Advens
SECURITY FOR THE DIGITAL AGE

Nouveaux rôles dans la cybersécurité : Regards croisés

Apparition du directeur cybersécurité & Évolutions du RSSI

CESIN

INTRODUCTION

La sécurité n'est plus d'une option. Ce constat est une évidence pour les experts du domaine "Cyber". Pour autant, le niveau de protection des organisations et leur système d'information n'est pas encore satisfaisant. Les cyberattaques font régulièrement la une des journaux. Et chacun des audits réalisés par les sociétés spécialisées laisse apparaitre des faiblesses dans les dispositifs de protection.

Cependant, pour les dirigeants d'entreprise, ou pour les responsables de structures publiques, le sujet de **la cybersécurité s'invite de plus en plus régulièrement à l'ordre du jour des instances de gouvernance.** L'accélération des attaques, de plus en plus médiatisées et impactantes, la pression réglementaire croissante et la dépendance de l'économie au « numérique » font du sujet Cyber une problématique qui ne peut plus être oubliée.

Malgré tout, on peut se demander si tout le monde est passé des paroles aux actes. **Les organisations accordent-t-elle les moyens nécessaires à la maîtrise des risques de sécurité ? Les ressources en place sont-elles suffisantes et adaptées ? Le pilotage de cette problématique est-il le bon ?**

SOMMAIRE

1.1 La « fonction » sécurité

La problématique de la cybersécurité est traitée dans les organisations par un certain nombre de ressources. Celles-ci sont traditionnellement issues des équipes de la direction des systèmes d'information. Dans les groupes les plus matures, on trouve également ces ressources dans les différentes entités ou business units de l'entreprise. L'ensemble des forces vives qui contribuent à la sécurité, à temps plein ou non, en tant qu'activité principale ou secondaire, constitue la fonction Sécurité.

Cette fonction est plus ou moins structurée selon l'activité des entreprises, leur appétence au risque, ou les obligations réglementaires et normatives. Dans tous les cas, son pilote est traditionnellement le responsable de la sécurité des systèmes d'information, le RSSI.

Comme son nom l'indique, il est responsable de cette problématique. Cependant on peut se demander s'il a toutes les clés pour y arriver… et s'il est le pilote le mieux adapté dans sa forme actuelle.

1.2 R... Comme Responsable ? Vraiment ?

Le RSSI est donc responsable de la sécurité. Mais dans les faits, qu'en est-il ? Protection contre les attaques, conformité vis-à-vis des référentiels, sensibilisation des équipes, maîtrise des risques apportés par les tiers et par les partenaires, déploiement des technologies de sécurité, etc. La fiche de poste est souvent dense.

Les sujets sont variés et doivent être traités à différents niveaux dans l'organisation. Direction des systèmes d'information, ressources humaines, direction des achats, direction juridique mais aussi entités métiers : nombreuses sont les entités concernées.... parfois sans lien direct avec le RSSI ou sa direction de rattachement.

> ***Direction des systèmes d'information, ressources humaines, direction des achats, direction juridique mais aussi entités métiers : nombreuses sont les entités concernées....***

Technologies de protection, système de détection, activités d'audit et de contrôle, action de communication et de sensibilisation, veille et analyse des menaces : les facteurs de coût sont nombreux et le budget associé parfois conséquent. A cela s'ajoute une sensibilisation très relative des différentes parties prenantes, parfois même parmi les plus haut placées dans l'organisation.

Le RSSI est-il en mesure d'assurer la sécurité de son organisation face à la variété des activités, la transversalité de la discipline, l'augmentation des besoins, le besoin d'influence et de capacité de décision ? A-t-il les moyens nécessaires pour y parvenir ? Face à une tâche aussi importante, et dont les enjeux peuvent être vitaux pour l'organisation, les instances dirigeantes (COMEX, conseil d'Administration ou équivalent) devraient se poser ces questions. Le RSSI doit-il voir son poste évoluer ? Le casting pour le poste doit-il également évoluer ?

2. VOICI VENU LE DIRECTEUR CYBER !

Depuis quelques années, plusieurs organisations, dans différents secteurs, et de différente taille et maturité, ont nommé un Directeur de la Cybersécurité. Le changement de titre est-il purement symbolique ou traduit-il une évolution dans la gouvernance et le pilotage de la sécurité ?

