ERNST & YOUNG

envue 21

UNE INITIATIVE **D'ERNST & YOUNG** EN PARTENARIAT AVEC **L'ECHO** ET **DE TIJD** | 14 DÉCEMBRE 2012

Sécuriser les données d'entreprise

Des questions concernant ce sujet ? Vous voulez consulter ce dossier également en ligne?

www.echo.be/envue

Entreprises et organismes publics sont confrontés à une foule d'évolutions technologiques qui se succèdent à un rythme effréné. Celles-ci se traduisent par de nouveaux médias, de nouveaux appareils, de nouvelles applications et de nouvelles formes d'organisation informatique. Des phénomènes qui modifient en profondeur la manière d'entreprendre. Dans un tour de table avec trois spécialistes d'Ernst & Young, nous étudions les opportunités et risques découlant de ces nouvelles tendances. Dans ce dossier, nous aborderons également plusieurs sujets brûlants comme l'évolution du rôle du CIO, l'importance de la protection des données et les possibilités en matière de facturation électronique dans le cadre d'interviews avec de hauts responsables de Borealis, Coca-Cola et Mobistar. Enfin, nous discuterons d'une enquête relative à l'ampleur des médias sociaux et la sécurité de l'information. Une lecture obligatoire pour tous ceux qui veulent rester au fait des dernières évolutions dans l'univers de la technologie de l'information.

Préambule

Innover en toute sécurité

Le CIO d'aujourd'hui fait face à de nombreux défis. D'abord et avant tout, le contexte économique difficile oblige les organisations à se focaliser en premier lieu sur les opportunités d'économies, d'optimisation et d'innovation. En outre, nous sommes sans cesse sollicités par de nouvelles évolutions technologiques. Numérisation, smartphones, tablettes, médias sociaux, big data, cloud: toutes ces nouveautés exercent une influence significative sur notre manière d'entreprendre et de nous organiser.

Ces tendances – et d'autres – amènent des implications importantes pour l'avenir de votre entreprise. S'il veut formuler une réponse adéquate à ces défis, le CIO devra intégrer de manière proactive ces nouvelles technologies à des solutions pour son entreprise. Des solutions qui aident l'entreprise à atteindre ses objectifs. Ce n'est possible que s'il parvient à se débarrasser de son image de technicien - pour se révéler comme un communicateur hors pair. Un missionnaire des temps modernes ? Nous devons peu à peu évoluer de l'alignement traditionnel entre le business et l'IT vers un contexte de fusion dans lequel l'IT s'intègre naturellement dans toutes les branches de l'entreprise.

La protection des informations doit être la préoccupation de chaque membre de l'organisation.

Certaines entreprises sont tellement pressées de concrétiser ces nouvelles opportunités qu'elles perdent de vue l'aspect sécurité. Et cela avec toutes les conséquences néfastes que cela implique, comme le vol de données confidentielles et les problèmes d'image qui les accompagnent.

La protection de l'information n'est pas une question purement technique. Une gestion responsable de la technologie et de l'information relève de la culture d'entreprise. La direction doit bien entendu montrer le bon exemple, élaborer des directives claires. Le suivi de ces directives incombe à chaque collaborateur. Ceux qui se montrent négligents en seront pour leurs frais.

Rudi Braes, managing partner Ernst & Young

Colophone

Une initiative d'Ernst & Young

Andy Deprez, associé Ernst & Young Advisory
Bernard Ghigny, associé Ernst & Young Financial Services **Marc Joostens**, Ernst & Young Tax Consultants **Tim Wulgaert**, director Ernst & Young Advisory **Matthias Penninck**, senior manager Ernst & Young Tax Consultants
Maxime Raymond, manager Ernst & Young Advisory

Editeur responsable :
Bernard Ghigny, associé Ernst & Young Financial Service

Coordination Ernst & Young :
Anne-Sophie Jaspers

www.ey.com/be/envue
Suivez Ernst & Young sur twitter : EY_Belgium
Tél. : 02 774 91 11

Une réalisation de Mediafin Publishing

Coordination : Veronique Soetaert
Rédaction : Mediafin
Lay-out : David Steenhuyse
Photo : Emy Elleboog, Wim Kempenaers
Editeur : Dieter Haerens

Info ? publishing@mediafin.be

L'INFORMATIQUE EN MUTATION

De la technologie au business

Numérisation, facturation électronique, cloud computing, médias sociaux, appareils mobiles… les départements informatiques n'ont jamais été confrontés à une succession aussi rapide de changements, au point de négliger parfois des questions essentielles comme la protection de l'information et la conformité aux exigences légales. Pour relever ces nouveaux défis, il est dans l'intérêt du CIO de se défaire rapidement de son image de technicien, et se concentrer pleinement sur l'essentiel : le business. Trois spécialistes d'Ernst & Young y détaillent les raisons.

Le contexte dans lequel opèrent les départements informatiques a radicalement changé. Comment cela s'explique-t-il ?

Andy Deprez: Je distingue deux grandes tendances. Tout d'abord, les tâches informatiques classiques perdent en importance. Ce qui était auparavant le cœur de l'informatique relève aujourd'hui du produit de base que l'on peut aisément soustraiter. Les connaissances techniques pointues ne sont plus aussi pertinentes pour le CIO.

Deuxièmement, le contexte économique difficile que nous connaissons incite à privilégier l'optimisation, l'efficacité et l'innovation. Les innombrables évolutions techniques et informatiques peuvent y contribuer. Pensez aux nombreux nouveaux appareils, canaux et applications. Le business souhaite de plus en plus avoir la possibilité d'utiliser ces évolutions au profit des objectifs de l'entreprise. Le CIO est parfois pris de vitesse, et il néglige ainsi des aspects comme la protection de l'information et la conformité à la réglementation. Il est donc temps de redessiner fondamentalement le rôle du CIO.

Bernard Ghigny: Traditionnellement, le CIO était un technicien issu du département informatique. Ce département se profilait alors comme un fournisseur interne et exclusif de solutions informatiques pour l'entreprise, en appui au « cœur d'activité » de l'entreprise. Avec l'essor de nouvelles solutions externes à la fois attrayantes et compréhensibles pour les membres du business – qui ont ainsi nettement gagné en maturité dans le domaine de l'informatique –, le CIO subit une pression croissante de ses utilisateurs. Le business est ainsi tenté d'implémenter ces solutions alternatives « peu coûteuses et flexibles » directement avec des fournisseurs externes. C'en était ainsi fini de l'exclusivité des départements informatiques. Ces derniers ont ainsi dû subir une importante transformation pour redevenir concurrentiels et trouver de nouvelles solutions qui répondent plus adéquatement aux besoins en évolution constante des utilisateurs.

À quoi ressemble le nouveau CIO ?

