NTT Security

Livre blanc

Gérer le risque du multi-sourcing

Il y a 20 ans, la décision d'externaliser ou non son informatique se prenait sans demi-mesure. C'était tout ou rien. Une entreprise devait soit choisir de tout garder en interne, soit confier cette mission à un partenaire externe.

Depuis, l'infogérance a beaucoup évolué. Certaines entreprises en sont même à leur troisième, voire leur quatrième variante. De même, plutôt que de sélectionner un seul fournisseur, la plupart préfèrent désormais une solution interne/externe mixte autour de plusieurs prestataires. Aujourd'hui, de nombreuses entreprises ne diraient pas qu'elles ont externalisé leur infrastructure IT, mais parleraient plutôt de solution multi-fournisseur.

Le cabinet Gartner définit ce « multi-sourcing » comme « le provisionnement méthodique de services IT et métiers à partir d'un mix optimal de ressources internes et de fournisseurs externes en vue d'atteindre les objectifs de l'entreprise ». Cette définition révèle le processus décisionnel stratégique qui sous-tend une démarche de multi-sourcing. Dans cette approche, le recours à différents fournisseurs n'a rien d'accidentel.

Lorsqu'il est bien maîtrisé, le multi-sourcing permet aux entreprises de bénéficier des innovations de différents fournisseurs spécialisés, voire de libérer tout le potentiel de leurs solutions SaaS, le tout dans un modèle informatique étroitement connecté et intégré. Grâce à cette approche, elles peuvent atteindre plus rapidement leurs objectifs opérationnels et stratégiques. Toutefois, cette interdépendance contraint également les entreprises à songer très sérieusement aux moyens de capitaliser sur les ressources de plusieurs fournisseurs (parfois en concurrence directe) au sein de leur écosystème – le tout en gérant les risques pour l'intégrité et la disponibilité de leurs services métiers. Ceci est d'autant plus vrai à l'heure où le cloud s'impose comme un élément clé de la stratégie numérique des entreprises. De fait, ces dernières savent bien que leurs fournisseurs de services IT pourront introduire des failles dans des environnements qu'elles ont pris soin de structurer au millimètre, avec des conséquences nuisibles sur la stabilité de leur infrastructure.

Multi-sourcing et sécurité

D'après notre expérience, les entreprises qui créent un cadre de gouvernance multi-fournisseur – qu'elles comptent le piloter elles-mêmes ou le confier au principal sous-traitant – se concentrent généralement sur les dimensions commerciales et contractuelles de l'offre de service. Or, le fait d'évaluer les fournisseurs uniquement à l'aune de leurs engagements SLA (Service Level Agreements) ne leur permettra pas de repérer d'éventuels risques de sécurité, notamment au niveau de l'accès aux données sensibles mais également de leur transfert entre de multiples plateformes et zones géographiques soumises à différents régimes réglementaires. Car si les entreprises ont tendance à juger un partenaire potentiel sur ses compétences dans son domaine d'expertise, elles semblent ne pas évaluer avec la même rigueur les fonctionnalités et processus de sécurité de ce fournisseur. Or, pour bien gérer le risque, il est indispensable de soumettre le partenaire potentiel à une batterie de questions sur ses processus de sécurité, le but étant de découvrir s'ils s'intégreront aux opérations et à l'architecture de sécurité de l'entreprise cliente. Mais pour inscrire cette gestion du risque dans les engagements contractuels du fournisseur, encore faut-il savoir déléguer la responsabilité des contrôles et indicateurs de sécurité tout en restant seul maître à bord. C'est pourquoi NTT Security aide ses clients à évaluer et à interagir avec les parties prenantes de leur stratégie multi-fournisseur – du positionnement de ces fournisseurs dans leur profil risque global à la rédaction et l'application des termes du contrat.

