Ce dossier est publié par Mediaplanet et n'est pas sous la responsabilité des éditeurs de Trends-Tendances

SEPTEMBRE 2017 **WWW.INFOSENTREPRENDRE.BE**

MEDIA PLANET

Risk & Compliance

Jo Willaert (FERMA) : « Les entreprises doivent réfléchir autrement. »

© COVERPHOTO : PRIVÉ

DANS CETTE ÉDITION

INTRODUCTION

Etes-vous prêt pour la prochaine crise ?

Dans le contexte actuel, la gestion de crise est une composante de plus en plus importante du management d'entreprise. Aucune organisation n'est à l'abri d'une crise dans notre société. Explications par Pieter Timmermans, administrateur délégué de la FEB.

Les crises peuvent frapper les entreprises sous diverses formes : attaques terroristes, accidents industriels, incendies, accidents du travail très graves, agression ou occupation, rappel d'un produit, catastrophe naturelle. En cas de crise, l'image et la fierté de l'entreprise sont inévitablement en jeu, de même que ses valeurs et parfois sa continuité. C'est pourquoi je voudrais insister sur ce qui me semble le plus important : soyez prêt !

Le management quotidien

Vous vous demandez peut-être : mon entreprise a besoin a t'elle d'une gestion de crise élaborée dans les moindres détails ? La réponse est oui! La gestion des risques doit donc occuper une place centrale dans les processus stratégiques généraux de l'entreprise. Elle aide en effet à identifier ce qui menace l'entreprise et à y remédier. Elle vise à gérer les dangers de telle manière qu'ils deviennent acceptables, afin d'offrir une sécurité raisonnable par rapport à la réalisation des objectifs de l'organisation. Une bonne gestion des risques augmente les chances de réussite des autres objectifs de l'entreprise. C'est donc à plus d'un titre qu'elle doit faire partie du management quotidien.

Pieter Timmermans
Administrateur délégué de la FEB

Une bonne gestion des risques augmente les chances de réussite des autres objectifs de l'entreprise.

Identifier les menaces

Il va de soi qu'à mesure que l'on identifie les menaces et risques qui pèsent sur son entreprise, ce processus a déjà un certain effet préventif. La prise de conscience des risques en permet la gestion consciente. La réflexion sur les menaces potentielles est évidemment l'occasion d'introduire une certaine attitude de sécurité et plus encore une culture de sécurité. La personne consciente de son rôle et de sa contribution dans la prévention et la gestion des risques appliquera les consignes de sécurité de manière plus consciencieuse, hésitera moins à signaler des risques ou incidents et prendra plus vite ses responsabilités en cas de nécessité. Je parle ici à la culture générale de l'entreprise : des valeurs comme l'ouverture d'esprit, la transparence, la communication et la confiance mutuelle favorisent la détection rapide des points faibles et évitent que l'on étouffe de petits incidents ou des erreurs humaines qui peuvent ensuite aboutir à une crise aux proportions gigantesques.

Les secteurs stratégique

Certes, une crise aura un impact plus important dans certains secteurs ou installations que dans d'autres. Certaines entreprises ont une telle importance stratégique que leur défaillance peut paralyser l'ensemble de la société. Parmi les secteurs stratégiques, citons l'approvisionnement énergétique (centrales nucléaires, raffineries de pétrole), les télécommunications (téléphonie, internet, stockage de données) ou les transports (ports maritimes, aéroports). Cette 'infrastructure critique' a indéniablement l'obligation et la responsabilité sociétale de prévoir les menaces, de détecter les problèmes le plus tôt possible, d'aborder le mieux possible une éventuelle crise et rétablir au plus vite le service.

De la crise à la leçon

Je voudrais terminer par un credo qui, je pense, doit également être répété: une crise peut aussi être une opportunité. C'en est même la traduction littérale en chinois : la notion de crise est constituée des idéogrammes signifiant 'menace' et 'chance' ou 'danger' et 'opportunité'. On considère qu'il existe une cohérence entre ces oppositions apparentes et qu'une crise n'est donc pas qu'une menace. L'expérience nous apprend que c'est effectivement le cas.

RISK & COMPLIANCE SEPTEMBRE 2017 ▪ **Managing Director:** Leoni Smedts ▪ **Head of Production:** Daan De Becker ▪ **Business Developer:** Nicolas Mascia ▪ **Project Manager:** Jérôme Hulin - Tel: +32 2 421 18 34 - E-mail: jerome.hulin@mediaplanet.com ▪ **Rédaction:** Philippe Van Lil, Frédéric Vandecasserie, Joris Hendrickx ▪ **Lay-out:** i GRAPHIC - E-mail: info@i-graphic.be ▪ **Print:** Roularta ▪ **Distribution:** Trends-Tendances ▪ **Mediaplanet contact information:** Tel: +32 2 421 18 20 - E-mail: info.be@mediaplanet.com ▪ D/2017/12.996/48

Paiements sécurisés : comment éviter les fraudes ?

Nicolas Ancot, general manager de BCC Corporate After-Market

General manager de BCC Corporate After-Market, Nicolas Ancot supervise les activités de sa société dans les domaines de la gestion du risque, des finances, de l'informatique et de la conformité aux normes légales et sectorielles. Il est donc bien placé pour parler de la sécurité des transactions.

Quelles sont vos activités ?

Nicolas Ancot : « BCC Corporate est le leader belge pour l'émission de cartes Visa et Mastercard aux entreprises. Nous sommes également actifs dans de nombreux pays européens. Début mai, notre entreprise a été rachetée par AirPlus, une société du groupe Lufthansa. Nous émettons des cartes de crédit classiques, assorties de différents grades d'assurances associées, par exemple des assurances-voyage, pour couvrir le rapatriement d'un employé en cas d'accident à l'étranger, ou des assurances-vie, s'il faut déplorer un incident très sérieux. Les autres types de cartes sont la TravelKey, pour les réservations de voyages et d'hôtels, et la carte ePay, dédiée aux transactions sur internet. »

Quels sont les grands types de fraudes aux paiements aujourd'hui ?

N. A. : « On en distingue quatre : la fraude interne commise par des membres du personnel ; les attaques sur les systèmes informatiques, par exemple de gros commerçants, par des hackers qui récupèrent des numéros de cartes dans leurs bases de données pour les réutiliser frauduleusement ; les fraudes liées au blanchiment d'argent et au financement du terrorisme ; les fraudes transactionnelles, où l'on récupère les données de la carte d'un utilisateur honnête pour les employer à mauvais escient. »

Comment lutter contre ces malversations ?

N. A. : « Pour la fraude interne, les entreprises peuvent définir de manière flexible les limites d'utilisation des cartes au niveau des individus, des départements ou de l'entreprise dans son entièreté. Il est aussi possible de bloquer l'utilisation d'une carte pour retirer du cash à un distributeur ou pour faire des achats au supermarché, et de la limiter au paiement des restaurants, hôtels et voyages. L'entreprise peut choisir sa façon de gérer le risque et la modifier de manière régulière. »

Et face aux attaques ?