Deprez: Le nouveau CIO doit réfléchir à partir des nouveaux besoins de ses clients – qu'ils soient internes

Andy Deprez, Bernard Ghigny et Marc Joostens. ©Emy Elleboog

ou externes. Ces clients ont énormément gagné en maturité et sont généralement bien informés. Ils ne demandent plus un savoir-faire informatique : ils veulent des solutions qui contribuent à l'optimisation, à l'efficacité, à l'innovation. Le CIO doit travailler de manière proactive et « emballer » les innovations technologiques dans des solutions qui donnent du sens à l'entreprise. De plus, il doit apprendre à communiquer par rapport à ces solutions avec ses collègues managers, à partir de business-cases solides. Le nouveau CIO a une fonction de missionnaire, dans le cadre de laquelle il peut se reposer sur son équipe pour les connaissances techniques et les tâches opérationnelles quotidiennes.

Marc Joostens: Ces nouvelles tâches requièrent un nouveau profil. Idéalement, le CIO contemporain doit être issu des ventes ou de la finance. Une personne qui « sent » le business pourra communiquer de manière plus efficace avec ses collègues d'autres départements. Mais cela reste de la théorie – dans la pratique, il en va souvent autrement.

Le CIO d'aujourd'hui doit être capable de traduire l'innovation en solutions qui donnent du sens au business.

Andy Deprez, associé Ernst & Young Advisory

Tendances

En tant que consultants, vous êtes proches de ce qui se passe sur le terrain. Quelles sont les questions que vous posent vos clients ?

Deprez: La facturation électronique est l'un des nouveaux services qui suscite un vif intérêt. Nos clients sont généralement assez bien informés des possibilités techniques. Leurs questions portent surtout sur l'aspect coût et le gain d'efficacité. En combien de temps un tel investissement est-il rentabilisé ? Combien d'équivalents temps pleins pouvons-nous économiser ? Ces questions sont révélatrices de la maturité du marché.

Joostens: Le succès de la facturation électronique dépend totalement de son adoption par les clients et fournisseurs. Les points sensibles concernent la protection des données et la conformité avec la législa- >

tion, surtout au regard de la fiscalité et de la TVA.

Ghigny: Il est important que les autorités ne restent pas à la traîne dans ce domaine. En matière de facturation électronique, le législateur avait imposé l'utilisation de certaines technologies. Heureusement, on constate aujourd'hui un retour en arrière : l'idée que des lois doivent être neutres d'un point de vue technologique pénètre peu à peu les esprits. L'administration doit fixer des règles de base, comme l'obligation d'authenticité, d'intégrité et de confidentialité des données. Toutefois, il reste préférable de laisser le choix final de la technologie aux entreprises.

Joostens: Une autre tendance voit les autorités fiscales recourir de plus en plus aux audits électroniques. Elles étudient alors la conformité à la loi des différents systèmes et processus. Nos clients veulent s'y préparer à temps.

La protection des informations est-elle également un sujet brûlant ?

Deprez: Nous avons été récemment approchés par une entreprise de production industrielle qui développait une innovation critique. Celle-ci voulait éviter toute fuite d'informations relatives à cette innovation. Les questions pertinentes à se poser seraient alors : comment allons-nous gérer ces informations ? Comment pouvons-nous les protéger ? Nous recevons également des questions de l'industrie pharmaceutique relatives à la protection des informations sensibles, où l'innovation des produits est fondamentale.

Joostens: Nous recevons également de nombreuses


©Emy Elleboog

La sécurité de l'information dépend entièrement du maillon le plus faible.

Bernard Ghigny, associé Ernst & Young Financial Services

sollicitations de ce type de la part du secteur des télécommunications. Les opérateurs ne cessent de déployer de nouvelles technologies réseaux et de nouvelles applications. La protection des données sensibles des clients constitue dans ce cadre une préoccupation fondamentale. Dans ce secteur, la pression est souvent telle que cet aspect est parfois négligé. Récemment, des informations clients confidentielles d'un opérateur ont été publiées. Un tel incident occasionne des dommages irréparables à la réputation de l'entreprise. Nous allons alors adopter un regard proactif en se posant les questions suivantes : qu'est-ce qui est bien protégé ? Qu'est-il possible d'améliorer ? Quelles sont les données sensibles ?

Ghigny: Dans le secteur financier, les banques cherchent à nouveau à réduire les coûts en remplaçant leur réseau d'agences par des canaux électroniques, même si ces nouveaux canaux génèrent d'importants défis en terme de sécurité et de conformité.

Les entreprises gèrent-elles le cloud de manière adulte ?

Ghigny: Elles ont de plus en plus conscience de l'importance du cloud. Les possibilités sont généralement connues. Les questions sont plutôt du type : qu'allons-nous conserver en interne ? Qu'allons-nous sous-traiter ? Qu'allons-nous envoyer dans le cloud? De nombreuses questions portent sur la sécurité. Des entreprises internationales qui offrent des services en ligne accordent une grande importance à cet aspect. Elles font dès lors très souvent appel aux services de parties indépendantes pour contrôler périodiquement la qualité de leur système de sécurité : en effet, pour ces entreprises, la réputation est fondamentale !

Deprez: Des questions concernant la sécurité de l'information se posent également dans le cadre de l'utilisation des smartphones, des tablettes et des médias sociaux. Ces appareils amènent de nombreux défis pour l'entreprise, confrontée à de réels dangers au niveau de la protection des données.

Joostens: Les managers sont souvent placés devant le fait accompli. Chacun des collaborateurs veut son propre appareil, surtout parmi la jeune génération. Lorsque de nouveaux collaborateurs arrivent dans

Six conseils pour protéger vos informations confidentielles

La gestion des informations confidentielles n'est pas une sinécure. Cependant, les six conseils suivants vous seront sans doute très utiles.


© Shutterstock

1. La technologie n'est qu'un élément de la protection des informations

Une protection technologique solide s'avère bien entendu être un prérequis. Cependant, les pare-feux et autres antivirus ne suffisent pas pour garantir la confidentialité de vos données. La sécurité ne relève pas uniquement de la responsabilité du département informatique.

2. La protection de l'information est la responsabilité de tous

Les problèmes de protection des informations sont souvent imputables à une défaillance humaine. Des mécanismes de contrôle sont utiles, mais certainement pas suffisants. La culture d'entreprise est de loin le facteur le plus important. Veillez donc à ce que la sécurité soit ancrée dans votre culture.

3. Le maillon faible détermine le niveau de protection

Un seul maillon faible, un seul collaborateur inattentif suffit pour mettre en péril toute la sécurité des informations de votre entreprise. Identifiez ces points faibles et apportez-y des solutions lorsque que c'est possible.

4. Faites appel à un conseiller externe

En matière de sécurité, il arrive assez souvent que des détails apparemment sans importance soient négligés. Pour être certain de disposer d'une protection optimale et de respecter les normes principales, il est préférable de faire appel à des conseillers externes. Un audit de sécurité d'une entreprise spécialisée vous permettra de dormir sur vos deux oreilles.

5. Tenez compte du client

Si vous voulez protéger les informations de clients, prenez en compte leurs préférences ; quelles sont les informations les plus confidentielles à leurs yeux ? Par quels canaux veulent-ils être approchés ? Où se situent leurs sensibilités en matière de sécurité ?

