

Préambule

C'est le château du Tremblay, au cœur des Yvelines qui a hébergé cette année l'off-site CIJ. Le format, le lieu et l'organisation étaient, comme toujours, irréprochables, et l'ambiance à la fois studieuse et détendue, toujours aussi agréable.

Côté contenu, de nombreux et passionnants sujets, souvent complémentaires et brûlants d'actualité ont ouvert d'intéressantes perspectives :

- **Alignement du SI avec la stratégie du cabinet**
- **Quel type de cloud choisir ?**
- **DSI 2.0 → Retour d'expérience 1 an après**
- **IT as a business development aid**
- **La fin de l'âge de cuivre**
- **Les techniques des pirates et comment s'en protéger**
- **L'assurance des cyber-risques**

1. Alignement du SI avec la stratégie du cabinet

La question posée par **Maxime Gardereau** du cabinet de conseil **PROVADYS** est la suivante : « Comment mettre en œuvre une transformation digitale et repositionner le DSI au sein du cabinet ? ».

La réalité du marché est que la révolution numérique est en marche (livraison par drones, imprimantes 3D, big data...). De plus en plus de secteurs d'activité « s'uberisent » : taxis (uber), hôtels (airbnb), transports en commun (blablacar)...

A quand l'uberisation des avocats ?

La transformation digitale doit être un objectif fort des cabinets. La technologie ne doit cependant pas être une finalité mais bien un moyen d'accélérer le business. Le DSI doit d'emparer de cette tendance et incarner cette transformation.

Partons d'un constat : comment est perçue la DSI par le métier : à 90% au moins comme une entité gérant les opérations. L'innovation, la seule partie visible et représentant une valeur ajoutée importante vis-à-vis du métier n'est que la partie émergée de l'iceberg ; celle à laquelle le DSI n'a que très peu de temps à consacrer.

Il faut donc inverser la tendance et la perception. Voici quelques pistes :

- Mettre en place une « DSI as a service » → catalogue de services (industrialiser, standardiser)
- Standardiser les fonctionnalités universelles
- Adopter des architectures souples mais solides (cloud)
- Cultiver la réactivité
- Permettre au métier d'innover et garder une longueur d'avance sur le marché

Comment initier la transformation ?

- 1- Fixer la stratégie (le rôle du DSI vis-à-vis du métier en particulier)
- 2- Expérimenter et déployer → Faire des POC, se tromper, savoir jeter
- 3- Transformer les usages

Côté méthodologie, des approches comme DevOps ou Lean peuvent parfaitement d'appliquer.

Au bout du compte, Si le DSI 1.0 ne change pas, il est condamné car il restera un centre de coût. Il doit intégrer de la stratégie et du leadership dans son quotidien, se focaliser sur les services qui permettent de se différencier et de générer de l'activité et remplacer les applications commodités par des solutions standard.

Le point de vue d'Altis consulting

Le DSI technicien a vécu. L'enjeu glisse progressivement (et en fonction des tailles des organisations) de la capacité à mettre en place et à gérer au quotidien une infrastructure et des outils nécessitant toujours plus d'expertise technique, à la capacité à relever des challenges business aux côtés des équipes métier.

Pour cela, le DSI doit se mettre en situation d'innover et apprendre à gérer des partenariats et des contrats (d'externalisation en particulier) plutôt que des serveurs.

Les faits sont cependant têtus : sur le terrain, les petites et moyennes organisations (mais pas que) ont encore très souvent une vision classique de la DSI. Autant que les réticences vis-à-vis du cloud, c'est la perte de contrôle de ce sujet que les DSI maîtrisent souvent le mieux –l'infrastructure- qui freine cette évolution, inéluctable à moyen terme cependant.

2. Quel type de cloud choisir ?

Christian Domange (Canopy) et Eric Cullerier (Mimecast) nous font un point de situation sur les solutions cloud et leur degré de maturité.

D'une manière générale, la question vis-à-vis du cloud est dorénavant plus de l'ordre du « Quel type de cloud faut-il mettre en œuvre » que du « Faut-il y aller ».