Autrefois Responsable, le pilote de la sécurité devient Directeur. **Le RSSI devient-il naturellement Directeur Cybersécurité lorsque le poste est créé ?** RSSI et Directeur Cybersécurité peuvent-ils cohabiter ? Le changement d'une lettre dans l'acronyme manifeste-t-il une profonde évolution ou la suite logique d'une montée en maturité ?

Le CESIN et Advens se sont penchés sur la question. Pour ce faire, plusieurs Directeurs Cybersécurité ont été sollicités, issus de contexte et de secteurs variés (CAC 40, Administration, ETI…). Et le CESIN a, en parallèle, décrit et publié une fiche de fonction du Directeur Cybersécurité.

Directeur de la cybersécurité, Directeur de la sécurité des systèmes d'information, Directeur de la sécurité numérique… Pour le moment, les titres sont variés. L'appellation ne semble pas normalisée.

Coquetterie pour amateur de profils LinkedIn percutant ? Véritable choix réfléchi pour faciliter l'adhésion des équipes en fonction de la culture d'entreprise ? Alignement sur les autres dénominations dans l'organisation ? Il est encore trop tôt pour identifier l'impact du titre sur le quotidien de celui que nous nommerons le Directeur Cybersécurité.

Quant au choix du genre, le recours au masculin est une habitude qui va finir par prendre de l'âge et ne plus être adapté. **Plusieurs des Directeurs.trices Cybersécurité sollicités pour cette étude sont des femmes !**

2.1 Quel fait déclencheur ?

Avant de s'intéresser au profil du Directeur Cybersécurité, Il est intéressant de comprendre quel a été le fait déclencheur de son arrivée. Chacune des organisations sollicitées a son vécu par rapport à la cybersécurité. Et **la décision de créer le poste de Directeur Cybersécurité n'a pas toujours la même origine.** On note cependant deux cas de figure sur l'ensemble des personnes interrogées.

Premièrement, la décision peut faire suite à un incident de sécurité. Il s'agit la plupart du temps d'un incident impactant pour l'organisation et pour ses activités les plus critiques ou les plus rentables. Le choc provoque une prise de conscience relativement soudaine, qui mène les directions générales à nommer un Directeur Cybersécurité. Cette nomination dans l'urgence pourrait sembler être la solution de facilité pour tranquilliser le COMEX. Pour autant, dans les cas de figure rencontrés, la nomination s'est accompagnée des moyens nécessaires et d'une véritable légitimité. Et elle a donné lieu à un suivi régulier par les instances dirigeantes des sujets Cyber.

Deuxièmement, l'arrivée du Directeur Cybersécurité peut être la suite logique de la montée en maturité de l'organisation. Elle peut traduire une réussite personnelle du RSSI qui devient Directeur Cybersécurité, notamment car il a réussi à convaincre la direction du besoin d'évoluer et de monter en puissance sur le sujet. Mais elle peut traduire également une montée en maturité de la direction elle-même. Cela peut être lié à :

- **Une évolution de la pression réglementaire** (tendance accélérée suite à l'apparition du RGPD, mais également de la LPM ou de la directive NIS par exemple),
- **Une prise de conscience le poids de la "Cyber"** dans la réussite des activités de l'entreprise (développement de services numériques, importance du chiffre d'affaire lié au commerce en ligne, fabrication de produits qui sont désormais connectés etc.),
- **Ou tout simplement un alignement** avec les pratiques des concurrents du secteur !

2.2 Quelles nouveautés par rapport au métier de RSSI ?

Pour celles et ceux qui douteraient des différences ou des évolutions apportés par ce nouveau rôle, il est intéressant d'étudier certaines activités portées par le Directeur Cybersécurité – et qui n'ont pas toujours été portées par le RSSI jusqu'à présent.

Le premier exemple est la sécurité des produits réalisés ou vendus par l'organisation. Dans de nombreux cas de figure, le RSSI ne portait son action que sur les systèmes d'information utilisées par les fonctions support. Depuis quelques années, dans l'industrie notamment, le RSSI a étendu son champ d'action aux SI industriels (il en est de même dans la santé pour le biomédical par exemple).