D'ICI 2020,

90 % DES DÉPENSES INFORMATIQUES S'EFFECTUERONT HORS DES BUDGETS IT DES ENTREPRISES [1]

En réalité, l'informatique n'a pas toujours pu intégrer une telle discipline à toutes les décisions technologiques de l'entreprise. La puissance et l'accessibilité quasi universelle de technologies et utilitaires « as a Service » (de Dropbox™ pour

1. Communiqué de presse : "Gartner Says Every Budget is Becoming an IT Budget"

partager rapidement un fichier avec un collègue ou un partenaire, jusqu'à Amazon Web Services™ pour mettre rapidement en place un environnement de développement) ont ouvert la voie de l'autosuffisance dans le monde de l'entreprise. Aguerris aux nouvelles technologies, les utilisateurs achètent, gèrent et provisionnent de plus en plus leurs propres services et solutions. Et cette tendance du Shadow IT ne fait que s'accentuer : d'après le Gartner, 90 % des dépenses informatiques s'effectueront hors du budget IT des entreprises d'ici à 2020. Le problème, c'est que les utilisateurs signent des contrats directement avec des fournisseurs externes qu'ils gèrent en solo, sans tenir compte des risques potentiels d'hétérogénéité du support pour eux-mêmes et de sécurité pour leur entreprise. Or, pour maîtriser parfaitement leurs risques de sécurité, ces entreprises ont besoin d'une visibilité totale sur toutes les technologies susceptibles de contourner les différents contrôles et dispositifs de sécurité en place.

Question de responsabilité

L'intégration de solutions externes disparates à un régime de gouvernance multi-fournisseur permet aux entreprises de reprendre le contrôle intégral de leur chaîne d'approvisionnement IT. Lorsque ces services sont intégrés et gérés par l'IT à la demande des utilisateurs, ils sont alignés tant sur les exigences métiers que sur les impératifs de sécurité. En revanche, toute incapacité des entreprises à reprendre le contrôle pourra non seulement les exposer à des risques considérables, mais aussi à de sérieuses répercussions financières et sur leurs réputations.

40 %

DES ENTREPRISES QUI NE RECOURENT PAS OU N'ENVISAGENT PAS DE RECOURIR À DES SERVICES EXTERNES INVOQUAIENT DES CRAINTES QUANT AU PARTAGE DE LEURS DONNÉES [2]

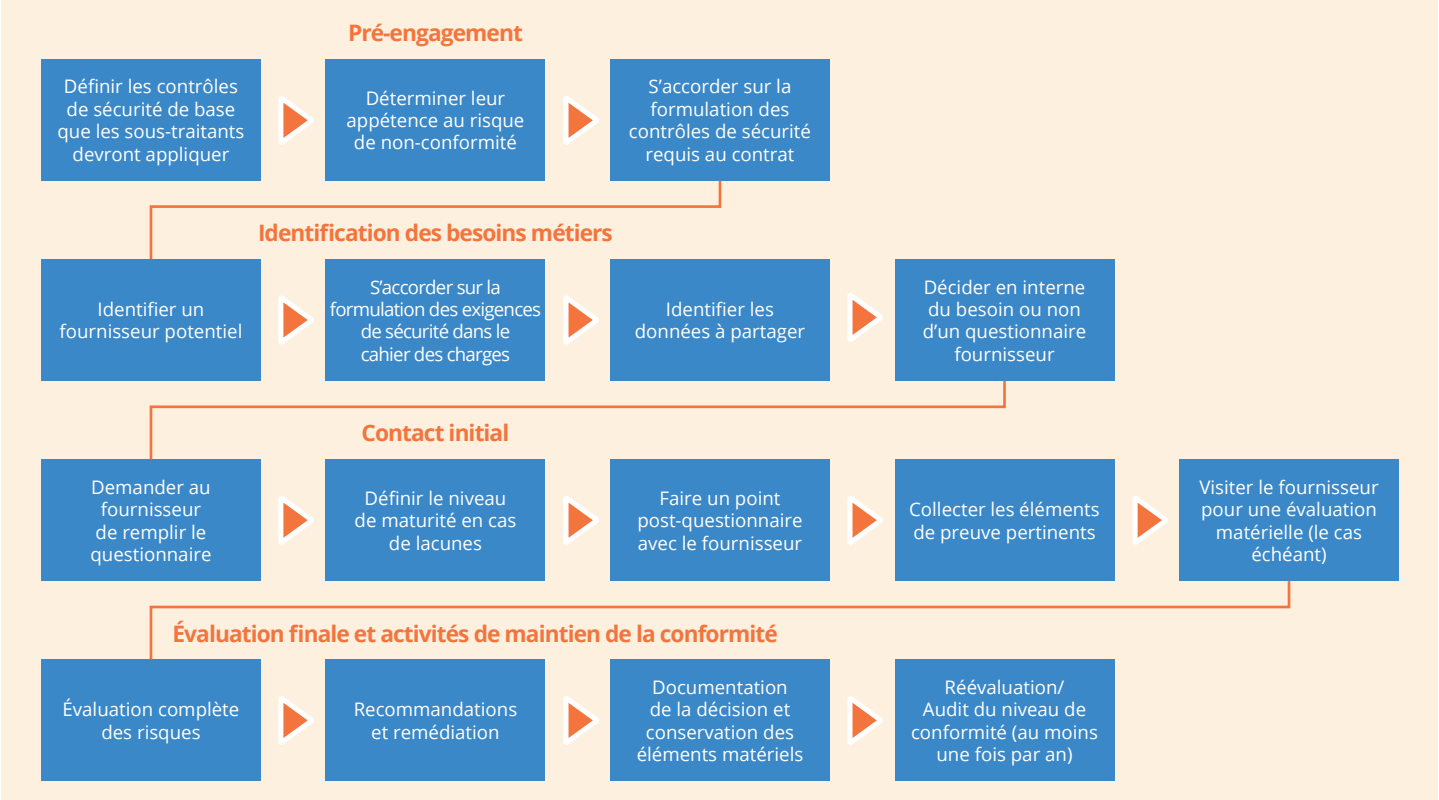
Dans des secteurs ultra règlementés comme la finance, la santé et l'industrie pharmaceutique, multi-sourcing ou pas, les entreprises n'ont aucun moyen d'échapper à leurs obligations en se défaussant sur des fournisseurs externes. C'est à elles, et à elles seules, que revient la responsabilité de leur conformité règlementaire. De fait, de nombreuses violations de données de grande ampleur peuvent être attribuées aux manquements de ces intervenants externes. En réaction à la condamnation d'une entreprise britannique à une lourde amende pour manque de contrôles de l'un de ces fournisseurs IT, Mark Steward, directeur de la FCA (Financial Conduct Authority) chargé de la répression et de la surveillance des marchés, a déclaré : « Les autres firmes recourant à ce type d'externalisation sont maintenant prévenues : rien ne justifie l'absence de contrôles et de systèmes de supervision robustes. »

