102

CIO.FOCUS

Septembre 2015

Le rôle central des DSI même là où on ne l'attend pas

En bref

Partout, l'informatique est partout ! Et cela a une conséquence souvent négligée : le DSI est de ce fait lui aussi partout impliqué. Même aux endroits les plus inattendus.
Ainsi, par exemple, combien de DSI sont conscients de leur rôle central dans un bon déroulement de contrôle fiscal ? Pourtant, certaines entreprises ont eu quelques ennuis parce que leur DSI n'était pas sensibilisé à ce problème.
Bien entendu, les DSI de grandes entreprises ont des préoccupations souvent plus stratégiques. CIO a ainsi interviewé le nouveau DSI groupe de Total, la première capitalisation boursière française. Frédéric Gimenez y révèle ses préoccupations et projets.
Parmi les difficultés classiques du rôle du DSI, il y a les relations avec les fournisseurs. Heureusement, les DSI peuvent s'appuyer sur certains clubs d'utilisateurs. Le plus dynamique est probablement l'USF, le club des Utilisateurs de SAP Francophones. En amont de sa prochaine convention, son président Claude Molly-Mitton nous a révélé les défis que l'éco-système SAP allait devoir relever.
Enfin, Catherine Chambon, commissaire divisionnaire dirigeant la Sous-Direction de la Lutte Contre la Cybercriminalité (SDLC) à la Direction Centrale de la Police Judiciaire (DCPJ), est intervenue dans nos colonnes pour rappeler quelques messages de bon sens. Si la cybercriminalité est un fléau qui n'est pas prêt de disparaître, beaucoup de négligences sont commises qui en augmentent les conséquences.

Sommaire

Juridique

Contrôle fiscal : rôle central et responsabilité élevée pour le DSI

Marc Lamort de Gail est expert-comptable associé du cabinet Incivo, spécialisé dans l'assistance au contrôle fiscal des comptabilités informatisées.

Contrairement à ce que, sans doute, il pourrait croire au premier abord, le DSI a un rôle essentiel dans la préparation et la réalisation d'un contrôle fiscal dans son entreprise. Et les difficultés demeurent aujourd'hui importantes, entraînant des risques financiers majeurs.

« Oui, il y a des contrôles fiscaux qui se passent mal pour des raisons informatiques » martèle l'expert-comptable spécialisé Marc Lamort de Gail. Animateur de deux groupes de travail au sein de l'Académie des Sciences et Techniques Comptables et Financières, il soupire : « les DSI ne s'en préoccupent que s'ils sont confrontés au problème, donc trop tard, alors que les risques juridiques et financiers sont importants pour les entreprises. »

Le sujet du contrôle fiscal est, contrairement à ce que l'on pourrait croire au premier abord, très transversal. Bien entendu, les premiers concernés sont tout de même les directeurs financiers (DAF), les responsables comptables, le responsable fiscalité, etc. D'autres directions, parce qu'elles fournissent les éléments permettant d'établir les comptes et donc les bases d'imposition, sont également concernées : DRH, Direction Commerciale... Et puis des experts techniques sont également nécessairement impliqués : la direction juridique, parfois la direction qualité... et la DSI. Marc Lamort de Gail souligne : « la vraie difficulté est que chacun comprenne les autres, un exemple de problème étant le sens différent donné au mot *archive* par un DSI et par un directeur juridique. »

Que vient faire le DSI dans cette galère ?

Mais en quoi le DSI est-il donc spécifiquement concerné ? « Le contrôleur peut demander à accéder à toutes les données justifiant directement ou indirectement les résultats comptables et fiscaux, donc pas seulement à la comptabilité » explique Marc Lamort de Gail. De ce fait, le contrôleur doit comprendre le système d'information et il faut donc lui présenter. Il peut être amené à examiner la GRC, la gestion des stocks, la gestion des tarifs, la paye... Les données purement marketing ne sont normalement pas concernées, sauf exception, par exemple lorsque ces données permettent de comprendre pourquoi tel tarif a été appliqué à Untel.
Si le PGI est évidemment la première cible du contrôleur, la vérification peut intégrer des fichiers de tableur ou du décisionnel. En effet, ces outils peuvent permettre de comprendre la logique tarifaire et de vérifier que le profit déclaré est bien le profit réel. « Il faut être capable de récupérer les données sur le chemin d'audit sur tous les exercices concernés » insiste Marc Lamort de Gail.
Et comme le contrôle porte sur un minimum de trois ans mais peut être étendu dans certains cas à des données pouvant dater de six à dix ans, il faut être capable de présenter les évolutions du système d'information. Ces évolutions doivent donc être documentées. Depuis 2014, les obligations afférentes ont été renforcées.
Marc Lamort de Gail relève : « être prêt pour un contrôle fiscal permet aussi de simplifier le contrôle interne continu qui est, au fond, une démarche similaire au contrôle fiscal. » Le contrôle interne continu va ainsi permettre de détecter les erreurs d'imputation et les fraudes internes.
En cas de contrôle inopiné, en général ciblé suite à un soupçon, un contrôleur peut arriver dans l'entreprise, demander à accéder à ce qu'il désire, le copier et l'emporter. Encore faut-il que cela soit techniquement possible...

