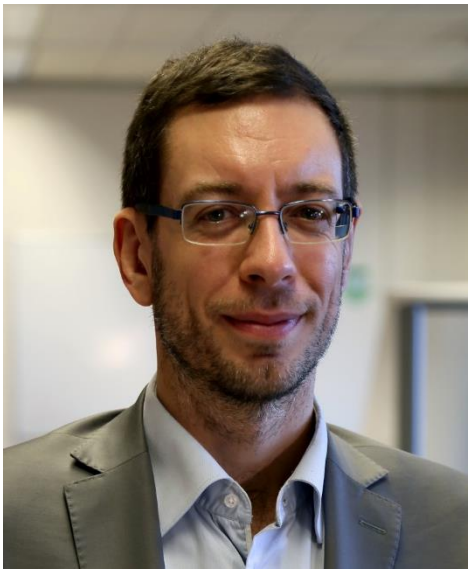
La cybersécurité post-covid rimera-t-elle vraiment avec souveraineté ?



Raphaël MARICHEZ
Expert cybersécurité
Chef de service (services du Premier ministre)

Le milieu de la cybersécurité s'inquiète à juste titre des conséquences de la crise du coronavirus sur la soutenabilité des budgets de sécurité. Mais au-delà des quantités, c'est la mutation du métier même de la cybersécurité qui se trouve brutalement accélérée.

Pour redynamiser son activité, l'entreprise devra démontrer la robustesse de son outil de production et la fiabilité de ses produits et services : la cybersécurité fait partie de l'équation.

Le retour allégué de la souveraineté permettrait-il de répondre positivement aux enjeux de cybersécurité de l'entreprise ?

La mutation de la cybersécurité dans la transformation numérique.

Depuis plusieurs années, les DSI ont déjà largement entamé un virage structurant vers une **externalisation accrue** des activités de haute technicité et aux coûts d'investissements élevés (hébergements, clouds…). Selon les contenus des fiches de postes de RSSI ou CISO correspondantes, il serait attendu des responsables cybersécurité qu'ils délaissent leur expertise technique en architectures et conceptions de sécurité, au profit de connaissances sur la configuration des services des principaux *fournisseurs de services cloud* (CSP, Cloud Service Providers).

Le RSSI d'une entreprise recourant au cloud computing deviendrait garant de **la conformité des configurations des services de cloud à une politique** adossée aux référentiels du CSP. C'est à mon avis une voie de garage avec peu de valeur métier.

La cybersécurité de l'entreprise ne créera demain de la valeur ni en se concentrant sur l'informatique traditionnelle détenue en propre par les DSI que les métiers délaissent, ni en étant l'opérateur humain des interfaces de gestion des CSP.

Le potentiel du responsable cybersécurité réside dans son aptitude à piloter les risques en appui des métiers et en exploitant des outils facilitateurs évitant la répétition de tâches à faible valeur.

Vers le directeur de la cybersécurité, plus proche des métiers, du risque opérationnel, et de la gestion de crise[1].

L'entreprise moderne crée sa richesse par l'utilisation du numérique. Celles qui montrent les plus fortes croissances sont les entreprises construites autour d'un socle numérique, « digital-native » (Doctolib, Blablacar, Uber, AirBnb…). À l'extrême, la création de valeur part d'un produit numérique simple auquel on ajoute, par itérations, des fonctionnalités. Même dans le monde de l'industrie traditionnelle comme l'automobile, l'innovation par le numérique permet la

[1] CESIN « directeur cybersécurité » https://www.cesin.fr/fonds-documentaire-le-directeur-cybersecurite-decrypte.html

création de valeur et la capacité à se distinguer sur un marché mondialisé.

Dans les entreprises qui innovent et réussissent, **les métiers deviennent leur propre direction du numérique**. En sous-traitant massivement par commodité et pour éviter des investissements humains et financiers déraisonnables, ils entraînent la **fragmentation de leur outil numérique de production** (hébergement, réseau, devops, supervision, exploitation applicative, y compris la sécurité opérationnelle…), parfois sans avoir conscience de la cascade de sous-traitance derrière le prestataire qui joue le rôle d'intégrateur de solutions.