N. A. : « Ici, il faut des procédures informatiques très strictes, qui combinent l'infrastructure, les firewalls, etc., avec des instructions précises pour le personnel. Par exemple, nous n'envoyons jamais un numéro de carte par e-mail sans l'encrypter. Nous sommes en outre certifiés PCI-DSS. Il s'agit d'une norme internationale relative à notre secteur et à celui de l'e-commerce ; il réglemente les processus et la structure informatique de la sauvegarde, du stockage et de la communication des données. Même les terminaux de paiement et les distributeurs de billets sont certifiés : l'insertion du code PIN entre le clavier et le système qui lit et interprète ce code doit toujours être encryptée par exemple. Nous avons également l'obligation de former et de sensibiliser notre personnel. »

Aujourd'hui, on distingue quatre grands types de fraudes aux paiements.

Et pour les autres types de fraudes ?

N. A. : « Tout nouveau client potentiel suit un processus très rigoureux : on vérifie une série de facteurs comme la résidence, le fichage et la solvabilité. On examine également des listes internationales liées au terrorisme et au blanchiment d'argent. Par la suite, un monitoring permanent permet de bloquer les transactions douteuses éventuelles et de les signaler à la Cellule de traitement des informations financières. Face aux fraudes transactionnelles, les technologies ont beaucoup évolué ces dernières années grâce aux cartes à puce. L'authentification et les transactions de celles-ci sont monitorées en permanence en background grâce à des logiciels qui évaluent la probabilité d'une transaction frauduleuse en temps réel. En fonction du risque évalué, la transaction sera autorisée ou non. »

Quelles sont les évolutions légales récentes pour renforcer la sécurité ?

N. A. : « Ces dernières années, il y a une très forte accélération. Hormis le PCI-DSS, les normes sont toutes européennes. L'Europe est même très en avance sur les autres continents. Il y a deux ans, une norme sur les «interchanges» est apparue. Initialement, il s'agissait de limiter le niveau de commissionnement des commerçants, mais elle a aussi introduit des règles de sécurité. Par ailleurs, la deuxième version du «Payment Services Directive» est en cours de transposition dans la loi belge. Ce texte régit les normes de concurrence entre les banques et des institutions comme la nôtre. Il prévoit aussi des renforcements pour la sécurité, notamment l'authentification forte des clients. Autre réglementation très importante : la General Data Protection Regulation, qui concerne donc la protection des données privées. Elle entrera en application l'an prochain. Enfin, il y a la directive contre le blanchiment d'argent, l'Anti-Money Laundering, dont la cinquième version est en préparation. »

BCC CORPORATE
An AirPlus Company

WWW.BCC-CORPORATE.BE

Philippe Van Lil
redaction.be@mediaplanet.com

Marijke Bruyninckx

Directeur de Prévention et Intérim

Les agences d'intérim ont également leur part de responsabilité : elles doivent aussi s'assurer que l'intérimaire travaille dans de bonnes conditions.

Sécurité et bien-être des intérimaires : peut mieux faire !

Chaque année, en Belgique, plus d'un demi-million de personnes œuvrent comme travailleurs intérimaires auprès d'un employeur. Marijke Bruyninckx, directeur de Prévention et Intérim, relève que leur sécurité et leur bien-être au travail ne sont pas toujours optimaux.

Comment les agences d'intérim agissent-elles en matière de sécurité et de bien-être ?

Marijke Bruyninckx : « Tout d'abord, elles sont reconnues légalement afin de mettre des travailleurs intérimaires à la disposition des employeurs. Ensuite, chaque mise au travail se fait selon une procédure très stricte visant, tout comme pour les travailleurs permanents, à les protéger contre des abus éventuels d'employeurs véreux ou contre des situations potentiellement dangereuses dans leur travail. »

Dans ce cadre-là, quelle est votre mission ?

M. B. : « Depuis notre création il y a 20 ans, elle est de lutter contre les accidents de travail et les maladies professionnelles des intérimaires. Nous agissons via deux volets : d'une part, la sensibilisation des employeurs et des intérimaires ; d'autre part, l'appui aux agences d'intérim. »

Avec quel effet ?

M. B. : « Depuis lors, les conditions de travail des intérimaires se sont considérablement améliorées. Le signal le plus fort est la baisse de plus de 60 % du nombre d'accidents de travail en 20 ans. Toutefois, le secteur de l'intérim fait encore face, chaque année, à des accidents graves et mortels. C'est pourquoi, fin 2016, nous avons lancé une campagne visant à écarter les employeurs qui représentent un danger potentiel important pour les intérimaires. La législation sur le bien-être au travail est d'ailleurs très claire à ce sujet : elle exige un engagement ferme de la part des agences d'intérim à enquêter à propos des antécédents des employeurs désireux d'engager des travailleurs intérimaires. La loi protège aussi ces derniers contre les maladies professionnelles dans le cadre de l'exécution de leur travail. »

À quels types de risques les intérimaires sont-ils couramment exposés ?

M. B. : « Comme les autres travailleurs, ils font face à de nombreux problèmes potentiels. En voici quelques exemples. Dans le secteur de la pétrochimie, ils sont en contact avec des agents chimiques tels que le mercure, le benzène et des vapeurs nocives. Dans les soins de santé, les infirmières travaillent dans un environnement avec des rayons X ou des infections telles que l'hépatite. Dans l'agriculture, les intérimaires doivent tenir compte du tétanos, de la maladie de Lyme, etc. Dans les usines, conduire un chariot de manutention où des poids importants sont soulevés représente par exemple un risque potentiel. Toutes ces fonctions requièrent la plus grande vigilance et la meilleure protection possible. »

Comment cela se traduit-il ?

M. B. : « Le législateur exige expressément que l'employeur fournisse à l'agence d'intérim les informations nécessaires quant au poste de travail. Depuis 1997, il existe une fiche par poste de travail, sur laquelle l'employeur indique tous les risques associés au poste ainsi que les mesures de protection à prendre. Ceci constitue le premier pas vers une sécurité optimale de l'intérimaire. Toutefois, force est de constater qu'après 20 ans, beaucoup de fiches de poste de travail s'avèrent incomplètes. Trop d'employeurs sous-estiment encore l'importance de l'analyse des risques d'un poste de travail. Le manque de connaissance sur ces risques est encore plus criant dans les PME. Les entreprises auraient tout à gagner à renforcer leur coopération avec des services externes de prévention. Les agences d'intérim ont également leur part de responsabilité : elles doivent aussi s'assurer que l'intérimaire travaille dans de bonnes conditions. »

De quels outils disposez-vous pour faciliter ces conditions de travail ?

