qui rend la surveillance de ces relations essentielle.	Les sociétés conservent d'importantes quantités de renseignements sur leurs clients. Elles ont besoin de règles claires quant à la quantité de données conservées, qui y a accès et comment elles sont stockées. Même si les sociétés sont déjà tenues de respecter certains règlements sur la protection des données en vigueur dans divers territoires, leur niveau de rigueur peut varier.	Une société doit comprendre l'incidence qu'un cyberincident pourrait avoir sur différentes unités fonctionnelles ou gammes de produits ou de services, et y être préparée, afin de s'assurer que des contrôles des risques appropriés sont en place. Les sociétés doivent également simuler les atteintes et les interventions, ainsi que les étapes probables nécessaires pour rétablir les systèmes, reprendre les activités et recouvrer la confiance des investisseurs ou des clients en cas d'atteinte. C'est également là que les défaillances de contrôle de base peuvent prolonger le temps d'arrêt et avoir des conséquences importantes sur le plan financier.

Ce cadre est directement lié à des notions plus générales de discipline sur le plan opérationnel et de gestion du risque qui sont intégrées à notre analyse fondamentale des placements. La sensibilisation au cyberrisque permet de mettre à l'épreuve en temps réel l'efficacité des systèmes de gestion du risque que nous évaluons.

Étude de cas : Coupang

Coupang est un exemple où l'incident de cybersécurité est rapidement devenu secondaire face aux préoccupations plus générales en matière de gouvernance et de transparence. Coupang est une société de commerce électronique qui exerce ses activités en Corée du Sud, souvent appelée l'Amazon de la Corée du Sud. La société a divulgué une atteinte à la vie privée à grande échelle touchant des dizaines de millions d'utilisateurs, mais le moment et la séquence de ces divulgations ont soulevé des questions sur l'asymétrie de l'information et la question de savoir si les mauvaises nouvelles étaient « gérées » plutôt que communiquées de façon transparente. À la suite de cet incident, le titre a fait l'objet de ventes massives et son rendement a été inférieur à celui des indices de référence. Plus important encore, la situation a mis en évidence les préoccupations existantes en matière de gouvernance. Le contrôle des fondateurs a été concentré au moyen d'une structure à deux catégories, limitant ainsi l'indépendance du conseil d'administration. Dans le cadre de cette structure, la transmission à un échelon supérieur et les défis sont devenus plus difficiles, en particulier lors d'une situation de crise.

Du point de vue des placements, le problème ne portait pas seulement sur le coût direct de l'atteinte, mais également sur un changement dans notre point de vue sur la qualité de l'équipe de direction et la confiance dans sa prise de décisions. Nous avons déterminé que le processus décisionnel de la société n'était pas suffisamment équilibré et que les compromis entre le positionnement juridique, l'intervention sur le plan opérationnel et la communication avec les parties prenantes ont été mal gérés. Lorsque des divulgations de cette nature sont retardées ou incomplètes, la confiance à l'égard de la direction tend à diminuer. Dans ce contexte, le cyberincident est devenu un prisme de la qualité de la gouvernance, où le risque était moins un effet ponctuel sur les bénéfices et plus un escompte durable appliqué à l'entreprise.

Étude de cas : LY Corporation

LY Corporation est une société japonaise d'Internet et de technologie qui exploite une application de messagerie, du commerce électronique et de la publicité numérique, et gère des solutions de technologie financière et de paiement mobile. LY présente un contraste utile par rapport à Coupang, car ses problèmes portaient moins sur la divulgation que sur la complexité et l'exécution des activités. L'incident du rançongiciel concernant Askul a révélé des défaillances de contrôle de base au niveau des filiales, ce qui n'est généralement pas inhabituel. La question la plus importante a été de savoir ce que la réponse de la société à l'attaque révélait sur la structure globale de l'entreprise. Dans le cas de LY, l'exécution a été relativement décentralisée au sein d'un portefeuille d'entreprises, les systèmes étant fondés sur des infrastructures existantes et des intégrations multiples. Cela a accru la probabilité d'incidents et l'incidence opérationnelle, le cas échéant. La communication et la transmission à un niveau supérieur à l'échelle des filiales pourraient être plus lentes et la reprise pourrait prendre plus de temps, car les systèmes n'étaient pas entièrement normalisés. Il y a également eu un problème sur le plan réglementaire, en particulier autour de LINE (une application de messagerie exploitée par LY), qui a accru la surveillance et prolongé la durée de ces événements.