Ce livre blanc vous invite à faire le point sur les mesures à prendre pour instaurer un cadre de gouvernance des processus de sécurité et de réduction des risques commun à tous les fournisseurs, garant d'un écosystème collaboratif de confiance. Il s'agit essentiellement d'établir un scénario gagnant-gagnant pour les clients, les fournisseurs et les partenaires technologiques impliqués.

Multi-sourcing : comment gérer le risque

À l'ère du numérique, comme avec la plupart des applications de sécurité, il est bien plus difficile d'intégrer des fonctionnalités de gestion des risques à un système existant que de les prévoir dès sa conception. En clair, pour parvenir à un contrôle de sécurité intégral et transparent sur tout leur environnement multi-fournisseurs, les entreprises ont tout intérêt à faire le nécessaire en amont. Toutefois, d'après notre expérience, beaucoup s'appuient déjà sur un écosystème de plus de 20 services disparates lorsqu'elles se mettent

Schéma 1 : Étapes recommandées pour l'évaluation des sous-traitants



en quête d'une solution de gestion des risques multi-fournisseurs. Ces fournisseurs pourront couvrir un vaste champ de domaines (gestion des effectifs, gestion réseau, services sans fil, solutions de collaboration, ou encore gestion des terminaux mobiles). Non seulement ils font déjà partie des meubles, mais ils s'avèrent souvent indispensables au bon fonctionnement de l'entreprise.

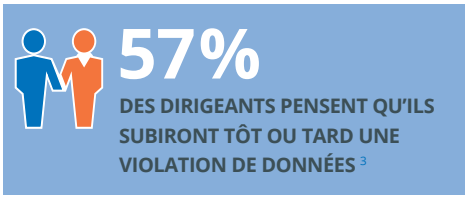
1. Évaluer les risques

Dans le cadre de leur modèle de gouvernance multi-sourcing, de nombreuses entreprises décident de recourir d'emblée à une évaluation des risques externes inhérents à tous ces services, en fonction de leur profil risque et de leurs obligations de mise en conformité. Ce bilan initial est pour elles le seul moyen de cerner l'étendue et la gravité de leurs éventuels manquements – en particulier dans les domaines de la protection des données et de la gestion des accès et des identités (IAM) associée, désormais soumis au Règlement Général sur la Protection des Données (RGPD) de l'UE. D'après l'étude mondiale Risk:Value de NTT Security, 40 % des entreprises qui n'ont pas recours ou n'envisagent pas de recourir à des services externes invoquaient des craintes quant au partage de leurs données.

