Du cyber logos, de la dimension holistique de l'action, et de la stratégie globale des organisations

Alice LOUIS
Dirigeante
Cabinet de Conseil DIcé

Ilhame CHOUKRANI
Dirigeante
Cabinet de Conseil
Potentiels

La transformation digitale, l'évolution des usages, la prolifération des menaces issues du Cyberespace ainsi que le recours aux Systèmes d'intelligence artificielle faible, obligent les acteurs du secteur public et privé à **repenser de manière globale et continue leur stratégie** en y intégrant notamment un modèle de gouvernance capable de répondre efficacement à ces nouvelles exigences, s'agissant, en particulier, de la Cybersécurité.

Rappelons à titre liminaire que la cybersécurité comprend *« les usages défensifs et offensifs des systèmes d'information […]. Elle prend en compte* ***les contenants****, c'est-à-dire les moyens techniques (réseaux informatiques, téléphoniques, satellitaires…) utilisés pour l'échange de données, qui peuvent faire l'objet d'opérations d'infiltration, d'altération, de suspension voire d'interruption,* ***comme les contenus****, c'est-à-dire l'ensemble des informations qui circulent ou sont stockées sur des supports numériques (sites Internet, bases de données à caractère personnel, messageries et communications électroniques, transactions dématérialisées…).*
La cybersécurité porte aussi bien sur la protection et ***l'attaque d'équipements informatiques*** *(la guerre pour ou contre l'information), afin de les surveiller ou d'en prendre le contrôle, que sur* ***les renseignements disponibles sur la Toile*** *(la guerre par l'information), avec de possibles atteintes à la réputation, le vol de données sensibles, des actions de piratage numérique et autres campagnes de dénigrement ». (Définition et historique de la cybersécurité, Nicolas Arpagian, PUF, 2015)*

Du cyber logos & de l'alignement des stratégies

Penser « la sécurité et la gestion des risques », avec raison et rationalité, permet d'élaborer une stratégie cyber en vue d'assurer une véritable protection du patrimoine informationnel des Organisations. A cet effet, le levier de ce qu'il est coutumier d'appeler « **la stratégie d'entreprise** [1] », ici entendue comme l'ensemble des choix d'allocation de ressources qui définissent le périmètre d'activité d'une Organisation en vue de réaliser ses objectifs[2], **peut être actionné afin de s'inspirer des meilleures pratiques adoptées, dans ce domaine, par les Dirigeants des entités**. Etant d'ores et déjà précisé que « la stratégie des Organisations » et « la stratégie cyber » auront tout intérêt à s'aligner ainsi qu'à se nourrir l'une de l'autre, afin de garantir une performance durable et résiliente.

Aussi, les fondamentaux de la **Stratégie d'entreprise** nous rappellent, en tout premier lieu, que les entités évoluent dans un monde dit « **V.I.C.A** ». En substance, ce dernier oblige les Organisations à développer une stratégie qui incorpore une double temporalité, d'une part, une approche robuste et durable, et, d'autre part, une posture d'agilité permanente afin de pouvoir s'adapter à leur environnement. Ce concept qui est parfaitement

[1] Employé dans son sens générique, cela englobe l'ensemble des organisations.

[2] https://fr.wikipedia.org/wiki/Stratégie_d%27entreprise

applicable **à la cybersécurité (Cf. qualification dans l'encart qui suit)** met immédiatement en évidence les défis auxquels les Organisations sont confrontées pour protéger leurs actifs numériques dans un paysage imprévisible, en rapide évolution, et, de surcroît, géopolitiquement instable.

Le concept V.I.C.A appliqué à la cybersécurité

La volatilité dans le contexte de la cybersécurité fait référence à l'évolution rapide de la nature des menaces, avec l'émergence régulière de nouvelles méthodes d'attaque et de variantes de logiciels malveillants.
L'incertitude fait référence au défi de prévoir et de se préparer aux menaces futures, compte tenu de la nature en constante évolution du paysage des menaces.
La complexité fait référence à la complexité des systèmes d'information, de la gestion des dépendances, avec plusieurs appareils, plates-formes, applications interconnectés et SIA qui créent des vulnérabilités.
L'ambiguïté fait référence à la difficulté d'interpréter les données, de prendre des décisions éclairées dans un monde où les cybermenaces peuvent être déguisées ou cachées.

Focus sur les Cyber-responsabilités des dirigeants.