Les mises en œuvre de solutions cloud répondent en général à 3 types d'objectifs :

- Améliorer l'infrastructure et réduire les coûts de possession (virtualisation) → IAAS
- Ajouter une nouvelle expérience utilisateur (mobilité, collaboratif, Office 365) → SAAS
- Réinventer le business (applications nativement cloud pour aller vite) → PAAS

Du fait des besoins et des degrés d'exigence très variés, les offres cloud ont évolué jusqu'à proposer des environnements hybrides (c'est-à-dire partiels) qui ont conquis 19% des organisations en 2014.

Dans le même ordre d'idée, les offres de cloud privé évoluent vers des approches de type « Managed private cloud » dans lesquelles les fournisseurs proposent certains services supplémentaires en plus du simple hébergement.

Pour faire un choix de type de cloud et un niveau de service associé, Christian et Eric recommandent d'évaluer le besoin de chaque application selon une matrice indiquant d'un côté :

- Les exigences de chaque application en termes de modèle d'investissement (capex/opex), niveau de confidentialité, degré de standardisation, besoin en personnel, time to market, complexité vis-à-vis de la mobilité

De l'autre, les différents types d'infrastructure :

- On premise, cloud privé, PAAS, SAAS, cloud public

Le point de vue d'Altis consulting

Si l'agilité des offres cloud en général et leur capacité à décharger les DSI de ce qui tend à devenir des « commodités » ne font plus débat, on peut cependant comprendre la réticence de certaines organisations à basculer, tant l'offre est complexe et mouvante et sachant qu'un certain nombre de questions concernant la sécurité et la confidentialité restent posées dans de nombreux cas.

Le raisonnement par application n'a par ailleurs de sens qu'à partir du moment où une réflexion globale sur la mission de la DSI et l'évaluation de ses coûts futurs a été menée. C'est donc cela le point de départ.

3. DSI 2.0 – Retour d'expérience 1 an après

Raphaël Helion, DSI de **PWC** nous livre un premier retour d'expérience sur son vaste projet de transformation lancé il y a un peu plus d'un an :

La situation de départ est une organisation avec plusieurs milliers d'utilisateurs, des applications anciennes et redondantes, une infrastructure vieillissante et complexe et une DSI agissant en tant que centre de coût.

La stratégie d'évolution est d'abord venue du métier. Elle se décline en mots-clés comme : business first, transform ourselves, increase influence & reputation, technology enabled, flexibility, agility.

La vision DSI de cette stratégie part de deux fondamentaux :

- IT 2.0 = FO 2.0 (front-office) + BO 2.0 (Back-office)
- Centre de coût → Centre de service → Centre de profit

La DSI a identifié et lancé 30 projets et s'est donné 15 mois pour les achever. Ils couvrent les domaines de l'infrastructure, le service à l'utilisateur, la gestion des applications et la sécurité.

Les principes de départ sont les suivants :

- Autofinancement
- Objectif de baisse du coût global de 20% à horizon 5 ans
- Réalisation au forfait.

Le processus global de transformation est le suivant :

Due diligence	Choix fournisseurs & solutions	Négo & contractualisation	Transition	Transformation
Business case Vision Macro-planning	Pas de RFP	Intervention de cabinets juridiques externes	Mise en place d'une gouvernance Transfert de connaissances Centre de support Cloud privé Process et outils de comm.	Go to cloud Nouveaux services Nouvelles équipes

Les enseignements tirés de cette expérience à ce stade sont les suivants :

- Plutôt que diffuser largement un RFP qui traduit une vision unique, sélectionner quelques acteurs comme autant de partenaires potentiels et leur demander d'être créatifs
- Définir un business case sur 5 ans (complexe, donc se faire aider)
- Chercher le sponsorship de quelques personnes influentes en interne
- Ce projet nécessite de nouvelles compétences (gestion des contrats par exemple) et se heurte à la résistance de certaines personnes qu'il faudra remplacer
- Le modèle cloud n'est pas encore très mature. C'est une limite à prendre en compte
- Ne jamais perdre de vue l'objectif de la DSI d'être un partenaire du métier.

Le point de vue d'Altis consulting

Ce projet impressionne, autant par son ambition et son avant-gardisme que par l'enthousiasme et l'engagement de son instigateur et pilote.

S'il est difficile d'imaginer tel projet à court terme dans les organisations de taille plus modeste, il est en revanche important que les grands acteurs ouvrent la voie sur des approches novatrices et intéressant d'en mesurer l'impact une fois la transformation achevée.