Étant donné que la sécurité n'est pas au cœur des priorités de tous vos fournisseurs, la prudence impose d'établir une gouvernance multi-fournisseur pour placer votre collaboration sous le signe de la confiance. Penchons-nous quelques instants sur les processus associés.

2. Intégrer la notion de confiance au processus d'engagement des fournisseurs

Pour exploiter tous les avantages du multi-sourcing, les entreprises doivent adopter un modèle qui leur permette de bénéficier du vaste champ d'expertise des fournisseurs choisis, sans pour autant s'exposer à des risques inutiles. Pour établir une relation de confiance, la cybersécurité doit être au cœur de chaque décision d'achat. Comme nous l'avons déjà évoqué, les entreprises restent les seules véritables responsables de la sécurité de leurs données et de leurs systèmes. Par conséquent, un bilan de sécurité complet devra identifier les éléments « à risque » parmi les fournisseurs existants. Une fois qu'une entreprise connaît clairement les risques inhérents à chaque fournisseur, elle pourra cibler beaucoup plus précisément les clauses de sécurité à intégrer à ses contrats. Ou elle pourra tout simplement se mettre en quête d'un autre partenaire plus à même de répondre à ses exigences de sécurité. En somme, une évaluation de vos sous-traitants vous permettra de mieux protéger vos ressources stratégiques, mais aussi d'établir et d'entretenir des relations de confiance avec vos fournisseurs nouveaux et existants.



3. Etablir et maintenir une bonne visibilité sur les risques de sécurité inhérents à chaque fournisseur IT

Lorsque vous engagez un nouveau fournisseur de services informatiques, il est primordial d'aborder avec lui les questions de cybersécurité très en amont ; d'où l'importance d'impliquer d'autres fonctions (gestion des fournisseurs, contrôle qualité et surtout achats) dans le développement et la maintenance de votre méthodologie d'évaluation des risques fournisseurs. Tous les acteurs internes doivent se mettre au diapason des exigences de sécurité de votre entreprise afin de poser les bonnes questions au bon moment, et ce tout au long des processus d'achat et d'évaluation.

Elles pourront également veiller à la présence de certaines clauses aux contrats :

- Votre entreprise doit pouvoir procéder à un audit des pratiques de sécurité d'un fournisseur pendant toute la durée du contrat. Pour cela, il vous faudra peut-être trouver un terrain d'entente sur le monitoring de certaines fonctionnalités comme les contrôles IAM, l'activité des terminaux et du réseau, ou encore l'analyse des logs. Dans de nombreux cas, les entreprises s'inquiètent de la charge de travail supplémentaire que représente le suivi de l'écosystème de leurs fournisseurs en plus du leur. Pour éviter de surcharger leurs équipes internes, elles peuvent alors confier leurs opérations de monitoring externe à un fournisseur de services de sécurité managés (MSSP). Après tout, l'instauration d'un cadre de gouvernance des sous-traitants n'a pas grand intérêt si les entreprises ne disposent d'aucun moyen de contrôle du respect des engagements pris par lesdits fournisseurs.
- Les règles de conformité à respecter (PCI DSS, RGPD, etc.) doivent être clairement énoncées. D'après notre expérience, lorsque leurs fournisseurs ne détiennent pas les certifications demandées, les entreprises doivent souvent étendre le périmètre de leurs propres audits, avec pour conséquence une augmentation des coûts et de la complexité de leur mise en conformité.

4. Se préparer à d'éventuels incidents dans un environnement multi-fournisseurs

On entend souvent dire que la complexité est l'ennemi de la sécurité. Or, même les modèles de gouvernance multi-sourcing les mieux conçus sont pour le moins alambiqués. D'autre part, comme le risque zéro n'existe pas, 57 % des dirigeants pensent qu'ils subiront tôt ou tard une violation de données, selon un rapport d'étude NTT. La bonne nouvelle, c'est que la sensibilisation croissante des entreprises aux cyberattaques les incite non seulement à mettre en place des plans d'intervention sur incident, mais aussi à les tester dans le cadre de leur plan de continuité d'activité (PCA).

