EY
Building a better working world

enVue 29

UNE INITIATIVE **D'EY** EN PARTENARIAT AVEC **ECHO CONNECT** ET **TIJD CONNECT** | 5 DÉCEMBRE 2014

Des Big Data à la banque numérique

Internet mobile, médias sociaux et Big Data convergent vers une révolution numérique qui donnera naissance à un client numérique et informé. Pour les organismes financiers, il s'agit d'un défi de taille, mais aussi d'une opportunité rêvée d'en finir avec le spectre de la crise, de renouer avec l'innovation et de se concentrer totalement sur le client. Et c'est urgent. Partout apparaissent de nouveaux services comme Apple Pay ou Sixdots, et de nouveaux phénomènes comme les prêts P2P (peer-to-peer) gagnent du terrain à vue d'œil. Les organismes financiers sont désintermédiarisés, leurs chaînes de valeur subissent une cure d'amaigrissement et le client est plus exigeant et volatil que jamais. A l'occasion de notre grande interview, quatre spécialistes de BNP Paribas Fortis, Belfius et EY nous livrent leurs sentiments sur la réponse des banques face à la révolution numérique. Plus loin dans ce supplément, nous abordons également le règlement général sur la protection des données, à savoir le nouveau cadre législatif européen en matière de protection des données qui entrera en vigueur en 2017. Nous nous intéressons aussi à la journée typique d'un CISO, un Chief Information Security Officer, passons au crible le dernier Baromètre CFO et analysons la réaction du secteur des assurances à la numérisation. Enfin, nous revenons sur les principaux résultats de l'enquête « Get ahead of cybercrime ». En résumé, cette nouvelle édition constitue une lecture obligatoire pour tous ceux qui s'intéressent de près ou de loin au secteur financier.

Des questions sur ce sujet ? Vous souhaitez également consulter ce dossier en ligne ?

www.echo.be/envue

Préambule

« A Perfect Storm »

La transformation numérique des institutions financières connaît un brusque coup d'accélérateur. C'est la conséquence de l'arrivée à maturité de l'Internet, ainsi que de l'essor des smartphones et des médias sociaux. Sans compter la capacité à traiter de manière rapide et efficace une quantité impressionnante de données. Les quatre ingrédients d'une tempête parfaite sont réunis. Et elle aura un énorme impact sur l'ensemble du secteur.

D'autant que le moment est propice. À présent qu'elles ont – pour la plupart – passé avec brio les stress-tests européens, les institutions financières européennes disposent à nouveau d'une marge de manœuvre et de l'énergie nécessaire pour investir dans l'innovation et la relation client. Chez EY, nous considérons la révolution des données comme une occasion fantastique pour les banques et les assureurs de regagner la confiance du client par les canaux numériques, en améliorant l'interaction. Bien entendu, tout changement est également porteur de menaces. De nouveaux acteurs surgissent à l'extérieur du secteur. Armés de nouveaux modèles d'affaires, ils grignotent les marges et érodent les chaînes de valeur des banques et des compagnies d'assurance, les contraignant à prendre position à leur égard. En interne, les organismes financiers sont obligés d'adapter la totalité de leur organisation à cette nouvelle manière de faire des affaires, et ce n'est pas une sinécure. Chez EY, nous disposons de l'infrastructure et des ressouces nécessaires pour aider les organismes financiers à mener à bien de tels changements. Non seulement de par notre longue expérience dans toutes les ramifications du monde bancaire et des assurances, mais aussi parce que le principe du « numérique d'abord » est inscrit dans notre ADN.

Pour les banques et les assureurs, la révolution des données est une occasion fantastique de regagner la confiance des clients.

Rudi Braes, managing partner EY Belgique

Colophon

Une initiative d'EY

Bernard Ghigny, associé EY FSO
Benoit Gérard, associé EY FSO
Sylvie Goethals, associée EY FSO
Kris Volkaertrs, associé EY FSO
Filip Bogaert, directeur EY FSO
Ingmar Christiaens, associé EY Advisory
Kristof Dewulf, senior manager EY Advisory

Editeur responsable :
Marc Cosaert, associé EY Transaction Advisory Services

Coordination EY : Anne-Sophie Jaspers

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

Une réalisation de Mediafin Publishing

Coordination : Tim De Geyter, Veronique Soetaert
Rédaction : Mediafin
Lay-out : Christine Dubois
Photographes : Dries Luyten, Shutterstock

Info? publishing@mediafin.be

Echo CONNECT

LA BANQUE DU FUTUR

La réponse numérique à

La révolution des données rebat les cartes dans l'univers des banques. Que veut le client numérique ? Comment répondre à l'arrivée de nouveaux acteurs comme Apple Pay ou Sixdots ? À quoi ressemblera l'agence bancaire du futur ? Nous avons écouté les réponses des plusieurs experts expérimentés : Mieke Debeerst, Director Corporate & Marketing Communications chez Belfius, Gunter Uytterhoeven, directeur marketing chez BNP Paribas Fortis, Benoît Gérard et Bernard Ghigny d'EY.

Comment appréhendez-vous la révolution numérique ?

Uytterhoeven : Un certain nombre de changements se sont greffés récemment et très rapidement sur les révolutions du mobile et d'internet, qui ont toutes deux eu besoin de 40 ans pour arriver à maturité. Subitement, 60% des Belges possèdent un smartphone, et une grande partie de la population communique abondamment sur les réseaux sociaux. Cela crée une foule de réseaux et de nouvelles formes d'interaction dans le cadre desquelles des informations personnalisées sont échangées très rapidement. À cela s'ajoutent les Big Data, les énormes quantités de données qui résultent de ces interactions, et la technologie qui convertit ces données en informations utiles. Ces évolutions ont subitement commencé à se croiser, avec pour résultat un big bang qui a donné naissance non seulement à une génération d'entreprises proposant de nouveaux modèles d'affaires, comme Uber, Airbnb et Alibaba, mais aussi à un nouveau profil de client, capable de maîtriser les technologies numériques et très exigeant.

Debeerst : La grande question est : comment les banques peuvent-elles gérer ce phénomène ? Comment traduire cette révolution en services qui apportent une réelle plus-value à nos clients ? Les banques offrent la possibilité d'effectuer des opérations en ligne depuis plus de 10 ans, la plupart d'entre elles disposent déjà d'excellentes solutions et applications de mobile banking. À présent, nous devons franchir une nouvelle étape.