M. B. : « Le législateur a chargé notre institution de créer une base de données centralisée. Celle-ci enregistre tous les résultats relatifs à la santé des travailleurs intérimaires. Elle permet d'éviter des répétitions inutiles d'examens médicaux pour des postes de travail similaires possédant les mêmes risques pour la santé. En pratique, après la sélection d'un intérimaire pour un poste, la base de données vérifie s'il est apte médicalement. Dans l'affirmative, il peut commencer à travailler immédiatement chez l'employeur. Pour le secteur intérimaire, cela représente un gain de temps et de coûts très significatif. »

Cette base de données présente-t-elle d'autres avantages ?

M. B. : « Oui, elle fait ressortir notamment quelques tendances. Ainsi, le type de risque le plus fréquent est lié à la manutention des charges (17,51 %), suivi par le bruit (9,76 %) et le travail à un poste de sécurité (9,06 %). Le travail posté, le tétanos et le travail de nuit suivent avec 6 %. Ces tendances permettent d'envisager des solutions pour diminuer les risques : la formation aux techniques de manipulation des charges, l'achat de matériel ergonomique, la réévaluation de l'efficacité des tâches... plutôt que, tout simplement, le fait de se tourner vers un médecin du travail ! »

Prévention et Intérim

WWW.P-I.BE

Philippe Van Lil
redaction.be@mediaplanet.com

« Beaucoup d'entreprises s'attaquent trop tard à l'absentéisme »

La problématique de l'absentéisme dans les entreprises n'est pas nouvelle. Force est toutefois de constater que beaucoup d'organisations n'ont pas d'approche décisive face aux absences. Et ce, alors que les coûts de l'absentéisme peuvent représenter jusqu'à 2,6 % du total des coûts salariaux pour une entreprise belge. « Lutter de manière ciblée contre l'absentéisme est pourtant à la portée de chaque organisation », affirme Gretel Schrijvers, médecin du travail et directrice générale de Mensura.

Aucun employeur n'y échappe : le nombre de travailleurs absents augmente chaque année. Ces derniers temps, ce sont surtout les chiffres spectaculaires de l'absentéisme de longue durée qui ont fait la une des journaux. Ils ont augmenté de 70 % en 10 ans selon l'Institut National d'Assurance Maladie-Invalidité (INAMI). Fin 2016, on dénombrait pas moins de 392.000 travailleurs absents un an ou plus pour cause de maladie. Soit 5 % des Belges de 20 à 64 ans et un coût annuel pour la société de 5 milliards d'indemnités. Vient s'ajouter à cela le fait que l'absentéisme de courte durée ne cesse, lui aussi, d'augmenter.

Impact financier

L'absentéisme perturbe les organisations et met la planification et la production sous pression. Il oblige les collègues à effectuer le travail des absents ou les employeurs à chercher des remplaçants. En plus de difficultés d'ordre pratique, il entraîne un impact financier. Les employeurs doivent supporter des coûts directs considérables, comme le salaire garanti, les assurances et l'ONSS. Les coûts indirects (notamment les remplacements, les heures supplémentaires et les pertes de production et de qualité) doivent aussi être pris en compte. Ensemble, l'absentéisme de longue durée et celui de courte durée représentent en moyenne 2,6 % du total des coûts salariaux d'une entreprise belge.

Éviter l'absentéisme grâce à la prévention

Prendre des mesures préventives ou dissuasives permet aux employeurs d'avoir un impact positif sur l'absentéisme. Gretel Schrijvers: « Pour prévenir au maximum l'absentéisme évitable, les organisations doivent s'attaquer à ses causes. Elles peuvent à cette fin faire appel à un service externe qui utilisera de façon ciblée leur budget de prévention légal pour améliorer le bien-être physique et mental des travailleurs, et optimiser les conditions de travail. Les entreprises sont généralement conscientes de la nécessité de lutter contre l'absentéisme. Mais souvent, elles ne réagissent que lorsque le problème est devenu urgent. Ou elles interviennent de manière trop fragmentée pour obtenir un résultat durable. »

Selon Gretel Schrijvers, bien comprendre l'absentéisme est capital pour une approche ciblée. « Où le bât blesse-t-il exactement ? Grâce à toutes les données disponibles, les entreprises doivent avoir une vue claire de leur problématique spécifique. Un audit de leur absentéisme et leur politique existante leur apporteront également une aide précieuse et constitueront à leur tour la base d'un plan d'approche. »

De la compréhension à l'action

Un plan d'approche efficace passe d'abord par une politique d'absentéisme aboutie. « Chaque organisation désireuse de s'attaquer sérieusement à l'absentéisme doit d'abord élaborer une vision, une mission et un protocole. Ceux-ci seront à la base de toutes les actions à entreprendre. Il ne s'agit donc pas de documents qui partiront directement aux archives : l'entreprise communiquera régulièrement à leur sujet. Avec les supérieurs hiérarchiques et tous les collaborateurs. Qu'elle le veuille ou non, une organisation qui n'évoque jamais l'absentéisme ouvre la porte au problème. En d'autres termes, le pas à franchir pour rester chez soi dans certaines situations est de plus en plus petit. » Il convient également de ne rien laisser au hasard sur le plan juridique.

Les analyses et procédures risquent d'être inutiles si elles ne sont pas concrètement traduites dans la pratique quotidienne. « Sans sensibilisation, pas de changement des comportements », poursuit Gretel Schrijvers. « La formation et l'encadrement sont des composantes essentielles de chaque approche de l'absentéisme. Si, par exemple, les responsables hiérarchiques n'ont pas appris à mener des entretiens d'absentéisme, votre entreprise se tire une balle dans le pied. »

Le nombre de travailleurs absents augmente chaque année. Ces derniers temps, ce sont surtout les chiffres spectaculaires de l'absentéisme de longue durée qui ont fait la une des journaux. Ils ont augmenté de 70 % en 10 ans.

Outils en ligne

L'absentéisme diffère d'une entreprise à l'autre. Mais avec une approche adaptée, chaque entreprise, quelle que soit sa taille, peut lutter efficacement contre l'absentéisme, selon Gretel Schrijvers. « Afin d'aider les organisations à comprendre ce que leur coûte l'absentéisme et où se situent les principales lacunes, nous offrons sur notre site web deux outils faciles à utiliser : le Calculateur Coût de l'absentéisme et le Compas de l'absentéisme. Les éclairages qu'ils apporteront permettront aux entreprises d'utiliser la prévention comme arme dans la lutte contre l'absentéisme. »

mensura
Protecting your human capital

WWW.MENSURA.BE

redaction.be@mediaplanet.com

Pour plus d'informations sur l'impact du GDPR, visitez **www.infosentreprendre.be**

Risk management : décider en connaissance de cause

Au vu des nombreuses incertitudes économiques et politiques actuelles, les entreprises doivent se doter d'outils adaptés pour soutenir leur stratégie. Pour Jo Willaert, président de la FERMA, le risk management doit être considéré comme l'un des piliers de cette stratégie.

Que recouvre exactement la notion de risk management ?