6. N'oubliez pas le cadre légal

Dans les projets liés à la protection des informations, le législateur n'est souvent pas pris en compte. Ainsi, par exemple, si vous envisagez de remplacer des contrats papier par des contrats numériques, veillez à respecter scrupuleusement le cadre législatif.


©Emy Elleboog

La conformité à la législation est un aspect souvent négligé dans l'implémentation de nouveaux projets informatiques.

Marc Joostens
associé Ernst & Young Tax Consultants

une entreprise, ils ne demandent même plus s'ils sont autorisés à utiliser tel ou tel appareil. Leur première question est souvent : « Comment puis-je connecter cet appareil au réseau de l'entreprise ? » Nous devons accompagner cette évolution, veiller à ce qu'elle puisse s'accomplir de manière totalement sécurisée. Il en va de même pour l'utilisation des médias sociaux qui se développe de manière de plus en plus évidente.

Nouvelle réalité

Comment le CIO peut-il gérer cette prolifération d'appareils et de canaux de communication ?

Deprez: Il est en tout cas impossible de s'opposer à la tendance prônant pour chacun de choisir son propre appareil. Nous recommandons surtout d'informer les collaborateurs sur une utilisation responsable et de les informer sur les risques. Il est plus intéressant de se focaliser sur la recherche d'attitudes positives que de rechercher la protection en imposant des interdits, qui seront de toute manière contournés. Ainsi, vous pourriez promouvoir l'utilisation de mots de passe performants, ou expliquer que laisser traîner son smartphone ou son ordinateur portable représente un risque réel. Il est dans l'intérêt de chacun d' adopter une attitude responsable.

Ghigny: Cette attitude est également payante lorsqu'il s'agit de gérer les médias Facebook, Twitter et autres LinkedIn. Jusqu'à récemment, les entreprises étaient très réticentes à l'égard des médias sociaux. Notre conseil ? Ne vous laissez pas effrayer par les risques, mais donnez des directives qui indiquent clairement ce qui est possible et ce qui est interdit avec les nouveaux médias. Chez Ernst & Young, nous avons par exemple réalisé un screening de tous les profils LinkedIn de nos collaborateurs. Conclusion : il était possible de faire mieux. Nous avons donc créé un modèle qui permet à nos collaborateurs de rationaliser et d'optimiser leur profil LinkedIn. Ils en ont été très satisfaits.

Joostens: En matière de protection des informations, il faut une politique axée sur les points essentiels. La réalité actuelle est complexe, et les flux d'informations ne sont jamais totalement étanches. Il est essentiel d'identifier ce qui doit être protégé, et dans quelle mesure.

Qui porte la responsabilité de protection de l'information ?

Deprez: Chaque collaborateur de l'entreprise. Le CIO doit bien entendu créer une architecture optimale et assurer la sécurité des systèmes. Mais les pare-feux et les antivirus ne suffisent pas. La sécurité est une question technique à 30% et une question d'organisation, de processus et de mentalité à 70%. La culture de l'entreprise est cruciale dans la qualité de la protection de l'information. Chacun doit s'en sentir responsable.

Quatre étapes vers une protection efficace de vos informations

La Global Information Security Survey 2012, une enquête à grande échelle menée par Ernst & Young (lire en page 11), révèle que la plupart des organisations doivent d'urgence réformer leur sécurité informatique. Les réflexions à court terme et les solutions prêtes à l'emploi ne suffisent plus. Les organisations qui veulent sérieusement combler leurs lacunes peuvent suivre les quatre étapes suivantes :

1. Reliez la **stratégie** de protection de l'information à la stratégie générale de l'entreprise, et associez les objectifs de protection de l'information aux objectifs d'affaires généraux. C'est la seule manière d'obtenir une approche intégrée.

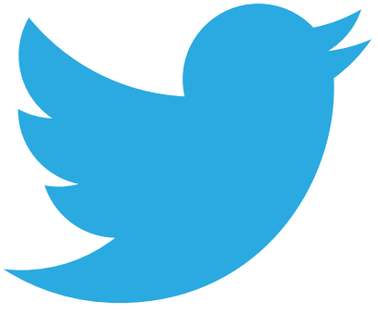
2. Vous envisagez d'implémenter une nouvelle **architecture** et d'acquérir de nouvelles **technologies** ? Il est alors préférable de bien redéfinir vos besoins en terme de sécurité des informations. Vous serez ainsi mieux à même d'identifier le travail à réaliser. Ce sera l'occasion d'éliminer certains obstacles et de dissiper d'éventuels préjugés susceptibles de contrecarrer ce changement fondamental.


© Shutterstock

3. Réalisez le **changement** en créant un environnement qui permet à l'organisation de réformer sa sécurité informatique de manière efficace et durable. Ceci s'avère être l'unique manière d'obtenir une solution à l'épreuve du futur.

4. Avant de procéder à l'implémentation d'une nouvelle technologie, étudiez en profondeur les **opportunités** et **risques** qu'elle implique. Les médias sociaux, les grands volumes de données, le cloud et les applications mobiles ne sont pas des phénomènes de mode. Veillez à ce que votre organisation s'y adapte à temps.

Stay updated by following us on Twitter



twitter.com/EY_Belgium

Ernst & Young goes social

EY_Belgium - our official corporate twitter account
EY_lifeBelgium - what it is like to work at Ernst & Young

MÉDIAS SOCIAUX

De nombreuses opportunités, mais aussi des risques

Le nombre d'internautes et d'utilisateurs de médias sociaux ne cesse de croître, et il est presque désormais impossible d'imaginer la vie d'une entreprise sans ces outils. Mais hormis les nombreuses possibilités et défis qu'ils apportent, ils sont également porteurs de risques. Les entreprises qui apprennent à les gérer efficacement posséderont une longueur d'avance sur la concurrence.


© RV

Plus de 170 millions de personnes visitent leur compte Facebook tout les jours, contre 40 millions pour Twitter et 22 millions pour LinkedIn. Le cap des 3 milliards d'internautes devrait être atteint d'ici 2016. En d'autres termes, l'existence des médias sociaux va encore persister. Une récente enquête menée par Ernst & Young indique que 67% des personnes interrogées reconnaissent que les médias sociaux influencent comportement d'achat. Cette tendance va d'avantage s'accentuer avec l'essor des smartphones et tablettes ou encore l'intégration croissante de médias sociaux dans la télévision et les autres médias. Les médias sociaux offrent des possibilités prometteuses en matière de marketing, d'études de marché et d'interaction en temps réel avec les clients. Ils constituent également des outils très efficaces pour les entreprises. Des applications comme Chatter en Yammer sont utilisées dans un nombre croissant d'organisations comme vecteur de collaboration et de communication entre les salariés, voire avec des partenaires externes. Ils ajoutent une dimension supplémentaire à la communication et aux canaux de collaboration comme l'e-mail, le chat et les logiciels collaboratifs. Dans ce domaine aussi, des risques existent en matière de contrôle et de protection de l'information.