Ghigny : Cette révolution intervient à un moment très intéressant pour le secteur financier. Après la crise, les banques ont dû se concentrer sur la consolidation de leurs bilans, parfois tout simplement pour survivre. À présent que la poussière est quelque peu retombée, le secteur peut à nouveau focaliser toute son énergie sur le client. C'est d'ailleurs urgent et indispensable.

Le client aux commandes

Comment le client réagit-il ?

Debeerst : Dans la révolution numérique, le client est aux commandes. Il veut pouvoir faire ses opérations bancaires où il le souhaite, et sur le canal de son choix. Les données présentes sur chaque canal doivent être adaptées de manière à ce que le client reçoive chaque fois la réponse appropriée. Un énorme défi, mais aussi, c'est vrai, une gigantesque opportunité pour tout le secteur.

Gérard : Une récente enquête révèle que l'expérience client est le principal critère dans le choix d'une banque. La proximité d'une agence, qui arrivait en tête il y a quelques années, est rétrogradée en cinquième position. La donne est complètement différente.

L'avenir est-il entièrement numérique ? Ou les agences bancaires vont-elles subsister ?

Uytterhoeven : Il ne s'agit certainement pas de faire un choix entre l'agence bancaire et les canaux numériques. Ils sont complémentaires. Un client qui modifie des données sur son application pour smartphone et appelle ensuite le call-center, attend de la personne qui lui répond qu'elle soit parfaitement au courant. Notre marque numérique, Hello Bank!, en est un bon exemple : parfois, nous la complétons par des agences temporaires.

la demande du client

Benoit Gérard (EY), Mieke Debeerst (Belfius), Gunter Uytterhoeven (BNP Paribas Fortis) et Bernard Ghigny (EY).

Les banques disposent d'excellents atouts pour résister aux nouveaux acteurs qui rabotent leurs chaînes de valeur.

Gunter Uytterhoeven, Directeur Marketing Communication, Campaign and Channels BNP Paribas Fortis

© Dries Luyten

Ceux qui pénètrent dans cette agence pop-up peuvent par exemple essayer les Google Glass, surfer gratuitement en ligne ou recevoir une boisson. C'est une expérience supplémentaire en plus de la présence mobile. Le contact humain reste crucial, continue à générer de la valeur ajoutée. Notre but est de renouveler l'endroit et le contexte dans lequel il est établi. Il ne s'agit plus du guichet derrière une vitre, après avoir fait la file pour retirer du cash.

Debeerst : Le client ne se rend plus dans une agence pour régler une transaction, il le fait via d'autres canaux. Quelle expérience fournissons-nous dans l'agence ? Proposons-nous des rencontres avec des experts ? L'aidons-nous à utiliser son smartphone ? Allons-nous mettre notre réseau d'agences à la disposition de nouveaux partenaires complémentaires ? Notre réseau d'agences et notre contact humain sont des atouts essentiels, mais il est très difficile de les exploiter de manière innovante.

Big Data

Jusqu'où ira la banque du futur dans les Big Data ?

Ghigny : Comment la banque gère-t-elle les énormes quantités de données qu'elle reçoit de ses clients ? La sécurité est cruciale. La technologie est mature, mais nous avons un rôle éducatif à remplir, en mettant en garde les clients qui adoptent un comportement à risque. La protection des données à caractère confidentiel est également primordiale. Comment les banques demandent-elles à leurs clients l'autorisation d'utiliser leurs données sans se montrer indiscrètes ?

Debeerst : Une enquête révèle que 80% des clients demandent des propositions plus nombreuses, meilleures et plus proactives de la part de leur banque, et ils n'ont aucune objection à ce que celle-ci exploite les données qu'elle possède pour le faire. 20% des clients opposent un refus de principe. Nous le respectons. Mais nous devons apporter un meilleur service à ces 80%, ce qui se fait déjà de manière très efficace au sein de notre secteur. C'est précisément à ce niveau que les Big Data doivent tenir leurs promesses.

Uytterhoeven : Nous utilisons encore trop peu les grandes quantités de données. Les possibilités existent, mais nous devons nous montrer très prudents. Un paiement qui n'est pas passé, une facture GSM plus salée que prévu : le client veut en être informé. Nous pouvons aussi aller un peu plus loin : si nous pouvons démontrer que ses pairs paient leurs télécommunications beaucoup moins cher, notre client nous en sera reconnaissant. Les outils sont là. Certains clients attendent encore plus, par exemple que nous les aidions à obtenir un abonnement de GSM moins cher. Même si nous le pouvions dans le respect total de la protection des données et de la vie privée, la véritable question reste : où s'arrête le rôle de la banque ?

>

>

Nouveaux acteurs

Comment les banques appréhendent-elles l'arrivée de nouveaux acteurs qui grignotent leurs marges ?

Gérard : Il est clair que les banques sont sous pression dans un certain nombre d'activités-clés. Voyez les sites web qui comparent des produits et services bancaires ou des assurances, ou les acteurs qui proposent des interfaces très sexy comme Apple Pay, Google Wallet et Sixdots. Dans notre pays, nous voyons se développer de nouveaux modèles d'affaires en matière d'octroi de crédits, notamment le prêt peer-to-peer et le crowdfunding. Subitement, un détaillant chinois en ligne comme Alibaba propose des services de private banking. Ces acteurs s'insèrent entre la banque et le client, grignotent les marges et la chaîne de valeur. Et cela va très vite.

Uytterhoeven : Les banques doivent se réinventer d'urgence. Avec un objectif : combler les attentes du client. Pas uniquement par une stratégie purement incrémentielle. Il faut aussi de l'innovation disruptive.

Comment les banques peuvent-elles continuer à jouer leur rôle dans un paysage qui change aussi vite ?

Uytterhoeven : Une banque possède plusieurs avantages uniques. D'abord et avant tout, une banque connaît tous ses clients personnellement grâce à son réseau d'agences très dense. Plus le monde devient numérique, plus s'accroît le besoin de véritables contacts, j'en suis convaincu. Deuxièmement, les banques disposent de pare-chocs financiers pour absorber le risque de contrepartie. De nombreux acteurs alternatifs n'ont pas des poches aussi bien garnies. Troisièmement, notre longue expérience de l'informatique, de la sécurité et de la protection de la vie privée est un plus. Les nouveaux acteurs pourraient s'y brûler les ailes. Les banques qui exploitent ces atouts de façon adéquate dans le monde numérique en récolteront certainement les fruits.

Debeerst : Le métier de banquier ne se remplace pas aussi facilement. Tous les Apple et Google de ce monde le comprennent parfaitement. Pour proposer Apple Pay, Apple se repose sur des partenariats avec des banques. Notre rôle est donc respecté. Cela ne veut pas dire que nous devons rester les bras croisés. Il nous incombe également de rechercher des partenariats dans le cadre desquels nous prenons nous-mêmes l'initiative.