4. IT as a business development aid

Pierre-Marie Davodeau (Renkan consulting), Richard Legendre (Altis consulting) et Harry Pfeffer (LexisNexis) se sont succédés pour faire part de leur vision de l'impact possible de l'IT sur le développement commercial d'un cabinet.

Pierre-Marie fait tout d'abord un constat : la fonction « Business development » n'est pas identifiée comme une activité autonome dans la moitié des cabinets et, pour les 24% d'entre eux ayant créé un poste de CBDO, ce poste a été confié au CMO dans 80% des cas.

Le système d'information d'un cabinet représente une mine de données, souvent inexploitées, qui peuvent avoir un impact réel en matière de business development, en identifiant, en recoupant, en échangeant et en traitant celles qui ont une réelle valeur (agrégats financiers, analyse d'impact des emailings, fréquence de certains échanges emails...).

Une bonne cartographie de flux associée aux données du CRM permettra par exemple de mieux cibler les contacts et échanges à privilégier.

J'ai ensuite pris le relais en partant du constat que :

- 1- Les budgets IT augmentent constamment. Pour autant, la part réellement consacrée au BD reste très faible.
- 2- Les cabinets ont la plupart du temps une vision floue du coût réel des prestations facturées, donc une difficulté évidente à en estimer le prix de vente au départ
- 3- La technologie va vraisemblablement faire sous peu irruption dans le métier même des avocats et transformer la manière de le pratiquer, donc de le vendre
- 4- Le business model des cabinets va donc, par la force des choses, évoluer significativement. Et l'IT sera au cœur des nouvelles approches de business development.

J'ai choisi deux exemples pour illustrer cela :

Tout d'abord, les avocats, du fait de leur culture et de leur pratique de prix élevés, travaillent quasi-exclusivement en mode silo et pas en mode projet (nomination de chefs de projets, chiffrage par rubriques, planification, gestion de ressources...). Du coup, ils n'ont qu'une idée approximative de la rentabilité d'un dossier.

La pression sans cesse plus forte des clients sur les prix et la réduction progressive de la facturation à l'heure forcent les cabinets à plus de rigueur pour maintenir leur marge. La gestion de projets est l'une des clés.

Il ne faut cependant pas se leurrer : la réduction (par une meilleure maîtrise) du coût de revient sera vite absorbée par une pression supplémentaire sur les prix.

L'échappatoire est alors une évolution du modèle économique vers plus de volume et une optimisation plus grande des ressources. Cela suppose des outils au cœur même du processus commercial.

J'ai ensuite fait le pari que, d'ici quelques années, une part significative des dossiers sera traitée par des robots. Je ne parle pas là de tâches périphériques, mais bien du travail actuel des avocats :

- Recherche des données de base (contexte du client, du dossier, doctrine et jurisprudence liée à la problématique posée)
- Analyse et sélection des éléments pertinents
- Application de règles de déduction – calcul d'une probabilité de succès
- Rédaction du résultat. Selon le cas, un avis, un contrat, des conclusions...

Si l'on regarde bien autour de nous (finance, presse, médecine...) il y a de nombreux exemples – émergents, certes- d'irruption de l'Intelligence Artificielle dans des processus évolués. Dans le domaine du droit, des solutions commencent à se développer, basées sur la technologie Watson d'IBM (par exemple le projet de robot-Avocat ROSS) ou plus inédites (la technologie ACE de Ravn). De gros cabinets font leurs propres expériences, tel le laboratoire Nextlaw labs créé par Dentons pour développer les technologies de demain.

Cette nouvelle répartition des tâches réduira les coûts en même temps qu'elle permettra d'offrir de nouveaux services (Obtention d'un avis express via un site web par exemple).

Là encore, un nouveau modèle économique va émerger. La question est de savoir si les cabinets traditionnels vont être capables de faire ce saut dans l'inconnu ou s'ils vont attendre d'être dépassés par de nouvelles structures décomplexées et plus agiles.

Harry Pfeffer a ensuite choisi d'alerter sur le risque de non-respect des règles en matière de données personnelles : Les processus automatisés de type big data, les outils d'e-marketing et les systèmes de gestion passive des données ont en effet tendance à stocker de grands volumes d'informations, pas toujours en phase avec la réglementation.

