Le cyber risque dans la gouvernance de l'entreprise

Pourquoi et comment en parler en Comex ?

cigref
réussir le numérique

cigref réussir le numérique

DEVELOPPER LA CAPACITE DES GRANDES ENTREPRISES A INTEGRER ET MAITRISER LE NUMERIQUE

Le cyber risque dans la gouvernance de l'entreprise

Pourquoi et comment en parler en Comex ?

Octobre 2016

LE MOT DU PILOTE

Il est convenu que les risques liés à la sécurité des systèmes d'information sont grandissants. En quelques dizaines d'années, nous sommes passés d'une dimension anecdotique (avec les premiers virus développés à la fin des années 1970) à une menace internationale, multiple, structurée et organisée pouvant provoquer des dégâts considérables. Le sujet est abordé maintenant au niveau étatique, il s'invite régulièrement dans l'actualité avec la médiatisation de certaines attaques et a même été utilisé dans des scénarios de films à succès.

Cette menace s'est développée en parallèle de la diffusion de plus en plus importante du monde numérique. Et les entreprises sont elles aussi également concernées. Le CIGREF a mis en place début 2016 le groupe de travail « Cybersécurité » que j'ai animé toute cette année, car en effet, si la sécurité numérique occupe régulièrement le devant de la scène médiatique, son traitement reste encore trop souvent un sujet d'experts, alors que les enjeux peuvent concerner les processus vitaux des entreprises. Une bonne compréhension des risques liés à la cybersécurité doit permettre de donner à la sécurité numérique sa juste place au sein de chaque entreprise.

Le présent document s'adresse aux décideurs dans les entreprises, et propose quelques recommandations opérationnelles qui doivent permettre de faciliter la prise en compte de la sécurité dans la mutation numérique des entreprises. Les sujets qu'il aborde synthétisent les réponses aux questions que nous nous sommes posées dans le groupe de travail, à savoir :

- Quel est le positionnement de la cybersécurité dans la cartographie des risques ressentis par les dirigeants ?
- Quels sont les indicateurs pertinents et réalistes pour faire de la SSI (Sécurité des Systèmes d'Information) un sujet au Comex ?
- Quels messages déployer pour être efficace ?
- Quelles initiatives mettre en place pour que les dirigeants s'approprient effectivement les enjeux de la cybersécurité ?

Certaines de ces questions ont trouvé des réponses, d'autres non. Mais une chose est sûre : s'il y a une analyse de risque à faire, c'est bien celle de la cybersécurité, à l'aune du contexte de chaque entreprise. La cybersécurité doit être traitée à sa juste place dans la gouvernance de l'entreprise, de manière transversale et en liaison avec toutes les parties prenantes (*Top management*, Comités d'audit, Directions Métiers, Ressources Humaines, Juridique, Audit et Risques, et bien sûr DSI). Ce risque polymorphique va continuer d'évoluer, et les dispositifs associés à la gestion de ce risque devront plus que jamais être questionnés, *challengés* par les décideurs pour les adapter à la réalité du moment et à l'évolution de la menace.

Par ailleurs, les Administrateurs de nos entreprises sont de plus en plus conscients de ce risque transversal, du fait des questionnements des autorités de contrôle d'une part, mais aussi du fait de l'évolution des législations (Loi de Programmation Militaire par exemple) d'autre part. Et il est très probable que, dans un futur proche, les DSI et les RSSI soient régulièrement questionnés sur la mise en place de mesures proportionnées de gestion du risque cyber et *challengés* en Comex sur la pertinence des dispositifs en place.

Jean-Jacques Tourre
Pilote du groupe de travail
Responsable Cybersécurité Groupe - Total

Le CIGREF, association de Grandes Entreprises, a été créé en 1970. Il regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...). Le CIGREF a pour mission de développer la capacité des grandes entreprises à intégrer et maîtriser le numérique.

TITRE DU RAPPORT : LE CYBER RISQUE DANS LA GOUVERNANCE DE L'ENTREPRISE : POURQUOI ET COMMENT EN PARLER EN COMEX ?

EQUIPE DU CIGREF

Jean-François PÉPIN – Délégué général
Sophie BOUTEILLER – Directrice de mission
Frédéric LAU – Directeur de mission
Flora FISCHER – Chargée de recherche
Sylvain ALLARD – Chargé de mission
Marie-Pierre LACROIX – Chef de projet
Josette WATRINEL – Secrétaire de direction
Josette LEMAN – Assistante de direction

REMERCIEMENTS

Nos remerciements vont à Jean-Jacques TOURRE (Responsable Cybersécurité Groupe - Total), qui a piloté cette réflexion.
Nous remercions également les personnes qui ont participé aux travaux :