Dans la majorité des cas, le dirigeant n'a pas conscience de l'étendue de sa responsabilité sur le plan civil (l'obligation de répondre du dommage causé à autrui suite à une faute de gestion) comme sur le plan pénal (l'obligation de répondre des infractions commises y compris dans l'hypothèse d'une faute non intentionnelle).
Plus particulièrement avec le RGPD qui a introduit une obligation de sécurité renforcée, ainsi que les sanctions visées aux articles 226-16 et suivants du Code pénal qui dispose qu'en cas de *« faille de sécurité ayant entraîné la destruction, la perte, la divulgation ou l'accès non autorisé à des données personnelles de clients ou de salariés traitées par l'entreprise, la responsabilité pénale de l'entreprise pourra être engagée sur divers fondements énoncés aux articles suivants »*.
Néanmoins, le dirigeant pourra « s'exonérer » de cette responsabilité notamment en **déléguant ses pouvoirs à une personne, pourvue de la compétence, de l'autorité et des moyens nécessaires pour faire respecter la réglementation**.

https://www.zdnet.fr/actualites/les-pdg-vont-devenir-personnellement-responsables-des-incidents-de-securite-cyberphysiques-assure-le-gartner-39908865.htm Les comportements à risque des dirigeants fragilisent la cybersécurité (cio-online.com)

En conséquence, les meilleures méthodes de modélisation de la Stratégie d'entreprise peuvent être empruntées pour être transposées.

Dès lors ce constat effectué, **et poursuivant cette analyse « miroir**, il conviendra de recommander aux Organisations d'intégrer **la Summa divisio** (micro (i), macro (ii)) suivante, pour réaliser un diagnostic global visant en « interne », à identifier et partager les forces et les faiblesses de l'Organisation eu égard aux objectifs fixés, et par ailleurs, en « externe », à mettre à jour (et à partager) les opportunités et les menaces.

Citons, à titre d'exemple, **les évolutions technologiques** (l'actualité récente de Chat GPT nous démontre toute l'importance de cette prise en considération)**, l'hyper régulation** (RGPD, NIS 2, DSA, DMA, LME, IA At, Cyberbesurity Act, etc.), ainsi que **les impacts d'ordre sociétal et environnemental**.

In fine, il parait essentiel de formaliser la stratégie « cyber », notamment afin de déterminer qu'elle est sa contribution réelle à la stratégie plus globale de l'Organisation. Etant précisé que cette matérialisation (qui peut s'inspirer des modèles existants qui distinguent ce qui suit) **comporte un enjeu de confiance numérique**.

(i) En premier, la perspective générale ou encore appelée l'intention stratégique. Il convient de formaliser la vision, les missions, les valeurs portées par la Cybersécurité, en lien avec la Stratégie de l'Organisation ;

(ii) En deuxième lieu, « donner du corps » aux services proposés. Il convient de formaliser la proposition de valeur ainsi que son modèle opérationnel afférent (« architecture de valeur et dimension financière, autrement dénommée « l'équation économique »).

Plus particulièrement, il s'agira en l'espèce :

- D'identifier les enjeux politiques, économiques, sociaux, technologiques, environnementaux et légaux qui vont influencer les stratégies,

- De co-construire en intégrant des itérations avec l'ensemble des fonctions (en particulier, les entités qui délivrent auprès des clients/citoyens/usagers, les fonctions IT, les équipes en charge de la régulation, de la conformité, de l'audit et du contrôle) en détaillant ce que la stratégie va produire comme valeur finale,

- D'expliciter ce en quoi la proposition de valeur sera unique, différenciée, substantielle,

- De traduire la stratégie dans un langage compréhensible /pédagogique.

- De définir la chaine de valeur qui va concourir à produire **le socle de la confiance numérique**.

Extrait des travaux « Horizon Cyber 2030, Perspectives & Défis »
Campus Cyber*

L'ultra-connectivité, liée à l'accélération des échanges de données et de leur vitesse ;
L'ultra-cloisonnement, liée à l'exacerbation des souverainetés, en raison de la méfiance géopolitique et des craintes face aux dépendances entre écosystèmes numériques ;
L'ultra-green, liée au renforcement des idéologies environnementales et de sobriété numérique face au changement climatique ;
L'ultra-réglementation, liée au durcissement réglementaire.

*https://campuscyber.fr/insider-horizon-cyber-2030/

De la dimension holistique de l'action & de l'efficience de l'exécution

Si l'élaboration de la stratégie constitue une étape clé, sa mise en œuvre n'en est pas moins importante. C'est précisément l'articulation entre différentes composantes qui va impacter positivement l'efficacité d'une exécution stratégique.
Les composantes relèvent de deux dimensions distinctes : les dimensions dites « hard » (i), et les dimensions dites « soft » (ii).

(i) ***Les dimensions « hard »*** *englobent les fondations suivantes :*

- **Une Stratégie** de l'Organisation en matière de cybersécurité, clairement définie et communiquée à tous les niveaux de l'organisation ;

- **Les Systèmes, autrement dit** les processus, les procédures et les outils (les systèmes informatiques doivent être configurés pour protéger les données à caractère personnel et les actifs de l'entreprise).