Les Directeurs Cybersécurité interrogés ont **un périmètre très large, incluant l'ensemble des activités du groupe,** et donc bien souvent la sécurité de ce qui est vendu aux clients. C'est assez naturel pour les sociétés les plus jeunes et les plus centrées sur l'informatique, comme les fournisseurs de services numériques ou les hébergeurs. Pour les grands groupes industriels, dans l'automobile, les transports ou l'énergie par exemple, cette évolution n'est pas toujours simple. Elle est accélérée par les nouveaux services vendus et la transformation des produits fabriqués en objets connectés ou composants de la « smart » société (smart car, smart city, smart grid, etc.). Cela traduit dans tous les cas la prise de conscience par l'entreprise de l'importance business de la sécurité.

Pour certains, ils sont même la garantie « Cyber »

Les autres exemples concernent le développement de l'organisation et par exemple les fusions-acquisitions ou l'élaboration de partenariats scientifiques et industriels. Tous les Directeurs Cybersécurité n'interviennent pas sur ces sujets. Mais ils sont de plus en plus sollicités en amont de ces projets très souvent stratégiques. Pour certains, ils sont même la garantie « Cyber » que l'entreprise souhaite intégrer lors d'un rachat ou d'une décision d'investissement dans une startup.

2.3 D'où vient le Directeur Cyber ?

En toute logique deux cas de figures se présentent, selon que le Directeur Cybersécurité soit issu, ou non, de la filière Cybersécurité.

Certains des Directeurs Cybersécurité interrogés sont d'anciens RSSI. Dans ce premier groupe, certains ont bénéficié d'une promotion interne, passant ainsi de RSSI à Directeur Cybersécurité. Pour d'autres, cela fait suite à un changement d'employeur.

Dans tous les cas, ils avaient tous de nombreuses années d'expérience dans leur organisation.

Dans le second groupe, les Directeurs Cybersécurité n'avaient pas d'expérience en matière de cyber. Dans tous les cas, ils avaient tous de nombreuses années d'expérience dans leur organisation. Ils y ont occupé différents postes et témoignent d'une connaissance très large et pointue des métiers de leur employeur.

La question de l'origine n'est pas anodine. Pour un sujet associé à autant de complexité et d'expertise, **ne pas avoir travaillé dans le domaine est-il un problème ?** Vu des RSSI déjà en poste, c'est une vraie interrogation, pour ne pas dire une menace – petit clin d'œil au jargon de la discipline !

Parcours d'un Directeur Cyber

Olivier Ligneul
Directeur Cybersécurité EDF et vice-président du CESIN en charge des grandes entreprises et des administrations

---

Comment devient-on directeur Cybersécurité d'un groupe comme EDF ? Votre parcours est-il 100% Cybersécurité ?

Mon parcours n'est pas issu à 100% du domaine de la cybersécurité. J'ai démarré dans le secteur des Telecom puis j'ai basculé dans la Cyber. Cette évolution a été assez logique, compte-tenu de certaines problématiques similaires telles que le besoin d'accessibilité des réseaux depuis l'extérieur de l'entreprise, l'ouverture de ces réseaux et donc les enjeux liés à l'exposition des systèmes d'information.

Avez-vous été recruté à ce poste en tant que RSSI ou en tant que Directeur Cybersécurité ? Quel est la différence selon vous ?

J'ai démarré dans la Cybersécurité en tant que responsable de l'activité Conseil & Assistance de l'ANSSI, lors de sa création. C'était mon premier poste dans le domaine. Il y a 5 ans, j'ai intégré EDF, mon employeur actuel. J'y suis entré en tant que RSSI, avec un statut de cadre supérieur. J'avais le rôle de RSSI mais aussi de CTO. Il y a deux ans, le groupe EDF a souhaité se doter d'un dirigeant à la tête de la sécurité des systèmes d'informations de tous les domaines informatiques et m'a proposé d'évoluer vers le poste de Directeur Cybersécurité du groupe.

La principale différence, de mon point de vue, est le changement de posture : on passe d'un rôle où l'on doit mettre en œuvre la cybersécurité et fournir les moyens associés à un rôle où il faut assurer la cybersécurité de l'entité. Le fait d'assurer la cybersécurité permet, en lien avec le métier, de la garantir. Auparavant, l'approche était plus focalisée sur une fourniture de moyens.

