La force de l'engagement[MD]

ARTICLE D'EXPERT

Gouvernance de la sécurité des systèmes d'information : un facteur clé de succès pour les organisations

Assurer la sécurité des systèmes d'information dans une grande organisation est un véritable défi. Seule une bonne gouvernance est à même de rassurer la direction générale, les clients et partenaires, les actionnaires et in fine le grand public. Comment définir une gouvernance adaptée ? Quels sont les prérequis à sa mise en œuvre ? Et pourquoi est-il primordial de développer une vision opérationnelle claire ? Les réponses à toutes ces questions dans cet article.

LA SÉCURITÉ, UN SUJET TRANSVERSE

L'expérience montre que la sécurité des systèmes d'information n'est pas qu'une question technique ou qu'un sujet d'organisation et/ou de communication. Au sein d'un grand groupe ou même dans une société aux responsabilités réparties, il est essentiel de mettre en place une gouvernance de la sécurité adaptée à la culture de l'organisation, capable de fédérer l'ensemble des actions.

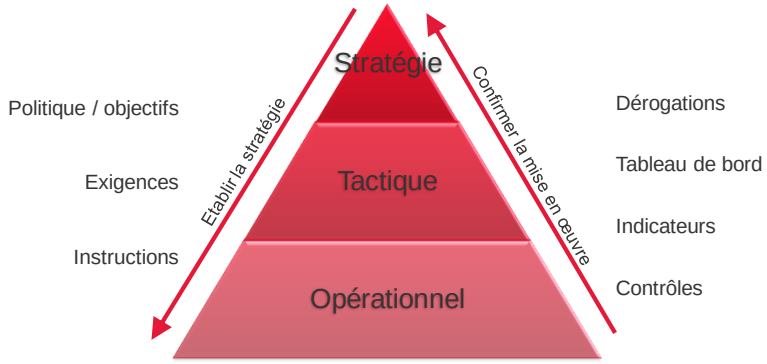
LA SÉCURITÉ, UNE PRÉOCCUPATION PERMANENTE

Rien n'est jamais acquis dans un monde où la menace évolue, où de nouvelles vulnérabilités apparaissent tous les jours, où les besoins du métier changent, où le système d'information s'ouvre à de nouveaux utilisateurs et moyens d'accès. La vigilance doit rester une affaire de tous les instants et les exigences doivent évoluer.

UNE GOUVERNANCE ADAPTÉE

Pour atteindre les objectifs fixés, la gouvernance doit impérativement fonctionner dans deux directions :

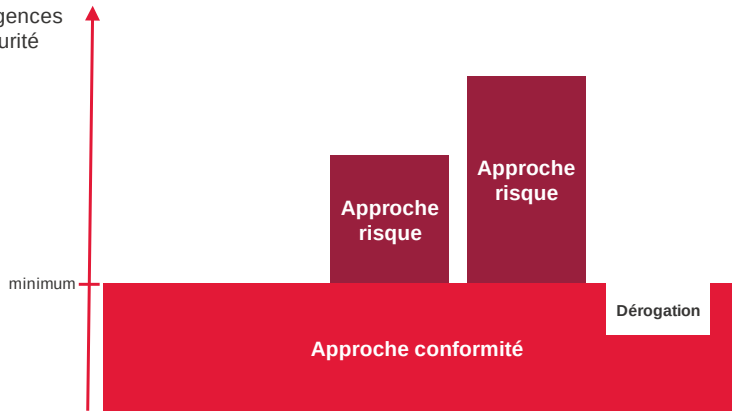
- Top Down, pour définir et communiquer ce qu'il y a à faire
- Bottom Up, pour confirmer ce qui a été fait.



ÉTABLIR LA STRATEGIE

En fonction du niveau de maturité de l'organisation, deux approches complémentaires peuvent être exploitées :

- Une approche dite « conformité » en définissant, de préférence de manière collégiale, une politique, des exigences et des instructions à respecter. Ces éléments doivent s'imposer à tous comme le minimum requis. Toute divergence doit être formalisée dans une demande de dérogation qui comporte obligatoirement un plan de convergence. Cette approche permet de partager un vocabulaire et des pratiques communes et ainsi de faire progresser une organisation vers une cible qui devrait être revue tous les ans.
- Une approche dite « risque » en proposant une méthode d'analyse des risques. Chaque contexte est étudié spécifiquement et les objectifs de sécurité s'appuient clairement sur les enjeux. Cette approche permet d'adapter la sécurité au contexte métier et d'impliquer les responsables métier dans la démarche.



La sécurité ne peut pas être considérée comme une pratique à part : elle doit s'appuyer sur et s'intégrer dans la stratégie de l'organisation. Elle doit utiliser les leviers à disposition et interagir avec les processus en place. Par exemple, le déploiement de la sécurité passe par des projets. Un sponsor doit notamment être identifié et impliqué pour chaque projet significatif. Autre exemple, la sensibilisation auprès des collaborateurs doit être déployée en lien avec la communication interne, garante de l'image de l'entreprise.

Comme dans les autres domaines, la gouvernance de la sécurité doit s'appuyer sur les principes suivants :

- Participation : tous ceux qui sont concernés participent à l'élaboration des décisions qui les concernent.
- Subsidiarité : les décisions doivent être prises, autant que possible, au niveau des personnes qui en subiront les conséquences. Le pouvoir de décider est délégué à l'échelon supérieur quand l'échelon inférieur ne peut pas s'organiser et décider à son niveau.
- Autorité : les responsabilités spécifiques sont reconnues et dotées des compétences et moyens requis.

CONFIRMER LA MISE EN ŒUVRE

Dicter des exigences sans vérifier leur application, c'est faire la politique de l'autruche. La boucle de retour est indispensable pour mesurer l'efficacité des actions mises en place et piloter l'amélioration continue, pour prendre des décisions éclairées ainsi que pour sensibiliser, communiquer et rendre compte. Enfin, cette boucle de retour permet de justifier des demandes d'investissement ou d'évolution.

La direction générale a besoin d'être rassurée sans pour autant avoir besoin de maîtriser tous les détails. Elle va particulièrement s'intéresser à un niveau **stratégique** :

- La maturité atteinte par rapport à un référentiel de bonnes pratiques
- Les risques résiduels
- Les incidents (et leurs impacts sur le métier)
- Les coûts

La communication remontante, qui cible la direction générale, doit donc s'attacher à montrer que le travail est fait et à obtenir le sponsorship nécessaire pour passer à l'étape suivante.

DEVELOPPER UNE VISION OPERATIONNELLE AFFINEE

Le pilotage au quotidien de la sécurité par le responsable de la sécurité du système d'information (RSSI) nécessite également une vision **opérationnelle** sur :

- Les quantités d'incidents et d'anomalies par type
- Les vulnérabilités exploitables et le déploiement des correctifs
- L'avancement des projets sécurité
- L'adoption et l'efficacité des processus sécurité.

Idéalement, la production des indicateurs devrait être embarquée dans les procédures. Les indicateurs doivent permettre de suivre un niveau mais aussi de dégager des tendances qui peuvent nécessiter des actions correctives voire de nouveaux projets structurants.

En conclusion, la gouvernance de la sécurité des systèmes d'information dans un groupe ou une organisation aux responsabilités réparties doit comporter une branche descendante qui en diffuse les prescriptions et une branche remontante qui en mesure l'application via un mode de reporting simple, adapté et modulable. C'est dans ce contexte qu'une amélioration continue de la sécurité peut voir le jour en s'appuyant sur les retours terrain.

Thibaut Chevillotte, Manager Sécurité, CGI Business Consulting