

Opportunités et risques liés aux médias sociaux

Les médias sociaux représentent un outil puissant et permettent aux sociétés d'étendre la valeur de leur marque ; ils peuvent aussi ternir cette marque du jour au lendemain. Le monde compte plus de 18 plateformes de médias sociaux dont le développement est bien avancé et auxquelles les entreprises portent un intérêt croissant. Étant donné la visibilité, le risque, le suivi et les réponses en temps réel nécessaires pour gérer efficacement ces plateformes, les sociétés doivent établir d'importants protocoles destinés à leur utilisation afin d'y être présentes dans les meilleures conditions. Les sociétés qui utilisent ces plateformes doivent identifier les responsables appropriés et autorisés par leur service de communication afin de communiquer, d'initier, de fournir et/ou de publier des informations sur celles-ci. Il existe de nombreux facteurs de risque clés à aborder relatifs aux médias sociaux, mais également de nombreux avantages ou opportunités à saisir. Parmi les avantages et opportunités figurent (figure 1) :

- **Communiquer avec les clients**- La capacité de communiquer avec les clients est l'aspect le plus important des médias sociaux. Développer une marque et la promouvoir sur différents réseaux de médias sociaux peut créer une plus grande valeur et une meilleure connaissance de la marque.
- **Intelligence marketing**- Le marketing de médias sociaux offre à la société la possibilité de surveiller la marque et d'écouter ce que le public en dit. Les bénéfices qu'en tire la société en jouant un rôle plus important dans les médias sociaux sont une connaissance bien plus fine des informations qui circulent sur elle, ce qui peut avoir une valeur inestimable. Grâce à cela, la société peut améliorer son marketing, ses efforts de développement commercial et d'autres leviers de création de valeur pour renforcer sa compétitivité.
- **À l'écoute de la réputation de la marque**- Rester à l'écoute de la réputation et suivre les mesures faites sur les médias sociaux de la société est essentiel pour rester en tête dans la reconnaissance de la marque et identifier les signes de risque d'atteinte à la réputation.

Certains des risques (figure 2) les plus courants comprennent :

- **Risque d'atteinte à la réputation**- Les dommages à la réputation d'une société découlant d'un incident sur les médias sociaux peuvent faire plier une société, que ce soit son directeur général qui affirme quelque chose de controversé sur son compte Twitter ou une vidéo de salarié dénigrant

la société qui se propagerait. Selon un important éditeur, « Une crise liée à la réputation peut faire perdre des dizaines de millions d'euros de valeur à une société. Ce risque a augmenté car la montée des médias sociaux en ligne a pour conséquence de rendre les crises moins prévisibles, celles-ci pouvant se produire plus rapidement ».¹

- **Atteinte à la sécurité des données** - Selon une recherche de Forrester :

*De la reconnaissance au détournement de marque en passant par la coordination des menaces, les cybercriminels utilisent depuis des années les plateformes de médias sociaux pour augmenter l'efficacité de leurs attaques. Il est clair que le risque lié aux réseaux sociaux ne porte pas uniquement sur les dommages causés à la marque et à la réputation, mais constitue une menace de cybersécurité qui peut entraîner d'importantes violations de données, de nombreux problèmes de conformité et d'importantes pertes de revenus liées à la fraude et aux ventes de contrefaçon, avec une quantité d'autres risques.*²

- **Ingénierie sociale**- Les employés de la majorité des sociétés sont avisés et beaucoup ont une présence sur les réseaux sociaux, notamment sur des sites importants tels que Facebook, LinkedIn, Quora et Twitter. Chaque plateforme a le potentiel de fournir à un pirate informatique plusieurs points de données clés sur les employés. L'utilisation de ces mêmes données permet de pirater le compte de l'employé au niveau de l'entreprise par falsification et lancement d'une attaque d'ingénierie sociale sur la société. Eu égard à la multitude d'options pour passer par les comptes de réseaux sociaux avec des données exposées, les attaquants peuvent recueillir