La **concentration des acteurs numériques** est particulièrement prononcée dans le « bas » de la chaîne de valeur qui constitue le socle de l'outil de production : outils de communication, stockage, calcul en ligne, sécurité opérationnelle de ces services. Et, ce qui n'est pas anecdotique, « l'**effet réseau** » incite à opter pour la même solution que son partenaire, client ou fournisseur, pour des raisons de coopération et de facilité de prise en main.

Le coronavirus aura été le game changer de la transformation numérique.

En quelques jours, 8 millions de travailleurs français ont été placés en télétravail, souvent dans l'urgence. Les métiers ont adopté comme jamais une utilisation décomplexée de l'informatique vue comme un consommable facilement accessible : réseaux, stockage, serveurs, sécurité opérationnelle.

Les plans de continuité d'activité pré-établis ont pu amortir le choc de sidération des premiers jours sur les moyens préexistants des DSI et pour une partie réduite de l'activité et un nombre limité de salariés. Le redémarrage au maximum du possible de l'activité nominale via le numérique a fait voler en éclat les principes de précautions managériaux, sécuritaires voire budgétaires. Les souscriptions aux services de cloud computing ont explosé.

À court terme, la crise sanitaire aura favorisé l'utilisation massive d'outils numériques parmi un faible nombre d'acteurs, rarement français ou européens, ainsi que la fragmentation des outils numériques de production auprès d'une cascade de sous-traitants.

Perte des frontières ?

Le principe de colocalisation du lieu de travail avec le lieu de production, qui survivait encore par inertie ou habitude, a été totalement balayé, bien sûr à l'exception des activités industrielles traditionnelles nécessitant une présence humaine.

L'industrie traditionnelle adhère par essence aux territoires dans lesquels elle produit et verse des salaires. Ce n'est pas le cas pour l'industrie des services et encore moins pour le numérique. La « dé-territorialisation » du travailleur, qui promet d'être durable, appelle à la poursuite de la transition vers le cloud, la fragmentation de la chaîne de production, et l'abandon du critère géographique dans la localisation des ressources numériques.

Le responsable cybersécurité doit englober, dans sa gestion de risque, l'activité extra-périmétrique, portée par le salarié hors sol, et portée par les outils de production hors sol. Deux facettes d'une même tendance, et qui emportent chacune des évolutions de risques différentes que le responsable cybersécurité doit intégrer - ou accepter d'être relégué aux archives.

Perte de souveraineté ?

Alors que revient le discours de la souveraineté sous l'angle de l'autonomie de production, l'absence de maîtrise de maillons nécessaires à l'outil de production doit évidemment interpeller. L'argument

simpliste de la nationalité ou de l'autonomie de toute la capacité de production mérite une contre-analyse.

Le risque de disruption de l'activité de l'entreprise trouve sa source dans l'intégration, au sein de la chaîne de production, d'acteurs non facilement substituables et placés dans un rapport de force largement asymétrique et défavorable au client : ce dernier n'est pas en mesure d'imposer ses propres conditions. En matière numérique et davantage encore en cybersécurité, nous sommes très loin de l'objectif !

Pour autant, la souveraineté de l'entreprise n'est pas un vain concept. Elle est la condition de l'exercice de son libre arbitre dans le cadre du marché, et notamment la liberté de choisir ses fournisseurs selon leurs caractéristiques. Or, l'informatique devient un consommable (réseau, stockage, opérations), au même titre que l'énergie (électricité, fuel…). Le moyen de parvenir à la liberté de choisir repose ainsi sur trois nécessités :

- connaître les caractéristiques du service auquel on souscrit (auditabilité, standards) ;
- évaluer en quoi ces caractéristiques répondent aux besoins métiers (expertise, lien avec le métier) ;
- pouvoir changer de fournisseur en cas de besoin (réversibilité, diversité des fournisseurs).

Les responsables cybersécurité, dans la chaîne de création de valeur, doivent accompagner le mouvement naturel des métiers vers les solutions externalisées et notamment basées sur le *cloud computing*. Il s'agit notamment d'intervenir sur les services de stockage, les réseaux orchestrés par logiciel, les environnements d'intégration et de déploiement continus, et les outils de sécurité opérationnelle.