Cadre

Une gestion inadéquate des médias sociaux peut parfois avoir de graves conséquences pour la réputation d'une organisation ou de ses marques. Expressions de mécontentements et plaintes, justifiées ou non, peuvent prendre des formes virales. Les comptes des entreprises sur les médias sociaux peuvent faire l'objet d'abus, d'attaques ou de piratage. Les employés peuvent passer trop de temps sur les médias sociaux privés pendant les heures de travail ou les utiliser comme outil de harcèlement. Pour maîtriser les risques, une politique ou gouvernance claire est indispensable.

Il est impératif alors de distinguer les différentes raisons pour lesquelles les médias sociaux sont utilisés : communication, marketing, recrutement, collaboration interne entre employés. Il ne faut pas oublier que vos propres collaborateurs utilisent les médias sociaux à des fin privées, leurs comptes privés pouvant souvent avoir un lien avec l'organisation.

Pour maintenir une séparation nette entre les différentes approches d'aborder le problème et les types de responsabilités qu'elles incombent, il est préférable d'élaborer un cadre de travail où chaque canal possède son propre responsable. Les risques pourront alors être identifiés séparément pour chaque utilisation.

© Shutterstock

Gouvernance

Les organisations qui se sont jetées sur les médias sociaux trop rapidement ou sans stratégie réfléchie ont été confrontées à plusieurs types de risques, ayant dans le pire des cas un impact sur leurs parts de marché ou leur réputation.

Une politique efficace en matière de médias sociaux exige d'abord une évaluation initiale, suivie d'une stratégie intégrée, de directives, d'une campagne de sensibilisation auprès des utilisateurs et enfin d'un monitoring permanent.

Les organisations qui disposent d'une stratégie intégrée et d'une gouvernance structurée concernant les médias sociaux ont prouvé qu'elles sont beaucoup mieux à même de maîtriser le caractère volatil et parfois risqué de ces outils. Certaines d'entre elles parviennent même à en tirer d'énormes profits.

Une gestion inadéquate des médias sociaux peut parfois avoir de graves conséquences.

Tim Wulgaert, director Ernst & Young Advisory

FACTURATION ÉLECTRONIQUE CHEZ BOREALIS

La fin de la facture papier

Le producteur de plastique Borealis propose la facturation électronique depuis juin de l'année passée. Aujourd'hui, plus de la moitié des fournisseurs ont adopté cette solution. Eddie Van den Eede, responsable européen pour la comptabilité fournisseurs, nous explique le succès de son projet.

Comment se déroule votre processus de facturation papier ?
Eddie Van den Eede: Comme dans la plupart des entreprises de taille significative, il s'agit d'un système bien huilé. D'abord nos fournisseurs nous envoient une facture papier par courrier. Celle-ci est scannée manuellement. Ensuite le logiciel intègre un système de reconnaissance optique de caractères. Il lit les informations pertinentes et les enregistre dans notre système ERP. Enfin ces données sont traitées par la comptabilité. Nous archivons ensuite les documents sous forme électronique pendant sept ans, comme la loi le prescrit.

Quelle était votre principale motivation lorsque vous avez adopté l'alternative électronique ?
Van den Eede: Réaliser des économies. La facture papier coûte facilement trois euros au fournisseur. Pour le client, ce prix peut atteindre quatre euros. Je vois les choses de la manière suivante : l'envoi et le traitement de documents papier engendre une multitude de tâches. Chez le fournisseur, la facture doit être imprimée, mise sous enveloppe, timbrée et envoyée à la poste. Le client trie son courrier, ouvre les enveloppes et scanne les documents manuellement. Le résultat ? Une image électronique de la facture qui n'est plus lisible de manière optimale.

Le principal défi reste l'accompagnement de nos fournisseurs.
Eddie Van den Eede, Accounting Services manager Borealis

Supprimer l'ensemble du détour papier vous permet non seulement de réaliser des économies importantes, mais aussi d'enregistrer des gains d'efficacité et de qualité.

Implémentation

Comment s'est déroulée la mise en œuvre du projet ?
Van den Eede: L'implémentation technique est assez simple. Deux jours de travail ont suffit à un programmeur pour faire en sorte que le système ERP accepte également des factures en format PDF. Le fournisseur peut alors les envoyer très aisément par e-mail sur un serveur fixe.
Les défis se situent ailleurs. Tout d'abord, nous devions nous assurer que notre solution était conforme aux attentes du législateur. C'est pourquoi nous avons d'abord déployé le projet en Suède, en Finlande, en Belgique et en Allemagne. Ces pays autorisent déjà l'envoi de factures par e-mail. De plus, Borealis y dispose de sites importants, avec un volume de factures considérable.
Dans d'autres pays, la législation n'est pas du tout au point. L'Autriche constitue ainsi un environnement difficile, parce que le législateur y exige que les factures électroniques soient certifiées. Cependant,

NUMÉRISATION, FACTURATION ÉLECTRONIQUE ET ARCHIVES ÉLECTRONIQUES

Votre entreprise exploite-t-elle totalement le potentiel disp

Aujourd'hui, de nombreuses entreprises ont déjà numérisé une partie de leur processus de facturation ou sont en train d'étudier des projets dans ce sens. Celles-ci sont souvent motivées par l'envie d'accroître l'efficacité du processus de facturation au sein de l'organisation. Et vous, êtes-vous prêt pour faire face à ce changement ?

Dans sa stratégie pour 2020, la Commission Européenne impose que la facturation électronique doit devenir le principal mode de facturation. Pourtant, son taux de pénétration dans notre pays est encore limité : à peine 35% des entreprises envoient ou reçoivent au moins une partie de leurs factures sous forme électronique. Pourquoi sont-elles si peu nombreuses ? Complexité technique, risque en matière de sécurité et incertitudes juridiques sont les principaux facteurs invoqués.
La pratique démontre pourtant qu'une approche multidisciplinaire bien étayée permet de développer un business case solide. Les questions de technologie et de sécurité ne posent aucun problème insurmontable, qu'elles soient résolues en interne ou sous-traitées à un service de e-facturation. Le cadre juridique représente également un point délicat. La facture est un moyen formel d'exercer son droit à la récupération de la TVA. Sur ce sujet, beaucoup de chemin a été parcouru pour tenter d'éliminer les incertitudes. De plus, des règles plus souples entreront en


© RV

A partir de 2013 les factures PDF sont autorisés en Europe.
Mattias Penninck, senior manager Ernst & Young Tax Consultants

© Wim Kempenaers

il est difficile d'obliger les fournisseurs à envoyer des factures certifiées, d'autant que cela représente un coût supplémentaire. Heureusement, la donne va changer : le 1er janvier 2013, les factures PDF simplement envoyées par e-mail seront juridiquement valables sur tout le territoire de l'Union européenne. De plus, nous faisons toujours appel à Ernst & Young pour auditer chaque solution que nous implémentons. Nous avons ainsi la garantie de la validité juridique de notre concept.

Quel a été le principal défi ?