Toutefois, parmi les entreprises pratiquant le multi-sourcing, c'est encore l'incertitude qui plane quant à l'impact d'un incident de sécurité chez l'un de leurs fournisseurs. Trop d'entreprises restent en effet sans réponse face aux questions suivantes :

- Quel serait l'impact sur ma productivité, la disponibilité et l'intégrité de mes systèmes ?
- Serais-je en infraction vis-à-vis de mes obligations réglementaires – notamment le signalement sous 72 heures de toute violation de données en vertu du RGPD ?
- Comment pourrais-je déterminer si le problème vient de mes propres systèmes ou de ceux de mon fournisseur ?

C'est pourquoi nous recommandons aux entreprises adeptes du multi-sourcing de préparer un plan exhaustif de communication et d'intervention sur incident en cas d'attaque majeure. Si le plan d'intervention le plus solide n'empêchera jamais une attaque d'aboutir, une réponse rapide peut faire toute la différence entre un incident qui fait la une des médias et un problème traité en toute discrétion, en partenariat avec vos fournisseurs.

2 et 3. Rapport Risk:Value 2017, NTT Security

5. Résilier un contrat

Les entreprises doivent également se ménager une porte de sortie. En clair, elles doivent prendre toutes les précautions nécessaires pour assurer une protection ininterrompue de leurs données et systèmes si elles venaient à résilier un contrat ou changer de fournisseur. Si les formalités d'une telle procédure sont avant tout du ressort des services achats et juridiques, les RSSI devront eux aussi maîtriser les procédures de résiliation et leur impact direct sur la sécurité de l'entreprise. Parmi eux figurent le renvoi des informations le cas échéant, le maintien des obligations de confidentialité du fournisseur, la passation entre deux fournisseurs de services, voire entre le fournisseur et l'entreprise elle-même. Certes, la sécurité doit faire partie intégrante des conditions du contrat, mais il est tout aussi important de formaliser la procédure de remise des actifs corporels ou incorporels à l'entreprise par le fournisseur en cas de résiliation.

Recommandations de NTT Security pour la gestion des risques inhérents au multi-sourcing

- Vous aurez tout intérêt à formaliser les contrôles de sécurité au moment de la prise d'engagements contractuels, plutôt qu'après coup et hors de tout régime de gouvernance du multi-sourcing. La sécurité ne doit plus être reléguée au second plan : les entreprises doivent poser les bonnes questions au bon moment, avec le soutien de tous les collaborateurs impliqués dans le processus d'achat.
- Les entreprises déjà liées à plusieurs fournisseurs doivent intégrer la sécurité de façon transparente afin de ne pas entraver la gouvernance et les processus en place avec les sous-traitants existants. Pour cela, elles ont besoin d'une approche holistique, en phase avec leurs objectifs métiers.
- Les entreprises doivent se pencher tout autant sur les garanties apportées par leurs fournisseurs externes que sur les avantages attendus par les nouveaux systèmes et approches. Les professionnels de la sécurité IT peuvent contribuer à cette démarche en évaluant et en recommandant les fournisseurs qui présentent le meilleur rapport bénéfice-risque dans le cadre d'un modèle concerté de gouvernance du multi-sourcing.
- Nombre de nos clients trouvent qu'il est plus efficace et plus rentable de faire appel à des experts pour évaluer leur exposition aux risques de sous-traitance et développer un programme de sécurité pérenne. Une telle démarche pourra nécessiter l'apport de spécialistes aguerris aux risques inhérents au multi-sourcing – non seulement pour planifier et exécuter vos évaluations des risques, mais aussi pour surveiller en permanence votre infrastructure à la recherche de menaces ciblées.

L'entreprise NTT Security

NTT Security est la branche et centre d'excellence sécurité du groupe NTT. Nous mettons notre expertise au service des entités du groupe NTT en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation numérique. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500 experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services de sécurité managés (MSS) mais également de conseil stratégique ou technologique aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Visitez **www.nttsecurity.com/fr-fr** pour en savoir plus sur NTT Security ou **www.ntt.co.jp/index_e.html** pour le groupe NTT.