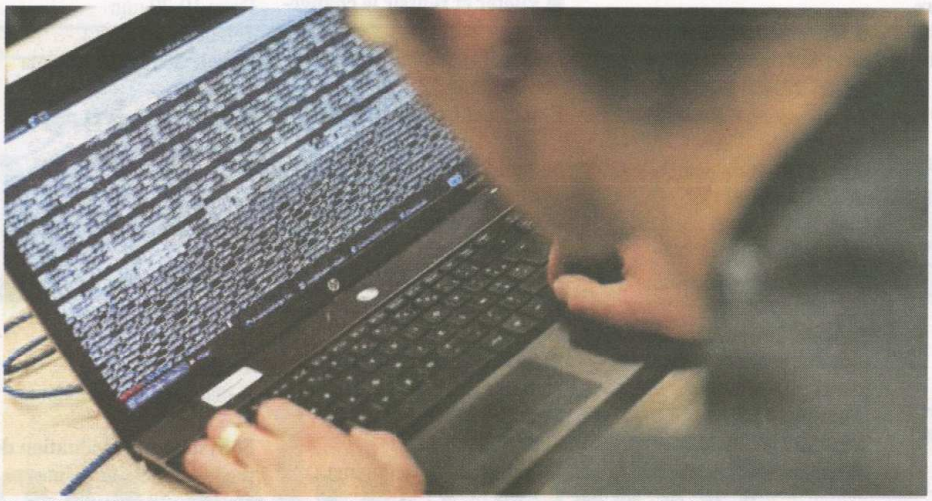
Insécurité numérique

Les nouvelles armes des dircoms

L'émergence du numérique et la démocratisation des technologies poussent les responsables de la communication à travailler dans un nouvel environnement qui bouleverse leurs habitudes et transforment leur métier. Une nouvelle génération de risques tels que l'usurpation d'identité corporate ou encore les attaques de données personnelles émerge et peut avoir des retombées désastreuses sur la bonne santé de l'entreprise ainsi que sur sa réputation. Pour y faire face, les dircoms peuvent désormais faire usage de nouveaux outils visant à sécuriser l'information propre au groupe, mais doivent également sensibiliser les salariés sur les risques du tout-numérique. Oubliez donc vos clichés sur la gestion communicationnelle traditionnelle des crises et découvrez les nouveaux enjeux virtuels de cette pratique grâce à Raja Bensaoud, enseignante en droit des affaires et communication stratégique.



La globalisation des technologies expose les responsables de la communication à de nouveaux types de risques tels que l'usurpation d'identité corporate ou encore les attaques de données qui peuvent avoir des retombées désastreuses sur l'entreprise et sur son image. Pour y faire face, les dircoms peuvent recourir à de multiples outils afin d'automatiser un maximum de tâches. Le plus connu d'entre eux, baptisé multiposting, diffuse plusieurs canaux numériques à la fois, ce qui réduit l'exposition au piratage de l'information.

Raja Bensaoud, enseignante en droit des affaires et communication stratégique (Ph. R.B.)

■ Une menace réelle pour les entreprises

La digitalisation expose les entreprises à bon nombre de risques pouvant menacer directement ou indirectement leurs dispositifs de communication. Il peut tout d'abord s'agir de diffusion d'informations erronées ou trompeuses (fake news) visant à tromper les agences de presse et les internautes pour ternir la réputation du groupe. Elles prennent le plus souvent la forme de faux communiqués ou d'un post sur les réseaux sociaux. Le danger peut également provenir d'attaques ciblant des données confidentielles concernant un secret de fabrication ou encore des algorithmes de brevets. Les responsables com doivent également se méfier des détournements de logo appelés «Logobusting» mais également des «bad buzz» qui ont la particularité de se propager rapidement.