Les informations liées à des personnes physiques ou morales et de type

- Démographique (âge, date de naissance, ethnie, informations issues du passeport)
- Antécédents (emplois, formation, informations judiciaires ou médicales)
- Biométrique (taille, poids, couleur des yeux, groupe sanguin...)
- Correspondance privée...

La règle est de ne collecter que les informations utiles, d'y appliquer des mesures de confidentialité raisonnables, de ne les conserver que pendant la période nécessaire à leur usage et de permettre à la personne concernée de les consulter sur demande.

Le point de vue d'Altis consulting

La première menace pour les cabinets d'avocats en général est la standardisation, paradoxalement initiée par les cabinets eux-mêmes, qui va tirer les prix vers le bas. La seconde est le piège consistant à se réfugier sur le créneau haut de gamme, dont le périmètre va se réduire inexorablement.

Les cabinets sont donc condamnés à se réinventer, à inviter la technologie dans chaque étape de leur quotidien, à exploiter chaque information disponible -dans le respect des règles concernant les données personnelles- et, bien entendu, à revoir leur modèle économique.

5. La fin de l'âge de cuivre

Selon **Bouygues Telecom**, le réseau cuivré, donc le RTC, donc l'ADSL sont condamnés à court terme :

- En 2018, les nouvelles lignes RTC cesseront d'être commercialisées
- En 2020, le réseau RTC cessera d'être exploité par étapes. (par plaques)

Quel est donc l'avenir de la téléphonie fixe ?

- Mise en œuvre d'autocommutateurs de type IPBX + SIP (protocole de VoIP)
- Communication unifiée via le PC (Lync de Microsoft ou Jabber de Cisco par exemple)
- Substitution fixe/mobile ou plutôt convergence du fixe vers le mobile.

Les postes de téléphone tels que nous les connaissons (reliés à un réseau distinct) vont donc disparaître au profit d'applications. La transition passera éventuellement par des postes de téléphone branchés sur les PC.

Les différents sites d'une organisation seront progressivement reliés en IP et un seul sera muni d'un autocom. Cela pose d'ailleurs aujourd'hui un problème de localisation géographique pour les appels d'urgence.

Les applications de type Lync ou Jabber vont dans un premier temps prendre en charge les échanges de message en interne, puis la voix en interne, puis en externe. La question de la portabilité des numéros fixes se pose alors.

Le point de vue d'Altis consulting

En d'autres termes, la téléphonie fixe est morte, « skypeisée » à défaut d'être « uberisée ». Paix à son âme...

6. Les techniques des pirates et comment s'en protéger

Christophe Kiciak, consultant sécurité chez **Provadys** a proposé un tour d'horizon des techniques des pirates et fourni quelques clés de base pour s'en protéger, ou tout au moins sensibiliser les gens aux différents types d'attaques.

Il y a peu de statistiques concernant les incidents de sécurité en Europe car il n'y a pas d'obligation de les déclarer, contrairement aux Etats-Unis. On peut cependant affirmer que le piratage, souvent opportuniste, est à 80% l'œuvre de mafias et devenu plus rémunérateur que le trafic de drogue.

L'objectif est en général de s'approprier de la puissance de calcul ou de l'espace de stockage, revendus ensuite au marché noir.

On estime qu'il y a eu en 2014 43 millions de cyber-attaques, soit 117.000 par jour. Cela génère une augmentation forte du coût de la sécurité pour la plupart des organisations.

La cible la plus prisée actuellement est l'Europe du fait de son moindre niveau de sécurisation comparé aux Etats unis. La plupart des sociétés ont le sentiment d'être bien protégées. Pourtant, dans 95% des cas, un test d'intrusion permet d'exfiltrer des données sensibles.

Au-delà des équipements de sécurité, nécessaires, c'est souvent l'humain qui est le maillon faible.