Mohammed J. Khan, CISA, CRISC, CIPM

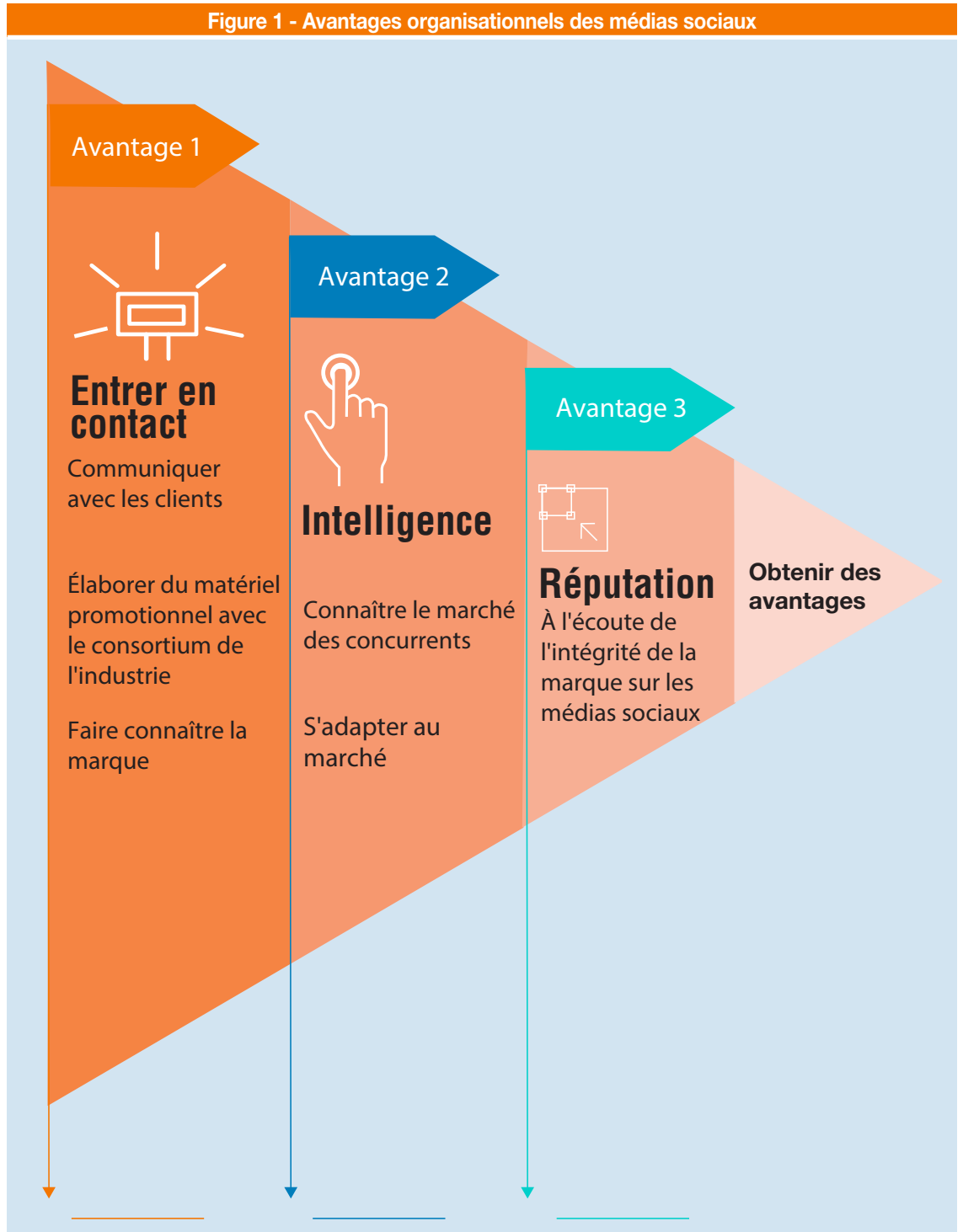
Est un directeur d'audit mondial chez Baxter International, une société mondiale de dispositifs médicaux et de soins de santé. Il affiche à son actif plus de 12 ans d'expérience axée sur la protection de la vie privée, la sécurité et la gouvernance de l'information. Plus récemment, il s'est concentré spécifiquement sur la cybersécurité des dispositifs médicaux, les cadres de protection de la vie privée au niveau mondial, et a aidé sa société à prendre des initiatives stratégiques et rentables dans les domaines de l'audit et de la conformité. Khan a travaillé auparavant pour une importante société de conseil en tant que professionnel de l'assurance et de conseil, et avant cela, il a travaillé comme un professionnel mondial de la planification des ressources et du business intelligence dans une importante société de technologie. Khan a aidé à développer et à publier plusieurs publications et les a présentées lors de conférences de l'industrie axées sur la vie privée et la cybersécurité.

Avez-vous des commentaires à faire sur cet article ?

Consultez les pages du *Journal* du site de l'ISACA® (www.isaca.org/journal), trouvez l'article et cliquez sur le lien Commentaires pour partager vos idées.

<http://bit.ly/2sUGrw7>

Figure 1 - Avantages organisationnels des médias sociaux



Source : M. Khan. Reproduction autorisée.

ces données pour accroître leurs progressions en matière de piratage dans les comptes.