Van den Eede: Sans aucun doute celui de convaincre les fournisseurs. Dans les quatre pays où nous avons lancé le projet, nous avons approché environ 1400 fournisseurs, que nous avons invités, comme la loi l'exige, à signer un contrat tout simple. A ce jour, 720 d'entre eux l'ont fait. 130 autres travaillent à une solution. 350 fournisseurs ont refusé et 200 n'ont pas encore réagi. Nous obtenons ainsi un volume d'environ 26 à 27% de factures électroniques. Notre objectif est d'arriver à 50 ou 60%.

Comment expliquez-vous que le système soit adopté aussi lentement ?

Van den Eede: Si vous additionnez les avantages, le passage à la facturation électronique devrait se dérouler très rapidement. Mais manifestement, l'idée n'a pas encore pénétré le marché. Je dois chaque fois réexpliquer qu'une facture électronique est autorisée par la loi. De nombreuses entreprises ne sont manifestement pas conscientes des nouvelles grandes tendances qui se dessinent dans le paysage informatique. Je trouve cela un constat alarmant. Généralement, les grands fournisseurs sont au courant, mais ils préfèrent rester à l'écart. En fait, notre demande de facturation électronique leur impose de faire une exception à un processus papier bien huilé, qui est souvent sous-traité de surcroît. Pourtant, cela ne leur coûterait pas beaucoup de temps ni d'argent. Au contraire, ils feraient des économies. Mais leurs priorités sont manifestement ailleurs. Il est également significatif que nous soyons nous-mêmes très peu contactés par des fournisseurs désireux d'adopter la facturation électronique. Sur nos 1400 fournisseurs, à peine trois nous ont demandé de leur propre initiative s'ils pouvaient nous envoyer leurs factures sous forme électronique. Cela prouve que le taux d'acceptation sur le marché reste très bas. Je me considère dès lors plutôt comme un accompagnateur de nos fournisseurs dans un nouveau monde numérique.

ponible ?

vigueur dans toute l'Union européenne au 1er janvier 2013. Si vous voulez instaurer un système de facturation électronique qui satisfait à toutes les règles en matière de TVA, la technologie, la sécurité et les processus opérationnels doivent être parfaitement imbriqués. À partir de 2013, un État membre ne pourra en effet plus exiger qu'une entreprise utilise une technologie donnée pour envoyer ou recevoir des factures sous forme électronique. Ainsi, il sera possible de n'utiliser par exemple que des formats PDF déjà autorisé en Belgique. A condition toutefois que l'intégrité du contenu, l'authenticité de l'origine et la lisibilité des factures dans les archives soient garanties. Tout contrôle opérationnel constituant une « trace d'audit » entre un acte et sa facturation pourra alors être utilisé pour fournir ces garanties. L'entreprise elle-même devra confirmer que ces processus peuvent offrir de telles garanties au fisc. Pour le démontrer, vous devrez valider vos processus et systèmes de facturation et d'archivage en fonction des critères précités. Ceci se fera de préférence durant des ateliers et sur la base d'une documentation suffisante.

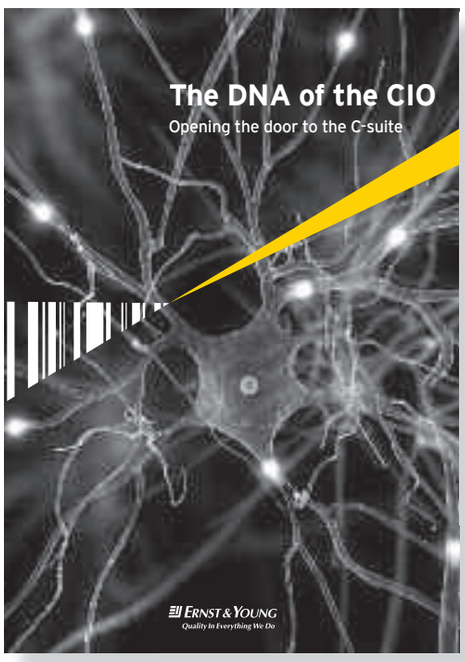

© Shutterstock

ERNST & YOUNG
Quality In Everything We Do

Thought Leaderships

Ernst & Young publie chaque année différentes études. En partageant notre connaissance et notre expertise nous espérons pouvoir vous aider à atteindre vos buts professionnels.

Vous pouvez télécharger les études sous-mentionnées et un tas d'autres via **www.ey.com/be**



GLOBAL INFORMATION SECURITY SURVEY 2012

Hausse des incidents à prévoir

C'est une piqûre de rappel à ne pas négliger : 45% des entreprises belges s'attendent à une augmentation du nombre d'incidents de sécurité. C'est ce que révèle le rapport « Global Information Security Survey 2012 » d'Ernst & Young.

Cela fait 15 ans qu'Ernst & Young suit de près les grandes évolutions mondiales en matière de sécurité informatique. Plus de 1850 managers de 64 pays, tous impliqués dans la sécurité informatique, ont contribué à la dernière édition du Global Information Security Survey (GISS). Nous vous énumérons ci-cessous les cinq constats les plus marquants pour notre pays :

1.

À peine un participant à l'enquête sur dix estime que son dispositif actuel de sécurité informatique répond aux besoins de l'organisation. « Le CIO est de plus en plus souvent pris de vitesse », constate Maxime Raymond, senior manager chez Ernst & Young spécialisé en IT Risk. « Les défis se succèdent à un rythme effréné : nouveaux marchés, volatilité économique, sous-traitance, interventions publiques, durcissement de la réglementation... Tout ceci rend la sécurité informatique plus complexe que jamais. »

2.

62% des participants belges – 15% de plus que la moyenne mondiale – signalent une hausse de la vulnérabilité interne. Un facteur très important dans ce domaine est la combinaison de nouvelles technologies et de collaborateurs négligents, ignorants, voire parfois animés d'une intention de nuire.

3.

La moitié des organisations belges interrogées ont recours au cloud computing, l'utilisation de matériel, programmes ou données externes par Internet. Cependant, à peine une entreprise sur quatre a pris des mesures pour réduire les risques, comme l'utilisation des techniques de codage spéciales ou une surveillance plus stricte des fournisseurs de solutions cloud.

4.

Les collaborateurs d'un tiers des entreprises interrogées utilisent des smartphones et tablettes pour consulter des informations de l'entreprise en ligne. L'utilisation de tels appareils privés dans le cadre professionnel génère d'énormes flux d'informations difficiles à contrôler entre l'organisation et le monde extérieur.

« Une gestion responsable de ces appareils, notamment par un dispositif de codage, peut être une solution », explique Raymond.

5.

Avec une hausse de 5% du budget consacré à la sécurité informatique, la plupart des entrepreneurs belges semblent décidés à opérer un mouvement de rattrapage au cours des années à venir. Principales priorités ? La formation, la sensibilisation et la sécurisation des nouvelles technologies.