Antoine BAJOLET – TDF
Pascal BASSET – PMU
Catherine BOUTIN – ADP
Philippe BRUNELIERE – Monoprix
Nicolas BURTIN – Caisse des Dépôts
Bernard CARDEBAT – Areva
Philippe CROSNIER – BPCE
Jamal DAHMANE – Essilor
Michel DAN – Solvay
Romain DAYAN – Edenred
Brigitte DECLERCK – AGIRC-ARRCO
Benoit DELMAS – Saint Gobain
Jean-Luc DEZA – Saint Gobain
Béatrice EZZEDINE – CNAF
Nicolas FERNANDEZ – Saint Gobain
Catherine FIMES – MGEN Technologies
François FROMANGE – Plastic Omnium
Emmanuel GARNIER – AG2R La Mondiale
Arnaud GODET – SCOR
Benoit HERMENT – Elior
Mylène JAROSSAY – LVMH
Philippe JOUZIER – Klésia
Sylvain LAMBERT – Pôle emploi
Olivier LIGNEUL – EDF
Christophe MAIRA – Ramsay Générale de Santé
Mathilde MAJOT – Auchan
Carlos MARTIN – Carrefour
Marc MENCEL – Nexter Group
Alice MILANOVA – MAIF
Philippe MONTEIL – Areva
Joël NOIROT – SNCF
Thierry OLIVIER – Société Générale
Pauline ORDINES – SNCF
Didier PERRET – AP-HP
Patrick RAFFIER – Eramet
Pierre RAUFAST – Michelin
Damien RESSOUCHES – Conforama
Philippe SABIO – Groupe Pomona
Jacques SIBUE - Engie
Antonio SILVESTRI – CNAF
André SONNOIS – Edenred
François-Xavier VINCENT – AXA

Ce document a été rédigé par Sophie Bouteiller, Directrice de mission CIGREF.

POUR TOUT RENSEIGNEMENT CONCERNANT CE RAPPORT, VOUS POUVEZ CONTACTER LE CIGREF AUX COORDONNEES CI-DESSOUS :

CIGREF, Réseau de Grandes entreprises
21, avenue de Messine 75008 Paris
Tél. : + 33.1.56.59.70.00
Courriel : contact@cigref.fr

Sites internet :
http://www.cigref.fr/
http://www.entreprise2020.fr
http://www.histoire-cigref.org/
http://www.questionner-le-numerique.org
http://www.entreprises-et-cultures-numeriques.org

SOMMAIRE

1. La cybersécurité est-elle un sujet stratégique pour l'entreprise ? 1
1.1. La cybercriminalité, une menace grandissante 1
1.2. L'engagement de la responsabilité des dirigeants en matière de risque cyber 5
2. Face au risque cyber, quelles réponses ? 6
2.1. Considérer la nature polymorphique du risque cyber 6
2.2. Organiser la gestion opérationnelle du risque cyber et communiquer 7
2.2.1. En théorie 7
2.2.2. En pratique 8
2.3. Maintenir, voire renforcer les actions : quelques pratiques 9
2.4. Suivre et remonter des indicateurs pertinents pour le Comex et pour le CA 11
3. Conclusion 13

FIGURES

Figure 1 : Rôle du Comité d'audit en matière de cybersécurité – IFA, Mars 2016 3

Figure 2 : Méthodologie de maîtrise des risques – AMRAE, Juin 2016 7

1. LA CYBERSECURITE EST-ELLE UN SUJET STRATEGIQUE POUR L'ENTREPRISE ?

Les enjeux et défis numériques[1] auxquels sera confrontée l'entreprise d'ici 2020 ont amené le CIGREF à définir sept axes stratégiques. La cyber sécurité est l'un de ces axes, avec pour ambition de **positionner ce sujet comme un domaine stratégique pour la compétitivité des entreprises.** Dans le plan stratégique CIGREF 2020, cet axe est formulé comme suit : *« En matière de sécurité et de gestion des risques numériques, le CIGREF accompagnera les entreprises dans leur compréhension et la maitrise des enjeux. Il poursuivra ses actions, notamment de formation et de sensibilisation des dirigeants et d'information des collaborateurs,* ***en faisant de ce thème un sujet de Comité Exécutif et de Conseil d'Administration.*** *Il veillera également à partager et faire connaître les meilleures pratiques, organisations et méthodes permettant aux entreprises de mieux faire face aux nouvelles menaces à l'horizon 2020 ».*

1.1. La cybercriminalité, une menace grandissante

En termes de gouvernance des risques, il revient déjà aux Conseils d'administration et aux Comités d'audit d'assumer la responsabilité des implications légales des choix de gestion de l'entreprise. Aujourd'hui, ces décideurs s'organisent pour intégrer la dimension du cyber risque dans cette gouvernance. Si les dirigeants américains ont intégré cela depuis plusieurs années déjà (voir la publication de 2014 de la NACD – *National Association of Corporate Directors* – *Cyber-Risk Oversight – Director's Handbook Series*), en France, cette approche est beaucoup plus récente. La publication récente de l'IFA[2], *Rôle du comité d'audit en matière de cybersécurité* (2016) en est l'illustration.