Quel est le principal challenge du Directeur Cyber selon vous ?

Le premier challenge, selon moi, c'est déjà d'être reconnu comme la personne en charge de la cybersécurité pour l'ensemble du groupe et de gagner la légitimité auprès des autres organes de direction. Il faut faire en sorte que cette nouvelle fonction existe, en complément des autres fonctions et dans une organisation complexe. Lorsque l'on est issu d'une fonction associée à la technique, considérée comme une fonction support, il peut être difficile de faire comprendre aux autres acteurs de l'entreprise le rôle d'une direction cybersécurité par nature transverse et dont l'objectif se focaliser sur la protection des intérêts de l'entreprise, de ses processus et de son patrimoine immatériel.

Kevin Heydon

Chief Information Security Officer, L'Occitane, CISSP ®

Comment devient-on directeur Cybersécurité d'un groupe comme L'Occitane ?

... en ne venant pas de la cybersécurité ! En effet, j'étais encore le directeur SI du Manufacturing et de la R&D lorsque j'ai proposé au Groupe de fonder le département Infosec en 2015, pour répondre à un besoin latent de notre direction générale.

Sur un thème en rupture de notre culture Groupe (du moins à première vue) et suscitant de nombreux a priori, être déjà perçu comme « orienté métier » par nos dirigeants de l'époque a bien plus joué qu'une expertise, développée par la suite. Il m'était naturel de sponsoriser et incarner Infosec en réfléchissant aux enjeux de l'entreprise, avant de plonger dans les considérations techniques.

Avez-vous été recruté à ce poste en tant que RSSI ou en tant que Directeur Cybersécurité ? Quel est la différence selon vous ?

J'ai eu la chance de définir moi-même les critères clés de succès (et de mon acceptation du poste !) alors que je proposais la naissance d'Infosec. L'un de ces critères était une influence transverse dans toutes les directions métiers et techniques, à tous niveaux de

management, dans le monde entier, selon des priorités définies avec la direction générale. Un autre critère était la « liberté de parole » pour conjuguer pragmatisme et exigence, d'une manière à la fois bienveillante et sincère.

Ces deux critères, et l'aptitude à proposer et porter une stratégie, me font dire que nous parlons bien là d'un rôle de niveau direction. Et ce titre de directeur (ou de « CISO » aux US, où le mot « director » a bien moins de portée) a en effet facilité le point d'entrée chez certains grands patrons… il n'a en revanche rien changé au fait qu'une fois la porte ouverte, il faut être bon, facilitateur et convaincant !

Quel est le principal challenge du Directeur Cyber selon vous ?

Trouver la bonne posture, et celle de son équipe. Par exemple : comment être une équipe facilitante tout en fixant les bonnes limites, comment partager un regard critique tout en restant un allié, comment aider les autres à faire par eux-mêmes sans perdre le lien avec le terrain, etc.

C'est un équilibre instable au quotidien, et l'intelligence émotionnelle d'une équipe Infosec (et de son directeur) me semble au moins aussi importante que sa compétence technique. C'est aussi ce qui rend le job si particulier et si passionnant !

3.1 L'objectif ultime ?

Pour de nombreux RSSI, l'évolution vers le poste de Directeur Cybersécurité peut sembler un objectif ultime, à la fois pour la satisfaction personnelle mais aussi pour avoir enfin les clés en main pour réussir le défi de la cybersécurité dans son organisation. Cela peut se traduire par une émancipation de la DSI, l'obtention d'un budget indépendant, le rattachement à la direction de l'organisation. **Le passage au statut de Directeur Cybersécurité facilite la réalisation de ces aspirations.** Une question simple subsiste cependant : tous les RSSI sont-ils amenés à évoluer vers le poste de Directeur Cybersécurité ?

La réponse est déjà identifiée à ce stade : non, tous les RSSI ne vont pas devenir Directeurs Cybersécurité. D'une part, à ce stade, **toutes les organisations n'ont pas besoin d'un Directeur Cybersécurité.** Ce rôle est réservé aux structures les plus matures en matière de cybersécurité. Et également aux entreprises et organisations d'une certaine taille ou complexité en termes de Systèmes d'information. Pour une PME ou une ETI, si le numérique n'est pas au cœur des activités, la cybersécurité peut être piloté par un RSSI dans un premier temps.

