Appel à l'émergence d'une culture française de la sécurité nationale

Quand la DGSI alerte sur le déni de sécurité des consultants extérieurs

Nicolas ZUBINSKI | Consultant en Intelligence économique et Ingénierie d'affaires.

Note préliminaire : L'article a été publié initialement le 8 avril 2019 sur *Infoguerre*, Centre de réflexion sur la guerre économique, École de guerre économique (https://infoguerre.fr/).

Une récente note de la Direction générale de la sécurité intérieure (DGSI) relève l'existence de risques spécifiques de fuites informationnelles liés au recours à des consultants, mettant en lumière l'incurie de ces prestataires extérieurs en matière de sécurité. Bien que ce risque soit d'autant plus significatif pour les avocats (en ce qu'ils peuvent avoir à connaître de la commission d'infractions pénales par leurs clients sous couvert du secret professionnel), il concerne l'ensemble du secteur du *consulting*.

La thématique de la sécurisation des consultants extérieurs gagne progressivement en importance depuis 2016. En effet, si des actions de sensibilisation ou témoignages apparaissent régulièrement dans la presse spécialisée ou régionale (« avocats, sécurisez vos données » dans la *Gazette du Palais* ou « Comment ce cabinet d'avocat a été victime d'une cyberattaque » dans *Var-Matin*), la perception du risque s'accroît en 2016 avec les soupçons de piratage de cabinet d'avocats américains par des *hackers* chinois (cf. Dominique FILIPPONE). Vient ensuite, en 2017, une succession d'affaires de fuites de données par cyberattaque chez les majors du *consulting* mondial (cf. Yannick CHAVANNE).

À l'heure du Règlement général sur la protection des données (RGPD), du *Cloud computing* et du *BYOD* (*Bring your own device*, littéralement « apporter vos propres outils »), cette polémique fait ressortir les limites de la culture sécuritaire anglo-saxonne dans un environnement des affaires français où la confiance entre client et consultant est une valeur cardinale.

Une thématique régulièrement portée par les autorités publiques

La DGSI se mobilise régulièrement pour diffuser des alertes sécuritaires dans un souci de protection des activités économiques françaises. Ses *flashs*

« *Ingérence économique* » sont relayés par les acteurs institutionnels publics français sur des thématiques centrales de l'Intelligence économique (IE) et diffusés en priorité *via* le site *Internet* de la Direction générale des entreprises (DGE) rattachée au ministère de l'Économie et des Finances.

La résonance de ces *flashs* dépend grandement du relais des sources tertiaires. La difficulté d'accès à la source primaire d'information, notamment l'absence d'une base de données ouverte et facilement accessible sur le site de la DGSI, réduit la diffusion de son message (il est toutefois possible de retrouver l'intégralité des *flashs Ingérence* sur le site de la préfecture d'Île-de-France moyennant un léger exercice de veille).

Cette barrière méthodologique à l'accès d'une information utile et ouverte génère une dépendance vis-à-vis des relais médiatiques et divers influenceurs. Malgré cela, les *Flashs* n° 32 et 50 portant respectivement sur les « risques générés par le manque d'encadrement des stagiaires au sein des structures publiques et privées » et les « risques générés par le manque d'encadrement des consultants extérieurs » ont connu une meilleure diffusion au sein du public non spécialisé. Les relais non institutionnels, notamment la communauté de l'IE, ont en effet été particulièrement proactifs dans la diffusion de ces constats.

Une offensive efficace du milieu de la sécurité et de l'IE français

L'amorce vient de la DGE qui met en ligne le *flash* n° 50 (page *Web* modifiée pour la dernière fois le mardi 12 février 2019 14:50:57 à la date du 4 avril 2019), intitulé « risques générés par le manque d'encadrement des consultants extérieurs ». Ce *flash* s'est alors diffusé sur le *Web via* les canaux publics (Préfecture d'Île-de-France, CCI de Nièvre ou du Morbihan, etc.) et parapublics (Conseil supérieur de la formation et de la recherche stratégiques, Conférence des présidents des universités, Compagnie régionale des Commissaires aux comptes d'Alsace, etc.). La diffusion sur le *Web* s'effectue en parallèle dans les milieux spécialisés notamment sur le Portail de l'IE le 20 février et sur le site Veillecyberland.wordpress.com le 25 février. Après le cycle de diffusion primaire et secondaire, viennent les canaux tertiaires, au premier rang desquels LinkedIn, Twitter et Facebook sur lesquels les partages s'activent début mars.