Cette prise de conscience des Administrateurs a sans doute été suscitée par les récents incidents (Target, TV5 Monde, Sony) et par les actions prises par les pouvoirs publics dans divers pays pour sensibiliser et inciter (voire obliger) les acteurs à se protéger : institutions publiques et militaires, entreprises. Ainsi, au Royaume-Uni, toutes les entreprises du FTSE 350 sont tenues de fournir un bilan de santé en matière de cybergouvernance. Aux Etats-Unis, plusieurs directives obligent désormais les entreprises à présenter, dans leur rapport annuel, leurs actions en matière de cybersécurité (sur le risque de cyber incidents, l'ampleur du risque et la couverture par les cyber assurances par exemple). Ou encore, en France, la Loi de Programmation Militaire de 2013 renforce les obligations de sécurité des OIV (Opérateur d'Importance Vitale) et les pouvoirs de l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information).

[1] Réinventer les modèles d'affaire, multiplier les partenariats, repenser l'organisation pour mieux innover, valoriser les données, maîtriser les nouveaux risques numériques, promouvoir un cadre réglementaire, développer la culture numérique, attirer les talents, renforcer le e-leadership des dirigeants.
[2] Institut Français des Administrateurs

Dans le guide de l'IFA, il apparait que les Administrateurs perçoivent la cybercriminalité comme *« une menace grandissante, qui peut coûter très cher à l'entreprise (entre 400 et 600 milliards de dollars en 2014) (...), accentuée du fait du polymorphisme de la cybercriminalité (crime organisé, espionnage industriel, fraudes, …), de la globalisation de l'entreprise et de la sophistication des attaques : tout cela rend le risque encore plus difficile à maîtriser et à circonscrire »*.

L'IFA considère qu'il revient à chaque organisation de *« trouver l'équilibre entre la défense de ses principaux actifs face à des attaques cybercriminelles et le coût des mesures de cybersécurité »*. Et selon cet institut, les cyber menaces doivent être intégrées à la politique de gestion des risques et de gouvernance de l'entreprise, pour définir les moyens à mettre en œuvre afin d'assurer la protection des données et la défense des systèmes d'information. Ainsi, la cartographie des risques doit faire apparaître le risque d'une cyberattaque contre des actifs ou processus clés de l'entreprise : décrire les circonstances d'une attaque, les motivations possibles, les intentions et les techniques de l'éventuel pirate.

L'IFA pose donc la cyber sécurité comme une problématique de management des risques, qui dépasse largement le périmètre informatique.

Une menace grandissante mais des budgets toujours difficiles à obtenir

*Dans certaines entreprises, plutôt industrielles, les responsables des risques cyber rencontrent des problèmes récurrents de ressources et de budgets en matière de SI. En effet, dans ces métiers, les investissements en matière de gestion de risques sont prioritairement réalisés pour gérer les risques industriels, la cybersécurité n'est pas vue comme la priorité. Pourtant, avec le développement des objets connectés, du M2M (*Machine to Machine*) et de l'entreprise étendue, l'ouverture nécessaire des systèmes d'information et le développement de plateformes sont autant d'éléments qui augmentent les risques cyber.*

En termes de gouvernance, l'IFA recommande aux Administrateurs de concentrer leur attention sur 3 domaines :

Figure 1 : Rôle du Comité d'audit en matière de cybersécurité – IFA, Mars 2016

1. **Leadership et facteurs humains :** il s'agit *« d'évaluer le degré d'implication du management dans la gouvernance de la cybersécurité et le développement d'une culture sécurité »* et de *« promouvoir les personnes clés et les compétences »*
2. **Opérations, SI et conformité :** il s'agit *« d'apprécier le niveau de prise en compte de la cybersécurité dans les SI et les opérations au quotidien »*
3. **Gestion des risques et continuité d'exploitation :** il s'agit de *« définir le degré de prise en compte des cyber risques dans le dispositif de gestion des risques »*.

Ces formes d'interaction doivent permettre aux Administrateurs de poser des questions de diverses natures avec le management :

- Quels sont les principaux actifs critiques à protéger ? Sont-ils protégés et comment ?
- Quelle est l'exposition de l'entreprise au risque cyber et quel est le niveau acceptable ?
- Quels contrôles sont en place pour surveiller les réseaux, ceux des fournisseurs, les installations sur les appareils fixes et mobiles de l'entreprise ?
- Qui est responsable de leur protection ?
- L'entreprise dispose-t-elle d'un personnel formé et expérimenté en matière de prévention des cyber risques ?
- Les ressources allouées à la cybersécurité sont-elles suffisantes ?
- L'entreprise est-elle préparée en cas d'incident majeur ?

Les 3 domaines d'interaction mis en évidence par l'IFA sont également énoncés dans le guide de la *NACD* de 2014, sous la forme de 5 principes, et en plus des questions nécessaires à poser par les Administrateurs selon l'IFA, la *NACD* en a identifié d'autres, qui nous semblent intéressantes à indiquer en complément :

- Les aspects de cybersécurité sont-ils pris en compte et traités en temps opportun dans les moments clés de la vie de l'entreprise (fusion-acquisition, lancement de nouveaux produits, conclusion de partenariats stratégiques, …) ?
- L'entreprise participe-t-elle à des actions publiques ou privées dans l'écosystème de la cybersécurité ?
- L'entreprise est-elle assurée pour le risque cyber et si oui, que couvre l'assurance ?