Jo Willaert : « La démarche consiste à identifier et prévenir tous les risques pouvant surgir dans le cadre de l'activité d'une entreprise. Le risk management est l'un des piliers de la stratégie globale de l'entreprise. Le rôle du risk manager n'est pas pour autant de décider cette stratégie, mais bien de participer à son développement et à la définition des objectifs de l'entreprise. Il doit s'assurer que le management soit au courant des risques qu'il court dans la réalisation de cette stratégie. Si une compagnie veut par exemple se développer en Inde, où elle n'est pas encore active, le risk manager doit pouvoir évaluer l'ensemble des risques associés à cette opération. »

À quels enjeux spécifiques répond cette discipline ?

J. W. : « Les risques ne se limitent pas à ceux qui sont assurables ou dont on parle dans les médias, comme les risques politiques, économiques ou les régulations locales. L'environnement est de plus en plus volatile et complexe ; le risk management peut jouer un rôle essentiel dans le succès et la compétitivité d'une entreprise. En cas d'incidents comme une cyberattaque ou une pollution, on pense trop souvent à l'argent et à l'élément technique, mais il y a aussi la réputation de l'entreprise, la communication de crise… C'est aussi une forme de risque ! »

La digitalisation, les cyberattaques et l'évolution de la législation poussent les entreprises à réfléchir autrement.

D'ici mai 2018, les grandes et moyennes entreprises devront avoir toute la protection des données personnelles sous contrôle.

Jo Willaert
Président de la FERMA

Quels risques inquiètent le plus les entreprises ?

J. W. : « Les trois principaux risques cités par nos membres sont les incertitudes économiques, la continuité des activités et l'instabilité politique. Ils sont évidemment liés. On le voit par exemple avec les problèmes autour du Brexit ou de la nouvelle attitude économique des Etats-Unis : ils ont des conséquences sur la compétitivité des États, le blocage du commerce international, l'ouverture des frontières, etc. Depuis quelques années, la donne a changé. Auparavant, on connaissait au préalable et avec certitude les zones de dangers ou de difficultés pour les entreprises. Aujourd'hui, tout est devenu extrêmement difficile à prévoir. Les risques proviennent parfois d'événements imprévisibles comme le terrorisme »

À quelles entreprises s'adresse en priorité le risk management ?

J. W. : « À l'origine, la discipline est née dans les grandes entreprises. Aujourd'hui encore, le risk management concerne surtout celles-ci. Néanmoins, la discipline s'adresse aux entreprises de toute taille. L'incertitude économique mondiale, par exemple, est encore plus importante pour une petite société que pour une grande, qui a plus de possibilités pour réagir. Les PME ont vraiment le besoin et la volonté de travailler sur cette question. Même si elles n'ont pas les moyens d'engager un risk manager en interne, elles peuvent se tourner vers un professionnel externe, via de l'outsourcing ou de la consultance, ou suivre des formations. Leurs directeurs financiers peuvent par exemple jouer le rôle de risk managers. »

Sur quels éléments fondamentaux repose une bonne analyse, puis une bonne gestion des risques ?

J. W. : « Chez les décideurs - conseil d'administration ou management -, il n'est pas souvent de tradition de dévoiler tout ce qu'ils sont en train de faire. C'est assez logique. Toutefois, ils doivent pouvoir accepter le risk manager en tant que partenaire à part entière dès le départ. Le risk manager doit pouvoir se positionner par rapport à la stratégie de l'entreprise, en évaluer les risques et leur importance, déterminer si l'entreprise peut vivre ou non avec ces risques. Pour mener à bien

sa mission, il doit notamment avoir accès aux différents départements qui, chacun, sont confrontés à leurs propres risques. Une fois qu'il dispose de toutes les informations pertinentes, il peut identifier et évaluer les risques et ensuite émettre des recommandations, suggérer des mesures de prévention, etc. Il joue en quelque sorte le rôle de garde-fou, d'avocat du diable. Son rôle n'est pas de bloquer l'entreprise mais bien de s'assurer que le management prend des décisions en connaissance de cause. »

Quel regard portez-vous sur l'évolution de la législation européenne dans le domaine de la digitalisation ?

J. W. : « La digitalisation, les cyberattaques et l'évolution de la législation poussent les entreprises à réfléchir autrement. Le but de l'Europe est surtout de protéger le consommateur. D'ici mai 2018, les grandes et moyennes entreprises devront avoir toute la protection des données personnelles sous contrôle. Cela va évidemment contribuer à la protection contre les cyberattaques, mais cela ne résoudra pas tout : même des gouvernements sont attaqués ! Le plus important est que, depuis quelques années, on a affaire à une prise de conscience. Il y a trois ans, on considérait que c'était un problème du département IT. Aujourd'hui, les entreprises le voient de manière beaucoup plus large, presque comme un problème de survie. »

Philippe Van Lil
redaction.be@mediaplanet.com

GDPR

Des outils pour mieux gérer les risques

En mai 2018 entrera en vigueur le GDPR (General Data Protection Regulation), la nouvelle réglementation européenne sur la protection des données privées. Pour Dirk Van Droogenbroeck, country manager Belgium d'Excellium, une démarche structurée s'impose pour s'y adapter.

Dirk Van Droogenbroeck
Country manager Belgium d'Excellium

Qu'est-ce que la GRC ?

Dirk Van Droogenbroeck : « La GRC (Governance, Risk, Compliance) - ou gestion des risques de conformité - vise à créer une structure de gouvernance, tel un comité de pilotage se réunissant régulièrement, pour gérer le quotidien, prendre des décisions, définir les responsabilités des intervenants ainsi que des politiques et processus clairs. Elle doit également identifier tous les risques - financiers, physiques, IT... - liés aux actifs et aux objectifs de l'entreprise. »

Dans le cadre du GDPR, chaque entreprise doit s'assurer que les données personnelles, par exemple des clients, mais aussi des employés, soient protégées.

Quels avantages présente-t-elle dans le cadre du GDPR ?

D. V. D. : « Chaque entreprise doit s'assurer que les données personnelles, par exemple des clients, mais aussi des employés, soient protégées. Elle doit d'abord établir un registre exhaustif des données, de leurs traitements et de leurs flux dans l'organisation. Si un client commande en ligne, il communique ses infos au site web, mais ses données sont aussi utilisées par la logistique pour l'expédition, par la comptabilité pour la facturation, par le marketing, etc. Ceci correspond chaque fois à un traitement différent. »

Et ensuite ?

D. V. D. : « L'entreprise fait un DPIA (Data Privacy Impact Assessment) : elle établit les risques relatifs au traitement des données personnelles. Cela concerne la visualisation, les modifications ou la suppression des données par des personnes non autorisées. La GDPR prescrit d'établir des contrôles, mais laisse à chaque entreprise le soin d'en déterminer les modalités. Excellium a développé une méthodologie complète qui fait le lien entre les aspects juridiques, les aspects organisationnels et la sécurité IT afin d'identifier les problèmes à résoudre et mettre en place des mesures, selon les normes ISO 27001 et 27002. Nous établissons aussi des recommandations sur les processus, outils, améliorations de configuration et d'organisation, gestion des relations avec les clients et partenaires, etc. »

Y a-t-il d'autres facteurs de succès ?