Rien ne permet cependant d'affirmer que ces efforts suffiront pour relever les immenses défis qui se présentent. Au lieu de procéder au bouleversement total qui est pourtant nécessaire, de nombreuses entreprises se contentent trop souvent de modifications sur le vif ou de solutions à court terme. Cela provient notamment du fait que les responsabilités ne sont pas toujours confiées aux personnes adéquates.

« La création d'une organisation efficace, dans laquelle la responsabilité de la protection de l'information et des technologies relève des couches les plus élevées de l'entreprise, peut apporter une solution », explique Raymond. « Cela peut permettre d'enregistrer des résultats qui tiennent compte de l'équilibre entre les défis liés aux évolutions précitées et les limitations imposées à l'entreprise. Il s'agit en effet de mettre en place un dispositif d'évaluation et de contrôle des risques clair et univoque dans toutes les branches de l'organisation. Les points faibles apparaîtront beaucoup plus rapidement sur le radar, et les outils informatiques pourront être utilisés de manière plus efficace en combinaison avec d'autres procédures et méthodes. »

De plus amples informations ?

Vous pouvez consulter l'étude sur www.ey.com/GISS. Vous y trouverez également une série de recommandations concrètes destinées à renforcer la sécurité informatique de votre entreprise.

Vous avez encore des questions ou des observations ? N'hésitez pas à prendre contact avec

Maxime Raymond, Senior manager
Ernst & Young Financial Services
par e-mail :
maxime.raymond@be.ey.com
ou par téléphone au
+32 (0)2 774 60 23.

UNE BONNE POLITIQUE DE PROTECTION DES DONNÉES PERSONNELLES NE SE CONTENTE PAS DE SUIVRE LA LOI

Une politique de protection de la vie privée donne aux clients et aux collaborateurs ce dont ils ont besoin

Pour l'opérateur de télécommunications Mobistar, la protection légale de la masse de données personnelles qu'il traite représente une énorme quantité de travail. Mais l'entreprise est également à l'écoute des attentes de ses clients et édicte précisément ce que peut faire chaque collaborateur – et ce qui lui interdit. C'est la seule manière de créer une politique de protection des données personnelles digne de ce nom.

Pour l'opérateur de télécommunications Mobistar, la protection des données personnelles n'est pas une mince affaire. Depuis les récentes embauches dans les services à la clientèle et les points de vente, l'entreprise compte 1.800 collaborateurs. Avec ses 4,5 millions de clients qui représentent un chiffre d'affaires de 1,5 milliard d'euros, elle est amenée à traiter une énorme quantité de données personnelles. « Le grand nombre de clients "post paid" implique notamment le traitement de nombreuses informations personnelles dans les processus de facturation », explique Paul-Marie Dessart, secrétaire général chez Mobistar.


Paul-Marie Dessart, secrétaire général Mobistar. © RV

Des clients sensibles

« Mais la protection des données personnelles ne concerne pas que le flux d'informations sur les clients ; elle touche également les collaborateurs. Auparavant, cette matière n'avait jamais fait l'objet d'une approche globale, et nous ne contrôlions pas la cohérence de toutes les règles. Nous n'identifions pas non plus les nouvelles évolutions susceptibles d'avoir un impact sur la protection des données personnelles. Mais l'essor du trafic de données mobiles nous a obligés à prévenir ou dissiper les inquiétudes concernant les données personnelles. Même si leur numéro de téléphone fixe se trouvait déjà dans l'annuaire téléphonique, les clients ont une toute autre perception de leurs numéros mobiles. Or le législateur loge toutes les données personnelles à la même enseigne, qu'il s'agisse d'un numéro fixe ou mobile, d'une adresse ou du contenu d'un message texte. Nous devons donc aller plus loin que la législation pour prendre en compte les sensibilités des clients », explique encore Paul-Marie Dessart.

Mobistar a analysé la meilleure manière de gérer les questions de respect de la vie privée. « Nous avons fait un bilan de ce que veut le client. Dans le cadre d'ateliers, nos collaborateurs ont pu apprendre à connaître leurs habitudes. Ernst & Young nous a aidés avec un accompagnement et en nous briefant sur les meilleures pratiques en provenance d'autres pays. Lorsque l'on met sur pied un projet aussi large, on s'attaque fondamentalement à trois aspects : la gouvernance, les principes et la gestion des risques. La gouvernance exige que les responsabilités soient définies avec précisions pour tous les rôles dans l'entreprise et que l'on communique clairement à ce propos. Chacun doit avoir conscience de l'importance du respect de la vie privée, que l'on travaille au call-center, à la facturation ou dans l'entrepôt. Tous entrent en contact avec des données personnelles. »

Connaître les risques

La communication a été conçue de manière attrayante et pouvait être vue partout dans les bureaux de Mobistar. « Il fallait vraiment faire comprendre aux collaborateurs qu'ils devaient faire preuve de prudence et de discrétion par rapport aux données traitées chaque jour. Nous répétons d'ailleurs ce type de communication régulièrement, car les collaborateurs vont et viennent », poursuit Paul-Marie Dessart. Un deuxième axe de sa politique de protection de la vie privée portait sur les procédures et principes. « Faire en sorte que les procédures - par exemple de gestion des incidents - et les alarmes soient effi-

UNE POLITIQUE NÉGLIGENTE DE PROTECTION DES DONNÉES PERSONNELLES ACCROÎT LES RISQUES DE SANCTIONS SÉVÈRES

La loi belge n'est guère contraignante, mais l'Europe se montrera beaucoup plus stricte

Actuellement, la législation belge sur la protection des données personnelles est encore peu contraignante. Ce sont surtout les risques liés à leur réputation qui incitent les entreprises à adopter une politique en la matière. Mais un règlement européen beaucoup plus strict va bientôt entrer en vigueur. Et prévenir coûtera alors beaucoup moins cher que guérir.

« La base légale de la protection de la sphère personnelle réside dans une loi du 8 décembre 1992 relative à la protection de la vie privée. Cette législation dans sa forme actuelle est notamment basée sur la directive européenne du 24 octobre 1995. Sa transposition dans le droit belge s'avère beaucoup moins sévère que chez nos voisins, surtout en matière de justiciabilité. Les amendes sont particulièrement basses, et son application n'est presque jamais contrôlée de manière active. Les organisations doivent surtout veiller à ce que l'absence d'une politique de protection de la vie privée ne nuise pas à leur réputation. La loi fixe bien quelques principes, notamment sur la manière dont les données personnelles doivent être traitées. Leur traitement n'est possible que s'il est fait de manière loyale et licite, mais aussi s'il est lié à un objectif donné. Une organisation peut collecter suffisamment de données, mais pas plus que nécessaire pour l'objectif spécifique qu'elle vise. Et le principe de transparence exige que l'on informe la personne concernée sur l'utilisation de ces données », explique An Meheus, avocate chez Holland Van Gijzen. « Le règlement européen qui va bientôt entrer en vigueur aura cependant un effet direct sur tous les Etats membres. La Belgique ne pourra pas en donner d'interprétation propre, plus souple. En principe, la proposition de règlement du 25 janvier 2012 prendra effet d'ici deux ans. Et elle impose des normes beaucoup plus sévères. Ainsi les entreprises de plus de 250 collaborateurs seront-elles tenues de désigner un « Data Privacy Officer ». Les autorisations relatives à l'utilisation de données, qui sont encore très implicites aujourd'hui, deviendront beaucoup plus explicites. Les nouvelles règles auront également une plus grande force exécutoire. Toute fuite de données personnelles devra si possible être signalée à la commission de protection de la vie privée dans les 24 heures. Les contrevenants seront également passibles d'amendes qui pourront atteindre 450.000 euros par infraction, voire 2% du chiffre d'affaires annuel dans certains cas. La commission de protection de la vie privée pourra intervenir de manière beaucoup plus active et on s'attend à ce qu'elle en profite pour effectuer des contrôles à l'improviste dans les entreprises, par exemple », poursuit An Meheus.