In fine, l'IFA recommande aux Administrateurs la série d'actions suivantes :
« Quelles bonnes pratiques pour les membres de la gouvernance ?

- *Superviser le dispositif de gestion du risque cyber : un de ses Comités peut se voir confier une mission de suivi ;*
- *Mettre la cybersécurité à l'ordre du jour des réunions du CA au moins une fois par an ;*
- *S'assurer que l'entreprise a identifié ses informations critiques, à protéger en priorité ;*
- *Vérifier que les formations sont actualisées et prennent en compte les nouvelles sources de vulnérabilité liées à la cybercriminalité ;*
- *S'assurer de l'existence d'un RSSI et de la bonne adéquation des ressources allouées ;*
- *Avoir une présentation du dispositif de prévention et de détection d'une attaque cybercriminelle, avec ses conséquences ;*
- *Examiner le déploiement du dispositif de lutte contre les cyberattaques au sein du groupe (cellule de gestion de crise, PCA [Plan de Continuité d'Activité], …) et s'assurer de l'existence d'un processus de vérification de son bon fonctionnement ;*
- *Examiner le processus de remontée des cas d'attaques cybercriminelles au sein du groupe ;*
- *Examiner les résultats des tests réalisés par le management ;*
- *Vérifier l'existence et l'efficience d'un programme d'amélioration continue. »*

Autant d'actions de vérifications sur lesquelles il est vraisemblable que les DSI et RSSI seront de plus en plus sollicités dans les années à venir !

Focus sur l'identification des informations critiques pour l'entreprise et leur protection

Dans la mesure où il est impossible de tout sécuriser, il est nécessaire d'identifier les actifs critiques de l'entreprise et de sécuriser prioritairement ceux-ci.

1.2. L'engagement de la responsabilité des dirigeants en matière de risque cyber

Si la question de l'engagement de la responsabilité des dirigeants semble avoir un impact moins important en France qu'aux Etats-Unis, ils y sont tout de même sensibles. Ceci d'autant plus que les avertissements publics de la CNIL (Commission Nationale de l'Informatique et des Libertés) sur les données (et les amendes associées), mais aussi le règlement européen sur la protection des données à caractère personnel (qui prévoit des amendes pouvant aller jusqu'à 4% du chiffre d'affaires mondial de l'entreprise) sont devenus des réalités difficiles à ignorer et ont sans doute participé à la prise de conscience des dirigeants. Avec le numérique, les DSI mais aussi les Directeurs Marketing, Directeurs du Digital, Directeurs des Données et autres Directeurs Métiers vont supporter de plus en plus de responsabilités, en particulier sur le traitement des données personnelles. Charge à l'entreprise de trouver le bon équilibre en termes de répartition des responsabilités, sans oublier les responsabilités des fournisseurs (*SaaS*). Le numérique dilue la chaine de responsabilités, dans l'entreprise (DSI / Métiers) et en dehors (fournisseurs), qui deviennent alors de plus en plus complexes à identifier.

Mais alors, comment positionner la cybersécurité dans les discussions avec le Comex ? L'exposition des entreprises au risque cyber est plus ou moins importante selon leur cœur de métier, mais toutes sont concernées. **Quelle entreprise ne voit pas aujourd'hui ses clients impactés, l'image du groupe mise en jeu, et les dirigeants eux-mêmes concernés par le risque cyber ?** Pour nombre d'entreprises, le risque cyber est devenu un risque majeur qu'il faut vulgariser auprès du Comex, des Administrateurs et plus largement auprès de tous les utilisateurs. **Le sujet est encore trop souvent vu sous un angle technique alors qu'il est essentiellement organisationnel.**

Le risque cyber : un risque majeur pour un nombre croissant d'entreprise

*Certaines entreprises disposent désormais d'un département « Risques numériques ». Dans celles-ci, l'analyse du risque cyber est systématisée dans les projets et programmes (*security by design*), dans le cadre d'une démarche regroupant le risque numérique, l'audit interne et le juridique. Un plan d'audit et contrôle est présenté en moyenne 2 fois par an au Comex.*

Dans ces entreprises, les discussions en Comex se font dans des termes business *: impacts sur les clients et sur l'image de l'entreprise, et donc sur le chiffre d'affaires de l'entreprise, impacts sur les collaborateurs eux-mêmes, exposition des dirigeants et donc engagement de leur responsabilité.*

2. FACE AU RISQUE CYBER, QUELLES REPONSES ?

La réponse judiciaire est primordiale pour contrer ces cyberattaques, d'autant que la question des frontières se pose avec force, puisque ce risque, par nature transfrontalier, nécessite une coopération internationale qui n'est pas toujours évidente à coordonner. Les cybercriminels jouissent donc la plupart du temps d'un sentiment d'impunité.