Les Big Data offrent des possibilités inédites aux banques, à condition de les exploiter avec une grande prudence.

Bernard Ghigny, associé EY

Transformation

Quel est l'impact de l'évolution numérique sur le back-end des banques ?

Ghigny : D'abord et avant tout, l'ajout de canaux numériques aux autres canaux entraîne une augmentation des coûts. La révolution numérique n'exige pas seulement une adaptation du côté du front-end, dans les relations avec le client. Pour réellement devenir « omnicanaux » ou intégrer parfaitement les différents canaux, il faut une organisation et une communication interne parfaites. Ceci requiert une profonde restructuration du back-end, des processus, des compétences des collaborateurs. C'est toute l'organisation qui doit évoluer.

Debeerst : Cela demandera des investissements considérables. En informatique, mais aussi au niveau de nos collaborateurs. Le back-end se transforme de plus en plus en front-end, ce qui constitue un changement fondamental. Nous investissons pleinement dans l'accompagnement de nos collaborateurs en matière d'orientation client, de flexibilité et de maîtrise du numérique.

Uytterhoeven : Notre secteur est en difficulté, avec des taux très bas, une croissance en berne, une forte baisse des bénéfices et des hausses d'impôts. Et c'est précisément dans ce contexte que nous devons investir, dans des projets qui ne porteront peut-être pas immédiatement leurs fruits, mais qui sont indispensables pour garantir un avenir florissant.

Dans la révolution numérique, le client est clairement aux commandes.

Mieke Debeerst, Director Corporate & Marketing Communications Belfius

Numérisation pour le secteur financier

OPPORTUNITÉS

1. Différenciation

Les produits et services de base proposés par les organismes financiers se ressemblent de plus en plus. La numérisation leur offre la possibilité de se distinguer de la concurrence. Quelle information, à quel moment et par quel canal ? C'est désormais la question principale.

2. Nouveaux canaux

Les nouveaux canaux d'interaction avec le client offrent une mine de possibilités. Ceux qui les exploitent à bon escient pourront approfondir et enrichir leurs relations avec leurs clients.

3. Simplicité

À présent que le marché financier est techniquement accessible à des acteurs non financiers, la banque est considérée comme un concurrent pour des entreprises telles qu'Apple ou Google. Ces nouveaux acteurs leur enseignent que la convivialité et la simplicité sont les préoccupations premières des clients.

4. Enthousiasme

Les services numériques offrent une opportunité de retrouver un peu d'enthousiasme au sein du secteur, à la fois pour les collaborateurs et les clients.

5. Confiance

La confiance se construit par l'interaction, et l'interactivité est le principal atout du monde numérique. Pour les organismes financiers, c'est une occasion en or de regagner la confiance de leurs clients qui a été fortement ébranlée par la crise.

Debeerst : Il faut faire des choix. Nous devons revoir nos processus, et en retirer tout ce qui n'apporte pas de valeur ajoutée aux clients. Nous devons nous montrer sélectifs dans la location de moyens, nous concentrer sur les projets adéquats.
Gérard : Ceci requiert une autre approche de l'investissement. Peut-être la mode d'aujourd'hui ne sera-t-elle pas celle de demain. Qui sait si une application excellente en théorie sera réellement adoptée par le client ? L'incertitude relative au rendement sur investissements est beaucoup plus grande. Historiquement, les banques se caractérisaient par de très importants programmes d'investissement, de plusieurs dizaines de millions d'euros. À présent, il faut investir

Grâce à la révolution numérique, les cinq prochaines années seront extrêmement passionnantes.

Benoit Gérard, associé EY

de manière plus progressive : tester, réorienter, recommencer. C'est une approche beaucoup plus dynamique, beaucoup plus diversifiée de la gestion du portefeuille d'investissements.
Uytterhoeven : L'accent sur l'innovation augmente énormément dans l'ensemble du secteur. On ne peut établir de distinction entre les projets innovants et les autres. Chaque projet doit être porté par l'innovation. Auparavant, les banques étaient caractérisées par de longs cycles de projets séquentiels, qui passaient par un système d'entonnoir et dans lesquels chaque département voulait ajouter son petit grain de sel. C'est impossible dans le nouveau monde. Il faut livrer rapidement, et le client doit être au centre du projet du début à la fin.

Le client numérique-type n'existe pas

Qui est l'utilisateur-type des nouveaux services bancaires et d'assurances numériques ? Les statistiques ne permettent pas d'établir un profil univoque. Les services numériques sont énormément utilisés par la plus jeune génération, qui a grandi avec internet. Mais les jeunes ne sont pas les seuls à opter pour le numérique. Une très grande part de la génération plus âgée fait également beaucoup appel aux nouveaux outils.

En d'autres termes, il n'y a pas de profil typique de l'utilisateur des services financiers numériques. Pourtant, les banques identifient des **segments clairement délimités**, avec des besoins différents. Pour la génération plus ancienne, les canaux numériques sont déjà entrés dans les mœurs, mais ils sont utilisés d'une autre manière, pour répondre à d'autres besoins que ceux de la plus jeune génération.

Les banques et les compagnies d'assurances doivent aborder ces différents profils de la manière adéquate. Ainsi le consommateur un peu plus âgé, généralement un peu plus fortuné, utilise-t-il surtout les canaux numériques pour chercher **des conseils et des informations.** Lesquels doivent être complémentaires à ceux qu'il obtient lors des contacts personnels. Au sein de la jeune génération qui privilégie le smartphone, les grandes priorités sont **la simplicité et la convivialité** dans les transactions quotidiennes. L'aspect fun arrive en deuxième position.

Il est aussi important de tenir compte des moments de transition. Lorsqu'un consommateur de la plus jeune génération a besoin d'un produit plus complexe pour la première fois, comme un crédit hypothécaire ou un produit d'investissement, c'est l'occasion rêvée d'approfondir le contact et de développer la confiance du client. C'est une transition délicate, dans laquelle il faut investir suffisamment. Un **conseil personnalisé** est indispensable à ce moment, mais pensez aussi à la poursuite de la relation en ligne. Les canaux doivent se compléter parfaitement.

MENACES

1. Nouveaux acteurs

Les possibilités numériques donnent naissance à de nouveaux modèles d'affaires. Nombreux sont les nouveaux acteurs à l'affût, prêts à grignoter les marges et à raboter la chaîne de valeur des organismes financiers.

