PRÉFACE

En cette ère où les crises cybernétiques s'intensifient en fréquence et en complexité, elles ne se contentent plus d'être des probabilités lointaines ; elles sont devenues une fatalité inéluctable. La véritable interrogation se pose désormais autour de l'instant de leur survenue.

Je tiens à distinguer nettement ces crises cyber des innombrables incidents journaliers affectant les grandes entreprises. Elles ne sauraient être confondues avec les cyberattaques, désormais monnaie courante, presque ironiquement banales, tant pour les entités privées que pour les organismes publics, sans égard à leur envergure.

Ces crises cyber, dans leur particularité, se manifestent au moment où une attaque numérique submerge nos défenses – habituellement robustes –, franchissant les seuils critiques de nos organisations, et s'accompagnent même parfois d'un retentissement médiatique planétaire. Elles génèrent des conséquences financières, réputationnelles et humaines d'ampleur considérable.

Mon intention n'est pas de provoquer une terreur infructueuse, mais plutôt d'inciter à une vigilance constructive et bénéfique. Les experts en résilience, qu'ils s'orientent vers le cyber ou non, ne se drapent pas dans le manteau de la crainte, sachant pertinemment son effet contre-productif à long terme. Il convient toutefois de rappeler la malignité croissante des activités cybernétiques (cybercriminalité, attaques étatiques, hacktivisme) et le développement continu de leur portée à l'échelle mondiale. La plupart de nos systèmes numériques, sur lesquels repose notre interdépendance collective, ont été conçus davantage pour l'efficacité que pour la résilience, alors même que les assaillants, toujours plus structurés, ont presque normalisé le chantage aux données sensibles, d'une rentabilité extrême.

Il existe une responsabilité tacite qui nous incombe en cas de crise cyber : rendre des comptes non seulement aux collaborateurs, mais

aussi aux investisseurs, aux clients, à un cercle bien plus large de parties prenantes. Les répercussions ne se limitent pas au numérique ; l'ampleur des impacts réputationnels et financiers est souvent décuplée par le vecteur et la nature de l'attaque. Bien que d'origine discrète, souvent isolée et géographiquement éloignée, une cyberattaque peut engendrer une crise aux conséquences dévastatrices. Le paradigme dans lequel nous évoluons redéfinit les échelles de probabilité, les rapports de force et les risques associés.

Face à ces particularités devenues des paradigmes, la préparation à la crise cyber est d'une importance capitale. Si anticiper le pire n'est jamais agréable, la nature de nos activités rend cette démarche indispensable. Se préparer à une crise cyber va au-delà des bonnes intentions. Pour rehausser le niveau de cybersécurité de votre organisation, développer une mémoire procédurale adaptative face aux crises cyber, il est essentiel de concevoir un plan stratégique et de vous entourer d'une équipe d'experts qui l'orchestrera et vous accompagnera durablement. Cela inclut la vérification régulière des vulnérabilités techniques et humaines, la conception d'un plan de réponse d'urgence, le maintien de compétences techniques à la pointe, la sensibilisation continue des collaborateurs, la préparation de la direction générale à naviguer avec assurance en pleine tempête…

La crise cyber est un phénomène étonnant, surprenant, perturbant, lié à notre dépendance croissante au numérique. Elle incarne à la fois un moment d'effervescence redoutable et un silence absolu. Sa gestion, bien que partageant des similitudes avec celle des crises traditionnelles, s'en écarte considérablement en raison de la nature intelligente de la menace, du rapport au temps et des particularités de la communication de crise.

Pour que le numérique demeure un vecteur d'innovation positive, nous devons nous tenir prêts. Convenons ensemble qu'il est préférable de posséder des compétences exceptionnelles, même si elles ne sont que rarement sollicitées, que d'être désarmés au moment où nous pourrions amèrement regretter de ne jamais y avoir pensé.

Imade Elbaraka
Cyber Practice Managing Partner
Deloitte France et Afrique francophone