Ainsi, cette forme de réponse, si elle nécessaire, est insuffisante et insatisfaisante, surtout si l'on garde en tête que les Administrateurs considèrent qu'il revient à chaque organisation de *« trouver l'équilibre entre la défense de ses principaux actifs face à des attaques cybercriminelles et le coût des mesures de cybersécurité »*. Dès lors, comment s'organiser en interne ?

2.1. Considérer la nature polymorphique du risque cyber

Le risque cyber peut prendre au moins deux formes, selon l'ANSSI : sabotages (prise de contrôle de systèmes) et vols (détournements financiers, vol de données, vols de produits ou services). Ajoutons « l'hacktivisme », par idéologie (atteinte à l'image et/ou à la marque de l'entreprise) qui tend à se développer.

Ce risque est d'une grande complexité, liée à la nature changeante quasi permanente du risque dont les conséquences sont variées. Les vecteurs d'amplification sont également à l'origine de la complexité de ce risque : erreurs humaines, processus de déploiement ou d'installation, faiblesses des systèmes et réseaux, des postes de travail avec accès web et *smartphones*, des serveurs, ou encore attaques dans la durée et risques liés aux défaillances des sous-traitants et autres fournisseurs critiques. Par ailleurs, le terrorisme et les risques géopolitiques viennent aggraver la menace, car ces facteurs rendent le risque cyber plus complexe à identifier et à localiser.

Pour protéger l'entreprise, diverses actions peuvent être mises en œuvre :

- Prévention et protection du SI et détection d'événements anormaux ;
- Formation et sensibilisation des utilisateurs ;
- Gouvernance, contrôle et audits.

2.2. Organiser la gestion opérationnelle du risque cyber et communiquer

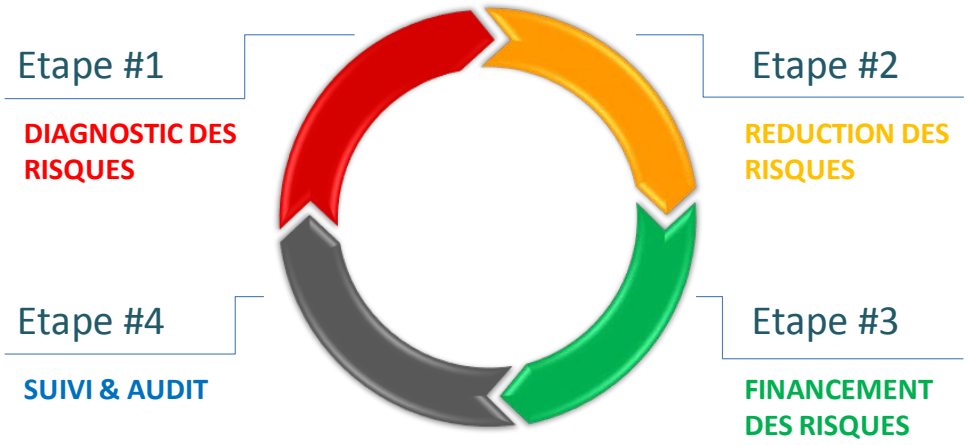

Figure 2 : Méthodologie de maîtrise des risques – AMRAE, Juin 2016

2.2.1. En théorie

Cette méthodologie de maîtrise de risques est une approche classique, les *Risks Managers* l'appliquent pour identifier et mitiger toutes formes de risques :

- Le diagnostic vise à identifier tous les risques ;
- La réduction vise à diminuer les risques ;
- Le financement vise à prévoir et assurer ou transférer le risque s'il se réalise : il faut financer leur prévention autant que leurs conséquences post-survenance (rétention ou assurance) ;
- Le suivi et l'audit doivent permettre d'actualiser la cartographie ; ils peuvent être assurés par un dispositif de suivi et de *monitoring* pour garantir une vision à jour des risques qui doivent être audités (audits des plans d'action définis).

S'agissant du risque cyber, les systèmes d'information sont en évolution permanente (globalisation, ouverture, mobilité), complexes à appréhender globalement (chaine de sous-traitance, externalisation de tout ou partie du SI, téléphonie, …) et pas uniquement techniques (humains, organisationnels, …). Dès lors, les risques associés le sont également et cela impose d'innover en termes de moyens et de réponses pour faire face à ces nouveaux risques, y compris réglementaires. Et pour les traiter de manière adéquate (en avoir une approche la plus holistique possible), la démarche doit être coordonnée entre le *Risk Manager*, le DSI, le RSSI, le *Chief Data Officer*, le *Data Protection Officer,* le Directeur juridique, le Directeur des Ressources Humaines, le Directeur de la Stratégie et tout(s) autre(s) acteur(s) jugé(s) pertinent(s).

Les solutions de réduction du risque sont autant techniques (*firewall*, sauvegardes, chiffrement des données, …) que liées à la mise en place de processus (analyse de risques,

règles de développement, normes de sécurité, …). Elles doivent être également humaines (formation et sensibilisation de tous les utilisateurs) et financières (assurances).

