ADMINISTRATRICES
ET ADMINISTRATEURS
ENGAGÉS

LES GUIDES DE L'**IFA**

MEMBRES DU GROUPE DE TRAVAIL :
Marie-Noëlle Brisson
Damien Chaminade
Christine Dubus
Nathalie Kestener
Anne-Hélène Monsellato
Marie-Hélène Rigal

AUDITIONS :
Vincent Loriot, ANSSI
Lumena Duluc, CLUSIF
Henri d'Agrain, CIGREF
Christian Poyau, ex-président de la commission,
co-président de la commission mutations technologiques
et impacts sociétaux du MEDEF

« L'IFA a décidé d'enrichir les compétences des administrateurs quant aux enjeux de transformations numériques et technologiques à travers la parution de deux guides, l'un portant sur la cybersécurité et l'autre sur l'intelligence artificielle. En effet, au-delà d'en être des actifs stratégiques, les données sont devenues pour toutes les organisations un sujet dont les conseils d'administration doivent s'emparer sous l'angle de la stratégie en général et numérique en particulier.

L'accélération de la digitalisation, mais également la pression réglementaire, conduisent à faire grandir la responsabilité des administrateurs, notamment sur l'impact des choix stratégiques, mais également en termes de surveillance des risques et des moyens alloués.

La formation constitue un outil majeur de compréhension, nécessaire à toute prise de décision éclairée et collégiale que l'IFA se propose ici de compléter prochainement avec un guide sur la gouvernance des données, indispensable pour contribuer à la qualité et la protection des données, s'interroger sur les données sensibles et leur exploitation dans un cadre souverain. »

SYNTHÈSE

La responsabilité des conseils d'administration sur les enjeux de sécurité numérique s'accroît rapidement dans un contexte global en constante évolution, qui se complexifie chaque jour un peu plus sur les plans réglementaire, géopolitique et technologique.

Organiser la gouvernance sur ces enjeux devient impératif, en veillant à former régulièrement les administrateurs à porter le sujet aux débats du conseil, directement, ou par l'intermédiaire d'un comité spécialisé ou d'un administrateur désigné. Au-delà d'une simple sensibilisation, il s'agit de donner la capacité aux administrateurs à interagir de façon concrète et poussée, au bon niveau, avec des experts opérationnels (RSSI, DSI, Directeurs Sûreté) et des experts risques et conformité de l'entreprise. Dans certains cas d'exposition jugée forte de la société, intégrer une expertise extérieure ou un administrateur ayant suivi un parcours certifiant permettra clairement de renforcer les compétences du conseil.

La sécurité numérique est un enjeu stratégique majeur pour le conseil d'administration et facilite une approche pratique de la gouvernance des données, depuis leur création jusqu'à leur destruction. Ce processus inclut la qualification des données (par exemple, sensibles ou critiques), leur fiabilisation, utilisation, traitement et stockage, soulignant ainsi l'importance de l'empreinte carbone associée. La gouvernance des données est la pierre d'angle de la digitalisation pour envisager de pouvoir réellement tirer parti de l'intelligence artificielle.

Le conseil doit clairement exprimer et formaliser son implication sur les sujets de sécurité numérique dans un dialogue avec la direction générale, et s'assurer de l'implication et de la solidité de cette dernière dans la mise en place et le déploiement du plan cyber.

La réflexion du conseil sur ce sujet doit s'articuler autour de trois axes majeurs pour assurer d'une préparation solide à tous les niveaux. Parce que la question de l'intrusion n'est plus de savoir si, mais quand elle va se produire, et qu'une crise ne se prépare pas le jour d'un incident critique, le conseil doit questionner comment la direction générale : 1) structure ses actions de prévention de façon dynamique (moyens techniques, organisationnels, financiers et humains sur l'identification et le suivi des risques et du contrôle interne, ainsi que la formation) ; 2) a anticipé et organisé le pilotage de crise

en gestion d'une attaque (les bons réflexes) et bâti son plan de reprise de l'activité ; et 3) quelles considérations elle a donné à une assurance cyber.

Le cadre existant doit être adapté avec la mise en place d'une démarche structurée. En effet, la cybersécurité met en exergue des outils jusqu'alors peu connus : la gouvernance des données, l'analyse de risques cyber, la gestion de crise, le plan de reprise d'activité, les tests d'intrusion, les scans de vulnérabilité, pour n'en citer que quelques-uns. Le conseil doit donc s'approprier ces outils et ces nouveaux processus, d'autant plus que certains sont exigés par les référentiels de conformité (ex. NIS2, RGPD).

Loin de n'être que dans le seul débat technique, les discussions autour des enjeux de cybersécurité construisent une autre forme de résilience de l'entreprise, toute aussi majeure, en ouvrant sur une véritable stratégie digitale et de la donnée et, partant, un nouveau champ d'opportunités possible.

SOMMAIRE

Access full guide (opens new website) https://www.ifa-asso.com/mediatheques/guide-securite-numerique-et-gouvernance-english/?cat=363

View Guide launch on YouTube (in French). https://www.youtube.com/watch?v=0rZT9eX-Gzw