Le double piège de l'archivage et de la traçabilité

L'archivage des données, même s'il est coûteux, doit être garanti. Une collaboration transverse entre les différentes directions -notamment DAF, Direction juridique et DSI- est nécessaire pour définir la profondeur et la durée des archives. Autrement dit : qu'archive-t-on et pour combien de temps ? Dans le cas d'un PGI, c'est quasiment la totalité du système qui est à archiver !
Or l'archive, au sens fiscal et juridique, n'est pas une archive au sens informatique. Pour le juriste et le fiscaliste, il s'agit de disposer des données dans un format normalisé (et donc *non-propriétaire*) avec preuve de non-modification et date certaine. Et cette archive doit contenir tous les éléments nécessaires !
Certaines obligations pèsent plus spécifiquement sur les créateurs du système d'information, éditeur ou intégrateur notamment. Ainsi, la documentation des logiciels doit être disponible et elle doit explicitement présenter les évolutions du système. Par exemple, cette documentation doit permettre de démontrer qu'à aucun moment la suppression d'un enregistrement du système de caisse ou d'une écriture comptable n'est possible. En cas de manquement, l'éditeur et/ou l'intégrateur peuvent ainsi se voir infliger une amende administrative pouvant atteindre 15% de leur chiffre d'affaires ou 1500 euros par licence de logiciel vendue.

Le FEC n'est pas une mince affaire

Lorsque le contrôleur fiscal arrive dans l'entreprise, il va demander en tout premier lieu, normalement et en dehors de cas particuliers de contrôles pré-ciblés (par exemple sur le Crédit Impôt Recherche), le FEC (Fichier des Ecritures Comptables). Quoi de plus simple ? Contrairement à ce que beaucoup d'informaticiens peuvent croire, cela n'a,

justement, rien de simple car la fourniture du FEC est précisément l'un des premiers écueils lors d'un contrôle des comptabilités informatisées.
Le FEC doit être disponible lorsque le contrôleur le demande dans un délai très bref (le premier jour en principe). C'est un fichier texte dans un format normalisé comportant, selon les pays et les régimes fiscaux, de 18 à 23 champs par ligne. L'OCDE pousse une évolution de la norme pouvant comporter jusqu'à 1000 champs par ligne, adoptée à ce jour par certains pays comme le Portugal.
Le FEC contient, sans aucune compilation ou regroupement, la totalité des opérations de comptabilité générale. Lorsque la comptabilité comporte des millions de lignes, les volumes peuvent atteindre plusieurs giga-octets de données (voire, dans certains rares cas, tera-octets).
Parfois, même fournir un FEC répondant aux normes est impossible. « Les plus grandes difficultés surviennent avec des groupes étrangers implantés en France dont le PGI est centralisé dans un autre pays, éventuellement en SaaS, et dont les responsables sont incapables de fournir un FEC au bon format voire ne comprennent même pas l'importance de pouvoir le faire » observe Marc Lamort de Gail.
Or une non-présentation d'un FEC conforme peut être sanctionnée par une amende dont le montant minimum est de 5000 euros par exercice, ou 10% des redressements effectués, si ceux-ci sont supérieurs. Parmi les erreurs à éviter, notons la modification pour « rendre présentable » le FEC, surtout sous Excel qui a la fâcheuse tendance à transformer les séparateurs de façon non-conforme. Le FEC ne doit jamais être modifié faute de quoi il devient de ce seul fait non-conforme.

Un décisionnel particulier, premier outil du contrôleur

Une fois que le contrôleur fiscal dispose du FEC, il va pouvoir l'analyser avec des outils qui ressemblent à du décisionnel classique. En France, les contrôleurs disposent du logiciel Alto 2 sur leurs ordinateurs portables. Celui-ci comprend un certain nombre de requêtes et d'analyses pré-paramétrées qui vont permettre au contrôleur de repérer des anomalies. L'idée est de pouvoir rapidement cibler des points à contrôler plus particulièrement.
Des éditeurs ont développé des outils dédiés à l'analyse des données natives du système d'informations comprenant des progiciels courants du marché (Oracle Business Suite, SAP, etc.). Les principaux sont deux éditeurs canadiens : Idea et ACL. Au départ, ces outils étaient dédiés à l'audit et le fisc s'en est dotés dans la plupart des pays. Ces logiciels sont une sorte de décisionnel assurant une traçabilité des opérations et comportant une interface de programmation.
Ce n'est qu'après cette étape d'analyse du FEC que le véritable contrôle fiscal commence, une fois les pistes d'audit identifiées. Le but de cette démarche en deux temps est d'augmenter la productivité des contrôleurs.
Dès lors, le contrôleur va pouvoir demander à accéder aux justificatifs de chaque opération, donc en particulier aux données du système d'information ayant concouru directement ou indirectement à l'établissement de la comptabilité. L'entreprise peut procéder elle-même aux extractions demandées ou recourir à un prestataire spécialisé comme la société de Marc Lamort de Gail. Celui-ci insiste : « à tout moment, il faut être capable d'extraire ce qui est demandé, les traitements particuliers pouvant être fournis en général sous quinze jours. »

Le désastre peut être total pour des raisons informatiques

La situation peut parfois tourner à la vraie catastrophe pour des raisons purement informatiques. Le fisc peut en effet juger que la comptabilité est non-probante,

notamment si l'intégrité des données ne peut pas être garantie ou si la traçabilité est insuffisante. Dans ce cas, la comptabilité présentée est simplement rejetée et le fisc va définir par lui-même la base imposable. En général, le calcul fait par le fisc est moins favorable à l'entreprise que celui présenté par celle-ci... qui ne peut pas rétorquer en présentant une comptabilité qui a déjà été rejetée au départ !

Marc Lamort de Gail se souvient : « mon pire cauchemar a été une entreprise où je devais dialoguer avec des interlocuteurs changeant sans cesse au sein d'une DSI, d'une DAF et d'un infogérant avec des équipes en Inde parlant mal anglais et ne comprenant pas les enjeux. »

Dans le pire des cas, en général lorsqu'il y a une forte suspicion de fraude, le fisc peut engager une procédure judiciaire aboutissant à la pose de scellés ou à la copie (éventuellement intégrale) du système d'information. Les systèmes de caisse sont les plus sensibles et les plus porteurs de risques : ils ne doivent en aucun cas permettre l'effacement de données. En cas d'effacement de données (réel, supposé ou simplement possible), l'entreprise et ses dirigeants sont soumis à un risque pénal.