2. Risque de transformation

La transformation de l'ancien monde en monde numérique est un processus dangereux pour les banques et les compagnies d'assurance. Parmi les risques, citons les doubles frais, les incompatibilités entre les systèmes, les investissements trop rapides et la frustration des clients.

3. Le back-office doit suivre

Le numérique ne touche pas que le front-office. C'est une transformation qui s'étend des relations avec le client à la comptabilité, en passant par la gestion des risques et les opérations – pour résumer, elle touche toutes les branches de l'entreprise.

4. Personnel

La révolution numérique exige également une bonne dose de flexibilité de la part des collaborateurs. La culture conservatrice traditionnelle doit subir une mise à niveau.

5. Sécurité

Gérer et continuer à garantir la sécurité dans un environnement numérique constitue un énorme défi. Simultanément, l'expérience des banques et des compagnies d'assurances constitue un atout qui peut les différencier des nouveaux acteurs.


EY
Building a better working world
OSAKA
Reece
JOIN OUR HIGH PERFORMING TEAMS
Audit | Accounting | Tax | Transactions | Advisory
When you work at EY, you learn how to be part of a high performing team that works together to tackle client issues. And you create the relationships with clients and colleagues that will continue to build your career – wherever that career may take you.
Find out more, visit ey.com/careersbelgium
top EMPLOYER BELGIË BELGIQUE 2014
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS
EY Building a better working world TEAM BELGIUM OFFICIAL PARTNER
Official partner of the Royal Belgian Hockey Federation.
© 2014 EYGM Limited. All Rights Reserved. Image: ©PHDPH.com

NOUVELLE LÉGISLATION EN 2015

La protection des données personnelles

L'évolution extrêmement rapide des Big Data impose une mise à jour du cadre législatif relatif à la protection des données à caractère personnel. Le Règlement général sur la protection des données sera probablement adopté dans le courant de l'année 2015. Et il est préférable de commencer à vous y préparer dès maintenant.


© Shutterstock

Le texte approuvé du règlement (Proposal of General Data Protection Regulation, en abrégé GDPR) est attendu dans le courant de 2015. Après une période transitoire de deux ans, le GDPR entrera en vigueur dans tous les États membres en 2017. Pas étonnant dès lors que la protection des données progresse énormément sur la liste des priorités du Chief Risk Officer, du Chief Information Officer et du Compliance Officer.

Limitation des données

Le GDPR repose sur trois principes de base. Le premier, la limitation des données au minimum nécessaire, implique que le responsable du traitement des données ne peut collecter plus de données que ce qui est strictement nécessaire à un objectif donné. Dès que son objectif disparaît et que les données n'ont plus aucune utilité, elles doivent être effacées. Bien que les applications Big Data collectent par définition le plus grand nombre de données possibles, le principe de limitation n'y fait a priori pas obstacle. À condition de surveiller scrupuleusement la légalité des applications. Le principe de limitation des données implique par ailleurs que les données ne puissent être accessibles qu'aux personnes qui doivent en disposer pour leur fonction. Juridiquement, l'idée est claire, mais sa traduction en directives stratégiques et en opérations concrètes est souvent une autre paire de manches. Elle exige une série d'outils technologiques, comme un système adéquat de gestion des droits d'accès et une architecture des données ciblée. Vous avez dès lors intérêt à y mettre de l'ordre avant de procéder à l'implémentation du GDPR.

Transparence

L'attention des médias pour les questions de protection de la vie privée, les nouvelles obligations en matière d'information et des conditions plus strictes concernant l'utilisation d'autorisation comme justification du traitement des données personnelles accroissent la demande de transparence, le deuxième pilier du GDPR.
Conséquence ? De nombreuses organisations devront revoir en profondeur leur fourniture d'informations précontractuelle et leurs conditions. Mais aussi vérifier si elles ont suffisamment de raisons de conserver les données collectées par le passé et de les affecter à des objectifs alternatifs.
De plus, le GDPR ancre les droits du sujet des données. Chacun peut demander à consulter les données collectées à son propos et retirer à tout moment une autorisation donnée, à la suite de quoi le responsable sera contraint d'effacer les données. Il est impossible de garantir ces droits sans une architecture des données de qualité et une bonne compréhension des processus de traitement et des structures de gouvernance. Cette obligation devrait également améliorer la qualité des données. Car les sujets auront rapidement accès à leurs données et pourront eux-mêmes rectifier les éventuelles erreurs.

Responsabilités

Le principal changement réside dans les responsabilités. Le responsable du traitement et le sous-traitant de données personnelles seront désormais conjointement responsables et tenus au respect du GDPR. De plus, il sera obligatoire de documenter les efforts consentis par le biais d'audits et de Privacy Impact Assessments, alors que la charge de preuve sera inversée au profit du sujet des données. Par ailleurs, la surveillance sera harmonisée et durcie, avec une sanction maximale de 5% du chiffre d'affaires mondial. Vous avez donc tout intérêt à bien vous préparer à ce nouvel arsenal législatif.

Le responsable du traitement des données et le sous-traitant sont conjointement responsables de toute méconnaissance des dispositions du Règlement général sur la protection des données.

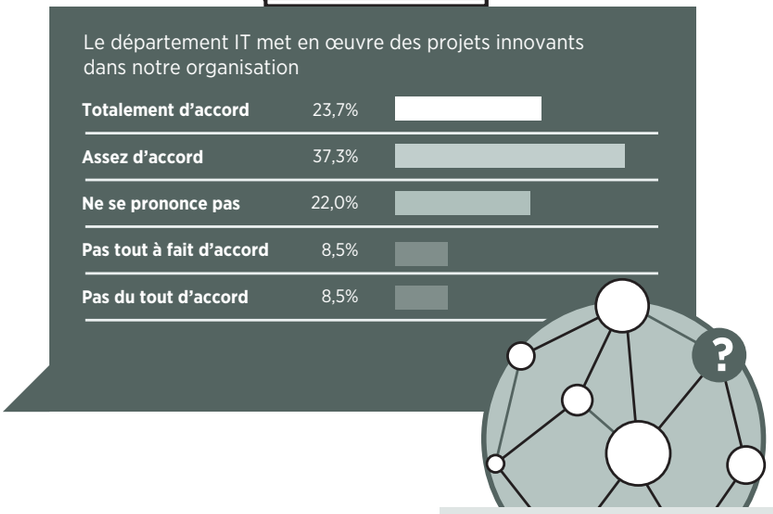

Sylvie Goethals
associée EY Financial Services Organisation
sylvie.goethals@ey.be.com


Filip Bogaert
director EY Financial Services Organisation
filip.bogaert@ey.be.com

BAROMÈTRE CFO : LES DONNÉES DONNENT DES AILES AUX CFO

Big Data entre finance et informatique

Cela ne fait plus de doute aujourd'hui : les données sont devenues la clé de voûte de la finance. Mais comment le CFO contemporain appréhende-t-il les Big Data, les prévisions, la qualité des données et la gestion des performances dans la pratique ? Une réponse à l'aide de cinq affirmations extraites du Baromètre CFO.