D. V. D. : « Une bonne communication est primordiale ! Chaque collaborateur de l'entreprise est impacté dans sa manière de travailler et doit se sentir concerné et comprendre que ce qu'il fait dans son coin a des conséquences dans toute l'entreprise. Pour ce faire, nous organisons des sessions de sensibilisation pour des groupes de personnes issues de différents départements : juridique, finances, IT, marketing, etc. Ces sessions sont organisées d'une manière pragmatique et pas seulement théorique. »

EXCELLIUM
Your first call when it comes to IT and security

WWW.EXCELLIUM-SERVICES.COM

Philippe Van Lil
redaction.be@mediaplanet.com

L'Europe se penche sur la protection des données

Dès 2018, une nouvelle règlementation européenne sur la protection des données privées contraindra les entreprises à des adaptations. Laurent Deheyer et Michael Raison, respectivement cybersecurity consulting director et principal consultant de la société Approach, nous en dressent une esquisse.

Laurent Deheyer
Cybersecurity consulting director chez Approach

Le GDPR est abordée soit sous l'aspect juridique soit sous l'aspect informatique, mais pour bien la gérer, il faut nécessairement impliquer des profils différents.

Michaël Raison
Principal consultant chez Approach

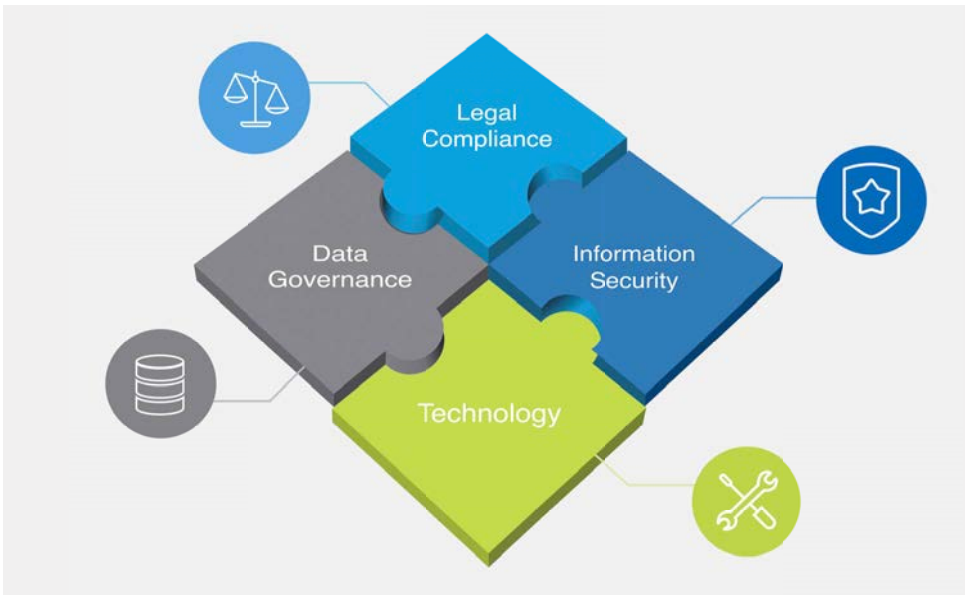
Dans certains cas, le GDPR impose la désignation d'un Data Protection Officer (DPO). Cette fonction peut être interne ou externalisée.

Quels changements la nouvelle règlementation entraînera-t-elle ?
Michaël Raison : « Le General Data Protection Regulation – en abrégé, RGPD en français et GDPR en anglais - entrera en vigueur en mai 2018. La nouvelle règlementation considère les données sur tout leur cycle de vie, de l'acquisition à la suppression, et fournit des détails imprécisés auparavant. Lors de l'acquisition, elle insiste beaucoup plus sur le consentement explicite d'un utilisateur. Exemple : plus de case cochée par défaut ! L'entreprise devra détailler toutes les finalités de l'utilisation des données et préciser celles des tierces parties qui y auront accès, comme des sous-traitants. Les contraintes augmenteront. Toutefois, dans le cadre de la libre circulation des données et du marché unique, cela ouvre aussi des portes. »

Quel est l'objectif de cette règlementation ?
Laurent Deheyer : « Il est entre autres d'harmoniser et renforcer les lois actuelles et de faciliter les échanges. Jusqu'ici, chaque État de l'UE pouvait traduire les directives européennes existantes. En outre, les contraintes du GDPR seront assorties de sanctions beaucoup plus lourdes. »

Les entreprises y sont-elles suffisamment sensibilisées et préparées ?
L. D. : « Au niveau des dirigeants et des comités de direction, nous avons aujourd'hui atteint un degré de sensibilisation qu'on aurait souhaité avoir il y a un an, à la publication du règlement. Au niveau des employés, cela varie d'un secteur d'activité à un autre, voire d'un département à un autre. Certains collaborateurs sont sensibilisés, d'autres le sont moins ou le voient comme une contrainte, par exemple au sein des départements marketing. Nous observons aussi qu'au sein d'une même entreprise, chaque département avance à son propre rythme : le département juridique peut déjà être avancé sur la question, tandis que le département informatique ne l'est pas du tout... ou vice-versa ! »

Quelles connaissances le GDPR implique-t-elle de maîtriser ?
L. D. : « En général, le GDPR est abordée soit sous l'aspect juridique soit sous l'aspect informatique, mais pour bien la gérer, il faut nécessairement impliquer des profils différents : des juristes, des spécialistes en gouvernance et gestion de flux des données, des experts en cybersécurité, des spécialistes du domaine technologique tel que le cloud ou le big data... »



Framework GDPR : la General Data Protection Regulation entrera en vigueur en mai 2018.

M. R. : « Nous agissons de manière structurelle sur quatre axes : juridique, gouvernance des données, technologie de l'information et sécurité des données. Nous travaillons avec une approche transversale et un large spectre couvrant tous les départements de l'organisation. Des données liées à la vie privée circulent dans toute l'entreprise : sont-elles sensibles ? Par où passent-elles ? À qui les transmet-on ? »

L. D. : « Il faut d'abord avoir une bonne connaissance de son entreprise et de ses relations avec l'extérieur - sous-traitants, partenaires, clients. Il faut cartographier le traitement des données et ses flux. Ensuite, il faut se demander si ce traitement respecte la réglementation et quels sont les risques. Enfin, il s'agit de mettre en place une équipe, des responsabilités et de définir le planning des opérations à effectuer. »

Qui doit se charger de ces tâches ?
M. R. : « Il faut définir un comité de gestion sur cette problématique au sein de l'entreprise, avec les acteurs principaux. Dans certains cas, le GDPR impose la désignation d'un Data Protection Officer (DPO). Cette fonction peut être interne ou externalisée. Afin qu'il ait un jugement objectif du traitement des données, ce DPO ne peut pas être impliqué dans l'opérationnel. »