Des préconisations perfectibles très orientées « *process* » et « *contract review* »

Les points d'alerte de la DGSI partent d'exemples concrets, réels et communs, suivis d'une liste de recommandations. Notons que les 10 recommandations de la DGSI sont, sur le fond, tout à fait pertinentes. Certaines sont essentiellement juridiques (telles qu'une *contract review* – vérification de la conformité contractuelle – sur la confidentialité et l'éthique), d'autres sont davantage axées sur la

sécurité des biens et des personnes (contrôle d'accès), etc. Les préconisations de la DGSI ne sont donc pas exclusivement orientées sur la prévention de la cybercriminalité, bien au contraire.

S'ajoute à cela une recommandation de bon sens, d'un point de vue sécurité, mais aux antipodes de la pratique actuelle du conseil : « interdire le recours à des outils et matériels du consultant, qu'ils soient personnels ou fournis par son employeur (PC portable, plateforme collaborative, etc.) ». Le *BYOD* est en pleine expansion, poussé par les *start-up*, la démarche collaborative mais surtout le manque de moyens. La DGSI fait apparaître, mais sans l'aborder, un problème qu'elle ne saurait résoudre seule : les limites de la culture française des affaires.

Le vecteur de modification comportemental des agents économique doit donc être principalement culturel. Ce faisant, miser sur des relais d'influence dans la communauté de la sécurité et de l'IE fait sens. Pourtant, la sphère d'influence IE ne s'est pas pleinement emparée de la question. Quelques initiatives sur les réseaux sociaux font suite à la sortie de ce *flash* n° 50 mais les différents acteurs ne l'ont pas encore totalement intégrée dans une grille de guerre informationnelle et culturelle. Cette polémique constitue ainsi une formidable opportunité de réflexion sur la construction d'une culture sécuritaire à la française en se différenciant de la *Safety Culture* anglo-saxonne ou de la *Sicherheitskultur* germanique ; remarquons d'ailleurs que l'expression « culture de sécurité » est avant tout une traduction du concept de *Safety Culture*.

Une riposte du secteur du *consulting* en France ?

Deux causes peuvent expliquer la lenteur de la parade informationnelle du milieu du *consulting* français. La première réside dans un défaut de la veille des prestataires et de leurs organismes professionnels. La seconde est plus complexe et s'explique par le risque que représente une communication trop agressive sur ce sujet.

Du déni de réalité à l'effet tunnel : effet collatéral de la culture des affaires en France

L'environnement français du conseil se distingue par la faible sensibilité au risque de fuites informationnelles qu'il estime négligeable, voire anecdotique. Les dirigeants des sociétés conseils estiment, malheureusement, que le risque vient presque exclusivement d'une attaque informatique, c'est-à-dire qu'il relève de la cybercriminalité. Cette vision du risque tend à écarter la principale cause des fuites informationnelles dans le secteur du *consulting* : la négligence. Dans ce contexte de déni du risque, les acteurs sont moins sensibilisés à la nécessité de surveiller ce type d'informations. Le manque de vigilance peut s'expliquer par un fondement de la culture française du conseil : la confiance mutuelle.

Cette culture française des affaires pourrait tirer son origine de la qualité de la protection juridique accordée en droit français. En effet, dans un contexte normatif et jurisprudentiel protecteur vis-à-vis des agents économiques (consommateurs, administrés, etc.), les sujets de droit abaissent leur vigilance face aux risques. À cet égard, la stratégie de la DGSI semble particulièrement pertinente.

Par ailleurs, cette culture française de la « confiance » dans les affaires aurait pu uniquement s'appliquer au contenu des prestations (qualité des méthodes, savoirs et savoir-faire, intelligence relationnelle, compréhension des enjeux, etc.), mais il semblerait que cette confiance se soit élargie à la sécurité. Remettre en cause la politique de sécurité d'un cabinet de conseil ou d'avocat ayant pignon sur rue et reconnu dans toute la profession comme expert serait incongru. Est-ce pourtant satisfaisant ? Ne devrait-on pas faire évoluer notre culture nationale sur ce point pour distinguer la qualité des consultants de la qualité de leur protection ? La possibilité de fuite existera toujours, quels que soient les moyens déployés. Pour autant, ne rien mettre en place pour s'en prémunir serait particulièrement nuisible, ne serait-ce qu'en termes d'image et rendrait la communication de crise de cabinet de conseil particulièrement ardue.