Focus sur la couverture du risque cyber

En termes de préparation, la gestion du risque cyber a des impacts en termes assuranciels et la question de la couverture du risque cyber est grandissante dans les entreprises. Mais il s'agit d'un risque nouveau, qui ne bénéficie pas encore de définition officielle : comment est pris en compte le risque cyber aujourd'hui dans les assurances ? Quel périmètre couvrent-elles ? Comment sont prises en compte les données personnelles ?

Pour l'AMRAE[3], la question de l'assurance cyber est complexe car les modèles d'assurance doivent être croisés avec la cartographie du risque cyber. Or, ce risque est mouvant et les dommages ne sont pas nécessairement physiques donc difficilement chiffrables : comment couvrir des dommages immatériels non consécutifs à un dommage matériel, comme par exemple le risque de perte d'image, qui est par nature très difficile à valoriser ? Il existe désormais des polices cyber « Dommages et Responsabilité Civile », qui viennent s'ajouter par exemple à une police « Tous risques informatiques ». Là encore, un travail précis d'analyse du risque est à faire dans l'entreprise par le Risk Manager*, le RSSI et le DSI pour permettre aux Administrateurs de juger de la pertinence de prendre ce type de police.*

2.2.2. En pratique

Sur le plan opérationnel, le lien entre le risque stratégique et les moyens de protection mis en place doit apparaître dans la cartographie des risques. **Une des méthodes pour faire ce lien est l'approche par les scénarios, car elle permet d'anticiper les menaces pouvant avoir des impacts sur le *business.***

En outre, cette approche permet d'avoir une cartographie la plus complète, utile et très claire pour le management et les Administrateurs, parce qu'elle correspond à une réalité en termes de risque pesant sur le *business* de l'entreprise. **Le *Risk Manager* doit la faire évoluer et l'adapter, d'autant qu'en matière de cyber, elle devient rapidement obsolète** (le cycle de mise à jour « recommandé » par l'AMRAE est *a minima* une fois par an, sachant que dans les télécoms par exemple, cette mise à jour se fait tous les trimestres).

L'important est de montrer au management, et aux Administrateurs le cas échéant, que l'entreprise est préparée à la survenance du scenario théorique et qu'elle peut l'adapter à la réalité du moment (*ie* être capable de proposer une réponse différenciée par rapport à la problématique rencontrée dans la réalité). D'ailleurs, il faut être attentif à valider la

[3] AMRAE : Association Management des Risques et des Assurances de l'Entreprise (www.amrae.fr)

cartographie (et la réviser) au bon moment par rapport aux sessions budgétaires annuelles de manière à chercher à obtenir les budgets les plus adaptés possibles au traitement.

Mais l'approche « cartographie » doit aussi être pensée comme un *Rubik's Cube* : proposer différents angles de vue pour casser l'approche par silos. Il y a une réforme à faire dans les entreprises en matière de gestion des risques, pour développer une approche à 360° qui mixe le court et le long terme, l'interne et l'externe, les risques forts et les risques faibles. Le numérique, de par sa transversalité, oblige les acteurs à développer une vision non pas morcelée mais holistique d'un risque (le risque cyber) qui devient global par nature.

2.3. Maintenir, voire renforcer les actions : quelques pratiques

Mettre en place une méthode de gestion de risques

- Travailler en binôme avec l'audit pour élaborer un plan de gestion des risques numériques à partir d'une analyse fine de l'évolution des risques dans l'environnement de l'entreprise.
- Travailler avec les Métiers pour comprendre leurs processus et les risques associés, de manière à obtenir une cartographie réaliste des impacts liés au risque cyber.
- Sortir la gouvernance de la cybersécurité de l'IT, tout en assurant l'équilibre avec la DSI.
- Travailler en liaison étroite avec l'audit interne, la direction des risques et le contrôle interne pour évaluer l'impact métier du risque cyber (pas le risque IT).
- Scénariser précisément les risques, en veillant à ce qu'ils soient réalistes car s'ils sont trop fantaisistes, ce n'est pas crédible. Il faut raconter une histoire : comme par exemple, 20 000 personnes n'ont plus accès à l'eau pendant une semaine, l'entreprise se fait voler 150 millions d'euros dans la caisse, 150 000 voyageurs sont bloqués dans les transports, …).

Informer le Comex et le CA

- Donner le bon niveau d'information, avec le bon langage (*business* non pas technique), pour permettre aux dirigeants de décider : parler de pérennité de l'entreprise, de *business continuity*, de revenus, de confiance, d'image, de protection de la R&D/innovation (à noter : ce dernier point arrive en tête des risques cyber dans les entreprises).
- S'appuyer sur l'actualité pour maintenir l'attention du Comex et du CA sur le sujet, présenter les risques à partir de retours d'expérience.
- Présenter des chiffres qui illustrent des faits, et corréler le risque au *business* de l'entreprise.