Vous organisez également sous peu des événements sur ces questions...
L. D. : « Oui, nous partons du constat que de nombreuses entreprises se sentent désorientées ou ne savent par où commencer. Avec, de surcroît, une pression sur le timing imposé par une mise en vigueur en mai prochain. Pour les aider, nous organisons notamment une série de tables rondes avec des décideurs de diverses entreprises de tout secteur. Nous contribuons aussi régulièrement à des conférences et forums professionnels sur la cybersécurité. Par ailleurs, en collaboration avec un partenaire, nous organisons aussi des formations certifiantes pour les DPO (Data Privacy Officer). Il est possible de s'inscrire à nos tables rondes, nos formations ou tout simplement demander plus d'informations sur notre site. Précisons que notre société est spécialisée en cybersécurité et notamment en conformité des systèmes informatiques. À ce titre, nous disposons de plus de 60 experts qui réunissent toutes les compétences pour accompagner nos clients dans leur conformité avec le GDPR. »

APPROACH

WWW.APPROACH.BE/NEEDS/GDPR

Philippe Van Lil
redaction.be@mediaplanet.com

Une cyberassurance pour assurer la continuité en cas de cyberincident

Les entreprises doivent établir une cartographie précise de leur sécurité informatique et étudier la meilleure manière de se prémunir d'éventuels cyberincidents. Sans oublier les risques résiduels qui doivent être pris en charge par une assurance. Nous avons demandé plus d'explications à Paul Caekebeke et Door Cooreman d'ADD Insurance Architects.

Paul Caekebeke et Door Cooreman d'ADD Insurance Architects

Les organisations sont de plus en plus exposées au risque d'une cyberattaque.

Quel est l'intérêt d'une cyberassurance ?

Caekebeke : « Les organisations sont de plus en plus exposées au risque d'une cyberattaque. Il importe, avant toute chose, de s'en préserver au mieux. Mais malheureusement, la sécurité à 100 % n'existe pas. De plus, à partir d'un certain niveau de sécurisation, les avantages d'une sécurité supplémentaire ne compensent plus les coûts qu'elle engendre. Et même la meilleure sécurité est insuffisante face aux erreurs humaines et à une «cyberhygiène déficiente». La meilleure solution revient dès lors à couvrir le risque résiduel avec une cyberassurance. »

Quel genre de risques courent les entreprises ?

Cooreman : « Un cyberincident peut non seulement entraîner un arrêt des activités (et donc une perte de bénéfices), mais aussi la corruption ou l'endommagement des données, ruinant ainsi leur fiabilité. L'organisation n'aura alors d'autre choix que de délier les cordons de la bourse pour tout restaurer. Qui plus est, le règlement général sur la protection des données (RGPD) impose d'informer dans un certain délai les personnes dont les données ont fuité. »

Caekebeke : « Un piratage entraîne presque automatiquement une cascade de frais. Il faut tout d'abord colmater la brèche dans la sécurité. Il faut ensuite identifier ce qui a disparu ou a été endommagé et le restaurer ou le reconstruire dans les plus brefs délais. Une entreprise peut également être victime de chantage. Dans ce cas, il est important qu'elle se fasse accompagner. Il peut aussi y avoir des attaques du site Internet. Or, ce site est souvent un important canal de vente et la moindre indisponibilité représente une perte de clients et de revenus. Enfin, votre entreprise peut être tenue pour responsable par des clients ou des tiers du préjudice qu'ils subissent en raison du cyberincident au sein de votre entreprise. »

Que recouvre concrètement une cyberassurance ?

Cooreman : « Pour couvrir tout cela, ADD a mis au point une cyberassurance qui décrit et couvre très largement tous les risques et coûts possibles. Ainsi, les entreprises bénéficient non seulement d'un filet de sécurité financier, mais elles sont également soutenues en pleine situation de crise par les spécialistes ad hoc. L'aide immédiate de spécialistes TIC, de juristes, d'experts en communication et extorsion ou d'autres consultants est au cœur des services de notre police d'assurance ; nous garantissons ainsi la continuité de l'entreprise et un incident ne sera plus nécessairement synonyme d'hémorragie financière. »

ADD les architectes en assurances

WWW.INSURANCE-ARCHITECTS.BE

Joris Hendrickx
redaction.be@mediaplanet.com

Le hacking, phénomène en croissance

Peter Magez
Country manager Belux chez Sophos

Lars Putteneers
Sales engineer chez Sophos

Les attaques massives de type ransomware - ou logiciel rançonneur - bloquent de plus en plus d'entreprises. Peter Magez et Lars Putteneers, respectivement country manager Belux et sales engineer chez l'éditeur d'antivirus Sophos, nous mettent en garde.

Quelles sont les attaques les plus courantes ?

Peter Magez : « Jusqu'il y a deux ans, il s'agissait surtout d'attaques par mail avec des pièces attachées. Aujourd'hui, ce sont plutôt des attaques de phishing, où l'on essaie de connaître le nom et le mot de passe d'un utilisateur. Il y a aussi le "drive-by download" : lorsque vous surfez sur une page web, même connue et respectée, vous êtes infecté sans le savoir à cause des liens publicitaires. Les hackers parviennent à introduire un morceau de code malicieux dans la publicité, qui télécharge automatiquement un malware sur la machine de l'utilisateur. Il peut aussi s'agir d'attaques spécifiques comme de l'espionnage industriel de grandes entreprises. »

Le hacking va-t-il encore s'intensifier ?

Lars Putteneers : « Selon nous, oui, notamment en raison de l'internet des objets. Même à la maison, une télévision ou un frigo peuvent être connectés à internet. Beaucoup de constructeurs n'ont pas encore sécurisé ce type de hardwares. »

Comment se prémunir des attaques ?

P. M. : « Soyez attentif aux mails provenant d'un émetteur inconnu. Il est relativement difficile de voir si un mail est normal ou non. On peut être victime d'une attaque de phishing avec un simple lien cliquable dans le mail, qui semble avoir le format d'un fichier ".doc" ou ".pdf". Toutefois, si on passe sur le lien avec la souris sans cliquer, on peut voir qu'il a une autre extension, par exemple un ".exe". Si vous cliquez, le lien vous redirige vers un site où se trouve la "payload", par exemple pour une attaque ransomware. Si vous recevez un mail de votre banque vous demandant de cliquer sur un lien pour renouveler votre carte bancaire, c'est clairement du phishing. Une banque n'enverra jamais ce type de message par mail ! »

Quels types de solutions proposez-vous ?

L. P. : « Outre l'antivirus traditionnel, nous proposons un produit spécifique aux entreprises : InterceptX. Il les protège contre les attaques de type ransomware avec un support 24 heures sur 24. Si les hackers sont organisés à l'échelle mondiale, nous aussi ! Nous disposons de centres de recherche et de développement tournant non-stop pour suivre tout ce qui se passe dans le monde et adapter nos logiciels en continu quand c'est nécessaire. »

SOPHOS
Security made simple.