En savoir plus

- L'Académie des Sciences et Techniques Comptables et Financières, initiative de l'Ordre des Experts Comptables, compte 65000 membres (dont 25000 à l'étranger et 20000 experts-comptables): DAF, auditeurs, contrôleurs de gestion, juristes, professionnels du chiffre (experts-comptables...), etc. Elle a consacré son Cahier numéro 20 au sujet du contrôle fiscal informatisé (accès libre - PDF).

- Marc Lamort de Gail est expert-comptable associé du cabinet Incivo, spécialisé dans l'assistance au contrôle fiscal des comptabilités informatisées. Au sein de l'Académie des Sciences et Techniques Comptables et Financières, il anime deux groupes de travail, l'un sur la préparation du contrôle fiscal des comptabilités informatisées, l'autre sur la mise en conformité à la nouvelle norme de l'OCDE sur les fichiers d'audit fiscal.

- Lors du Congrès de l'Ordre des Experts Comptables, qui a lieu au Palais des Congrès à Paris, Marc Lamort de Gail animera deux conférences sur le sujet du contrôle fiscal des comptabilités informatisées : le 30 septembre et le 1er octobre 2015 à 17h30 les deux fois. Site web de l'événement

Bertrand Lemaire
Rédacteur en chef de CIO

Stratégie

Frédéric Gimenez (Total) : « au-delà de la sécurité, notre défi est d'optimiser les coûts et amorcer la transformation numérique »

Frédéric Gimenez, le nouveau DSI groupe de Total

Frédéric Gimenez a été nommé DSI groupe de Total le 1er mars 2015 après vingt ans chez le pétrolier et avoir été notamment premier DSI de la branche Raffinage-Chimie après sa réorganisation. Il doit relever des défis en matière d'optimisation des coûts et de sécurité tout en amorçant la révolution numérique.

***CIO :* Comme votre prédécesseur, Patrick Héreng, vous venez de la branche *Raffinage*. Y-a-t-il une voie royale pour devenir DSI groupe de Total ou est-ce un complet hasard ?**

Frédéric Gimenez : Il n'y a pas de *voie royale*. En effet, le prédécesseur de Patrick Héreng, Philippe Chalon, venait de l'Exploration-Production. Patrick Héreng était issu de la branche Raffinage-Marketing aujourd'hui disparue. Cette branche regroupait une partie industrielle et une partie commerciale.

La réorganisation (à laquelle j'ai pris part) a abouti à la création d'une branche industrielle Raffinage-Chimie et à une branche majoritairement commerciale baptisée Marketing et Services. Les stations-services en sont la partie visible mais la branche distribue aussi du carburant pour les navires et les avions, des lubrifiants, des cartes de paiement, etc. La branche Raffinage-Chimie, quant à elle, s'est construite sur une logique de chaîne industrielle intégrée, les sites industriels « chimie » etant en aval des

raffineries et en général très proches géographiquement. Ce rapprochement a été très efficace en matière de synergies. Suite à cette réorganisation Total comprend aujourd'hui une holding groupe et plusieurs branches : EP (Exploration-Production), Gaz, RC (Raffinage-Chimie), M&S (Marketing & Services) et EN (Energies Nouvelles).

CIO : Quels ont donc été vos atouts pour être nommés, selon vous ?

Frédéric Gimenez : J'ai eu un parcours très varié dans l'IT au sein du groupe Total comme vous le savez. J'ai notamment participé à la création de la branche Raffinage-Chimie et donc à la création de sa DSI regroupée.
Or, bien que Raffinage et Chimie soient deux activités industrielles, leurs cultures étaient très différentes. La Chimie était basée à Bruxelles et très mondiale dans son approche, quand le Raffinage était basé à Paris avec une vision plus européenne. Et les solutions et modes de fonctionnement IT étaient là aussi très différents. C'est non seulement le fait d'avoir réussi à faire travailler ensemble ces équipes mais aussi les bons résultats obtenus dans la diminution des coûts lors de la fusion, qui ont du être remarqués au niveau groupe.
La dernière étape a été le lancement de la transformation digitale au sein de cette branche industrielle. Si, aujourd'hui, Marketing et Services, par nature au contact du client final, comprend bien les enjeux, c'est un peu moins évident de faire comprendre l'intérêt de cette transformation digitale pour les métiers plus industriels.

CIO : Justement, entre l'exploration-production et les stations-services avec les cartes de fidélité, il n'y a presque rien de commun en termes de besoins métiers. Quel est aujourd'hui le sens d'une DSI groupe chez Total ?

Frédéric Gimenez : La fédération autour des socles communs (télécoms, postes de travail, etc.) a longtemps été le grand combat de la DSI groupe. La taille d'un groupe comme Total est aussi une force pour le sourcing et la négociation avec les fournisseurs. Par exemple, les contrats de licences SAP, Oracle ou Microsoft sont négociés au niveau groupe et les usages optimisés par branches.
De plus, les SI des fonctions supports ou transverses (SIRH, SI financier...) sont de plus en plus construits en commun pour tout le groupe. Fondamentalement, il n'y a pas vraiment de différence entre la gestion d'un salarié d'une branche à l'autre.
Même dans des domaines plus proches des métiers des branches, il y a des synergies possibles. Certaines solutions développées dans une branche peuvent ainsi être réutilisées ailleurs car on retrouve des fonctions industrielles ou commerciales dans chaque branche. Par exemple, aussi bien sur les plates-formes off-shore et que dans les raffineries, on doit gérer la maintenance d'unités composées d'un ensemble de tuyaux, de pompes et de vannes. En fait, il y a plus de points communs que ce que l'on croit souvent. On a pu le voir quand on a fusionné Raffinage et Chimie, notamment. C'est la DSI groupe qui orchestre cette mutualisation.
De même, la révolution digitale est également assez transverse : réseau social d'entreprise (RSE), mobilité... tous ces sujets sont très agnostiques du métier.
Enfin et surtout, par définition, la sécurité IT relève de la responsabilité du Groupe.