- Faire intervenir des interlocuteurs pertinents devant le Comex et/ou le CA pour les éveiller aux impacts concrets du risque cyber : un expert reconnu (ANSSI, DGSI, …), un « *hacker* éthique », etc.
- Expliquer au Comex la manière dont l'évolution du risque cyber expose davantage l'entreprise, avec une répartition des responsabilités et une valorisation pour chiffrer le risque, et discuter des moyens financiers nécessaires pour gérer le risque :
    - Décliner les analyses de risques en fonctions de segments et applications SI ;
    - Identifier les périmètres informatiques sensibles et les isoler pour définir sur quelles parties sensibles il est nécessaire d'alerter le Comex ;
    - Mettre le focus sur les éléments les plus sensibles de l'entreprise, en particulier les données, et valoriser le risque en termes *business* : % perte potentielle de clients, % de perte du CA par exemple ;
    - Parallèlement, travailler sur la continuité d'activité.

Focus sur les Plans de Continuité d'Activité (PCA)/Plans de Reprise d'Activité (PRA)

Toutes les entreprises représentées dans le groupe de travail disposent d'un PRA/PCA. Les budgets alloués et la taille des équipes qui les gèrent et les mettent à jour évoluent en fonction de la criticité des systèmes d'information par rapport au cœur de métier de l'entreprise. Le rattachement des équipes est variable : Direction de la Conformité, Direction des Risques et de la Qualité, Direction des Systèmes d'Information, Direction des Opérations, Direction de la Production.

Sensibiliser et suivre

- Organiser un exercice de cyber crise avec le Comex, au minimum une fois par an.
- Mettre en place et réunir un comité de sécurité dédié à la protection des données : pour certaines entreprises en particulier, le sujet cyber sécurité apparait de plus en plus fréquemment dans les relations avec certains clients qui, soucieux de la protection de leurs données, exigent la mise en place de mesures de sécurité formalisées dans un « contrat » spécifique, qui implique un engagement de l'entreprise, en plus des mesures déjà existantes encadrant les relations client/fournisseur dans le cadre de services dans le Cloud.
- Responsabiliser les Métiers et autres acteurs (fournisseurs notamment) puisque le niveau d'exposition est de plus en plus difficile à mesurer dans un contexte d'entreprise ouverte.

***Organiser un exercice de cyber crise : exemple avec le* phishing**

La DGCCRF définit le phishing *(hameçonnage ou filoutage) comme une « technique par laquelle des personnes malveillantes se font passer pour de grandes sociétés ou des organismes financiers qui vous sont familiers en envoyant des mèls frauduleux et récupèrent des mots de passe de comptes bancaires ou numéros de cartes de crédit pour détourner des fonds ». La cyber crise peut donc être une simulation de* phishing *par exemple, pour tester les usages des collaborateurs, y compris du Comex. Ce type d'exercice doit se préparer en étroit partenariat avec la DRH et les Institutions Représentatives du Personnel. L'objectif ne doit pas être autre que de sensibiliser les collaborateurs et le Comex aux bonnes pratiques et bons réflexes à acquérir dans une telle situation.*
Comme dans tout type de crise, le département « Communication » de l'entreprise joue un rôle clé dans ce type de crise.

En complément de ces quelques pratiques, nous vous invitons à lire également un rapport de l'INHESJ : *Comment faire de la SSI un sujet de Comex ?*, disponible sur le site du CIGREF. Ce rapport fait le point sur l'évolution de la menace cyber et la réglementation, et propose une série de pratiques pour parler de cyber en Comex.

2.4. Suivre et remonter des indicateurs pertinents pour le Comex et pour le CA

Le rôle du RSSI, avec le DSI, est d'éclairer le Comex et le CA sur les risques : les expliquer, les qualifier et les valoriser, à l'aide d'indicateurs pertinents. Or, sur ce sujet, les entreprises ne sont pas toutes d'accord sur la nature des indicateurs à remonter aux dirigeants, d'autant que l'élaboration d'un tableau de bord peut se révéler très complexe et peu pertinente.

Les incidents : certaines entreprises ont choisi de remonter au Comex les incidents au cas par cas plutôt que de communiquer sur des indicateurs qu'elles jugent parfois peu pertinents car généralement tous « au vert » (nombre d'incidents par exemple). Cela dit, il existe plusieurs types d'incidents, dont certains sur lesquels il peut être pertinent d'informer le Comex en fonction de leur sinistralité :

- Les incidents répertoriés pour lesquels on voit l'impact et que l'on sait analyser ;
- Et éventuellement, les situations dangereuses et les « presqu'incidents ».

Le taux d'attaques : cet indicateur ne semble pas faire l'unanimité non plus car la définition d'une attaque n'est pas standard. Par contre, le taux de sinistralité, comparé au nombre d'utilisateurs ou d'appareils semble intéressant.

Le taux d'exposition de l'entreprise : cet indicateur fait l'unanimité, rapporté à un segment de risque et aux actions possibles à envisager pour le réduire/le couvrir, il est audible par le Comex.