WWW.SOPHOS.COM

Philippe Van Lil
redaction.be@mediaplanet.com

Se rapprocher du risque zéro...

Emma Germano
Country manager de Creditsafe

Travailler avec un client qui tombe brusquement en faillite sans honorer ses paiements... Le cauchemar de tout dirigeant d'entreprise. Heureusement, il existe des solutions pour lui permettre de gérer tout cela. Parmi celles-ci : Creditsafe. Emma Germano, sa country manager, nous détaille tout cela...

De quelle manière votre société vient-elle en aide aux entreprises pour limiter les risques financiers ?

Emma Germano : « En les informant le mieux possible quant à la santé financière de leurs futurs clients ! En résumé, nous compilons toute une série d'informations sur une société demandée. Cela va des données juridiques à la composition du conseil d'administration, en passant, bien entendu, par les bilans et par l'historique des paiements. Toutes ces données nous permettent ensuite de dégager une cote et une couleur, rouge, orange ou verte. Le rouge illustrant une cote indiquant que la relation avec cette société peut s'avérer risquée. Le vert, bien entendu, illustrant l'exact opposé. »

Que doit faire un industriel quand il découvre dans votre rapport que collaborer avec la société qu'il avait en tête comporte des risques au niveau financier ?

E. G. : « Tout d'abord, il faut savoir que nous n'intervenons jamais dans le processus de décision entre deux sociétés de collaborer entre elles ou pas. Nous apportons les informations nécessaires à notre client pour faire son choix. L'outil lui indique la décision objective à prendre. Mais, au final, c'est toujours lui qui décide. »

Quand l'un de vos clients décèle des risques dans sa relation avec un potentiel partenaire, quels sont les moyens de se prémunir ?

E. G. : « S'il veut collaborer malgré les risques, le mieux est bien entendu toujours de travailler selon le «prépaiement». C'est une excellente manière d'éviter de ne pas voir son argent si l'entreprise avec qui il collabore venait à faire faillite ! »

> S'il veut collaborer malgré les risques, le mieux est bien entendu toujours de travailler selon le «prépaiement».

Si vos recherches d'informations aboutissent à la conclusion qu'une société a été liée à du blanchiment d'argent, au financement d'une quelconque cause terroriste, ou de toutes autres activités suspectes ou délictueuses, est-il de votre devoir d'en informer les autorités ?

E. G. : « Notre outil «Compliance» se limite à rechercher et regrouper un maximum d'informations déjà publiées au sujet de fraude, blanchissement d'argent ou de terrorisme. Après information trouvée, toutes les décisions appartiennent à nos clients... À eux de voir selon leurs procédures internes ce qu'ils doivent entreprendre. »

L'économie étant par nature un secteur en perpétuel mouvement, on imagine que votre collaboration avec un client ne se limite pas à une fourniture unique des informations ?

E. G. : « Bien entendu. Nous tenons ceux-ci très régulièrement au courant de la cote que nous accordons aux entreprises via notre système de surveillance... Une société qui connaissait de réels risques de faillite il y a un moment a peut-être vu sa situation évoluer positivement. L'inverse étant vrai également ! De toute façon, le risque zéro n'existe pas. Mais on peut essayer de s'en rapprocher un maximum... »

creditsafe

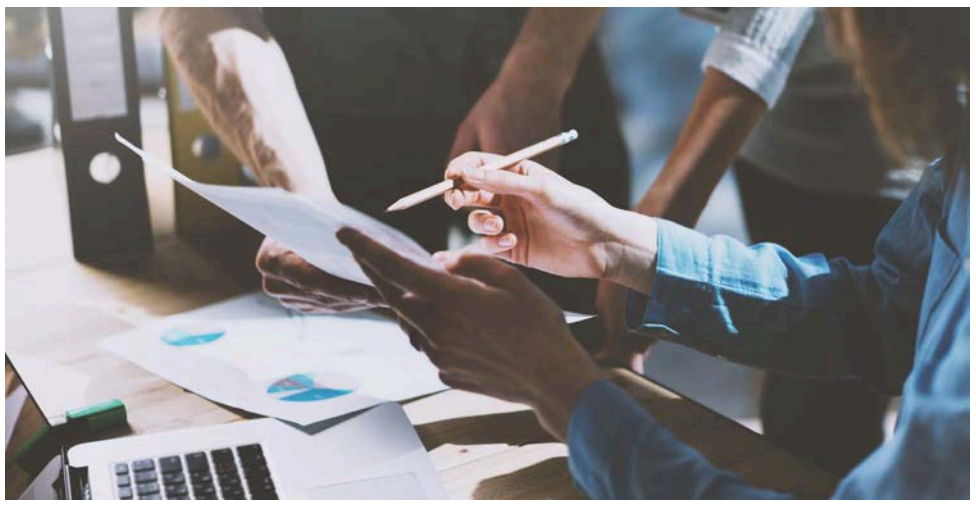
WWW.CREDITSAFE.BE

Frédéric Vandecasserie
redaction.be@mediaplanet.com

Quels risques externaliser auprès d'un assureur ?

Parce que cela n'arrive pas qu'aux autres, une société peut se prémunir contre un certain nombre de risques.

Le rôle d'un courtier est d'accompagner les entreprises, PME et indépendants dans l'étude des risques liés au fonctionnement de la structure, en leur proposant des solutions appropriées.



Au cours de la vie d'une entreprise, les risques auxquels celle-ci fait face vont évoluer aussi bien à cause de facteurs internes à l'entreprise (évolution de l'activité, de la technologie...) qu'externes (digitalisation, changement de réglementation, conjoncture...). Il est donc primordial de maintenir un dialogue avec son courtier pour s'assurer de bénéficier d'une couverture optimale dans la durée.

Nouveaux produits

De nouveaux risques émergent, tandis que certains autres prennent plus d'importance qu'auparavant. Toutes les branches de l'assurance sont concernées. À titre d'exemple, au cours de ces dernières années, les assurances de responsabilité (RC administrateurs, RC professionnelle...) ont connu une forte croissance, notamment en raison de l'évolution du cadre régulatoire. Les garanties proposées sont de plus en plus étendues, et de nouveaux produits (parfois hybrides) émergent, comme l'assurance Cyber.

Par ailleurs, les possibilités de couverture sont très larges, mais encore trop souvent méconnues. Par exemple, les entreprises sont généralement bien conscientes de l'intérêt d'une couverture incendie, mais sont souvent moins informées de la possibilité de couvrir les pertes d'exploitation à la suite d'un sinistre.

Gérer vos risques en RH

L'assurance est également un moyen de gérer vos risques en ressources humaines. En effet, outre la couverture en accident du travail, il est aussi possible de prévoir une couverture en cas de décès ou d'invalidité d'une personne clé de l'entreprise. La couverture « Keyman », permettant de couvrir les frais nécessaires en cas de remplacement de cette personne, ou encore de couvrir la perte financière consécutive à sa disparition.