Parallèlement, il y a eu des signes évidents d'amélioration. Les contrôles ont été renforcés, les cadres sont devenus plus uniformes dans l'ensemble des filiales et la direction a démontré sa volonté de régler les problèmes et d'investir dans les systèmes. Du point de vue des placements, cela a créé un profil de risque différent. Même si la société a pris des mesures claires pour améliorer sa gouvernance liée au cyberrisque, la structure organisationnelle actuelle indique que les cyberrisques persisteront probablement : LY a encore un certain nombre de filiales de différents secteurs, avec des structures de risque différentes et des équipes de direction distinctes. La crédibilité de la gouvernance est moins préoccupante, mais la volatilité sur le plan opérationnel devrait persister. Les incidents peuvent continuer de perturber l'exécution et demander trop de temps et d'efforts à la direction, ce qui peut nuire à l'exécution opérationnelle souhaitée. Ces questions et d'autres considérations ont servi à évaluer la société, mais la question clé est de savoir si les améliorations se produisent assez rapidement pour réduire la fréquence et la gravité de ces perturbations. Nous sommes d'avis que le profil risque-rendement demeure positif, compte tenu de la trajectoire haussière des changements apportés à la gouvernance de la société combinée à une évaluation peu contraignante.

Études de cas et analyses élargies

Nous constatons une dynamique semblable dans d'autres secteurs. Voici quelques exemples d'atteintes passées et de leur incidence sur les sociétés :

Soins de santé

Dans le secteur des soins de santé, l'incident lié à Change Healthcare souligne dans quelle mesure les incidents de cybersécurité peuvent être importants sur le plan financier lorsqu'ils touchent des infrastructures essentielles, tant en ce qui concerne les coûts directs que les perturbations opérationnelles généralisées.

Ventes au détail

Dans le secteur du commerce de détail, l'incident concernant Marks & Spencer illustre dans quelle mesure le choix du moment amplifie l'incidence, alors qu'une attaque par rançongiciel a perturbé sa chaîne d'approvisionnement pendant une période cruciale de magasinage des Fêtes. Les interruptions durant les périodes de pointe peuvent avoir des conséquences financières démesurées, même si l'entreprise sous-jacente demeure intacte.

Télécommunications

Dans le secteur des télécommunications, l'exemple de SK Telecom montre comment les obstacles réglementaires et juridiques peuvent persister bien au-delà d'un incident initial, car les organismes de réglementation ont imposé une pénalité financière de 200 \$ par utilisateur.

Dans ces exemples, l'interaction entre les incidents de cybersécurité et le modèle d'affaires sous-jacent est essentielle. En fin de compte, le cyber risque renforce un principe de placement plus large : des événements précis ont moins d'importance que ce qu'ils révèlent. Comme les atteintes sont maintenant plus répandues que jamais, leur survenance à elle seule fournit des renseignements limités; le véritable signal réside dans l'efficacité avec laquelle les sociétés anticipent et absorbent les perturbations et s'en remettent. Cela fait de la cybersécurité un prisme précieux pour évaluer la qualité de la gouvernance, la résilience opérationnelle et la crédibilité de la direction sous pression. Plutôt que d'essayer d'isoler la cybersécurité comme un intrant d'évaluation indépendant, nous l'intégrons à notre évaluation plus large du risque d'exécution, en utilisant les incidents comme preuve de la façon dont les sociétés se comportent en situation de tension et dans quelle mesure nous assumons l'incertitude. De cette façon, la cybersécurité ne sert pas seulement de facteur de risque, mais aussi de mise à l'épreuve continue et en temps réel de la durabilité du scénario de placement. ▲

Les renseignements ci-dessus de même que les sociétés ou les titres mentionnés ne doivent pas être considérés comme des conseils en placement, des recommandations d'achat ou de vente d'un titre ou une indication des opérations prévues à l'égard de tout produit de placement de MFS.

Le rendement passé n'est pas garant du rendement futur. Les prévisions ne sont pas garanties.

La diversification ne garantit pas un gain ou une protection contre les pertes. Le rendement passé n'est pas garant du rendement futur.

RENSEIGNEMENTS MONDIAUX

Sauf indication contraire, les logos ainsi que les noms des produits et services sont des marques de commerce de MFS^{MD} et de ses sociétés affiliées, qui peuvent être déposées dans certains pays.

Distribué par :

États-Unis – MFS Institutional Advisors, Inc. (« MFSI »), MFS Investment Management et MFS Fund Distributors, Inc., membre de la SIPC; **Amérique latine** – MFS International Ltd;

Canada – MFS Gestion de Placements Canada Limitée. **Note à l'intention des lecteurs du Royaume-Uni et de la Suisse** : Publié au Royaume-Uni et en Suisse par MFS International (UK) Limited (« MIL UK »), une société privée à responsabilité limitée inscrite en Angleterre et au pays de Galles sous le numéro 03062718, dont les activités de placement sont autorisées et réglementées par la UK Financial Conduct Authority. Le siège social de MIL UK, filiale indirecte de MFS^{MD}, se trouve au One Carter Lane, Londres, EC4V 5ER;