Christophe nous a fait part de son top 10 des techniques d'attaques des pirates :

- 1- Pirater le matériel → typiquement via un keylogger physique (clé USB qui s'intercale entre le clavier et l'UC et récupère toutes les frappes clavier, donc les mots de passe).
- 2- Accéder à des données chiffrées → Le chiffrement n'est plus actif lorsque les données sont en cours d'utilisation, ce qui met une limite claire à ce type de protection
- 3- Attaque sur les applications → plus simple sur un client lourd en lien direct avec la base de données qu'avec un client léger, plus standard mais avec plus de couches à traverser pour atteindre les données
- 4- Passer par la gestion des privilèges → De nombreux utilisateurs sont toujours administrateurs locaux de leur PC. Un virus peut donc facilement accéder à toutes les ressources
- 5- Configuration des équipements système → Un manque (fréquent) de précision crée une vulnérabilité immédiate.
- 6- Mots de passe trop faciles à identifier, protocoles anciens (DNS, DHCP, ARP, BGB) très utilisés mais peu sécurisés
- 7- Applications web → Difficiles à sécuriser car on y recense pas moins de 250 points d'attaque possibles. Ajoutons à cela que la sécurité est très peu enseignée dans les écoles de développement.
- 8- Equipements pas patchés régulièrement → il existe des outils full automatiques pour viser ces failles. Les mises à jour doivent donc porter sur chaque niveau de l'infrastructure : OS, réseau, applications (typiquement les outils de CMS web).
- 9- Le réseau interne → C'est un point de départ permettant une attaque réussie presque à tous les coups. Un LAN est particulièrement difficile à sécuriser du fait du nombre important d'équipements qui doivent être accessibles.
- 10- Le maillon humain → Les pièges par email, par téléphone ou encore don de matériel piégé sont des classiques d'une redoutable efficacité.

Le point de vue d'Altis consulting

Une chose est sûre : la sécurité va désormais peser de plus en plus lourd dans le budget global des DSI. L'utilisateur étant souvent peu sensible à ce sujet et du coup le principal point d'entrée des attaques, l'une des premières actions à mener est évidemment l'éducation.

Ensuite, étant donnée la tendance à la concentration des systèmes informatiques dans des silos (clouds privés ou publics), se pose la question de l'enjeu, beaucoup plus significatif pour un pirate, d'une attaque sur ces sites peu nombreux et plus « rentables », même si mieux protégés. C'est le « syndrome Die Hard IV ». Référence qui peut faire sourire, mais à méditer tout de même...

7. Assurer les cyber-risques

Michael, courtier en assurance nous a éclairés sur l'assurance des cyber-risques.

Pour rappel, une compagnie d'assurance est en zone de confort si elle est capable de mesurer un risque (sur la base de statistiques), si ce risque est mutualisable ou s'il reste aléatoire.

Le problème est que cela n'est pas vrai dans le cas du cyber-risque.

Dans cette situation, faute de statistiques et du fait de la technicité du sujet, l'assureur ne s'intéresse pas à la technologie en place, mais à la gouvernance mise en place pour limiter le risque. Cela est directement de la responsabilité du DSI et des équipes métier.

On estime dans la profession que le cyber-risque concerne

- De la malveillance à 50%
- Des erreurs humaines à 30%
- Des événements naturels à 20%

L'objet d'un contrat en cyber-sécurité concerne l'atteinte aux équipements IT d'une part et l'atteinte aux données de l'organisation d'autre part.

Il est important de noter que la majorité des cabinets d'avocats ne sont actuellement pas assurés pour des cyber-risques.

CONCLUSION

Cette édition 2015 de l'off-site CIJ était, de mon point de vue en tout cas, la plus riche et la plus aboutie de toutes. Cela est sans doute dû (outre la qualité inégalée des intervenants☺) au fait que nombre de sujets, récurrents depuis les 3 dernières années (externalisation, cloud, sécurité, évolution du rôle du DSI) ont atteint un niveau de maturité permettant un emboîtement beaucoup plus naturel entre eux et surtout permettant aux personnes présentes de se positionner et de se projeter vis-à-vis de chacun d'eux.

Pour autant, nous sommes vraisemblablement à l'aube d'une transformation majeure de l'organisation, du modèle économique et du métier même des cabinets d'avocats. Au-delà des incertitudes que cela engendre nécessairement, c'est un formidable challenge qui se présente pour la plupart d'entre nous.

Ne boudons pas notre plaisir !

Richard LEGENDRE

Fondateur – Altis consulting