Prendre les choses en mains

L'avocat conseille aux dirigeants d'entreprises d'appliquer d'ores et déjà une politique stricte de protection de la vie privée et de bien documenter le traitement des données personnelles en établissant des politiques adéquates (documents stratégiques). Il est également crucial de sensibiliser chaque membre de l'entreprise. « N'allez pas trop loin dans l'attribution d'autorisations d'accès aux données personnelles, et ne les maintenez pas pendant une durée inutile. Veillez également à la transparence en informant clairement les personnes de ce qu'il advient de leurs données sur les sites et les documents d'achats. Pour les collaborateurs, vous le ferez par le biais du contrat de travail. N'oubliez pas que chacun a le droit de contrôler et de corriger ses données personnelles. Les données personnelles sont dispersées dans toute l'entreprise et il est difficile d'en obtenir une vue globale. Pourtant, c'est essentiel. Des modifications importantes vont intervenir et elles auront un impact non négligeable sur les entreprises. Cela vaut d'ailleurs également pour les organisations publiques ou les ASBL ; y compris pour les hôpitaux, confrontés à des données personnelles sensibles qui font l'objet de règles encore plus strictes. »

Adoptez d'ores et déjà une politique active de protection de la vie privée : sensibiliser le personnel est important.

An Meheus, avocate Holland Van Gijzen

© RV

caces. Une personne non autorisée qui tente effectivement d'accéder à certaines données déclenche à la fois une alarme et un blocage, ainsi qu'un processus d'identification. Pour ce système, nous utilisons le meilleur logiciel disponible. »

Indépendamment du respect de la vie privée, la gestion des risques revêt une grande importance chez Mobistar. « L'analyse des menaces relatives à la confidentialité des données permet d'identifier systématiquement la vulnérabilité et le meilleur mode de prévention. Nous devons réitérer en permanence les analyses, car de nouveaux risques apparaissent régulièrement. Nous devons continuer à tester l'infrastructure de protection, les processus, etc., afin que la sécurité des données reste garantie. Mais avant cela, il est nécessaire de recommencer systématiquement à analyser ce que les clients attendent de notre part. Le client doit avoir confiance, bénéficier d'une grande transparence, conserver le contrôle et ressentir l'intérêt de tout ce processus. La loi prévoit de nombreuses dispositions sur l'accès du client à ses données, mais il doit également pouvoir obtenir des informations lisibles et compréhensibles, et dans un délai suffisamment court. »

Lorsque vous mettez sur pied un projet, vous vous attaquez à trois aspects : la gouvernance, les principes et la gestion des risques.

Paul-Marie Dessart, Secretary General Mobistar

Service clientèle

« Notre stratégie est centrée sur l'utilisateur final. Tout ce qui concerne le client mérite le meilleur service. Cela couvre certains aspects évidents, mais aussi le traitement de ces données personnelles. Dans notre branche, ce n'est d'ailleurs pas un hasard si Mobistar est le seul opérateur à disposer d'un département Fidélité des clients qui contribue à créer le 'happy customer'. Dans ce domaine aussi, le respect de la vie privée est l'un des processus susceptibles de faire la différence. Nous devons pouvoir rassurer les gens chaque fois qu'une faille de sécurité est évoquée dans les médias. »

Une politique de protection de la vie privée de qualité ne peut se contenter d'appliquer la législation. « La loi prescrit qu'un opérateur comme Mobistar doive séparer les "données privées" dans la chaîne d'information et les maintenir à la disposition de la personne concernée. Mais il faut surtout que l'ensemble du processus de production fonctionne de manière optimale au sein de l'entreprise, afin que vous puissiez également répondre aux attentes du client. Simultanément, les collaborateurs ne peuvent avoir accès qu'à ce dont ils ont besoin pour remplir leurs tâches. Nous pouvons immédiatement identifier ceux qui recherchent des informations qui ne les concernent pas, et c'est un excellent moyen de dissuasion. C'est pourquoi nous avons des lignes de politiques précises pour tous les profils de collaborateurs. »


©Emy Elleboog

L'ADN DU CIO

Le pont entre l'IT et le business

« Ces trois à six dernières années, nous avons vu apparaître d'énormes opportunités pour le CIO désireux d'innover et de participer à la réflexion stratégique. Pourtant, son rôle reste souvent en retrait dans les comités de direction », explique Andy Deprez, associé chez Ernst & Young Advisory. Dans l'étude « The DNA of the CIO », Ernst & Young décrypte le gouffre qui sépare les fonctions informatiques et le reste du business.

Le titre de CIO n'est apparu qu'il y a une quinzaine d'années, alors que les notions de CEO et de CFO sont courantes depuis 40 ans. Jusqu'à la fin des années 90, le CIO s'appelait simplement directeur informatique ou chef du service technique, et travaillait quelques étages sous le comité de direction, au propre comme au figuré. C'était un autre temps : l'e-mail était une nouveauté, l'Internet semblait être une mode passagère, l'informatique relevait avant tout du traitement de données. « Depuis lors, l'informatique a abandonné son rôle d'enabler, de facilitateur, pour devenir un driver, un moteur de l'entreprise », constate Deprez. « D'un instrument destiné à accroître l'efficacité, c'est devenu une manière de différencier une organisation de la concurrence. La crise qui s'est déclenchée il y a quatre ans a encore donné une nouvelle dimension au rôle potentiel du CIO. »

Communication

Les chercheurs d'Ernst & Young ont étudié ce qu'il advenait de ce rôle potentiel sur le terrain. Dans le cadre de l'étude « The DNA of the CIO », ils se sont entretenus avec plus de 350 managers de grandes organisations dans le monde entier. Constat irrémédiable : 87% des CIO sont convaincus qu'ils peuvent apporter une valeur ajoutée importante à leur entreprise. Ils sont très motivés à l'idée de rectifier la perception dépassée des autres membres du management, qui voient toujours l'informatique comme une fonction de support. Mais ils n'y parviennent pas toujours.

Le CIO qui ne veut pas devenir superflu doit veiller à ce que le « I » de son titre soit celui d'innovation.