AFFIRMATION 1

Le support informatique du département Finance n'est pas optimal

Lorsqu'on leur demande si le département IT met en œuvre des projets innovants, 61% des CFO interrogés se disent « assez d'accord » ou « totalement d'accord ». Ils ont conscience que l'innovation crée des outils qui peuvent les aider à formuler des prévisions plus fondées. De manière générale, les départements Finance se sentent donc soutenus par les services IT. C'est également ce que révèle la réponse à l'affirmation « Les projets innovants soutiennent la stratégie » : 80% des CFO interrogés se disent assez à totalement d'accord. **Pourtant, 64% des répondants trouvent les coûts trop élevés en raison de workflows et de processus inadéquats.**

Pour le développement de meilleurs outils stratégiques, les deux départements doivent apprendre à coopérer étroitement. À cet effet, il est préférable que les budgets soient alloués par la Finance, et que l'IT s'en tienne à son rôle fondamental de service de soutien.

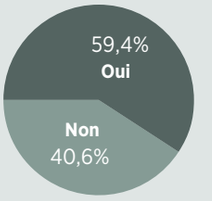
Les CFO ont conscience que l'innovation crée des outils qui peuvent les aider à formuler des prévisions plus fondées.

AFFIRMATION 2

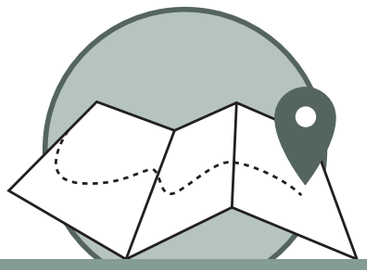
Une mauvaise qualité des données nuit au processus décisionnel

Avec six CFO sur dix qui estiment que des problèmes de qualité ont un impact sur le processus décisionnel, il y a du pain sur la planche en matière de qualité des données. Heureusement, la volonté est présente : **sept départements IT sur dix veulent investir dans la qualité des données.**

Avez-vous le sentiment que des données de mauvaise qualité nuisent à la prise de décision ?



CFO BAROMÈTRE
Le Baromètre CFO est une initiative de recherche indépendante émanant de la rédaction du CFO Magazine en collaboration avec EY. Un questionnaire sur un sujet actuel pertinent pour les CFO a été envoyé à un panel représentatif de CFO belges de multinationales de grande envergure et de taille moyenne. Le Baromètre CFO se concentre sur des activités locales, ses résultats sont donc très représentatifs du marché belge. Il s'agit d'un outil référence pour tout CFO actif en Belgique.



Lorsque vous pensez aux Big Data, quelle est la première idée qui vous vient à l'esprit ?

J'en conçois la valeur ajoutée, et nous y investissons	41,4%
J'en conçois la valeur ajoutée, mais nous n'y investissons pas	25,9%
Une mode liée à l'IT	17,2%
Une mode passagère	10,3%
Autre	5,2%

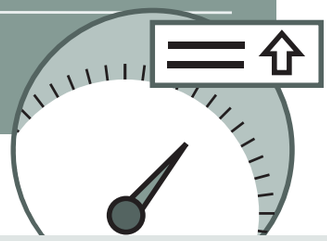
AFFIRMATION 3

Les Big Data, une mode avec une valeur ajoutée

Un nombre considérable (41%) de CFO est convaincu de la valeur ajoutée des Big Data et ne croit pas qu'il s'agit d'une simple mode passagère. Les applications les plus citées sont les optimisations opérationnelles et orientées client.

La première étape vers les Big Data consiste à garantir une qualité optimale des données de base. Une fois cette condition remplie, vous pourrez développer, avec les départements IT et Finance, une feuille de route qui établira précisément la manière dont vous utiliserez ces données. Ne vous laissez pas enivrer, mais ne soyez pas non plus trop conservateur.

Souvent, la volonté de se concentrer sur des données « certaines » constitue un obstacle. Le département Finance doit se départir de sa crainte des « probabilités » et **apprendre à travailler avec les variations et les indications de tendance qu'offrent les Big Data.**



Quelle est la signification principale de la gestion des performances pour votre entreprise ?

L'amélioration des processus ascendants	41,7%
La définition et l'évaluation de KPI	33,3%
La création de transparence dans l'entreprise	16,7%
La capacité à établir des fiches de score	3,3%
Rien de ce qui précède	5,0%

AFFIRMATION 4

La gestion des performances amène des améliorations de processus

Dans 80% des entreprises, la gestion de performance est pilotée par le département Finance. Cependant, seulement la moitié des CFO y voient une manière d'améliorer les processus.

Par ailleurs, l'enquête révèle que les départements opérationnels et les ventes semblent échapper à la gestion des performances. Pas étonnant dès lors que de nombreux projets affichent des performances sous-optimales. La propriété de la gestion des performances sera fonctionnelle, dans la mesure du possible, et supervisée par la C-suite, de préférence par le CFO ou du CCO, dans le cadre d'une vision englobant toute l'entreprise.

Croyez-vous qu'il soit possible de prévoir l'avenir à l'aide des données disponibles dans votre entreprise ?

Oui	49,2%
Non	50,8%

AFFIRMATION 5

La valeur ajoutée du forecasting n'est pas suffisamment exploitée

Neuf répondants sur dix organisent des exercices de prévision et de budgétisation, mais plus de 70% d'entre eux le font toujours dans Excel. **Trois CFO sur dix trouvent que les prévisions sont vraiment utiles, mais demandent beaucoup de temps.** Et de nombreuses entreprises ne dépassent toujours pas le stade de la budgétisation.

Il est difficile de qualifier cette attitude d'innovante. Avec les Big Data, des quantités croissantes de données chiffrées sont cependant mises à disposition pour établir des prévisions de plus en plus précises avec des paramètres de plus en plus divers. Cela dit, la valeur ajoutée de la prévision reste manifestement sous-estimée.