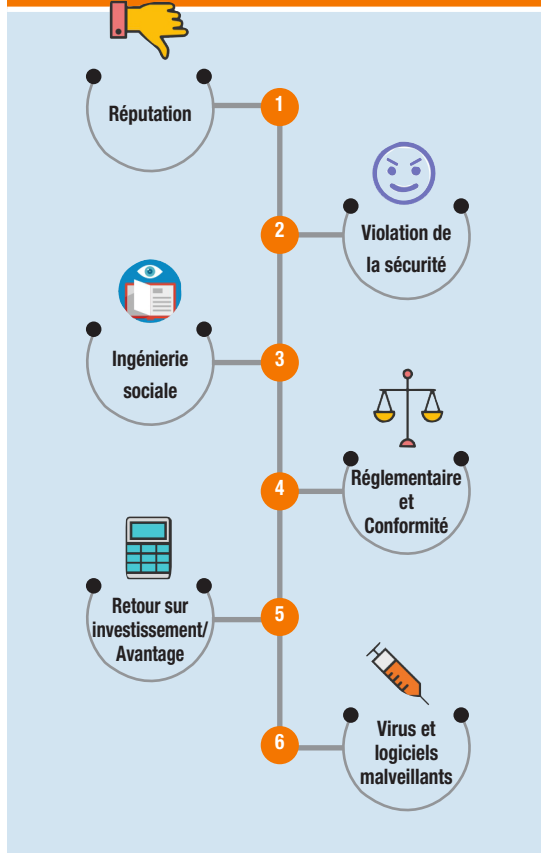
- **Violations réglementaires ou de conformité** : le nombre croissant de changements et de règlements relatifs à la protection de la vie privée à l'échelle mondiale a des répercussions sur la façon dont les données des clients sont utilisées dans l'espace des médias sociaux. Il existe quatre domaines clés à considérer :
 - Vie privée
 - Propriété du contenu
 - Atteinte à la propriété intellectuelle (PI)
 - Activités non autorisées
- **Conformité aux changements de l'environnement réglementaire**³: Ces changements réglementaires obligent la société à adapter sa stratégie si elle souhaite se conformer à l'échelle internationale. Cette approche, tout en étant nécessaire à une société qui utilise régulièrement les médias sociaux, peut entraîner une visibilité accrue de celle-ci auprès

“Les employés qui accèdent aux sites des médias sociaux peuvent agir comme ambassadeurs de la marque ; cependant, leur activité peut laisser entrer les virus et autres logiciels malveillants dans le réseau.”

des autorités.

Certains secteurs d'activité et certaines sociétés peuvent craindre cette situation compte tenu des audits réglementaires. Ceci est dû à leur forte exposition sur ces plateformes de

Figure 2 - Facteurs de risques liés aux médias sociaux



Source : M. Khan. Reproduction autorisée.

médias sociaux.

- **Retour sur investissement** : le bénéfice de la présence sur les médias sociaux pour une société est difficile à estimer et très subjectif. Le rapport risque/bénéfice, par conséquent, ne peut pas être calculé facilement, ce qui rend discutable la décision d'entrer dans l'espace des médias sociaux pour certaines sociétés.
- **Hameçonnage** : l'une des techniques populaires utilisées par les criminels consiste à inciter les individus à divulguer des renseignements personnels tout en se présentant comme un représentant fictif d'un professionnel ou d'une société légitime. Cette technique est l'élément clé pour collecter des données personnelles sur des personnes ou des organisations à des fins financières. En raison du manque de connaissance des techniques d'hameçonnage utilisées par les pirates

Cet article vous a plu ?

- Consultez le centre de connaissances pour obtenir plus d'informations, travailler en collaboration et entamer des discussions sur la gestion des risques et sur les audits/la surveillance continue.
www.isaca.org/risk-management





informatiques, les employés sont victimes de courriers électroniques, d'appels téléphoniques et de sites Web, ce qui entraîne une exposition accrue aux risques au niveau de l'entreprise.

• **Virus et logiciels malveillants :**

La capacité des pirates à pénétrer dans le réseau de l'organisation via des sites et des comptes de médias sociaux dangereux ouvre un nouveau vecteur de menace. D'une part, les employés qui accèdent aux sites des médias sociaux peuvent agir comme ambassadeurs de la marque ; cependant, leur activité peut laisser entrer les virus et autres logiciels malveillants dans le réseau. Selon les experts en sécurité, « Une majorité d'attaques actuelles utilisent simplement les plateformes sociales comme mécanisme de livraison, et ont été conçues dans la suite de l'ancien logiciel malveillant Koobface. »⁴

Prévenir les risques liés aux médias sociaux

Certaines sociétés s'efforcent de développer la meilleure solution pour gérer les risques liés aux réseaux sociaux. La première question à poser est qui, en fait, possède les plateformes de médias sociaux pour la société et, plus important encore, la gouvernance globale des médias sociaux des employés. Les médias sociaux ont des répercussions sur tous les services de la société, et chaque service, qu'il s'agisse de l'informatique, des finances, du marketing ou des ressources humaines (RH), a une vision différente de la façon dont les médias sociaux peuvent être ou seront utilisés par le service au nom de la société. Aucun règlement prescrit n'existe pour