La délicate question de la maturité en Cybersécurité...

Benjamin Leroux
Marketing & Innovation, Advens

Comment évaluer la maturité d'une société sur le sujet de la Cybersécurité ?

C'est une question complexe. La maturité ne dépend ni de la taille, ni du secteur d'activité de l'entreprise ou de l'organisation dans le

cas du public. Advens accompagne des clients très matures qui sont des PME et certaines grandes entreprises ont parfois des progrès à faire. C'est peut-être lié à l'appétence aux risques et à la gestion de ces risques… ce qui peut finalement dépendre de la direction et de la culture de la société.

Existe-t-il une méthode pour s'auto-évaluer ?

L'ANSSI avait publié des éléments il y a quelques temps. Et il existe différents référentiels sur les bonnes pratiques. Mais il est difficile de considérer qu'ils évaluent clairement la maturité – c'est plutôt une conformité aux bonnes pratiques ou à un certain niveau technique. Il faut essayer de se poser la question du poids de la Cybersécurité pour l'organisation que l'on protège et sa capacité à « faire bouger les lignes ».

Quels sont vos conseils pour progresser ?

Vaste question ! Le terme peut sembler pompeux mais la clé réside dans la valeur. Le pilote de la sécurité doit se poser la question de son apport pour son organisation et de l'apport de la sécurité pour cette organisation. Il faut démontrer par l'exemple que la sécurité est capable d'accompagner la transformation numérique et plus globalement être un levier de développement de la structure.

D'autre part, l'évolution du métier de RSSI vers celui de Directeur Cybersécurité ne sera pas possible – ou intéressante – pour tous les profils concernés. En effet, certaines des actions du Directeur Cybersécurité ne sont pas aujourd'hui toujours intégrées dans le périmètre traditionnel du RSSI, comme par exemple le pilotage global de la fonction sécurité, la définition de la vision et de la stratégie de sécurité et la participation aux instances de direction.

Pour les Directeurs Cybersécurité interrogés, cette évolution est sans doute la différence majeure entre les deux postes. **Le Directeur Cybersécurité n'est pas un « super RSSI ».** Le poste de Directeur Cybersécurité est, selon eux, un autre métier, dont les composantes politiques et managériales sont bien plus exacerbées que pour le poste de RSSI. Pour certains RSSI, c'est une évolution qui semble logique et passionnante. Pour d'autres, c'est un poste qui

pourrait manquer de sujets techniques et technologiques. **On voit ainsi poindre une cohabitation entre Directeur Cybersécurité et RSSI.** Et c'est logique : vu la tâche à accomplir, toutes les forces vives seront les bienvenues, une force de pilotage global et des forces plus spécialisées.

3.2 Vers une nouvelle organisation

Pour l'ensemble des Directeurs Cybersécurité interrogés, **l'organisation évolue vers un maillage de l'entreprise par plusieurs RSSI, chapeautés par le Directeur Cybersécurité.** Ce mode d'organisation se calque sur la logique présente dans certains groupes : le RSSI Groupe étant à la tête d'un réseau de RSSI, souvent en charge d'une filiale ou d'une business unit.

Certains Directeurs Cybersécurité ont fait le choix de RSSI consacrés à des périmètres informatiques. C'est notamment le cas dans l'industrie où le Directeur Cybersécurité s'appuie sur des RSSI en charge de l'informatique de gestion et des RSSI concentrés sur l'informatique industrielle. Ce découpage peut être encore plus ciblé selon les métiers de l'organisation, avec un périmètre industriel découpé en plusieurs axes (médical, nucléaire, IoT, etc.).

