Le Directeur Cybersécurité décrypté…

La place de la cybersécurité

La fonction cybersécurité est une fonction transverse de l'entreprise, qui adresse à la fois sa gouvernance, son cœur de métier et ses fonctions support. Pour répondre aux enjeux numériques des entreprises, les systèmes d'information sont en forte mutation en termes de services rendus, de périmètres couverts et de valorisation des données, mais aussi de structure devenue protéiforme, hyperconnectée et de plus en plus tournée vers le cloud. Ces systèmes d'information occupent désormais une place stratégique dans les activités de l'entreprise. La performance de l'entreprise est tributaire de la résilience de ses activités numériques et de la sécurité de son système d'information. L'évolution des menaces, en fréquence, en intensité et en dangerosité (intention, sophistication et volume) fait que les risques cyber deviennent prégnants et peuvent engager la pérennité de l'entreprise. Il se situent désormais dans les tout premiers risques à adresser. De fait, la cybersécurité devient un enjeu stratégique pour la protection de l'ensemble des activités métier.

Sa fonction

A ce titre, la cybersécurité doit être pilotée par un cadre dirigeant ayant la capacité à adresser pleinement le domaine, dans sa transversalité, son évolutivité et sa technicité. Il appartient à la Direction Générale de créer la fonction de Directeur Cybersécurité, de la positionner au niveau adéquat dans l'organisation de l'entreprise, de la doter d'un mandat formel et des moyens nécessaires à l'accomplissement de sa mission. Ces moyens doivent être à la hauteur des enjeux et doivent permettre la mise en place d'une gouvernance qui adresse les différents volets de la fonction.

Son organisation

La structure organisationnelle et technique à disposition du Directeur Cybersécurité doit être adaptée à l'activité de l'entreprise, sa sensibilité, sa taille, son organisation, sa géographie, sa culture et ses valeurs. Différents schémas sont possibles pour adresser l'ensemble de l'entreprise avec le niveau de granularité adéquat. Le Directeur Cybersécurité peut piloter un ensemble de responsables cybersécurité. Ces responsables peuvent gérer des entités, des filiales, des géographies ; ou ils peuvent se spécialiser sur des domaines fonctionnels (environnement industriel, services externalisés dans le cloud, portefeuille applicatif ou bien d'autres périmètres). Plusieurs modèles peuvent être mis en œuvre. Quel que soit le découpage à un ou plusieurs niveaux, avec des spécialisations verticales ou au contraire des approches plus transversales, il faut in fine mettre en place et piloter des équipes spécialisées dans les différents domaines des activités cyber. Parmi ces activités, une filière Cyberdéfense (SOC/CERT) est nécessaire. En effet, l'organisation en charge de

la cybersécurité doit permettre d'adresser les problématiques stratégiques comme opératives, cyberdéfense comprise.

La fonction cybersécurité, encore jeune, s'est fortement développée au cours des dix dernières années. Elle a été portée par des RSSI chefs d'orchestre, devant être présents à tous les niveaux, sur un périmètre toujours plus grand d'activités et ce qu'elles impliquent de domaines divers de compétences et d'expertise. Dans cette communauté, certains RSSI constitueront naturellement un vivier potentiel pour accéder à la fonction de Directeur Cybersécurité. D'autres RSSI vont plutôt évoluer vers une spécialisation en prenant en charge un périmètre particulier.

Ses objectifs

La Direction cybersécurité a une capacité d'action globale, ce qui permet de ne pas diluer ou disperser les ressources cyber. Elle est plurielle et intègre tous les talents et expertises nécessaires.

Elle doit être en mesure de piloter :

- L'identification de l'ensemble des risques Cyber et la spécification des stratégies et politiques ;
- Le catalogue de services et de solutions qui vont permettre à chaque partie d'intégrer la sécurité en amont dans ses activités et dans les projets de l'entreprise, en couvrant les dimensions techniques, contractuelles, assurancielles, organisationnelles et humaines ;
- Les dispositifs opérationnels de surveillance, détection et réponse aux incidents et de gestion de crise ;
- Les stratégies de continuité et cyber résilience des Systèmes d'Information ;
- Le développement de la culture sécurité, en filigrane de toutes ces activités.

Elle garantit la cohérence, la complétude, l'efficacité et l'amélioration continue de ces dispositifs. Cela nécessite d'évaluer la maturité et l'exposition aux risques et de produire un reporting permettant de conduire et adapter la stratégie le cas échéant.

Ses missions

Le Directeur Cybersécurité est un cadre dirigeant ayant reçu un mandat de la Direction Générale pour assurer la protection des informations de l'entreprise ainsi que la sécurité et la résilience des systèmes d'information. Il est en interaction avec le COMEX pour tout ce qui touche au domaine de la cybersécurité. Un positionnement en prise direct avec le COMEX est nécessaire et un rattachement à un membre du COMEX est à privilégier.