éliminer les risques liés aux médias sociaux ; cependant, voici certains domaines clés à prendre en compte pour prévenir les risques liés aux médias sociaux :

- **Lignes directrices :** en tant que bonne pratique, une politique générale de haut niveau doit être mise en place pour guider l'utilisation des médias sociaux par tous les employés de la société et tout tiers agissant en son nom. Ces lignes directrices doivent mettre en évidence les composants clés, comprenant :
 - **L'étendue et le périmètre :** définir la portée globale des lignes directrices de la politique établies par l'entreprise pour ses employés
 - **La finalité :** définir le but des lignes directrices pour la société, en particulier les modalités selon lesquelles les activités portées sur les médias sociaux auront lieu, ainsi que le type d'information à partager via ces activités
 - **Les objectifs :** définir clairement le résultat global qui doit être obtenu via cette présence sur les médias sociaux pour la société et la façon dont la plateforme des médias sociaux va permettre à la société d'y parvenir
 - **Les lignes directrices sur la propriété :** lignes directrices générales pour la création et la maintenance de tous les sites

“ Un plan de communication et de crise pour les médias sociaux solide doit être développé en cas de crise. ”

- de médias sociaux pour la société
- **Lignes directrices pour les contributeurs :** lignes directrices générales et principes régissant les contributeurs aux sites de médias sociaux
- **Plateformes de médias sociaux approuvées :** définition des attentes par les services qui évaluent les solutions de médias sociaux en dehors de la société pour démontrer comment la présence sur les médias sociaux contribuera

à la réalisation de l'objectif global de l'entreprise et, plus important encore, au degré d'utilisation et de sécurité de la plateforme

- **Formation et sensibilisation** : il est essentiel que la société incarne l'utilisation correcte de l'étiquette des médias sociaux lors de la formation d'intégration de tous les employés, en particulier dans des postes tels que les services marketing, ressources humaines et informatique qui représenteront la société dans leurs fonctions. Inculquer les bons comportements ainsi que les concepts des normes relatives aux médias sociaux qui s'alignent sur les politiques et aux processus organisationnels aideront à long terme, puisque de plus en plus d'employés participent sur les réseaux sociaux et représentent leur société, ses produits et ses intérêts.

- **Plan de communication et de crise pour les médias sociaux** : un plan solide de communication et de crise pour les médias sociaux doit être développé en cas de crise. Pour toutes les communications avec les médias et les parties prenantes, il doit y avoir un seul point de contact, généralement l'équipe de communication. Le personnel du service impacté doit être impliqué, bien entendu.

Il est essentiel de mettre en pratique le plan, notamment pour tester l'exécution des tâches préparées à l'avance qui seraient requises le cas échéant, en vue d'un contrôle progressif de la crise qui pourrait arriver à toute société, à mesure que sa présence sur les médias sociaux augmente avec le temps. Un tel dispositif demande beaucoup de collaboration et de communication entre les principaux services tout au long de l'année.

Conclusion

Les sociétés qui prévoient d'augmenter ou de diminuer leur présence sur les médias sociaux devraient être sensibilisées et faire preuve de vigilance. Il peut y avoir divers avantages et inconvénients pour une société à saisir les opportunités offertes par les plateformes de médias sociaux. Les sociétés qui envisagent de se lancer sur ces plateformes doivent mettre en place une politique et un plan de communication clairement définis. Il est nécessaire de tenir compte des facteurs appropriés pour une bonne gouvernance, un plan de communication en cas de violation, une politique d'utilisation des médias sociaux et des outils de suivi, qui sont tous importants pour atténuer les risques liés aux réseaux sociaux au niveau de l'entreprise.

Décider quels réseaux de médias sociaux utiliser, les évaluer et les gérer de manière évolutive au fil du temps est essentiel. La première étape consiste à comprendre les avantages et les inconvénients tout en gardant à l'esprit les mesures de base à prendre pour atténuer les risques.

Notes de bas de page

- 1 Spanier, G.; "Reputational Risk in the Social Media Age," *Raconteur*, 11 juin 2015, <https://www.raconteur.net/business/reputational-risk-in-the-social-media-age>
- 2 Hayes, N.; "Why Social Media Sites Are the New Cyber Weapons of Choice," *DarkReading*, 6 septembre 2016, www.darkreading.com/attacks-breaches/why-social-media-sites-are-the-new-cyber-weapons-of-choice/a/d-id/1326802
- 3 McNickle, M.; "5 Keys to the Legal Issues of Social Media in Healthcare," *Healthcare IT News*, 2 juillet 2012, www.healthcareitnews.com/news/5-keys-legal-issues-social-media
- 4 McAfee, "How Cybercriminals Target Social Media Accounts," <https://www.mcafee.com/us/security-awareness/articles/how-cybercriminals-target-social-media-accounts.aspx>