Note à l'intention des lecteurs européens (hors Royaume-Uni et Suisse) : Publié en Europe par MFS Investment Management (Lux) s. à r. l. (MFS Lux), une entreprise autorisée en vertu des lois du Luxembourg en tant que société de gestion pour les fonds domiciliés au Luxembourg, qui offre des produits et des services de placement aux investisseurs institutionnels. Le siège social de cette société à responsabilité limitée se situe au 4, rue Albert Borschette, Luxembourg L-1246. Tél. : 352 2826 12800. Le présent document est réservé aux investisseurs professionnels (dans la mesure où les organismes de réglementation locaux le permettent). On ne doit pas s'y fier et il ne doit pas être distribué si cela contrevient à la réglementation locale; **Singapour** – MFS International Singapore Pte. Ltd. (CRN 201228809M); **Australie/Nouvelle-Zélande** – MFS International Australia Pty Ltd (« MFS Australia ») (ABN 68 607 579 537) détient le permis numéro 485343 pour la prestation de services financiers en Australie. MFS Australia est régie par l'Australian Securities and Investments Commission; **Hong Kong** – MFS International (Hong Kong) Limited (« MIL HK »), entreprise privée à responsabilité limitée inscrite auprès de la Hong Kong Securities and Futures Commission (« SFC ») et réglementée par celle-ci. MIL HK est autorisée à exercer des activités réglementées de négociation de titres et de gestion d'actifs, et peut fournir certains services de placement à des « investisseurs professionnels » au sens de la *Securities and Futures Ordinance* (« SFO »); **pour les investisseurs professionnels en Chine** – MFS Financial Management Consulting (Shanghai) Co., Ltd. 2801-12, 28th Floor, 100 Century Avenue, Shanghai World Financial Center, Shanghai Pilot Free Trade Zone, 200120, Chine, une entreprise chinoise à responsabilité limitée réglementée pour fournir des services-conseils en gestion financière; **Japon** – MFS Investment Management K.K. est inscrite à titre d'opérateur d'instruments financiers, Kanto Local Finance Bureau (FIBO) No. 312, membre de l'Investment Management Association du Japon. Comme les frais assumés par les investisseurs varient selon les circonstances (produits, services, période de placement, conditions du marché, etc.), le montant total et les méthodes de calcul ne peuvent être indiqués à l'avance. Tous les placements comportent des risques, y compris les fluctuations de marché, et les investisseurs peuvent perdre le capital investi. Avant de faire des placements, les investisseurs devraient obtenir et lire attentivement le prospectus et les documents indiqués dans l'article 37-3 de la *Financial Instruments and Exchange Act*. **Pour les lecteurs en Arabie Saoudite, au Koweït, à Oman et aux Émirats arabes unis (à l'exclusion du centre financier international de Dubaï et du centre financier international d'Abou Dhabi). Au Qatar, réservé aux investisseurs avertis et aux particuliers fortunés. À Bahreïn, pour les investisseurs institutionnels seulement** : Les renseignements contenus dans le présent document sont strictement destinés aux investisseurs professionnels. Les renseignements contenus dans le présent document ne constituent pas et ne doivent pas être interprétés comme une offre, une invitation ou une proposition de faire une offre ou une recommandation de demander un produit, un service ou une stratégie de nature financière, ou un avis ou des conseils à cet égard. Même si nous avons pris grand soin de nous assurer que les renseignements contenus dans le présent document sont exacts, aucune responsabilité ne peut être assumée à l'égard de toute erreur ou omission ou de toute mesure prise sur la foi de ces renseignements. Vous ne pouvez reproduire, diffuser et utiliser le présent document (ou une partie de celui-ci) qu'avec le consentement de MFS international U.K. Ltd (« MIL UK »). Les renseignements contenus dans le présent document ne servent qu'à des fins d'information. Ils ne sont pas destinés au public et ne doivent pas être diffusés au public ni utilisés par celui-ci. Les renseignements contenus dans le présent document peuvent contenir des énoncés qui ne sont pas de nature purement historique, mais qui sont des énoncés prospectifs. Ceux-ci comprennent, entre autres, des projections, des prévisions ou des estimations de revenu. Ces énoncés prospectifs sont fondés sur des hypothèses, dont certaines sont décrites dans d'autres documents pertinents. Si vous ne comprenez pas le contenu du présent document, vous devriez consulter un conseiller financier autorisé. Veuillez noter que tous les documents envoyés par l'émetteur (MIL UK) ont été envoyés par voie électronique à partir de l'étranger. **Afrique du Sud** – Le présent document et les renseignements qu'il contient ne constituent pas une offre publique de titres en Afrique du Sud et, par conséquent, ne doivent pas être interprétés comme tels. Ce document ne doit pas être largement diffusé au public en Afrique du Sud. Le présent document n'a pas été approuvé par la Financial Sector Conduct Authority et ni MFS International (U.K.) Limited ni ses fonds ne sont enregistrés à des fins de vente au public en Afrique du Sud. Massachusetts Financial Services, Inc.^{MD}