Ingmar Christiaens
associé EY Advisory
ingmar.christiaens@be.ey.com


EY
Building a better working world
DOES YOUR BUSINESS STRATEGY WORK IN THE DIGITAL WORLD?
We all know digital is transforming how everything is done. Changing the possibilities. Affecting every individual, organization, business and government.
The big question is: What do you do?
Will you seize the opportunity? Or be left behind?
The digital world is still full of questions. We'll help you find the answers. At EY, we combine our deep commercial experience with the digital experience that comes from 50 years of working with the world's innovators.
Find out more, visit ey.com/careersbelgium
top EMPLOYER BELGIË BELGIQUE 2014
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS
TEAM BELGIUM
EY Building a better working world
OFFICIAL PARTNER
© 2014 EYGM Limited. All Rights Reserved.

FAIRE FACE À LA CONCURRENCE NUMÉRIQUE

Vers un équilibre numérique entre assureurs et courtiers

La révolution numérique redessine le paysage de l'assurance. Les courtiers et les assureurs doivent se répartir les tâches et se concentrer sur leur cœur de compétences. Des compétences centrées sur le client numérique, cela va de soi.

La Global Insurance Customer Survey (GCIS) d'EY révèle que la distribution des assurances a peu évolué ces dernières années. Courtiers et distributeurs exclusifs vendent toujours 50% des assurances non-vie et près de 30% des assurances-vie. Les bancassureurs continuent à dominer la distribution des assurances-vie, mais les canaux directs enregistrent une croissance moins rapide que prévu. Pourtant, les choses bougent dans le secteur. Les régulateurs s'en donnent à cœur joie. Les directives comme la MiFID2, IMD2 et PRIPS ne font pas qu'accroître la charge administrative des courtiers, qui éprouvent déjà souvent de graves difficultés et qui voient leurs marges fondre au soleil. La vague de consolidation en vigueur sur le marché des courtiers devrait encore prendre de l'ampleur au cours des années à venir.

La principale évolution est sans doute que le client numérique est devenu adulte. La GCIS révèle qu'il fait de plus en plus appel aux sites, forums et blogs dans son processus décisionnel. Le service après-vente est également de plus en plus numérique. Le client indique qu'il attend une interaction avec son assureur. Il veut pouvoir décider lui-même de la manière dont ce processus se déroule pour chaque interaction : par contact humain ou numérique.

Le client attend davantage d'interactions avec son assureur.

Repenser les canaux de distribution

Ces évolutions exigent une refonte radicale des canaux de distribution des produits d'assurance, et ce de la part de tous les acteurs du marché. Du côté des assureurs directs, la GCIS révèle que la proximité humaine manque au client. Chez les courtiers, c'est précisément l'inverse : dans ce segment, c'est souvent l'offre numérique qui laisse à désirer.

Le grand défi consistera dès lors à développer une approche réellement centrée sur les demandes du client et qui intègre harmonieusement les différents canaux. Il faut trouver un nouvel équilibre entre les compagnies d'assurances et les intermédiaires qui réponde aux souhaits des assureurs et des courtiers.

La révolution numérique permettra au courtier de faire l'économie d'une série de tâches administratives et lui fournira les outils nécessaires pour mieux comprendre son client. Il aura ainsi davantage de temps à consacrer à son cœur d'activité : assister le client. Pour la compagnie d'assurances, une stratégie numérique intelligente peut se traduire par de la croissance, une optimisation des coûts et une simplification d'un certain nombre de tâches répétitives ou doublées. Pour y parvenir, elles devront cependant accroître substantiellement leurs budgets numériques.

Les assureurs ont également intérêt à redessiner les combinaisons produit – canal – clients. Ils doivent reconnaître la valeur ajoutée des intermédiaires et respecter leur autonomie. De leur côté, les courtiers doivent accepter que les clients règlent un certain nombre de transactions directement avec l'assureur. Ils doivent également faire preuve de loyauté vis-à-vis des assureurs qui soutiennent leur développement numérique.

Dans cette nouvelle répartition des tâches, il sera également nécessaire de revoir les commissions. Cela dit, tous les acteurs peuvent en sortir gagnants, le système évoluant vers plus d'efficacité et une plus grande orientation client.

Redessiner la distribution des assurances n'est pas une mince affaire. Pour autant, le secteur belge des assurances a déjà su s'adapter à de nombreuses évolutions. Il n'y a dès lors aucune raison de penser qu'il n'y parviendra pas cette fois.


Kris Volkaerts
associé EY Financial Services Organisation
kris.volkaerts@be.ey.com


Benoit Gérard
associé EY Financial Services Organisation
benoit.gerard@be.ey.com


© Shutterstock

LE RÔLE DU CHIEF INFORMATION SECURITY OFFICER

Journal d'un évangéliste de la sécurité

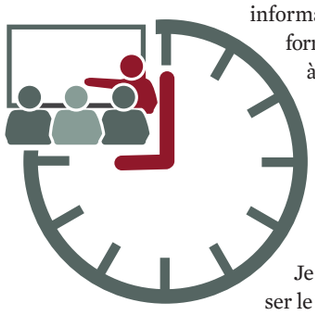
Vu la recrudescence des cybermenaces, la fonction de CISO a le vent en poupe. Mais de quoi s'occupe précisément le Chief Information Security Officer ? À quoi ressemble la journée typique du manager chargé de protéger les données et systèmes informatiques d'une entreprise ? Les réponses de Tim Groenwals, CISO à la SNCB.

8 heures Networking

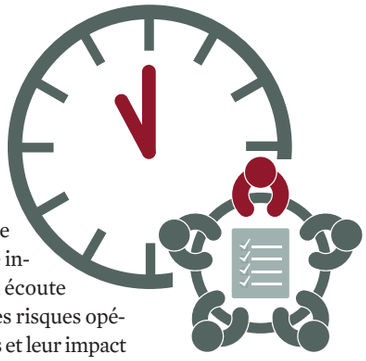
Dans le train, je téléphone à des CISO d'autres entreprises, que j'ai généralement rencontrés dans le cadre de réunions professionnelles. J'entretiens mon réseau et je discute des défis auxquels ils sont confrontés, des projets en cours chez eux, de la justification des budgets, de notre stratégie, et souvent de cybermenaces récentes. J'accorde une grande importance à ces réseaux : personne n'est parfait, nous pouvons tous nous inspirer des meilleures pratiques en cours chez des collègues.