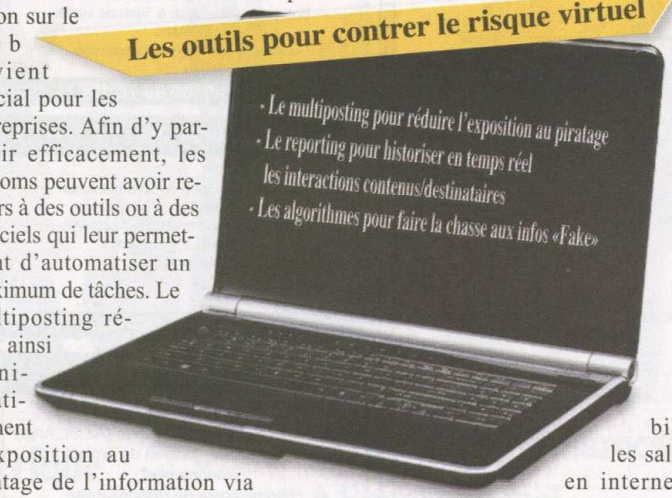
L'avis du spécialiste: Ces situations peuvent avoir de lourdes retombées sur le business de l'entreprise et sur sa réputation. La société peut ainsi perdre des clients ou encore souffrir de l'arrêt de fonctions opérationnelles. Par ailleurs, la restauration des données et le «retour à la normale» peut engendrer des dépenses supplémentaires ainsi qu'une perte de temps considérable.

■ De multiples outils pour préserver l'information

Dans un contexte aussi virulent, surveiller sa communication et sa réputation sur le web devient crucial pour les entreprises. Afin d'y parvenir efficacement, les dircoms peuvent avoir recours à des outils ou à des logiciels qui leur permettront d'automatiser un maximum de tâches. Le multiposting réduit ainsi significativement l'exposition au piratage de l'information via la diffusion de plusieurs canaux numériques à la fois tels que le mailing ou encore les réseaux sociaux à travers des plateformes comme Wiztopic. Pour garantir une traçabilité sécurisée des données du groupe, les responsables de la communication peuvent faire appel à des outils de reporting capables d'historiser automatiquement et en temps réel les interactions entre les contenus et leurs destinataires. Enfin, des algorithmes spécifiques peuvent être utilisés afin de «trier» l'information et de repérer puis supprimer les infos «fake». Des applications dans ce sens sont déjà proposées par Facebook ou encore LinkendIn.

L'avis du spécialiste: Au-delà de l'aspect purement technique, les dircoms ont clairement un rôle à jouer dans cette lutte contre le piratage des bases de données. Les responsables en communication des entreprises doivent en effet sensibiliser les salariés en interne sur les risques du numérique. Il s'agit, entre autres, d'attirer l'attention du personnel sur le caractère sensible de certaines données. C'est également à eux qu'incombe la lourde tâche de former les employés sur l'utilisation des réseaux sociaux et de les prévenir de l'usage abusif et inapproprié de ces espaces d'expression. Les dircoms peuvent enfin occuper la fonction de gestionnaires de communication de crise en cas de cyber-attaque, en ayant pour mission de rassurer les publics externes ainsi que les salariés.

Les outils pour contrer le risque virtuel



■ Les PME particulièrement exposées aux risques

Le danger du tout-numérique est présent partout dans le monde. En Maroc, la menace guette avant tout les PME, sous équipées en matière de sécurité informatique. Ces dernières ne disposent en effet pas d'une infrastructure technique capable d'assurer une veille de manière permanente. Les autres entreprises ne sont pas non plus totalement hors de danger puisque le nombre de celles certifiées ISO 27002 – ce qui représente la norme en matière de sécurité des systèmes d'information – demeure encore à l'heure actuelle particulièrement faible. Pour changer la donne, le ministère du Commerce et la CGEM organisent régulièrement des rencontres de sensibilisation dans ce sens.

L'avis du spécialiste: Les réseaux d'information de toute entreprise, quelle que soit son implantation géographique, peuvent à tout instant devenir la cible de «cyber-malveillance». En effet, les outils d'attaque sont désormais accessibles avec une facilité déconcertante. Ainsi, des logiciels de piratage sont partout commercialisés et des cyber-pirates peuvent être «loués» à l'heure. Le Maroc n'échappe pas à ce phénomène international, même si, à l'heure actuelle, il n'existe pas encore de statistiques concrètes sur cette tendance.

■ Une démarche pas totalement fiable

Les outils numériques utilisés par la fonction «communication» d'une entreprise pour lutter contre les dangers du digital présentent des vulnérabilités. Ils ne sont pas techniquement fiables à cent pour cent. D'autant plus qu'ils reposent en grande partie sur le comportement des salariés utilisateurs, qui n'ont pas toujours conscience des risques encourus.

L'avis du spécialiste: L'antidote absolu et parfait n'existe pas en termes de piratage des données d'information d'une entreprise. Les dircoms ne sont par ailleurs pas tous des ingénieurs en informatique et il existera toujours des hackers pour pratiquer la malveillance.❑

K. A.