La culture de sécurité en France mute progressivement du fait de la multiplication et de la prépondérance des acteurs anglo-saxons du conseil en France (voir le classement 2019 des cabinets de conseil établi par le magazine *Capital*). En important capitaux, idéologies et équipes, ces cabinets de conseil apportent également les méthodes de travail anglo-saxonnes, davantage sensibilisées aux risques et effets des fuites d'informations. Faut-il déplorer cet héritage anglo-saxon ? Pas nécessairement dans la mesure où il participe activement à la montée en compétences de l'ensemble de secteur du conseil en France. Pour autant, la qualité du vivier français des experts de l'Intelligence économique et le savoir-faire des Institutions publiques (telles que l'Agence nationale de la sécurité des systèmes d'information ou Anssi, la DGSI et le Service de l'information stratégique et de la sécurité économiques ou SISSE) permettent une mutation bien plus profonde de la culture sécuritaire en France.

En s'ajoutant à l'importation du modèle anglo-saxon, cette mutation culturelle, bien que laborieuse, conférerait un avantage comparatif particulièrement puissant : si la prise en compte de la sécurité par les consultants extérieurs se limite à l'application de *process* et au renforcement des clauses de confidentialité dans les contrats de consultance (approche anglo-saxonne), le collaborateur d'une société de conseil risque d'opter pour des stratégies de contournement encore plus néfastes. À l'inverse, la mutation de la culture sécuritaire à l'échelon national, bien que freinée par une certaine inertie, permet d'ancrer plus profondément chez les consultants leur devoir de protection des informations. Ce type de culture peut d'ailleurs être observé dans les milieux germaniques et scandinaves des affaires.

Du risque de dégradation de l'image au risque d'acculturation sécuritaire

L'opportunité de parler de ses faiblesses est une problématique usuelle de la communication de crise. Des sociétés de conseil qui révéleraient avoir connu des fuites informationnelles risqueraient de dégrader leur image, et à court terme, de devoir accroître leurs investissements informatiques, former leur personnel et se préparer à d'éventuelles actions contentieuses. À première vue, une certaine forme de discrétion en la matière semble dès lors préférable d'un point de vue économique.

La stratégie de communication des *leaders* mondiaux du *consulting* ayant eu à connaître des fuites d'informations s'inscrit dans cette approche. Leur argumentation vise plus spécifiquement à établir un lien entre « fuite » et « cybercriminalité » ou « attaque informatique ». Cette rhétorique offre un double avantage : préserver une certaine discrétion tout en adoptant une posture de victime d'infractions, donc occulter la piste de l'éventuelle négligence de leurs collaborateurs. Or, la rhétorique de la négligence était justement l'axe d'attaque d'un client du cabinet de conseil Deloitte dans un contentieux indemnitaire suite à l'affaire de 2017 (cf. Pat SWEET). Des acteurs américains avaient déjà alerté en 2016 le secteur sur l'importance de la négligence dans les fuites de données (*leaks*) dans un article au titre évocateur « *Negligence not malice. The biggest threat to law firm data security* » fragilisant la rhétorique de la victime de cybercriminalité.

En dehors de toute affaire spécifique, la rhétorique de la victime produit des effets sur la perception du risque. Elle renforce celle-ci de fuite informationnelle du fait de la cybercriminalité et s'avère être, pour l'intérêt général, un levier efficace de protection du patrimoine économique national. Et, elle supplante la rhétorique de la négligence. Or le risque le plus important, et la position la moins défendable dans un contentieux indemnitaire, est justement celui de la négligence des collaborateurs. La prise de conscience du risque de fuite par le biais d'affaires éloigne les sociétés de conseil d'une réflexion de fond sur leur culture de sécurité. En ce sens, la note de la DGSI, retranscrit cet équilibre habile entre nécessité d'alerter et nécessité d'élargir la réflexion aux cabinets de conseil. Qui plus est cette note vise « l'encadrement des consultants extérieurs », donc indirectement les cabinets de conseil. Les pouvoirs publics auraient-ils conscience du déni de réalité des prestataires de conseil ? Porter l'alerte auprès des clients plutôt que des prestataires est, sur ce point, une stratégie intéressante.

Par ailleurs, le secteur du conseil en France est essentiellement composé de Petites et moyennes entreprises (PME) qui, en termes de communication de crise, préfèrent la discrétion, comme l'a remarqué Guillaume Poupard, directeur général de l'Anssi, lors des Assises de la sécurité à Monaco : « Nos PME sont sans doute les premières ciblées […]. Et il y en a qui meurent en silence, qui mettent la clé sous la porte à cause d'attaques informatiques ». Il est fort à parier que cette tendance à la discrétion s'applique plus généralement aux cas de fuites d'informations.