9 heures-11 heures Réunion sur des projets

Le matin, je participe à des réunions sur des projets, et je rencontre parfois des parties externes. Je suis responsable de la prévention de la cybercriminalité sur nos sites Web, applications et systèmes. Cela se traduit par quatre domaines de travail : la sécurité informatique, la gestion du risque informatique, la gestion de la continuité du service informatique et la protection des données. Je suis entré à la SNCB fin 2013, après que des données des clients se sont retrouvées sur Internet. Depuis, ces quatre domaines sont pris très au sérieux. Je cherche également à intégrer les quatre aspects sous ma responsabilité dans tous les projets pertinents, au stade le plus précoce possible.



Je participe par exemple à un projet visant à proposer le WiFi dans les gares. La sécurité et la protection de la vie privée en constituent des éléments primordiaux. Pendant les réunions, j'essaie d'identifier les risques, je réclame de l'attention pour la vie privée des clients et j'analyse la continuité des systèmes informatiques. Après la réunion d'équipe, j'ai souvent des réunions individuelles avec des participants au projet.



11 heures-12 heures État des lieux avec l'équipe du CIO

Je fais un état des lieux avec le CIO et son équipe presque chaque jour. Nous y discutons de la stratégie informatique générale, des budgets et des projets. On écoute mon opinion sur la sécurité. La situation générale des risques opérationnels est également abordée. J'analyse les risques et leur impact possible, le CIO décide des actions que nous entreprenons.

En tant que CISO, je ne veux pas uniquement être un frein. Je veux apporter de la valeur ajoutée.

12 heures Lunch

Le midi, je me contente généralement d'un sandwich avec mon équipe. Celle-ci se compose de six collaborateurs fixes, et de plusieurs consultants qui apportent des compétences spécialisées que nous ne possédons pas en interne.

14 heures
Réunion d'équipe et réunions avec des collaborateurs

Je discute des projets avec mon équipe. Nous définissons ensemble l'approche à adopter. Je parcours les principaux aspects des projets. Nous faisons un bilan, nous nous répartissons les tâches, nous déterminons qui prendra contact avec qui et nous fixons les échéances.

Ensuite, j'ai une série de réunions individuelles avec des membres de l'équipe sur des projets. Lors de ces réunions, nous travaillons de manière plus concrète, pratique, nous entrons davantage dans le détail. Je consacre également beaucoup de temps au coaching individuel. L'aspect humain est très important à mes yeux.

16 heures Contacts informels avec la C-suite

En fin de la journée, il y a généralement un peu de temps dans les agendas pour communiquer de manière moins formelle avec les collègues managers. Je me penche régulièrement avec le CEO et le CFO sur le risque et la sécurité, parfois aussi avec la direction des ventes ou du marketing. Dans ces discussions, je me sens évangéliste de la protection informatique. Je défends la valeur ajoutée de la sécurité et de la protection de vie privée, j'insiste sur les investissements nécessaires, je demande à être impliqué dans les projets à une phase très précoce. Je transmets également des informations sur les budgets et les meilleures pratiques d'entreprises paires et je tente de faire de la sécurité et de la protection de la vie privée un réflexe chez les autres membres de la direction.

Après 18 heures

Bien entendu, les cybercriminels ne vont pas dormir à 18 heures. Je me tiens toujours disponible en cas d'incident. Cela peut aller du défacement d'un site web à un incident de protection de la vie privée en passant par une intrusion dans un système informatique. En cas de sinistre, j'ai surtout un rôle de coordination. Je tente de limiter les dégâts, et je prends contact avec les parties internes et externes pertinentes. Je crois beaucoup dans une communication ouverte sur les incidents : c'est la meilleure façon d'en tirer des enseignements.

7 conseils pour les CISO

1. **La sécurité informatique doit être un *enabler*.** Le CISO doit attirer l'attention sur la sécurité, mais sans se profiler comme un obstacle. Travaillez comme un évangéliste, et rendez les projets réalisables en apportant une valeur ajoutée.

2. **La sécurité dépasse l'informatique.** Pour le CISO, le savoir-faire technologique ne suffit pas. Vous devez traduire vos connaissances techniques en notions utilisables par les autres départements. Les métaphores et autres images sont souvent des outils très utiles.

3. **Soyez sur vos gardes.** Soyez sur vos gardes, mais veillez à ce que vos clients et collaborateurs ne perdent pas le sommeil. La sécurité est la valeur ajoutée qu'apporte votre fonction au reste de l'entreprise et aux clients.

4. **Développez la notion de responsabilité.** Une maîtrise parfaite des outils techniques n'est pas une garantie de sécurité pour l'entreprise. Le maillon faible est presque toujours l'aspect comportemental. Il est donc crucial de faire de la prévention. Le CISO y joue un rôle pédagogique.

5. **Entretenez des relations avec vos collègues.** Établissez un lien de confiance avec des collègues d'autres secteurs. N'essayez pas de réinventer l'eau chaude : posez des questions, inspirez-vous des meilleures pratiques. Osez faire confiance à des parties externes et à leurs connaissances spécialisées.

6. **Suivez une approche basée sur les risques.** Soyez conscient que des incidents auront lieu. Tout devient de plus en plus complexe, et une petite erreur est rapidement commise. Il n'est plus possible de rendre tous les systèmes étanches. Évaluez les risques, et concentrez-vous sur ceux qui ont l'impact potentiel le plus important.

7. **Connaissez vos adversaires.** Ne sous-estimez pas vos adversaires. Les incidents ne sont plus causés par des étudiants qui jouent aux pirates le week-end. Aujourd'hui, la cybercriminalité est l'œuvre d'organisations criminelles structurées, voire de concurrents ou d'États étrangers.

© Shutterstock

ÉTUDE: GET AHEAD OF CYBERCRIME

Pour une protection proactive de votre informatique

Toute entreprise sera tôt ou tard victime de cybercriminalité. Mais la grande majorité des organisations est très mal équipée pour faire face à cette menace. L'étude EY « Get Ahead of Cybercrime » se demande pourquoi tant d'entreprises continuent à faire du surplace dans ce domaine et paraissent incapables de sortir des starting-blocks.

La plupart des organisations (76%) se sentent de plus en plus exposées à la cybercriminalité. Pourtant, plus de deux tiers (67%) des entreprises interrogées ne disposent pas d'informations en temps réel sur les risques informatiques. Celles-ci sont pourtant indispensables pour contrer les menaces réelles qui pèsent sur la sécurité des systèmes IT. C'est l'une des principales conclusions de « Get Ahead of Cybercrime », l'étude mondiale annuelle d'EY sur la protection informatique pour laquelle 1.825 organisations de 60 pays ont été interrogées cette année.