Analyser sérieusement la sécurité des outils

Il ne s'agit plus de durcir un système d'information aux frontières définies (RSSI : « responsable de la sécurité des *systèmes d'information* »). Il s'agit de garantir une *activité de production* durablement optimisée face aux multiples *risques numériques* (sécurité numérique), ou face aux risques informationnels (*chief information security officer*). Les solutions pour y parvenir ne seront pas uniformes. Elles dépendent : des cas d'usages (une moto va plus loin qu'un tank) ; des expertises et ressources humaines disponibles (le chiffrement sans bonne gestion des secrets et des terminaux présente un intérêt réel, mais limité) ; enfin de ce qu'offre le marché (réinventer la roue donne rarement un meilleur produit que l'original).

Sur l'exemple classique de la visioconférence parmi d'autres, les nombreux outils disponibles se distinguent par facilité et type d'usage (conférences, réunions, ateliers, entretiens), passage à l'échelle, disponibilité, confidentialité des flux et/ou des données d'annuaire, intégration avec d'autres outils collaboratifs, fonctionnement embarqué dans les navigateurs, facilité d'installation, fonctionnalités ou protections supplémentaires accessibles selon le type de licence acquise... Les choix de Zoom, Webex, Teams, Tixeo, Jitsi, et consort, peuvent tous se justifier selon le cas, le contexte d'usage et les options souscrites.

L'analyse factuelle des risques introduits par l'utilisation d'outils tiers sur l'information et l'activité de l'entreprise entre pleinement dans le mandat du responsable cybersécurité. Malheureusement, la reprise virale de messages simplistes et sensationnalistes est plus rapide et invite à sensibiliser *a minima* les dirigeants. Ces messages relayés de proche en proche mélangent des faiblesses d'implémentation réelles, mais corrigeables, des

utilisations dangereuses (sciemment ou non) de la part d'utilisateurs non habitués, ou des facilités d'usage intrinsèques et assumées du service fourni.

Il convient ainsi de faire le tri et d'apporter aux utilisateurs les informations simples et nécessaires sur les conditions d'utilisation des outils.

"Ce qui est simple est toujours faux. Ce qui ne l'est pas est inutilisable." (Valéry)

On attend bien du responsable cybersécurité qu'il se livre à une analyse fouillée, vérifiée, au-delà des synthèses globalisées et recopiées sans analyse, des **caractéristiques précises des différents outils** du marché au regard des besoins de l'entreprise qui ne sont pas les besoins d'une autre. Il s'appuiera sur des consultants, sur des études comparatives étayées et sourcées (par exemple NSA[2], Orange Cyberdéfense[3], ou experts indépendants), sur des organismes reconnus (MITRE), sur la documentation technique voire le code source.

Pour que la sécurité soit rendue simple pour l'utilisateur, le responsable cybersécurité ne peut pas faire l'économie d'un questionnement propre à l'entreprise, et d'une réflexion amont solide dans une matière complexe mêlant technique et stratégie. Sécurité, patriotisme, maîtrise du tiers, continuité d'activité, constituent différents critères de choix tous vertueux, mais qui ne sont pas alignés. Il n'existe pas de recommandation d'un outil idéal dans l'absolu, car chaque usage est différent : tant mieux pour la concurrence, l'innovation et pour la résilience de l'activité.

Sécuriser le volet numérique de l'activité

La fragmentation des composantes numériques de la chaîne de production rend celle-ci vulnérable à des disruptions soudaines affectant certains maillons, disruptions dont la fréquence d'apparition devrait augmenter[4]. Or il n'est pas objectivement évident que la relocalisation nationale[5] amène, à fonctionnalités similaires, une meilleure sécurité de fonctionnement, une économie et/ou une meilleure efficacité. Parce qu'il existe des dispositifs de sécurité et de contrôles, la France s'accommode très bien de ne produire aucun disque dur ni aucun disque SSD sur son territoire, alors que ces supports indispensables de nos données embarquent de l'électronique et du logiciel de haute technologie[6].

Plutôt que de miser sur des fournisseurs monopolistiques, l'entreprise pourrait s'inspirer du concept de **résilience productive**[7], afin de reconquérir la maîtrise de sa chaîne de production comprise comme un écosystème :

-> Distribution, redondance : Recours à des plateformes, ou des hub, qui permettent de distribuer la charge de travail sur plusieurs fournisseurs tout en maintenant un standard d'interopérabilité entre les éléments amonts et aval de la chaîne de production.

-> Agilité, diversité : aptitude à intégrer et s'interfacer rapidement avec des technologies et des fournisseurs divers pour réduire les risques spécifiques à certains fournisseurs, pays ou technologies.

