Violation de données, bien gérer la crise pour limiter les pertes

Mars 2018, le scandale Cambridge Analytica fut lourd de conséquences pour Facebook : un cours de bourse qui dévisse de 8 milliards de dollars, une perte de confiance de 40 % des internautes, la suppression de millions de profils utilisateurs privant le réseau social de revenus publicitaires immédiats.

Cette actualité nous enseigne que les impacts d'une violation de données ne se bornent pas à une sanction financière. Ils sont vastes et s'appliquent sur le long terme : perte de confiance des clients, utilisateurs, partenaires, impactant l'activité, voire la pérennité de l'entreprise.

Une réalité comprise par la chaîne hôtelière Marriott, qui face à une violation massive de données a déployé une stratégie de communication particulièrement efficace. En effet, lorsque la presse a titré le vol d'informations confidentielles de près d'un demi-milliard de clients du réseau d'hôtels Starwood, Marriott avait déjà déployé des mesures concrètes de communication et de réduction des impacts : communiqué expliquant les faits, création d'un centre d'appels et d'un site Internet dédié permettant aux clients de savoir s'ils ont été touchés.

Le RGPD, facteur de l'aggravation du risque réputationnel et business

Ces violations de données ont éclaté dans un contexte très suspicieux quant à l'utilisation des données mais aussi dans un contexte médiatique très dynamique, après l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD). Dorénavant, tout incident portant atteinte à la vie privée de résidents européens est sujet à une couverture médiatique sans commune mesure avec ce qu'elle n'était sous l'ère de la loi Informatique et Libertés de 1978.

Plus encore, elles apparaissent dans un contexte sociétal où la protection des datas devient une préoccupation majeure. D'après une étude : « En 2017, 85 % des Français se disent préoccupés par la protection de leurs données personnelles en général, soit une augmentation de 4 points par rapport a? 2014 ».

La gestion de crise, composant incontournable de la réponse à une violation de données

Sur la route, attacher sa ceinture n'empêchera pas l'accident mais en limitera l'impact. De même, se doter d'un dispositif de gestion de crise n'empêchera pas la survenance d'une violation de données mais en minimisera les conséquences.

Anticiper est donc le mot d'ordre. Il faut identifier des scenarii de crise pour déterminer les capacités opérationnelles nécessaires et les actions de remédiation associées. Il est aussi capital d'intégrer une stratégie de communication de crise, vous conférant un avantage stratégique majeur : contrôler l'espace médiatique en s'exprimant le premier, limitant les conséquences sur votre activité et réputation.

Enfin, tester votre plan de gestion de crise est une condition sine qua non à la coordination des équipes et à la prise de décision : la pertinence et l'exactitude des informations remontées aux directeurs et COMEX permettront de déployer des mesures adaptées.

À l'heure où le risque réglementaire induit indubitablement le risque réputationnel, il est vital de connaître le niveau réel d'exposition et de vulnérabilité de votre organisation, qu'il s'agisse de vos pratiques marketing ou de la sécurité effective des données personnelles dont vous avez la responsabilité. Sans cela, toute organisation devra subir ce que les États et armées appellent la surprise stratégique. Pour paraphraser le Général d'Armée Pierre de Villiers, elle est l'apanage de ceux qui n'ont pas su prévoir. Ceux finalement qui se sont refusés à prévoir et imaginer les scénarii les plus imprévisibles.