Exemple de tableau de bord trimestriel « Risque cyber », partagé avec le Comex et le CA

			Impact on Critical Assets									
Type of Cyber Risks		**Main Scenario**	**Personal Data**	**Strategic Data**	**Cash**	**Critical process**	**Reputation**	**Level of Threat (0-4)**	**Pre-Event : adequacy of prevention controls (0-4)**	**Post-Event: response effectiveness (0-4)**	**Residual Risk Level 2016Q1**
Targeted computer attacks against the company (●)	A1	Unauthorised users try to break into systems	✓	✓	✓	✓	✓	3	2	2	●
	A2	Service interruption due to denial-of-service attack				✓		2	4	3	●
	A3	The company web site is defaced					✓	3	4	3	●
	A4	Industrial espionage	✓	✓			✓	3	2	3	●
	A5	Criminal activity	✓		✓			4	3	3	●
	A6	Terrorism, State-sponsored hacking, Hacktivism (for politically or socially motivated reasons)	✓	✓		✓	✓	4	2	2	●
Malware (Malicious computer program) (●)	B1	Intrusion of malware in critical operational servers				✓		2	3	2	●
	B2	Large infection of workstations with malware	✓	✓			✓	3	4	2	●
	B3	Implemention of a time bomb that leads to data loss by a disgruntled developer				✓		2	2	2	●
	B4	Phishing attack leads to theft of company data	✓	✓			✓	4	3	3	●
Information (data breach: damage, leakage and access) (●)	C1	Portable media containing sensitive data (laptop, Blackberry, iPad, USB drives, portable disks, etc.) is stolen / lost / disclosed	✓	✓				3	2	3	●
	C2	Supplier deficiency or targeted attack against key supplier that leads to sensitive data stolen / lost / disclosed	✓	✓				4	2	2	●
	C3	Email or social media misuse / inadequate usage cause sensitive data disclosure	✓	✓			✓	2	2	2	●
	C4	Inefficient retaining / archiving / sharing of information that leads to sensitive data loss / disclosure	✓	✓			✓	3	1	2	●
Regulatory compliance (●)	D1	Unawareness of potential regulatory changes have an impact on the operational IT environment				✓	✓	3	2	2	●
Brand e-reputation (●)	E1	Campaign on social networks of malicious statements against the company					✓	2	2	2	●

Colours used to illustrate risk assessment are as follows

Low	●	*No material risks.*
Medium Low	●	*No material risks but further analysis required.*
Monitor	●	*Material risks exist that were not previously on the risk radar or insufficient visibility. Management action taken is likely to be proportionate and risks are deemed manageable.*
Monitor closely	●	*Material risks persist with extremely limited visibility. Management action taken but uncertainty on its effectiveness or efficiency or timeliness.*
High	●	*Material risks persist and require an urgent plan and implementation or no visibility at all.*

Threat level, prevention and response effectiveness (0-4): very low,low, medium, high, very high

A noter :

- Les notes des colonnes *Niveau de menace*, *Prévention* et *Réaction* sont fictives et ont été attribuées pour l'exemple.
- Les lignes du tableau reprennent la classification COBIT.
- Les couleurs dans la colonne *« Residual Risk Level »* sont déterminées en fonction de 3 critères : niveau de menace, niveau de prévention et capacité de réaction

3. CONCLUSION

Le risque cyber ne revêt pas la même importance pour toutes les entreprises, et n'est pas uniforme puisqu'il peut impacter des domaines très différents d'un secteur à l'autre (systèmes industriels dans l'industrie, données personnelles et chaine d'approvisionnement dans la grande distribution, etc.). Ainsi, dans certains secteurs d'activités (banques et assurances notamment), les dirigeants sont déjà très sensibilisés. Ceci s'explique par une régulation forte, et par le fait que le risque cyber soit déjà pris en compte par les agences de notation. D'autres secteurs par contre peinent à considérer ce risque comme un vrai risque stratégique.

Ainsi, sans jouer à se faire peur, le risque cyber doit être traité, analysé et bien positionné sur l'échelle des priorités dans l'esprit des dirigeants, en fonction de leurs enjeux *business*. Il n'est pas pour autant nécessairement un sujet de Comex. Les moyens humains et financiers doivent être alloués à la hauteur de ces enjeux, mais, à nouveau, ils pourront être très différents d'une entreprise à l'autre, en fonction des risques identifiés.

La cybersécurité doit être traitée à sa juste place dans la gouvernance de l'entreprise. Les risques cyber suivent une tendance haussière, et le groupe de travail recommande aux entreprises qui n'auraient pas encore pris de dispositions pour les appréhender et les traiter à la hauteur des enjeux qu'ils peuvent représenter pour elles, en fonction de leur contexte, de le faire sans plus attendre.

CIGREF

21 avenue de Messine

75008 PARIS

Tel. : +33 1 56 59 70 00

cigref@cigref.fr

www.cigref.fr