> ***Le RSSI couvre tout le spectre des mesures de sécurité, des plus techniques aux plus organisationnelles***

Au-delà du secteur industriel, l'organisation peut évoluer vers un découpage en plusieurs périmètres, définis en fonction du métier de la structure à protéger. **Les activités du RSSI évoluent alors également.** Elles sont concentrées sur l'identification, le déploiement et la maîtrise des dispositifs de sécurisation de son périmètre. Cela ne signifie plus un poste 100% dédié au système d'information. Le RSSI couvre tout le spectre des mesures de sécurité, des plus techniques aux plus organisationnelles – dans le respect des orientations fixées par le Directeur Cybersécurité, voire dans certaines organisations tout en s'appuyant sur les familles de solution et le cadre général fixés par le Directeur Cybersécurité.

De RSSI à Responsable Cybersécurité ?

Mylène Jarossay
Présidente du CESIN

En parallèle de l'émergence de la fonction et du terme Directeur Cybersécurité, que devient l'appellation RSSI, va-t-elle perdurer ?

Même si le métier est jeune, le titre de RSSI est désormais bien connu et implanté dans les entreprises. **Il faut donc veiller à ne pas créer de la confusion autour d'un changement d'appellation.**

Néanmoins, nous pouvons noter que le terme cybersécurité a remplacé, dans nos langages usuels, celui de SSI. Ce terme cybersécurité adressait au départ un périmètre restreint. Désormais, il est devenu le terme le plus utilisé et s'est imposé comme un standard de fait, recouvrant l'intégralité de la fonction SSI. Il se trouve que ce terme a un équivalent en anglais dont l'orthographe est proche, et qui est très largement utilisé dans le monde. En résumé, **il ne serait pas étonnant que progressivement les RSSI désirent porter le titre de Responsable Cybersécurité.** Disons simplement qu'il s'agit d'une modernisation du nom.

Cela harmoniserait les appellations entre ce nouveau nom et celui de Directeur Cybersécurité. Ainsi les entreprises qui mettent en place une Direction Cybersécurité auraient un Directeur Cybersécurité, avec probablement des Responsables Cybersécurité sectoriels dans ses équipes, par exemple un Responsable Cybersécurité Industrielle ou un Responsable Cybersécurité Europe.

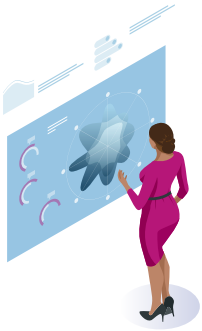
Dans tous les cas, **il ne faut pas que ces évolutions de noms ne perturbent la promotion de cette fonction qui connait une forte croissance en ce moment** et dont le périmètre d'action évolue de façon très intéressante. Gardons donc cette double appellation tout le temps nécessaire !

En matière d'organisation, **l'un des cas particuliers identifiés à ce stade concerne un périmètre bien particulier : la Cyberdéfense.** Cette problématique est transverse dans l'organisation mais elle nécessite des compétences spécifiques qui vont justifier la mise

en place d'un périmètre particulier et donc d'un responsable dédié. Pilote du SOC et probablement du CERT, le responsable Cyberdéfense aura la vaste tâche de devoir identifier, coordonner et activer les différentes lignes de défense de l'organisation, en orchestrant protection, détection et réaction.

3.3 Les objectifs de la direction cyber

Quelle que soit l'organisation retenue, le Directeur Cybersécurité sera à la tête d'**une direction dont les objectifs doivent être clairs.**



Identifier l'ensemble des risques Cyber et spécifier les stratégies et politiques pour y faire face.

Elaborer et animer un 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.

Concevoir et mettre en œuvre les stratégies de continuité et cyber résilience des Systèmes d'Information.

Identifier, choisir et déployer les dispositifs opérationnels de surveillance, détection et réponse aux incidents et de gestion de crise.

Développement la culture sécurité, en filigrane de toutes ces activités.

La direction Cybersécurité doit par ailleurs avoir une capacité d'action sur l'ensemble des facettes de son organisation, et fédérer les initiatives en matière de protection, sécurité et résilience au niveau Cyber.

4.1 Description du poste

Notre étude a permis d'esquisser les contours d'une fiche de poste, réalisée en coopération le CESIN. **L'exercice est périlleux… étant donné la variété des contextes et la difficulté de dresser le portrait-robot d'un tel profil.** Rien que la description de la mission peut faire réagir ! Pour certains, la mission est d'assurer la sécurité ; alors que pour d'autres il s'agit d'aider l'organisation à se mettre en sécurité. La nuance n'est pas neutre dans certaines structures et peut faire débattre !

