Cyberattaques : les dirigeants face à leurs responsabilités

VALÉRIE LAFARGE-SARKOZY ET CÉLIA HAMOUDA
Avocate associée du cabinet Altana, expert du Club des juristes. Avocate chez Altana.

Nul ne peut plus l'ignorer : la transformation numérique offre aux entreprises un formidable levier de croissance en même temps qu'elle induit une prolifération de nouveaux risques aux conséquences économiques, juridiques et réputationnelles majeurs.
Les attaques récentes, telles que WannaCry et NotPetya, sont autant de manifestations de la menace que fait peser le risque cyber sur les entreprises. Elles mettent en exergue la nécessité pour celles-ci, et ce quelle que soit leur taille ou leur activité, d'adapter continuellement leur niveau de protection afin de limiter la vulnérabilité de leurs systèmes d'information.
Si des failles de sécurité rendues publiques nuisent nécessairement à l'entreprise, comme l'a démontré l'affaire Yahoo!/Verizon (pour rappel, le vol de millions de données à Yahoo! avait conduit Verizon à réduire son offre de rachat de ses activités Internet de 350 millions d'euros), des politiques cyber éprouvées se révèlent être, a contrario, de réels éléments de valorisation de l'entreprise, notamment dans la réalisation d'une opération de M&A.
Ce besoin de cybersécurité se fait, par ailleurs, d'autant plus pressant que l'absence de mise en conformité avec les obligations bientôt imposées par le èglement général sur la protection des données à caractère personnel (le RGPD) et la directive sur la sécurité des réseaux et des systèmes d'information (directive NIS) pourra s'avérer particulièrement coûteuse.
Les politiques de cybersécurité mises en place n'en seront que davantage scrutées et analysées.
Les entreprises qui seront jugées responsables d'atteintes à la sécurité des données personnelles s'exposeront à des sanctions pécuniaires pouvant atteindre 10 millions d'euros ou 4 % du chiffre d'affaires annuel. En outre, la généralisation des obligations de notification en cas de faille de sécurité – et notamment l'introduction de l'obligation d'informer les tiers d'une violation de données les concernant – entraînera nécessairement des conséquences financières et réputationnelles.
Les tiers victimes qui auront eu connaissance de cette violation par le biais de cette notification pourront, en outre, mettre en cause la responsabilité de l'entreprise victime de l'attaque pour demander la réparation de leur préjudice.
Par ailleurs, les cyberattaques sont par nature susceptibles de causer des dommages en cascade à la « supply chain ». Les cocontractants pourront alors se prévaloir de possibles manquements aux nouvelles obligations mises à la charge du responsable de traitement et du sous-traitant pour rechercher la responsabilité contractuelle de l'entreprise.
Les dirigeants ne peuvent plus, par conséquent, ignorer l'urgence de doter leurs entreprises d'une politique de cybersécurité efficace, efficiente et respectueuse de l'impératif de protection des données. Ne pas le faire pourrait être constitutif d'une faute de gestion engageant leur responsabilité si un tel manquement impactait significativement les résultats, voire la pérennité de la société. ■