LAETITIA AVIA

Avocate en droit du numérique

& MARIE SALIGNAT

Juriste, Cabinet AVIA Paris.

GOUVERNANCE DE LA CYBERSÉCURITÉ : COMMENT LA TECHNIQUE DEVIENT L'ENJEU STRATÉGIQUE DES ENTREPRISES EUROPÉENNES

EN EUROPE, LA CYBER A CHANGÉ DE STATUT : IL NE S'AGIT PLUS D'UNE AFFAIRE D'INGÉNIERIE, DE TECHNIQUE, RÉSERVÉE À QUELQUES SACHANTS QUI PARLERAIENT UN JARGON RÉSERVÉ À LEUR ÉCOSYSTÈME.

La cyber est maintenant un élément clef de la conformité et une affaire stratégique, de gouvernance.

Avec NIS2, DORA, le Cyber Resilience Act, ou encore le Cybersecurity Act, la cyber a pris quelques jalons pour atterrir sur le bureau du top management. Il ne suffit plus d'annoncer être conforme ; il faut savoir démontrer que la sécurité est non seulement mise en œuvre mais aussi comprise, organisée, pilotée, mesurée, documentée et améliorée en continu.

Trois dynamiques expliquent ce changement de paradigme. D'abord, la menace : les attaques se multiplient et se professionnalisent, elles visent autant les systèmes que les processus et l'organisation. Ensuite, **les dépendances :** cloud, prestataires IT, solutions SaaS, bibliothèques open source, sous-traitants, interconnexions… Souvent, la faille "naît" hors de l'entreprise, dans la chaîne de fournisseurs. Enfin, **la dimension systémique :** une interruption majeure ne touche plus seulement une DSI ; elle peut affecter toute une chaîne de valeur et des services essentiels.

C'est pourquoi la cyber devient un enjeu de confiance pour et envers les clients et partenaires.

Le RGPD avait déjà installé l'accountability au cœur de la conformité. Les dernières réglementations européennes viennent renforcer cette exigence en l'ancrant au niveau du **top management :**

- NIS2 exige ainsi que les organes de direction approuvent les mesures de gestion des risques, en supervisent la mise en œuvre et veillent à la formation des dirigeants.
- DORA formalise une logique comparable : l'organe de direction doit définir et approuver le cadre de gestion du risque lié aux technologies de l'information, piloter son déploiement, puis le réexaminer régulièrement

Les sanctions changent également de nature : au-delà des sanctions financières pour la société, ce sont également les gérants qui peuvent être poursuivis **pour faute de gestion** et se voir interdire d'exercer ces fonctions à l'avenir… D'où la nécessité pour eux de se saisir pleinement du sujet.

Une bonne gouvernance s'articule autour de cinq exigences concrètes.

Piloter : il est essentiel de mettre en œuvre une organisation claire, reposant sur des responsabilités précisément définies et une fonction de pilotage pérenne identifiée, capable de coordonner la DSI, le RSSI, la direction juridique et la direction des risques, d'aligner les priorités et de garder le top management constamment informé.

Maîtriser la gestion du risque : il ne s'agit pas ici d'assurer une absence de risques, mais de savoir comprendre et expliquer (i) ce que l'on protège, (ii) contre quelles menaces, (iii) avec quelles priorités et (iv) selon quelle proportionnalité.

Documenter et contrôler le risque cyber : une politique interne ne vaut rien si elle n'est pas formalisée, appliquée et vérifiable. In fine, le régulateur comme les partenaires exigeront des preuves opérationnelles : contrôles réalisés, indicateurs, tests, exercices de crise, audits et plans d'action suivis jusqu'à leur clôture. On passe ainsi d'une conformité déclarative à une conformité prête à être contrôlée, et facteur de confiance.

Maîtriser les dépendances : prestataires, cloud, logiciels, sous-traitants et chaîne d'approvisionnement sont tous susceptibles de générer un risque cyber et doivent par conséquent être intégrés dans la politique de conformité de l'entreprise. Cela implique une gestion rigoureuse des tiers, car les compromissions viennent souvent d'un maillon faible.

Sensibiliser et former : la cyber doit intégrer la culture interne de l'entreprise, du conseil d'administration au personnel d'accueil en passant par les différents corps de métiers techniques, opérationnels, administratif, le personnel d'entretien etc. C'est ce qui en fait un enjeu stratégique. Bien évidemment, une formation réussie repose sur un processus continu : former, répéter, tester, intégrer les retours d'expérience, et mettre à jour au fil des évolutions réglementaires et des incidents.

Ces cinq exigences répondent aux besoins des principaux textes applicables et sont, si elles sont bien mises en œuvre, suffisantes pour garantir une bonne gouvernance du risque cyber dans le temps.

Après l'avalanche réglementaire, Bruxelles affiche désormais un objectif de rationalisation : révision du « Cybersecurity Act », mesures de simplification, Digital Omnibus... Est-ce que cela veut dire que tout ce qui a été mis en place aura été vain ? Non. Car ni le risque cyber ni le niveau d'exigence ne reculeront. En revanche, cette évolution réglementaire rappelle que l'enjeu n'est pas seulement de déployer des mesures, mais de savoir décider, contrôler et rendre compte de sa résilience numérique pour l'adapter aux besoins réels.

C'est pourquoi la bonne gouvernance des enjeux cyber repose avant tout sur leur pleine maîtrise, et transforme une exigence de conformité règlementaire en avantage stratégique. ■

il faut savoir démontrer que la sécurité est non seulement mise en œuvre mais aussi comprise, organisée, pilotée, mesurée, documentée et améliorée en continu.