CIO : C'est à dire ?

Frédéric Gimenez : Le secteur de l'énergie est une cible fréquente, qu'il s'agisse de cyber terrorisme ou d'intelligence économique. Total est un groupe très visible d'une part, et d'autre part en concurrence dans un domaine startégique avec des acteurs chinois, russes, américains par exemple... Bref, nous sommes une cible évidente.

De plus, il y a désormais un gros enjeu sur la protection des sites industriels : une cyberattaque visant à un sabotage d'installations par la prise en main des équipements pilotés est un risque pris très au sérieux chez Total. L'ANSSI est aussi mobilisé activement sur ce sujet.
La DSI groupe a vocation à mettre en place les référentiels et les outils qui permettent de protéger l'ensemble du groupe.

CIO : Pour concilier sécurité, performance et moindre coût, quels sont les modèles adaptés à Total ?

Frédéric Gimenez : Depuis dix ans, nous avons procédé à beaucoup d'externalisation et de massification des prestations. Nous avons atteint un niveau suffisamment avancé. La tendance, aujourd'hui, est de recourir à de plus en plus d'applications en mode SaaS en particulier autour des métiers support (RH...) et marketing mais moins pour les métiers industriels où l'offre est plus limitée. Par contre, nous n'avons pratiquement pas recours au IaaS/PaaS externalisé et avons jusqu'ici privilégié le cloud privé interne. Pour l'heure, le IaaS/PaaS externalisé pourrait être envisagé pour garder de la flexibilité en lien avec la variation d'activité ou pour réaliser des pilotes sans avoir à créer une infrastructure dédiée.

CIO : N'y a-t-il pas, avec cette approche, un risque en matière de sécurité ?

Frédéric Gimenez : Oui, sans doute, nous avons à relever un grand défi en matière de sécurité. Historiquement, nous avions une approche plutôt périmétrique en matière de sécurité. Mais, aujourd'hui, nous travaillons sur une sécurité de l'ensemble du système d'information, qu'il soit interne ou externe.
Cette approche doit pouvoir rendre possible, sans risque inutile, le recours à du cloud externe mais aussi l'acceptation de terminaux non-Total pour accéder à notre système d'information.

CIO : Puisque l'on parle de terminaux non-Total, quelle est la place de la mobilité et du BYOD aujourd'hui chez Total ?

Frédéric Gimenez : Pour l'heure, nous n'acceptons pas de BYOD pour des raisons de sécurité, même s'il y a des pilotes en cours pour mieux appréhender les problématiques à traiter, notamment en termes de sécurité et de gestion des terminaux.
Le BYOD n'est d'ailleurs pas nécessairement une solution adéquate. Sous réserve de traiter la question du coût, fournir nous-mêmes des terminaux mobiles plus nombreux serait peut-être préférable. La mobilité en milieu industriel est aussi un vrai sujet. Au delà de la difficulté à fournir de la connectivité sans fil à des terminaux dans un monde de structures métalliques, il existe des normes anti-explosivité ATEX très strictes sur les outils électroniques pouvant pénétrer dans nos sites. Les pilotes mis en oeuvre avec des terminaux coûteux mais adaptés (durcis, étanches, ATEX...) montrent un potentiel de productivité des opérateurs bien supérieure à la méthode actuelle du bloc papier et du stylo.

CIO : En tant que DSI groupe, êtes-vous sollicité pour contribuer à l'amélioration du service rendu au client final, que ce soit en B2B ou en B2C ?

Frédéric Gimenez : Pas au niveau groupe. Pour le B2C et le B2B, les développements sont surtout portés par la branche Marketing et Services.
Il ne faut pas oublier les collaborateurs, qui sont aussi des clients finaux des outils que

nous mettons en place. Même si nous restons une entreprise d'ingénieurs où une ergonomie un peu difficile ne fait pas forcément peur, les collaborateurs ont de plus en plus de mal à comprendre que l'IT ne soit pas aussi simple dans l'entreprise qu'au domicile.

CIO : La dispersion géographique de vos collaborateurs incite-t-elle à développer des outils collaboratifs voire un réseau social d'entreprise (RSE) ?

Frédéric Gimenez : Voilà une actualité récente... Nous avons en effet créé WAT (Work at Total). C'est un portail qui regroupe les centaines d'Intranet historiques du groupe associé à un réseau social d'entreprise (RSE). L'ensemble utilise les technologies Microsoft Sharepoint 2013.
Nous avons commencé à déployer ce RSE cette année, pour l'instant auprès de 53 000 collaborateurs, et nous devrions terminer d'ici fin 2016 par les filiales les plus éloignées (exploration-production en particulier).
En six mois, un millier de communautés a été créé. La création est libre (quitte à ce que, dans quelques mois, nous supprimions les communautés inactives) et, de même, il n'y a pas de censure sauf en cas de non-respect de la charte de comportement. Les communautés peuvent être non-professionnelles car, même autour d'un hobby, si un collaborateur en France se rapproche d'un collaborateur d'Afrique, c'est un bénéfice. Nous voulons un outil de décloisonnement et de collaboration. Cela dit, une des communautés les plus actives est celle consacrée à la transformation digitale.

CIO : Quels sont les futurs grands chantiers à mener dans les prochaines années ? La transformation digitale, par exemple ?