-> Synergies locales : tirer localement profit d'opportunités de mutualisation, de partage, de partenariats, de regroupements de compétences, de services ou d'infrastructures.

[2] https://orangecyberdefense.com/global/blog/covid-19/video-killed-the-conferencing-star/

[3] https://www.nextgov.com/cybersecurity/2020/04/zoom-or-not-nsa-offers-agencies-guidance-choosing-videoconference-tools/164953/

[4] https://theconversation.com/apprivoiser-les-cygnes-noirs-enseignements-de-la-crise-du-coronavirus-135481

[5] Isabelle Méjean « La relocalisation est une fausse bonne idée » dans Le Monde publié le 24 mai 2020.

[6] Relire Softwar (1984, Thierry Breton et Denis Beneich)

[7] https://www.utopies.com/publications/covid-19-une-question-de-resilience-productive/

La responsabilité sociétale des entreprises mondialisées.

La souveraineté à l'échelle nationale dans le domaine de la cybersécurité passe par le maintien de capacités de création de valeur dans nos territoires, entraînant emploi, versement des salaires et pouvoir d'achat.

Or l'outil de production numérique, pour l'entreprise comme pour les CSP, est déconnecté du territoire géographique. La création de valeur en cybersécurité se fera au sein des métiers intellectuels non remplaçables par des algorithmes. Dans un nouveau cadre de travail à distance, s'ouvrent des perspectives enthousiasmantes de dynamisation de territoires éloignés des grandes métropoles, mais aussi des perspectives de concurrence acerbe entre territoires y compris à l'étranger. La concentration accrue de fonctions productives essentielles au sein d'acteurs numériques multinationaux présente alors un danger pour la stabilité de nos sociétés-nations, avec le risque de délocalisation totale de la création de valeur.

Une évolution des politiques de responsabilité sociétale et environnementale (RSE) des entreprises pourrait prendre en considération la dynamisation de nos territoires dans les choix de recrutements, mais aussi... de sous-traitance !

Ainsi, la souveraineté dans le contexte cybersécurité reposerait sur deux objectifs distincts : d'une part une volonté de **sécuriser l'outil de production** ; d'autre le maintien ou la création **dans nos territoires de capacités productives intellectuelles**. Bien loin d'une vision simpliste d'un souverainisme isolationniste, ces deux objectifs n'ignorent pas la mondialisation et la concentration du marché de la cybersécurité.

Recommandations

La cybersécurité des entreprises devrait progressivement intégrer ou intensifier les activités suivantes :

- **se rapprocher des métiers** dans leurs objectifs de création de valeur et de continuité d'activité, notamment en accompagnant les transitions vers le *cloud computing* et le *DevOps* de manière sécurisée et pérenne ;

- rattraper le **backlog** de la crise, réviser la **gestion du risque** et sécuriser **le « nouveau normal »**, notamment en (re)construisant si nécessaire les principes et architectures permettant la sécurisation des services de *cloud computing* et du travail à distance pérenne ;

- maîtriser les risques numériques de **défaillances des chaînes de production** en recourant à **la diversification** des solutions, à **l'agilité** face aux événements imprévus, et à **l'automatisation** des tâches à faible valeur ;

- organiser l'analyse des risques numériques par **activités métier** et par **flux de services consommés**, plutôt que par systèmes d'information physiques et périmétriques ;

- **questionner, auditer et analyser en profondeur les caractéristiques** des outils et services numériques du marché, en particulier ceux fournissant le socle de l'outil de production, en vue d'assurer la **cohérence de la gestion des risques de l'entreprise** ;

- intégrer, pourquoi pas, un **objectif de responsabilité sociétale** conduisant à maintenir une activité numérique intellectuelle productive, incluant la sous-traitance, sur le territoire (région, pays, continent), sans méconnaître l'écosystème environnant.

L'entreprise peut donc aisément conjuguer sa propre souveraineté et sa cybersécurité, cette dernière éclairant la direction sur les choix stratégiques contribuant à la robustesse de l'appareil productif. Sans méconnaître la réalité du marché mondialisé des services numériques, la cybersécurité pourra trouver un terrain de coopération favorable avec la souveraineté comme enjeu de politique publique par le vecteur de la responsabilité sociétale et environnementale de l'entreprise, prolongeant ainsi dans le domaine de l'entreprise le volontarisme naturel des administrations publiques.