Intitulé

Directeur Cybersécurité

Statut

Cadre dirigeant

Mission

Assurer la protection des informations de l'entreprise ainsi que la sécurité et la résilience des systèmes d'information

Positionnement

Le Directeur Cybersécurité est **rattaché à un membre du comité exécutif** (ou équivalent). Il est parfois sous l'autorité du Directeur Administratif et Financier ou du Directeur des Risques. Il peut être rattaché à un Directeur Métier si la criticité de cette direction Métier en fait un sponsor pertinent.

Activités & Tâches

Piloter, manager et orienter la direction de la sécurité des systèmes d'information

En un mot « diriger » : Au-delà de la gestion des équipes ou du pilotage de grands projets, **le Directeur Cybersécurité doit se doter d'une vision en matière de cybersécurité** et la porter à tous les niveaux de l'organisation.

Sensibiliser l'ensemble des parties prenantes et des directions de l'entreprise à l'importance de la cybersécurité

La sensibilisation reste nécessaire et primordiale mais elle peut prendre une autre forme. **Cela peut passer par l'inscription du sujet Cyber aux plans stratégiques des différents Métiers de l'organisation.**

Le rattachement au COMEX (ou équivalent) permet de convaincre autrement, quand la sensibilisation n'a pas porté ses fruits…

Rendre compte auprès de la direction générale de la maîtrise des risques

La participation à différentes instances de pilotage, bien souvent parmi les plus hautes au sein de l'organisation, requiert d'apporter une attention stratégique au pilotage.

Faire accepter aux experts que dans certains cas le bon indicateur de pilotage n'est pas purement technique… et que parfois il est nécessaire de simplifier la situation technique pour rendre compte d'un état de fait ou pour faire prendre une décision.

Rationnaliser le portefeuille des dispositifs de sécurité et de maîtrise des risques, et en particulier les solutions technologiques en place dans les SI de l'organisation

Face à un existant parfois conséquent en matière de dispositifs de sécurité, disséminés dans les différentes entités de son groupe ou de son organisation, **il est désormais nécessaire de rationaliser les mesures en place** et de veiller à leur efficacité globale.

Accompagner les différentes équipes en charge de projet pouvant impacter la sécurité de l'organisation

Cela nécessite une compréhension aigüe des métiers de l'organisation, qu'il peut être difficile d'acquérir sans quelques années d'expérience dans la structure ou dans une organisation du secteur.

L'accompagnement passe par la mise en place d'une organisation et d'un réseau d'acteurs au sein du groupe.

Cependant, il ne suffit pas de se concentrer sur le « build ». Il est primordial de préparer et d'animer le « run » de la sécurité (au sens technique et opérationnel et bien au-delà).

Animer une communauté d'experts de la sécurité, rattachés hiérarchiquement ou non au Directeur Cybersécurité

L'humilité sera de mise pour entretenir les bons rapports avec les experts techniques mais aussi et surtout pour établir et conserver sa crédibilité ! Tous les Directeurs Cybersécurité n'ont pas le même bagage technique, informatique et cyber. Par ailleurs l'animation de la fonction Sécurité, **la valorisation de la filière et des métiers associées et l'apport de services aux différentes entités de l'organisation seront clés pour réussir...** au risque de voir apparaitre une shadow SSI !

Définir, défendre et piloter le budget de la Direction Cybersécurité et superviser le budget global de la SSI dans l'organisation

Le budget propre de la direction SSI peut évoluer à la baisse, grâce aux travaux de rationalisation ou à l'industrialisation de certaines activités. Pour autant **le Directeur Cybersécurité doit garder un œil sur l'ensemble des dépenses au niveau du groupe** – qui auront tendance à augmenter grâce à la prise de conscience et la montée en maturité de l'ensemble de la structure.

Faire face aux incidents de sécurité et aux crises de nature « cyber »

Plus de doute : il y aura une crise un jour ou l'autre... et les incidents sont déjà réguliers. **Il faut s'appuyer sur les bonnes expertises pour comprendre la nature des problèmes** et proposer les bonnes décisions à la direction.