Frédéric Gimenez : Effectivement, la transformation digitale en fait partie. Le DG du groupe, Patrick Pouyanné, a d'ailleurs annoncé la nomination d'un CDO pour accélérer la transformation numérique du groupe.
Nous sommes dans un contexte de pression sur les coûts. Nous prenons donc d'abord des initiatives pour répondre aux contraintes économiques. Les coûts IT du groupe ont ainsi pu être réduits de 10% cette année. C'est le résultat de nombreuses initiatives dans l'ensemble des structures SI du Groupe mais aussi d'initiatives transverses comme par exemple, la création en 2014 d'une filiale, Total Global Services, qui s'occupe de tout le socle mutualisé (postes de travail, télécom, etc.). Son directeur général, Dominique Pardo, est rattaché à la DF groupe comme moi. Nous sommes de vrais partenaires, sans relation hiérarchique.
Si l'optimisation des coûts et le renforcement de la sécurité restent la priorité, nous devons aussi faire évoluer le SI existant pour le préparer à la transformation digitale.
Enfin, il y a un enjeu autour de la gestion de la donnée. Marketing et Services exploite déjà les données clients et Exploration-Production a manipule depuis longtemps de très gros volumes de données sismiques. Mais il reste encore beaucoup à faire en particulier dans les entités industrielles, qui par une meilleure prise en compte des données disponibles pourraient optimiser le fonctionnement des usines.
Derrière la question des données, il y a bien entendu des aspects technologiques et de vraies questions de gouvernance. C'est un des grands défis que Total doit relever.

Sur le même sujet

5 mai 2015 : Frédéric Gimenez devient DSI groupe de Total après 20 ans chez le pétrolier

Stratégie

Claude Molly-Mitton (USF) : « malgré nos désaccords sur certains points, nos relations avec SAP sont apaisées »

Claude Molly-Mitton, président de l'USF (Utilisateurs SAP Francophones)

Claude Molly-Mitton est président de l'USF, le club des Utilisateurs SAP Francophones. Cette association fêtera ses 25 ans à la Convention qui se tiendra à Lyon les 7 et 8 octobre 2015 et qui se projettera sur les dix prochaines années (voire plus). Les relations sont aujourd'hui apaisées entre l'association et l'éditeur SAP malgré des divergences sur des sujets tels que les audits de licence ou les accès indirects. Et la sortie progressive de S/4 Hana est évidemment au coeur de l'actualité du club.

***CIO* : Les 7 et 8 octobre 2015, l'USF fêtera ses vingt-cinq ans lors de sa Convention annuelle à Lyon. Pourquoi avoir choisi le thème du *Monde Digital 2015-2025* ?**

Claude Molly-Mitton : Nous profitons de nos vingt-cinq ans pour nous projeter un peu en avant. Mais la date de 2025 n'est pas du tout innocente pour les utilisateurs de SAP !

En effet, cette année-là est la dernière de la garantie que l'éditeur assurera pour la maintenance de SAP Business Suite 7, notamment SAP ERP 6.0. Par conséquent, c'est aussi un clin d'oeil... Nous en profiterons pour essayer de voir ce qui pourrait se passer dans les systèmes d'information dans le monde.

Mais, comme d'habitude, avec nos conférenciers en plénières, nous pourrons aller bien au delà à la fois des systèmes d'information et de la date de 2025. Nous aurons ainsi les interventions de l'économiste Elie Cohen, du physicien-philosophe Etienne Klein, du

chirurgien-entrepreneur Laurent Alexandre, de l'économiste-éditorialiste Nicolas Baverez avec qui nous ferons de l'économie-fiction à l'échéance 2040, de l'avocat Yves Bismuth... et sans oublier Igor et Grichka Bogdanoff.

CIO : 2025, c'est demain pour un architecte IT…

Claude Molly-Mitton : Tout à fait. Et si l'effort de migration de SAP Business Suite vers S/4 Hana est similaire à celui pour passer de SAP Business Suite à un autre PGI (Microsoft, Oracle...), les cartes du marché seront forcément rebattues.
Rappelons que, selon l'enquête que nous avons menée parmi les utilisateurs SAP, 60% ne veulent pas migrer vers un progiciel concurrent parce que ce serait long et coûteux mais cependant parfaitement possible et envisageable. Ce n'est pas envisageable seulement pour 17% !

CIO : Ce sujet sera-t-il abordé dans les ateliers ou les plénières de la Convention ?

Claude Molly-Mitton : Pas directement mais des intervenants venus du siège de SAP viendront présenter en plénière la feuille de route des différents produits SAP.
De plus, nous disposons d'un groupe de travail sur S/4 Hana depuis Janvier qui sera bien sûr présent. En plus du travail opéré au sein de la Commission Base de Données, ce groupe de travail est, lui, dédié à l'offre en construction S/4 Hana (sur les plans technologiques et organisation). Il est rattaché à la Commission Gouvernance afin de marquer le caractère stratégique du sujet. Pour l'heure, ce groupe opère via un forum et sans réunion physique.
Pour leur part, nos ateliers resteront classiques pour la plupart, à base de témoignages d'entreprises au sujet de leurs projets.
Nous aurons cependant un atelier un peu particulier réalisé en partenariat avec l'INSA Lyon. Cette école d'ingénieurs sera bien sûr présente au Village des Ecoles dans l'espace d'exposition. Mais deux de ses étudiants viendront témoigner en atelier sur un stage réalisé dans un environnement SAP. Travailler sur un PGI est moins *sexy* et moins couru que développer des jeux vidéos ou faire un stage chez Google mais, pourtant, il y a nettement plus de travail, à la sortie de l'école, autour de SAP.
L'INSA Lyon viendra aussi présenter ses travaux de recherche sur l'alignement et l'agilité des SI et notamment des PGI.

CIO : Quels seront les autres sujets chauds abordés lors de la Convention ?

Claude Molly-Mitton : Outre une nouvelle note de perspective sur Hana, nous publierons une note de perspective sur les accès indirects à SAP, c'est à dire le fait d'utiliser une application tierce pour consulter ou interagir avec le coeur SAP. Cette application possède par définition un certain nombre d'utilisateurs n'ayant pas d'accès direct à SAP. Et ce sujet est un gros sujet de friction et de désaccord avec l'éditeur.
Nous l'aborderons d'ailleurs longuement lors d'une conférence de presse organisée durant la pause des ateliers le premier jour de la convention.