Dans ce contexte, la stratégie de la DGSI d'alerter les clients plutôt que les prestataires de conseils risque de créer un effet d'éviction des PME. En sensibilisant les clients, et donc en pariant sur le durcissement de leurs politiques achats, cela privilégiera les prestataires capables de s'adapter rapidement : c'est-à-dire les *majors* du *consulting*, celles-là même qui diffusent la rhétorique de la victime lorsqu'elles mettent en place une communication de crise. Pour mieux appréhender ce paradoxe, il est utile de distinguer la communication de crise liée à des affaires ponctuelles, de la communication d'influence aux fins de diffusion des bonnes pratiques dans le secteur du *consulting*.

Enfin, la stratégie de discrétion n'est-elle pas contre-productive à moyen terme ? Occuper le terrain informationnel est un moyen efficace de se prémunir d'une campagne agressive qui pourrait déstabiliser la profession. Qui plus est, l'action concertée est un bon levier d'influence et de promotion des spécificités sectorielles. Le secteur du conseil pourrait, par exemple, efficacement faire valoir certaines de ses contraintes structurelles pour relativiser la nécessité du « tout sécuritaire ». En outre, les autorités publiques en charge de la protection du patrimoine économique français, et plus particulièrement celle disposant de pouvoirs d'enquête (la DGSI), ont besoin de remontées d'informations pour analyser et prévenir les menaces. Cette démarche étant confidentielle, les sociétés de conseil auraient, ne serait-ce que par patriotisme économique, tout intérêt à échanger. Toutefois ces sociétés perçoivent dans cette démarche un risque de fuite, réel ou ressenti, trop important. Établir un lien de confiance entre les acteurs est donc primordial. De même, parier sur l'accompagnement en amont des cabinets de conseil permettrait d'ajuster l'articulation entre les stratégies de communication de crise et les stratégies de communication d'influence.

Quelles leçons tirer de cette polémique ?

Sur le fond, les solutions sont d'ores et déjà existantes, il ne s'agit donc que d'une question de coût, de temps et d'impulsion. Qui plus est, demander à tous les consultants extérieurs de devenir des sanctuaires informationnels ne serait ni économiquement viable, ni efficace en termes d'acceptation du message sécuritaire. Préconisons en la matière, comme tout expert en *management* des risques, d'adapter la réponse à la cartographie des risques.

D'un point de vue informationnel, cette polémique interpelle à plusieurs titres : elle amorce une mutation culturelle du secteur français du *consulting*, elle souligne le rôle moteur des institutions publiques et interroge le secteur français du conseil sur son déni de réalité.

Éléments de bibliographie

AFP, « Personne n'est à l'abri des cyberpirates, rappelle l'Anssi », *Le Point*, 11 octobre 2017 (www.lepoint.fr/).

Chavanne Yannick, « Fuite de données : Deloitte, Forrester… et maintenant Accenture » *ICT journal*, 11 octobre 2017 (www.ictjournal.ch/news/2017-10-11/fuite-de-donnees-deloitte-forrester-et-maintenant-accenture).

D. G., « Comment ce cabinet d'avocat a été victime d'une cyberattaque », *Var-Matin*, 21 janvier 2016 (http://varmatin.com/justice/comment-ce-cabinet-davocats-a-ete-victime-dune-cyberattaque-16304).

Declairieux Bruno, « Classement 2019 des cabinets de conseil », *Capital*, 22 octobre 2018 (www.capital.fr/votre-carriere/les-palmares-des-meilleurs-cabinets-de-conseil-1312189).

DGSI, « Risques générés par le manque d'encadrement des consultants extérieurs », *Flash* n° 50, février 2019, 4 pages (www.entreprises.gouv.fr/).

DGSI, « Risques générés par le manque d'encadrement des stagiaires au sein des structures publiques et privées », *Flash* n° 32, avril 2017, 5 pages (www.prefectures-regions.gouv.fr/ile-de-france/).

Filippone Dominique, « 3 Chinois accusés du piratage de 7 cabinets d'avocats *US* », *Le monde informatique*, 29 décembre 2016 (www.lemondeinformatique.fr/).

Higgins Kathryn, « Negligence not malice. The biggest threat to law firm data security », *The Global Legal Post*, 13 juin 2016 (www.globallegalpost.com/).

Iweins Delphine, « Avocats, sécurisez vos données », *Gazette du Palais* n° GPL266k2, 24 mai 2016, p. 9 (www.gazette-du-palais.fr/article/GPL266k2/).

Sweet Pat « IT company in legal challenge over Deloitte 'negligence' », *Accountancy Daily*, 9 octobre 2017 (www.accountancydaily.co/it-company-legal-challenge-over-deloitte-negligence).