Les résultats des participants belges révèlent que les entreprises manquent d'attention, de budget et de compétences pour mieux défendre des points faibles qu'elles connaissent pourtant. 49% des répondants modifieront à peine le budget total de leur protection informatique au cours des prochains mois, malgré la recrudescence des menaces. Ce n'est qu'une légère amélioration par rapport à 2013, lorsque 52% des répondants déclaraient geler leur budget.

Un des obstacles majeurs à une stratégie adéquate de protection informatique est le manque de collaborateurs spécialisés, selon près de la moitié (44%) des entreprises interrogées. Pas étonnant lorsque l'on sait qu'à peine 4% d'entre elles disposent d'une équipe d'analystes dédiés et spécialisés qui peuvent se concentrer sur les menaces informatiques. Ces chiffres aussi diffèrent peu de ceux de 2013, lorsque 50% des entreprises interrogées reconnaissaient un manque de collaborateurs spécialisés et 4% d'entre elles disaient disposer d'une équipe d'analystes pour les cybermenaces.

La négligence ou le manque de connaissance des salariés constitue la principale vulnérabilité. 85% des répondants belges y voient le facteur le plus influent sur le profil de risque de l'entreprise. L'accès non autorisé aux informations de l'en-

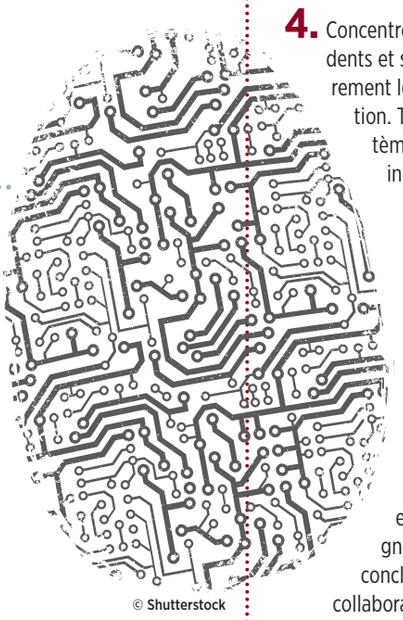
treprise et des contrôles ou une architecture de sécurité informatique obsolète arrivent respectivement en deuxième et troisième position avec 50% et 45% de réponses.
Les principales menaces sont le phishing, les logiciels malveillants et la fraude. Elles comptent parmi les priorités de respectivement 52, 50 et 24% des entreprises interrogées.


© Shutterstock

Approche proactive

L'étude de cette année démontre que les organisations doivent mieux se préparer aux attaques dans un environnement où les cyberintrusions sont inévitables. De plus, les menaces proviennent de sources de plus en plus inventives, qui disposent de ressources financières croissantes.
Les cyberattaques peuvent avoir de lourdes conséquences. Et celles-ci ne sont pas seulement financières. Elles peuvent aussi porter préjudice à la marque ou à la réputation d'une entreprise, causer la perte d'un avantage concurrentiel ou engendrer une non-conformité réglementaire. Les organisations doivent abandonner leur attitude réactive au profit d'une approche proactive et veiller à ne plus être une cible facile pour les cybercriminels, mais un adversaire redouté.
L'étude révèle également que trop d'organisations ne maîtrisent toujours pas les principes fondamentaux de la sécurité informatique. De plus, le Management Exécutif de ces organisations est trop peu attentif au problème et on constate une absence de procédures et pratiques clairement décrites. De nombreuses organisations ne disposent pas d'une équipe de sécurité opérationnelle, ce qui constitue un motif d'inquiétude grave.
Outre les menaces internes, les organisations doivent également réfléchir en profondeur à leur écosystème et à l'impact de leurs relations avec leurs clients et fournisseurs sur leur politique en matière de sécurité. Il est également primordial de collaborer avec des parties externes pour améliorer la cyber-sécurité. Il faut non seulement créer un écosystème d'affaires, mais aussi un écosystème de sécurité dans lequel les autres membres du secteur et les pouvoirs publics peuvent jouer un rôle. Car seule une préparation optimale aux menaces informatiques permettra à une organisation de profiter de ses investissements dans la cyber-sécurité. Les entreprises ne pourront garder une longueur d'avance sur les cybercriminels que si tous les composants sont présents et si les processus et systèmes de protection sont capables de s'adapter aux changements.
Vous trouverez l'étude complète sur www.ey.com/giss

Les organisations doivent se préparer à d'inévitables attaques informatiques
Kristof Dewulf, Senior Manager EY Advisory


© Shutterstock

5 conseils dans la lutte contre la cybercriminalité

Les organisations doivent considérer la sécurité informatique comme une compétence clé concurrentielle. Or ce n'est possible que si elles sont bien préparées, anticipent suffisamment les nouvelles menaces et se départissent de leur rôle de victime. Comment faire de la cyber-sécurité une compétence- clé ?

1. Soyez à l'affût. Le management doit prendre les menaces et risques informatiques au sérieux, et fixer les priorités nécessaires. Veillez à créer un processus décisionnel dynamique qui permet des actions préventives rapides. La vigilance est un maître-mot en cas de menaces possibles.

2. Connaissez les menaces. Les organisations doivent posséder une connaissance étendue, mais ciblée de toutes les menaces et de leur impact potentiel. Ce n'est possible qu'en investissant suffisamment de temps et de moyens dans l'analyse des menaces informatiques.

3. Protégez les joyaux de la couronne. L'organisation doit savoir quelles sont ses ressources les plus précieuses. Soyez particulièrement attentif à la durabilité de vos ressources premières et veillez à les protéger au mieux.

4. Concentrez-vous sur l'approche des incidents et situations de crise. Évaluez régulièrement les compétences de votre organisation. Testez l'étanchéité de votre système de protection en simulant des incidents et des situations de crise.

5. Continuez à apprendre et à évoluer. L'analyse a posteriori de la protection informatique est un élément crucial d'une approche adéquate. Les organisations doivent collecter et analyser toutes les données relatives aux incidents et aux attaques. Elles doivent éviter de continuer à travailler chacune dans leur coin et collaborer pour tirer des enseignements des incidents. Car les conclusions de cette analyse et de cette collaboration peuvent grandement améliorer la protection d'une entreprise.

Kristof Dewulf
Senior manager EY Advisory
Expertise: cyber security & data privacy
kristof.dewulf@be.ey.com

ERNST & YOUNG
Quality In Everything We D

EY
Building a better working world

Beautiful days.
We want you to have them

Audit | Accounting | Tax | Advisory | Transactions

At EY we believe in setting high standards and reaching new heights. A global brand needs a distinctive, confident and globally consistent name. From now on we are EY the world over.

Find out more, visit **ey.com/be**