CIO : Comment sont aujourd'hui vos relations avec SAP ?

Claude Molly-Mitton : Apaisées ! Notre approche est désormais de bien séparer les sujets et de formaliser accords et désaccords. Cela évite de voir des points sans conflits pollués par des tensions venues d'autres sujets.
Par exemple, nous travaillons bien ensemble sur des sujets techniques. Il n'y a pas

alors de pertinence à parler d'accord ou de désaccord. Il est souvent nécessaire de clarifier, de donner une grille de lecture aux membres de l'USF. Le document en Français pour comprendre la politique tarifaire de l'éditeur en est un bon exemple et il porte les deux logos de SAP et de l'USF.... mais nous avons pris bien soin de ne pas y inclure le sujet des accès indirects, qui sera traité par ailleurs de façon bien moins consensuelle !

CIO : Mais il y a des sujets plus chauds…

Claude Molly-Mitton : Nous avons notamment des désaccords sur les accès indirects.
Et de nombreux audits de licences continuent de mal se passer d'après les retours issus de nos adhérents. Nous n'avons pas encore de travail formel pour améliorer les procédures d'audit de licences mais cela devrait venir très prochainement. On ne peut pas faire que râler. Il nous faut aussi proposer et conseiller des bonnes pratiques en amont à nos membres afin d'essayer de réduire le risque de problèmes. Il faudra aussi bien les conseiller quand il peuvent dire « non » à SAP face à certaines demandes injustifiées dans le cadre de ces audits...

CIO : Au delà, quels sont les sujets d'avenir pour l'USF ?

Claude Molly-Mitton : S/4 Hana bien sûr. Nous voulons répondre à de nombreuses questions. Pourquoi migrer ? Pour quels avantages ? Pour quelle création de valeur ? Pour quel coût ? Quelle est la lourdeur du projet ? Le sujet est vaste et hautement stratégique mais comme nous l'avons déjà indiqué le contour de l'offre S/4 HANA reste encore bien trop flou (licences, roadmap, effort de migration) pour prendre une position tranchée en l'état.
Et chaque commission a évidemment ses sujets métiers ou techniques propres.

En savoir plus

- La *Convention USF 2015* sur l'agenda CIO
- Le site de la *Convention USF 2015*

A propos de l'USF et de la Convention 2015
L'USF (Utilisateurs SAP Francophones) est animée par 65 responsables bénévoles et est auto-financée en totale indépendance de l'éditeur SAP. L'association réunit 3000 individus issus de 450 organisations membres, dont 73% du CAC 40, 62% du SBF 120 et une cinquantaine d'administrations.
Fondée le 28 septembre 1989, l'association est le deuxième plus vieux club d'utilisateurs SAP dans le monde, créé juste après le VNSG aux Pays-Bas et avant le club allemand. Elle comprend 67 commissions, groupes de travail et groupes régionaux à l'origine de plus de 120 réunions physiques par an. La participation à ces réunions physiques s'est accrue de 58% sur ces 4 dernières années et de 17% rien que sur le premier semestre 2015 ! Les groupes régionaux permettent à des ETI d'adhérer à l'USF sans avoir à envoyer des représentants à Paris pour bénéficier des réunions.
De plus, l'association publie de nombreux livres blancs et notes diverses (au moins un document de référence tous les deux mois). Ces documents apportent de la valeur aux adhérents n'ayant pas le temps de participer aux réunions physiques. Enfin, l'association est reliée aux autres clubs d'utilisateurs SAP dans le monde au travers du SUGEN (SAP User-Group Executive Network).
Evénement majeur annuel de l'association, la Convention s'appuie sur, cette année, 86 partenaires exposants (dont SAP) et comprend 70 ateliers de retours d'expérience clients et 7 conférences plénières. Plus de 1 700 visiteurs cumulés sont habituellement présents sur les 2 jours de l'événement. Une soirée festive permettra de célébrer dignement le quart de siècle de l'association.
L'édition 2015 se situant à Lyon, le nombre de participants devrait être particulièrement élevé. A noter la présence de l'ADIRA (Association pour le Développement de l'Informatique en Rhône-Alpes) qui sera représentée à la Convention de l'USF par son président Yves Bismuth. Par ailleurs, l'ADIRA est partenaire de l'IT Tour organisé par Le Monde Informatique.

La parole aux métiers

Catherine Chambon (SDLC-DCPJ) : « gardez sur Internet le même bon sens que dans la vie physique ! »

Catherine Chambon, commissaire divisionnaire et sous-directrice de la lutte contre la cybercriminalité à la Direction Centrale de la Police Judiciaire

La commissaire divisionnaire Catherine Chambon dirige la Sous-Direction de la Lutte Contre la Cybercriminalité (SDLC) à la Direction Centrale de la Police Judiciaire (DCPJ). Elle combat ici les idées reçues pour développer les réactions adéquates en entreprises face aux cybercriminels. Elle présente également les collaborations et les différences de compétences entre tous les organismes pouvant lutter contre les cybercriminels au cours de leurs missions.

***CIO :* Quelle est la position et le rôle de la Sous-Direction de la Lutte contre la Cybercriminalité (SDLC) que vous dirigez ?**

Catherine Chambon : La SDLC est l'une des sous-directions de la Direction Centrale de la Police Judiciaire (DCPJ). Une telle sous-direction s'occupe d'un grand type de criminalité (criminalité organisée, criminalité financière...) ou d'opérations transverses (maillage territorial, police technique et scientifique...).

La DCPJ est elle-même l'une des directions centrales de la Direction Générale de la Police Nationale (DGPN) aux côtés de la DCPAF (Police aux Frontières), de la DCSP (sécurité publique), etc. La DGPN est pour sa part directement rattachée au Ministre de l'Intérieur.