Andy Deprez, associé Ernst & Young Advisory

Vous pouvez télécharger l'étude « The DNA of the CIO » sur www.ey.com/be. Vous avez des questions ou des idées concernant votre rôle de CIO? Prenez contact avec Andy Deprez d'Ernst & Young Advisory: andy.deprez@be.ey.com ou au +32 (0)2 774 62 47.

« Les CIO ont un background technique solide », explique Andy Deprez. « Mais il leur manque souvent des facultés de communication. De ce fait, ils ne parviennent pas toujours, dans les comités de direction, à convaincre de l'importance que peut avoir l'informatique pour l'organisation. Pour le CFO, il en va tout autrement. Il est significatif de constater que seuls 2 à 3% des candidats CEO sont d'anciens CIO, alors qu'ils sont 40 à 50% à être d'anciens CFO. Dès lors, on parle automatiquement un langage financier dans les salles de direction, ce qui convient moins au CIO. »

Croisement

Deprez plaide pour une pollinisation croisée : « Il faut qu'un plus grand nombre de personnes du business deviennent CIO. Ceux-ci penseront en fonction des besoins de l'entreprise et piloteront ainsi l'informatique. Prenez par exemple un manager de vente qui constate sur le terrain ce qu'il pourrait faire avec un iPad. S'il devient CIO, il développera des projets très proches du business. À l'inverse, il serait utile qu'un candidat CIO accumule d'abord de l'expérience dans le business. »

Cette pollinisation croisée implique également que le CIO quitte sa zone de confort. « Acheter et gérer des serveurs n'est plus une activité clé de l'entreprise depuis longtemps », affirme Deprez. « Tout cela peut être sous-traité. Le CIO qui ne veut pas être mis sur la touche doit faire en sorte que le "I" de son titre représente l'innovation. Il doit identifier les nouvelles tendances et technologies, et les canaliser en fonction des besoins qu'il observe dans le business. »

« De nombreux jeunes disposent déjà des appareils mobiles les plus performants dans leur cadre privé. Est-ce le rôle de l'organisation de les en équiper ? Peut-on les laisser utiliser ces appareils dans le cadre professionnel ? Si oui, comment le faire de manière efficace et sûre ? C'est au CIO de donner des réponses définitives à ce type de questions et de les traduire pour le comité de direction. Cela exige de la vision, du talent de communicateur et des compétences en coordination. Mais le CIO qui y parvient deviendra automatiquement une voix stratégique au sein du management. »

LE CIO DE L'ANNÉE TRAVAILLE CHEZ COCA-COLA

Placez l'accent sur le business

La CIO de l'année ne met guère de temps à justifier son titre. Car Sabine Everaet sait parfaitement comment elle s'est forgée une position solide dans son organisation. *It's the business, stupid.*

Le profil de Sabine Everaet ne se lit pas comme le plan de carrière d'une informaticienne. « Après mes études d'ingénieur commercial, j'ai travaillé dans la consultance. C'était l'époque où SAP s'est imposé et j'ai ainsi atterri dans l'informatique, mais côté business. » C'est en 1995 que Sabine Everaet est entrée chez Coca-Cola. D'abord comme Business Analyst, avant de devenir Business Partner. C'est à ce titre qu'elle a notamment mis sur pied la structure de gouvernance européenne avec l'équipe informatique. Depuis début 2009, elle est CIO pour Coca-Cola Europe.

Vert le front-office

« Ma principale contribution est d'avoir transféré les priorités business du back-office – ressources humaines, finances et infrastructures – vers le front-office, plus précisément le marketing et la communication d'entreprise. » Il ne s'agit donc pas d'une mission purement informatique, mais d'un projet business complet. Comment a-t-elle procédé ? « J'ai analysé les compétences de l'équipe et j'ai attiré de nouvelles personnes qui disposaient du savoir-faire nécessaire. Elles provenaient souvent d'agences de marketing. Ce n'étaient donc pas de purs informaticiens, ce qui nous permet d'être très performants dans le marketing et la communication. J'ai également collaboré étroitement avec le directeur marketing européen. »

Dans l'organisation européenne, le marketing louait systématiquement des plateformes mobiles à des agences marketing locales, ce qui augmentait considérablement les coûts. « Cela faisait un certain temps que les sites Web et l'hébergement central étaient coordonnés à l'échelle européenne. Mais aujourd'hui, nous disposons également d'une plateforme mobile européenne. Nous avons également transformé le call-center en Espagne en un Citizen Interaction Center, qui suit de manière beaucoup plus active les débats sur nos produits qui ont lieu sur les médias sociaux, et qui s'y engage avec des contributions informatives. » Pour soutenir tout cela, nous avons mis sur pied une structure de projet hybride, qui a brisé les barrières traditionnelles entre les fonctions.

Il faut conquérir une position solide en travaillant chaque jour avec le business.

Sabine Everaet, CIO Coca-Cola Europe

Au comité de direction

Pour Sabine Everaet, il est évidemment crucial de se tenir informée des technologies émergentes. « Mais lorsque vous analysez ce qui se cache derrière des termes à la mode comme les médias sociaux, la communication mobile, le cloud et le big data, vous devez le faire dans la perspective de leur impact possible sur le business. Le CIO qui le fait gagnera beaucoup en crédibilité. Au début, je participais pendant quelques heures au comité de direction européen pour y présenter un projet. Aujourd'hui, j'en suis devenu un membre formel. Il faut conquérir une position solide en travaillant chaque jour avec le business. Auparavant, je ne voyais le directeur marketing que durant les réunions. Aujourd'hui, nous discutons à peu près tous les jours. »

Elle ne propose pas de profil déterminé pour le job de CIO. « Le rôle dépend énormément du profil de l'organisation et de ses caractéristiques. Les CIO sont donc très différents, mais l'essentiel est de sentir et comprendre l'importance qu'ils devraient avoir pour l'entreprise. Il faut s'adapter aux activités et veiller à faire la différence. Faire preuve d'une grande flexibilité pour accompagner l'évolution des priorités et apporter une valeur ajoutée dans leur réalisation. »

Ce n'est certainement pas aisé, explique-t-elle, car le CIO doit également entretenir un bagage technique solide. « En outre, vous devez disposer de réseaux suffisamment larges. Pas question de se cantonner à sa spécialité : il faut oser sortir des sentiers battus. Ne restez pas dans votre cercle relationnel. Il faut suivre certaines tendances sociales. Parfois, je rencontre des gens que j'aimerais bien avoir dans mon équipe. Ce sont des gens qui réfléchissent de manière holistique, qui nouent des liens. C'est plus important que d'être très spécialisé dans une technologie donnée. »

Pensez-vous comme eux?

L'étude "L'ADN du CFO" d'Ernst & Young regroupe les avis et les aspirations de presque 1.000 CFO du monde entier. Découvrez non seulement ce qu'ils pensent de leur rôle et de leurs collaborateurs, mais également quelles sont leurs perspectives d'avenir.

ey.com/cfo

twitter.com/EY_Belgium

ERNST & YOUNG

Quality In Everything We Do