- **La Structure** organisationnelle conçue pour soutenir la sécurité juridique et informatique avec l'attribution de responsabilités claires, mais aussi l'organisation et la gouvernance informelles ; toutes au service du déploiement de la stratégie cyber.

(ii) ***Les dimensions « soft »*** *intègrent les sujets qui soutiennent les fondations :*

- **Deux volets inhérents au facteur « humain » dénommés « Staff & Skill » :**

Un juste calibrage de ressources et le développement de compétences pluri et interdisciplinaires sont essentielles. Les plans d'attraction, de rétention et de développement des ressources cyber sont essentiels pour capitaliser sur les connaissances des équipes et des organisations et faire face aux enjeux pénuriques du secteur. Une attention particulière doit être portée au développement des compétences comportementales dans un contexte anxiogène[3] qui

[3] https://www.presse-citron.net/sous-estimes-epuises-et-isoles-lappel-a-laide-des-francais-de-la-cybersecurite/

nécessite de grandes qualités de communication pour rendre le sujet accessible à différentes natures de d'interlocuteurs.

- Deux volets inhérents au facteur « culturel » dénommés « **Style & Shared Values ».**

En fonction de l'Organisation, il est important que les responsables en charge des sujets cyber alternent des « styles » qui favorisent la sécurité, la confiance, l'engagement ou l'autonomie des parties prenantes impliquées. Cela suppose d'adapter son style aux différentes populations concernées leurs besoins et facteurs de motivation. Le ciment qui relie toutes les dimensions les unes aux autres est celui de la Valeur Partagée et/ou des Valeurs Partagées. Plus que jamais, dans le monde hyper régulé/connecté/ cloisonné/green, additionner à des éléments tangibles de stratégie cyber des valeurs fondamentales qui encouragent la collaboration commune**, la cyber-conscience, la cyber-exemplarité et l'Ethique vont devenir essentielles, voire discriminantes**.

De l'impact sur la Stratégie globale des Organisations & de la création de valeur.

A titre de propos conclusif, il doit être réaffirmé avec conviction et vigueur que la cybersécurité est aujourd'hui incontournable pour l'ensemble des Organisations, et, dans ce cadre, l'élaboration d'une stratégie dédiée est devenue primordiale. En effet, **au-delà de servir la couverture des risques, cette dernière s'inscrit dans une démarche de création de valeur ; de valeur digitale mais aussi de valeur globale.**

Par ailleurs, s'agissant de la Data, les nombreuses fuites de données observées ces derniers mois démontrent que l'enjeu de la cybersécurité représente bien plus qu'un simple respect de la réglementation, a fortiori avec les avancées fulgurantes des modèles génératifs des Systèmes d'intelligence artificielle qui vont très probablement marquer un tournant dans ce domaine, y compris en matière de cyberdéfense.

Rappelons que le système Chat GPT, qui est une redoutable machine à coder, est capable de générer des attaques sophistiquées au vu des tests d'ores et déjà été effectués.

In fine, il est précisé que Chat Gpt enregistre toutes les données des Organisations.
Nonobstant les problématiques de droit de Propriété Intellectuelle, de Secret des affaires, de Vol de données afférentes (et accessoirement d'intelligence économique), **« *la diffusion massive* », sans contrôle, « *d'une telle technologie pourrait nous conduire à une situation de défiance généralisée* »** [4] génératrice de nouvelles menaces.

Focus Cybersécurité vs Chat GPT

« Les ingénieurs de Samsung ont utilisé ChatGPT pour évaluer le code source de l'entreprise.
Ils ont demandé au chatbot d'optimiser les séquences de test pour identifier les défauts dans les puces qu'ils concevaient.

Selon le site Web Techradar, en un peu moins d'un mois, la société a subi trois fuites de données causées par la fuite d'informations sensibles via ChatGPT.
Il est à noter qu'au début du mois, l'autorité italienne de protection des données, Garante Privacy, a temporairement interdit ChatGPT en raison de la collecte illégale de données personnelles […]

Enfin, l'Autorité a souligné qu'OpenAI n'alerte pas les utilisateurs qu'elle collecte leurs données.
*Selon l'annonce, il n'existe aucune base juridique sous-jacente à la collecte et au traitement massifs de données personnelles pour « former » les algorithmes sur lesquels repose la plateforme ».**

*https://www.linkedin.com/feed/update/urn:li:activity:7051824469362794496/

[4] Anne Alombert, maître de conférences en philosophie à l'Université Paris 8, s'interroge sur la philosophie d'outils comme ChatGPT et sur l'hégémonie du calcul et l'automatisation des facultés d'expression promues par la Silicon Valley. ttps://cnnumerique.fr/comment-penser-chatgpt