La SDLC est fondamentalement transverse car elle s'occupe de toute la criminalité qui s'appuie sur les Technologies de l'Information et de la Communication. Il peut donc s'agir de la criminalité contre les systèmes d'information ou les outils informatiques mais

aussi de la criminalité utilisant l'informatique comme outil pour commettre des crimes classiques. De ce fait, la SDLC a un rôle de soutien aux autres offices et sous-directions confrontés à des usages de l'informatique par les criminels qu'ils combattent.
Par exemple, nous créons des modèles pour le logiciel de recueil de plaintes en essayant de coller à l'actualité. Lorsqu'il y a eu une grande vague de défaçages de sites web par des islamistes, nous avons eu à gérer 1200 plaintes. Nous avions créé pour cela un modèle pour que les agents de terrain notent tout ce qui était nécessaire sans rien oublier. De plus, la structuration des données imposée par ces modèles facilite leur centralisation et la synthèse, y compris le cas échéant à l'international puisque les formes sont convenues à l'avance.

CIO : On entend beaucoup parler de la BEFTI (Brigade d'enquêtes sur les fraudes aux technologies de l'information) lorsque l'on parle cybercriminalité. Quelles sont vos relations avec elle ?

Catherine Chambon : La BEFTI est une brigade à compétence territoriale dépendant de la Préfecture de Police de Paris. Elle ne nous est donc pas rattachée car une sous-direction comme la nôtre a une compétence nationale. La BEFTI a comme objectif de résoudre des affaires dans la zone de compétence de la Préfecture de Police, c'est à dire Paris et la Petite Couronne, pour faire simple l'ancien département de la Seine. Cette zone géographique comprend de nombreux sièges sociaux de grandes entreprises souvent sujettes à des attaques. De plus, la BEFTI ne se préoccupe que des atteintes aux systèmes d'information, pas des autres crimes s'appuyant sur les TIC comme outils.

CIO : Comment fonctionnez-vous au quotidien entre cette organisation très pyramidale et les besoins de transversalité ?

Catherine Chambon : Notre organisation est en fait matricielle. Une sous-direction comme la SDLC a un rôle de pilote dans son domaine. Elle doit anticiper, effectuer un travail méthodologique, compiler les retours d'expériences et en tirer des leçons, etc. Nous donnons donc des moyens au terrain pour qu'il soit efficace. En retour, les services qui assurent le maillage territorial nous alimentent en constatations concrètes.

CIO : Travaillez-vous également avec l'ANSSI (Agence Nationale à la Sécurité des Systèmes d'Information) ?

Catherine Chambon : Bien entendu. L'ANSSI est un organisme qui dépend du Premier Ministre et qui est doté de compétences propres. Nous collaborons en ayant recours à leur expertise dans un cadre judiciaire ainsi qu'en nous formant du point de vue technique à leurs côtés. En retour, nous les alimentons en informations sur les pratiques techniques et les méthodes employées par les cyber-criminels. C'est donc un échange gagnant-gagnant entre deux organismes n'ayant pas du tout les mêmes tutelles.
Cela dit, nos compétences sont également très différentes. L'ANSSI s'occupe de cybersécurité, nous de cybercriminalité. La cybercriminalité est l'usage des moyens techniques informatiques pour commettre des crimes tandis que la cybersécurité est une préoccupation technique. Cybersécurité et cybercriminalité ont une zone de recoupement mais qui est loin de couvrir la totalité du périmètre de l'une ou de l'autre.
De plus, nous nous occupons de toute la cybercriminalité. Les victimes peuvent être aussi bien des particuliers, des petites entreprises... A l'inverse, l'ANSSI ne va s'intéresser qu'aux administrations et aux très grandes entreprises.

Cela dit, si nous découvrons un nouveau cheval de Troie, l'ANSSI sera évidemment intéressée.

CIO : Vous avez un passé de policier et une formation juridique. N'est-il pas gênant de ne pas être plus ou moins informaticien pour lutter contre la cybercriminalité ?

Catherine Chambon : Non, au contraire. Il est même important que le dirigeant de la SDLC ou de l'OCLCTIC [voir encadré], ait une expérience opérationnelle en police judiciaire pour que l'apport du service soit réellement utile, au delà de la seule technique.

CIO : De quelles ressources humaines disposez-vous à la SDLC ?

Catherine Chambon : Nous disposons d'équipes techniques (ingénieurs informatiques et télécoms par exemple) mais aussi d'équipes opérationnelles, pédagogiques, documentaires, aux relations internationales (Interpol...), etc. Un commissaire est d'ailleurs un ingénieur informatique qui s'est reconverti. Nous pouvons recourir à des ingénieurs internes mais aussi à des contractuels. Les profils au sein de la SDLC sont très divers.
Nos équipes techniques font de l'assistance quotidienne mais aussi de la veille et de l'anticipation. Elles aident les équipes pédagogiques pour créer des formations ou des kits pédagogiques à l'attention de tous les policiers, y compris ceux qui, sur le terrain, vont recueillir les plaintes des victimes. Un agent qui recueille une plainte doit en effet comprendre le contexte pour savoir collecter tous les éléments nécessaires et bien conseiller la victime. Selon l'échelon, l'action pédagogique sera différente, de la simple sensibilisation à la certification d'enquêteurs.

CIO : Quelle est la typologie de la cybercriminalité frappant les entreprises ?

Catherine Chambon : Toutes sont concernées par le phishing visant leurs clients ou leurs services internes. Il existe aussi, bien sûr, tous les types de malwares visant à prendre le contrôle du système d'information (en tout ou partie) ou bien à récupérer des données. Les vols de données sont également un type de cybercrime fréquent qui s'appuie sur les limites de la cybersécurité, tant au niveau technique qu'au niveau humain.
La cybercriminalité peut viser à l'espionnage comme à la déstabilisation voire, tout simplement, à l'extorsion de fonds (ransomwares...).