Tout ça, sans oublier, que votre courtier peut aussi vous conseiller en matière d'assurances « Groupe & Hospitalisation », généralement partie intégrante du package salarial, permettant de favoriser la rétention du personnel.

Se faire conseiller

Moralité : à chacun son métier. Et on ne s'improvise pas spécialiste de l'assurance. Donc, face aux possibilités de couverture existant sur le marché, il est primordial de se faire conseiller par un courtier compétent pour dégager les options qui conviendront le mieux à chaque société.

CET ARTICLE A ÉTÉ RÉALISÉ EN COLLABORATION AVEC PHILIPPE ET SÉBASTIEN VAN INGELGEM, ADMINISTRATEURS DÉLÉGUÉS DES ASSURANCES VAN INGELGEM.

Frédéric Vandecasserie
redaction.be@mediaplanet.com

Des écueils sur le chemin de la croissance

Manuel Basilavecchia
CEO de Netaxis Solutions

Pour gérer une société qui grandit, il faut une couche de management renforcée qui n'a pas la tête dans le guidon.

Trouver du financement et adapter sa structure constituent des défis majeurs pour une entreprise en croissance. Manuel Basilavecchia, CEO de la société Netaxis Solutions, active dans la conception de réseaux VoIP nous fait part de son expérience.

En termes de financement, quelles difficultés avez-vous rencontrées ?
Manuel Basilavecchia : « Nous avons commencé en 2010 comme consultants en télécommunication. Dans ce business, le retour est relativement rapide mais la marge assez faible. Seule solution : augmenter le nombre de consultants. Mais ceux-ci sont rares sur le marché. Pour assurer notre croissance, nous avons alors élargi notre panoplie de services, notamment avec de la maintenance, dont la marge est plus intéressante. Résultat : un succès rapide mais assez faible aussi, dans la mesure où nous n'avons pas pu nous étendre plus loin que notre marché naturel, le Benelux. Nous avons donc décidé de développer des produits logiciels et avons utilisé les marges générées par la consultance et la maintenance. Les cycles de vente de ceux-ci étant particulièrement longs, il s'est vite avéré que nous aurions besoin de sources de capitaux extérieures pour financer nos activités de recherche et développement. »

Comment y avez-vous fait face ?
M. B. : « A l'aide de notre banque et des Régions dans lesquelles nous travaillons, nous avons mis en place un programme d'investissement. Nous avons également fait appel à des personnes et entreprises que nous connaissions bien et qui avaient confiance dans la valeur de notre projet et donc dans un retour sur quelques années. Bouclé en deux phases, cet exercice nous a permis d'augmenter les fonds disponibles de 1,15 million d'euros, en termes de capital, de prêts subordonnés et de prêts à court terme. Nous avons ainsi pu poursuivre le développement de nos produits et notre expansion à l'international au-delà du Benelux. Toutefois, trouver du capital nous a semblé plus compliqué et surtout beaucoup plus long que ce que nous avions envisagé. »

Quelle importance la mise en place d'un comité exécutif revêt-elle ?
M. B. : « Elle est nécessaire pour une société en croissance avec un plus grand nombre de personnes. La taille rend les choses plus compliquées. Pour gérer une société qui grandit, il faut une couche de management renforcée qui n'a pas la tête dans le guidon. Nous avons un peu tardé à lancer ce comité exécutif mais, aujourd'hui, il fonctionne bien. Dans une société, il ne faut pas seulement des personnes pour produire et vendre, mais aussi pour optimiser son fonctionnement. »

netaxis solutions

WWW.NETAXIS.BE

Philippe Van Lil
redaction.be@mediaplanet.com

Gestion des risques : quelle place pour le big data ?

Le règlement général sur la protection des données (GDPR) a des implications dans la stratégie de gestion des risques, notamment en matière de big data. Les explications d'Alexis Gil Gonzales, fondateur et CEO d'Aleph Technologies.

Alexis Gil Gonzales
Fondateur et CEO d'Aleph Technologies

Dans la banque et les assurances, la détection de la fraude bénéficie des technologies big data.

Quelle place occupe le big data dans la stratégie de gestion des risques ?
Alexis Gil Gonzales : « De plus en plus importante dans de nombreux secteurs. Par exemple, dans la finance, la gestion des portefeuilles utilise traditionnellement des outils comme les simulations et le forecasting. Plus le volume de données analysé y est grand, plus la précision des modèles de risque et des prédictions l'est aussi. Dans la banque et les assurances, la détection de la fraude bénéficie aussi des technologies big data. Une réponse rapide à des situations de risque peut en outre augmenter la compétitivité d'une entreprise. »

Quelles sont les politiques de sécurité et de protection des infrastructures big data ?
A. G. G. : « Elles ne diffèrent pas trop par rapport aux infrastructures « traditionnelles ». L'important est de les définir et de les appliquer ! La sécurisation des données se focalise sur le contrôle des accès non autorisés, alors que leur protection vise à prévenir leur perte ou indisponibilité pour des accès autorisés. Vu le volume des données, leur implémentation dans un contexte big data implique des technologies appropriées. Une bonne gouvernance des données permet d'identifier rapidement et de monitorer des ruptures de conformité. Cette gouvernance englobe la qualité des données, leur sécurité et protection, leur consistance, leur interprétation, etc. »

Qu'apporte la régulation GDPR ?
A. G. G. : « Elle élargit le cadre légal précédent et renforce les pénalités en cas de non-conformité. L'aspect le plus épineux de cette régulation est probablement la confidentialité des données dès la conception des produits ou services. Cela pose deux problématiques : comment les sociétés ayant des infrastructures big data peuvent-elles s'assurer d'être en conformité avec le GDPR ? Comment les technologies big data peuvent-elles favoriser cette conformité avec la régulation GDPR ? »

Sur ce point, quelles sont les barrières ?
A. G. G. : « Une technologie trop complexe et un personnel peu qualifié. Cela s'améliore ces dernières années : les infrastructures big data peuvent être externalisées en ligne et gérées plus simplement. »

WWW.ALEPH-TECH.COM

Philippe Van Lil
redaction.be@mediaplanet.com

ADVIA CC

PLAY IT SMART, PLAY IT HARD BUT FAIR!

- **EU-CLAIMS**
- E-INVOICING
- CONTRACTING
- DUNNING STRATEGY
- WAKE UP CALL
- CASH COLLECTION
- LEGAL COLLECTION

EU-CLAIMS

Rapid & effective debt collection
within European Union.
No Cure, No Pay.

Contact: info@advia.be

www.advia.be

Hertendreef 30
BE - 2900 Schoten | ANTWERP | Belgium
T +32 (0)3 612 21 31 - F +32 (0)3 400 52 21

Part of DAS Legal Finance Netherlands