Le Directeur Cybersécurité :

1. Participe à l'élaboration de la stratégie de l'entreprise vis-à-vis des enjeux cybersécurité afférents à ses métiers. Apporte ainsi son expertise et sa vision en matière de cybersécurité pour cartographier et analyser les risques cyber au regard des enjeux métiers de l'entreprise.
2. Elabore la stratégie de cybersécurité de l'entreprise, qu'il fait valider par le COMEX, et rend compte de la déclinaison opérationnelle de la stratégie retenue.

3. Décline la stratégie cybersécurité et ses principes directeurs en programmes et plans d’investissements pluriannuels sur tous les domaines des systèmes d’information de l’entreprise (SI de gestion, opérations, SI industriels, objets connectés). Pilote le budget et les ressources humaines qui lui sont alloués à hauteur des enjeux à adresser.
4. Spécifie et met en place la gouvernance de la filière cybersécurité, définit notamment les rôles, les responsabilités et la comitologie, décline les orientations stratégiques à destination des directions et entités de l’entreprise et veille aux développements des compétences nécessaires.
5. Développe la confiance dans le numérique, avec le sponsoring du COMEX, auprès des salariés, clients, partenaires et fournisseurs et valorise la démarche Cybersécurité de son organisation auprès de ses clients et de son écosystème.
6. Interagit avec les régulations et les structures régaliennes nationales, européennes et internationales en charge, directement ou indirectement, de cybersécurité, afin de défendre les intérêts de son entreprise.
7. Pilote les processus de cybersécurité de prévention, protection, surveillance, détection, réponse à incidents et gestion de crises Cyber et anime les différentes équipes impliquées autour des activités associées. Participe aux dispositifs de gestion de crise métier.
8. Assure la conduite des équipes en charge d’activités opérationnelles spécialisées autour de la cybersécurité. Contribue à l’élaboration et au test des plans de continuité et reprise d’activité des systèmes d’information et des dispositifs de cyber-résilience.
9. Définit la doctrine Cybersécurité, maintient et contrôle la mise en œuvre des politiques, et contrôle les politiques dérogatoires, dans le respect de la réglementation en vigueur.
10. Veille à ce que les solutions et services numériques choisis et mis en œuvre soient alignés avec les enjeux de l’entreprise en matière de cybersécurité.
11. Vérifie la conformité, la performance et l’efficacité opérationnelle des dispositifs et des parties prenantes en charge de ou contributives à la cybersécurité de l'entreprise. Pilote le processus d’amélioration continue et de montée en maturité.
12. Rend périodiquement compte au COMEX de la situation comportant les aspects de gestion des risques numériques, sinistralité subie et évitée, situation humaine, technologique et budgétaire.

Le Directeur Cybersécurité peut être porteur de l’offre de cybersécurité de l’entreprise dans l’hypothèse où la cybersécurité est une composante des services ou solutions que propose l’entreprise à ses clients, ou un attendu des autorités de tutelle ou des régulations.

Ses compétences

Le Directeur Cybersécurité connait bien l’entreprise, ses projets, son cadre réglementaire et normatif, ses métiers et les enjeux qu’il sert. Il est garant auprès du COMEX du fait que l'entreprise dispose bien des ressources humaines, organisationnelles, techniques et budgétaires pour atteindre et maintenir le niveau de confiance recherché. Il combine des compétences managériales, de conduite de programme complexe, une expertise technique et réglementaire reconnue ainsi qu'une solide expérience en cyberdéfense. Il est à la fois le porteur de la vision stratégique et de la défense opérationnelle de l'entreprise face aux cybermenaces. Il a une parfaite compréhension des domaines

de l’informatique et du numérique, avec un focus particulier sur la protection des données. Il maitrise les différents concepts méthodologiques et organisationnels liés à la cybersécurité, et notamment les cadres méthodologiques de l’analyse des risques et de l’amélioration continue. Il porte une vision sur l’évolution des risques Cyber et sur les technologies pour y faire face. Il sait faire preuve d’agilité dans ses plans d’actions, face à l’évolution rapide des menaces. Interlocuteur reconnu vis-à-vis des différentes parties prenantes, il est à l’aise avec les équipes techniques comme avec les équipes juridiques, mais aussi les avec les spécialistes Métier. Il a une capacité de communication lui permettant de déployer un plan d’acculturation dans son domaine. Il dispose du leadership naturel permettant de mobiliser tous les acteurs de l'entreprise, en temps normal, comme en temps de crise.

La cybersécurité étant un domaine en cours de structuration, autour à la fois de la gouvernance d'entreprise, de la conformité réglementaire et de l'efficacité dans la protection opérationnelle, il n'existe pas encore de parcours de carrière type. Toutefois, la gestion des carrières des RSSI à fort potentiel doit intégrer cette opportunité. Aucun cursus ne prépare pleinement à cette fonction à ce jour. Les formations initiales à privilégier pour ce poste sont celles d’ingénieur dans le domaine de l’IT avec idéalement un double cursus complémentaire de cybersécurité et de management.