CIO : Y-a-t-il un profil type de cybercriminels ?

Catherine Chambon : Le cybercrime est pyramidal. Au sommet de la pyramide, vous trouvez des hackers de haut niveau qui développent des outils. En dessous, vous avez des personnes à la recherche de ces outils pour mener leurs entreprises criminelles (espionnage, extorsion, etc.). Et à la base de la pyramide, vous trouvez des exécutants techniques qui vont mettre les mains dans le cambouis et prendre les risques principaux.
Les équipes de cybercriminels recourent à des capacités d'ingénierie et s'organisent de façon très modulaire et flexible. Les spécialistes les plus pointus vont vendre des compétences mais éviter de s'impliquer personnellement dans l'opérationnel.
La cybercriminalité est un marché noir où on achète des outils, des compétences, de la force de travail, des moyens techniques... mais où l'on vend également des données.

Selon la qualité, la facilité d'usage et la performance des outils, leur prix va varier. Il y a donc des mouvements financiers entre les différents acteurs, avec des opérations de blanchiment comme on peut en trouver dans d'autres formes de criminalité organisée.
Comme vous voyez, nous sommes très loin de la cybersécurité.

CIO : Pour faire face à la cybercriminalité, avez-vous des bonnes pratiques à recommander ?

Catherine Chambon : Un premier conseil : gardez sur Internet le même bon sens que dans la vie physique quotidienne ! Par exemple, il ne faut pas exposer ses moyens de paiement, il faut réfléchir avant d'ouvrir un fichier reçu dans un spam, etc. Auriez-vous l'idée de donner votre clé d'appartement à n'importe qui, rencontré au coin de la rue parce qu'il se prétend plombier alors que vous n'avez pas de fuite ? De la même façon, il ne faut pas donner ses identifiants et mots de passe sans être absolument certain de l'identité des destinataires et de la légitimité de la demande.
Tout l'enjeu de la sensibilisation que nous menons est de faire en sorte que les gens retrouvent en ligne les réflexes de la vie courante. Les moteurs des imprudences des victimes peuvent bien sûr être l'appât du gain mais aussi l'altruisme, la volonté d'aider quelqu'un en difficulté.
Côté technique, je ne peux que recommander de suite les guides d'hygiène rédigés par l'ANSSI. Ils sont très clairs et compréhensibles par tout le monde.
Enfin, nous avons l'habitude de travailler en partenariat avec les entreprises et les organisations catégorielles pour faciliter les diagnostics et la rédaction de recommandations. Nous cherchons aussi à donner aux entreprises des outils de diagnostic et de prévention. Là où l'ANSSI va donner ces outils sur le plan technique, nous allons, nous, informer sur les problèmes comportementaux, les défauts de cuirasse exploités par les malfaiteurs.

CIO : Que doit faire une entreprise si elle se découvre victime ?

Catherine Chambon : Je vais renvoyer pour cela au guide *Réagir à une attaque informatique : dix préconisations* qui détaille les procédures pour éviter de détruire les preuves et porter plainte.
Il faut savoir qu'en ayant développé la plate-forme de signalement en ligne Pharos, nous avons grandement amélioré notre efficacité. Le nombre de signalements est en forte progression. En 2014, il y en a eu 137 000, à 56% en lien avec une escroquerie.
Cette plate-forme permet de recentraliser les signalements qui, auparavant, étaient dispersés sur tout le territoire, en fonction des domiciles des victimes. De ce fait, nous pouvons identifier les auteurs des crimes en évitant la dispersion des efforts dans des brigades territoriales.
Grâce au regroupement des plaintes des différentes victimes concernant les mêmes faits, nous sommes passés de 137 000 signalements à 6000 procédures. Les procédures en doublon ou inutiles sont donc évitées. Pharos devrait être la base du futur système de plainte en ligne pour tous les crimes et délits sur Internet. Pour l'heure, c'est juste une plate-forme de signalement avant le véritable dépôt de plainte.

En savoir plus

Avec une formation initiale juridique, Catherine Chambon est avant tout commissaire de police. Elle opère dans la Police Judiciaire depuis 1989 avec des postes spécialisés sur divers types de criminalité (infractions financières, criminalité organisée, fraude au moyens de paiement...). Elle a dirigé l'Office Central de Lutte Contre les Infractions aux Technologies de l'Information et de la Communication (OCLCTIC) de 2001 à 2006. Enfin, elle prend la responsabilité de la Sous-Direction de la Lutte Contre la Cybercriminalité (SDLC) en 2014. L'OCLCTIC est le service opérationnel de la SDLC. La SDLC comprend également des services de recherche, d'accompagnement pédagogique du grand public, etc.

Pour aller plus loin

- Réagir à une attaque informatique : dix préconisations : un livret PDF créé par la Direction Centrale de la Police Judiciaire (téléchargement libre, 5 Mo).
- Les guides d'hygiène rédigés par l'ANSSI
- Le portail de signalement Pharos

Bertrand Lemaire
Rédacteur en chef de CIO

Pour toute demande concernant CIO.focus :
contact-cio@it-news-info.com

Une publication de IT NEWS INFO : 40 bd Henri Sellier 92150 Suresnes
Rédacteur en chef : Bertrand Lemaire, blemaire@it-news-info.com
Tél. : 01 41 97 62 10
Principaux associés : Adthink Media et International Data Group Inc.
Président : Bertrand Gros
Directeur de publication : Bertrand Gros
Directeur général : Jean Royné
Président du groupe Adthink Media : Sylvain Morel

CIO est édité par IT NEWS INFO, SAS au capital de 3000000 €
Siret : 500034574 00029 RCS Nanterre