Moyens et prérogatives

- **Autorité hiérarchique** sur les membres de sa direction, dont probablement les RSSI sectoriels
- **Autorité fonctionnelle** sur les ressources impliquées dans la fonction Sécurité
- **Budget indépendant** et dédié à sa direction avec pouvoir d'engagement de dépenses

Relations internes et externes

- **Interne :** Le Directeur Cybersécurité est invité à interagir avec le plus de directions possibles au sein de l'organisation. Il a des relations régulières avec le COMEX, la DSI mais également les directions financières, Juridiques, RH, Achats et Risques / Conformité / Contrôle interne.
- **Externe :** groupes spécialisés, régulateurs, forces de l'ordre, confrères, etc.

Savoir-faire

- Compétences en matière d'analyse et de gestion des **risques**
- Compréhension poussée des **différentes activités de son organisation**
- Capacité à définir, défendre et piloter un **budget**
- Management d'équipes **au sens hiérarchique et fonctionnel**
- Production de reporting et de **KPI** relatifs à la cybersécurité
- Capacité à porter des sujets techniques auprès du **COMEX**
- Capacité à faciliter les prises de décision et **arbitrage**
- Solide culture informatique
- Connaissance des **fondamentaux de la sécurité** des systèmes d'information et des dispositifs de maîtrise des risques associés
- Connaissances du **cadre réglementaire applicable à son organisation** ainsi que des normes et pratiques sectorielles en matière de cybersécurité
- Compréhension des **technologies** de sécurité

Savoir-être

- Leadership, **capacité d'influence** et animation de communautés
- **Communication** orale
- Sens du **relationnel** et de l'interpersonnel
- Curiosité et attrait pour l'**innovation**
- Capacité de **résistance aux situations de stress**
- Pédagogie et capacité de **facilitation**
- Capacité à interagir avec des experts

Expérience professionnelle

Cette dernière section de la fiche de poste n'est pas la plus simple à renseigner. Comment concilier le juste niveau d'expertise en matière de cybersécurité et la parfaite compréhension des enjeux de l'organisation à protéger ?

La question n'est pas tranchée à ce stade et elle risque de faire débat !

Le passage à l'âge adulte ?

La création du poste et la nomination d'un Directeur Cybersécurité traduisent une véritable maturité de l'organisation en matière de cybersécurité. **Au-delà de l'aspect symbolique du rattachement et du titre, cette maturité traduit une forme de responsabilisation.** On reconnaît ainsi l'importance du sujet mais on souligne surtout le besoin de le faire piloter par un cadre dirigeant de confiance, capable de maîtriser un tel sujet et de faire face aux crises associées.

Légitimité du poste, augmentation des moyens, pouvoir et capacité d'influence : les moyens semblent réunis pour réussir le challenge. Est-ce que cela signifie qu'il n'y a plus d'excuse en cas de problème ? **L'arrivée du rôle de Directeur Cybersécurité traduit un changement de posture pour celui ou celle qui pilote la sécurité.** Il ne s'agit plus de remonter les problèmes ou de tirer la sonnette d'alarme. Il faut passer à l'action, trouver des solutions et assumer les choix. En un mot : assurer !

Il ne s'agit plus de remonter les problèmes ou de tirer la sonnette d'alarme. Il faut passer à l'action, trouver des solutions et assumer les choix. En un mot : assurer !

Quant à l'origine du Directeur Cybersécurité, son pedigree, son nombre d'années d'expérience dans la Cyber, la question mérite d'être posée. Mais la solution, comme souvent en matière de management et de leadership, va dépendre des personnes. Il faudra être capable de changer de métier et de l'accepter. **Le rôle du Directeur n'est plus celui d'expert Sécurité ou de pilote de la sécurité informatique.** Le quotidien évolue, tout comme la nature des activités. Pour celles et ceux qui l'acceptent, la réussite passera par une subtile alliance entre la maîtrise des problématiques de la cybersécurité, la compréhension des enjeux stratégiques des métiers et la connaissance des modes de fonctionnement de l'organisation.

Dvens

SECURITY FOR THE DIGITAL AGE

CESIN

SECURITY FOR THE DIGITAL AGE

advens.fr

Contact :
+33 1 84 16 30 25
contact@advens.fr