VERLINGUE
COURTIER EN ASSURANCES

Verlingue infos

Numéro 028
Novembre 2017

Courtier en assurances spécialisé
dans la protection des entreprises

www.verlingue.fr

Édito

Chaque jour, près de 200 000 cyberattaques ont lieu dans le monde*, et toutes les tailles d'entreprises sont touchées par ce fléau ; elles doivent désormais anticiper et évaluer ce risque. La cybersécurité est un défi pour les Directions des Systèmes d'Information, mais plus encore celui des Comités Exécutifs.

Jonathan Uzan, Directeur Cyber Defense chez Onepoint, nous apporte son éclairage sur l'explosion de ces cyberattaques et sur l'organisation des entreprises en France.

Au sommaire également de ce Verlingue Infos, un rapide état des lieux en matière de Protection sociale complémentaire avec des pistes de réflexions à quelques semaines de nouvelles évolutions attendues.

Enfin, la fiche technique qui accompagne ce Verlingue Infos présente Cyber Solution, l'offre de Verlingue pour aider les entreprises à gérer le risque cyber.

Je vous souhaite une bonne lecture de ce nouveau numéro de Verlingue Infos.

Éric Maumy, Directeur Général

*The Global State of Information Security® Survey 2016, PwC, CIO & CSO, octobre 2015

SOMMAIRE

RISQUES CYBER

La menace permanente

Plus d'un quart des PME & ETI françaises auraient été victimes de cybermalveillance l'an dernier, mais à peine 5 % d'entre elles sont assurées contre ces risques devenus majeurs. La menace ne cesse de grandir et les attaques informatiques sont de plus en plus complexes et diverses. Comment réduire son exposition et protéger son entreprise ?

L'environnement légal et réglementaire évolue et s'apprête à imposer d'importantes obligations aux entreprises qui traitent des données personnelles ou commerciales. Les conséquences financières d'une défaillance criminelle ou accidentelle sont passées au 1er rang des préoccupations des grandes entreprises. Pourtant les pratiques sont encore loin d'être exemplaires et les failles restent multiples.

Pourquoi cette accélération constante ?

En une année, les attaques ont progressé de plus de 50 %, quand leur coût pour l'économie globale est estimé entre 375 et 575 milliards de dollars.

Quatre facteurs aggravants expliquent pour partie la ruée vers ce nouvel eldorado :

- La croissance exponentielle de data stockées par les entreprises rend de plus en plus complexe leur sécurisation,
- L'absence de maîtrise des solutions d'externalisation (Cloud Computing) par les PME accroit leur vulnérabilité,
- Le blocage des systèmes est à la portée d'apprentis criminels qui achètent des solutions en mode SAS sur le darkweb pour rançonner leurs victimes,
- L'exposition à internet et aux réseaux sociaux finit d'achever de planter le décor de cette *murder party* dont les data sont l'enjeu. Les informations clients récupérées ne cessent de prendre de la valeur.

Quelles responsabilités ?

Les équipes dirigeantes d'entreprises font actuellement face au paradoxe de la transformation : alors que fin 2016, plus d'un tiers des ETI avaient enclenché un plan de digitalisation, à peine plus de 20 % d'entre elles se déclarent concernées par la cybersécurité. Les solutions de protection sont de plus en plus complexes et interdépendantes, rendant parfois le sujet opaque pour les Dirigeants. Au-delà de l'impact opérationnel, plusieurs d'entre eux ont vu leur responsabilité être mise en cause, et celle de leur entreprise. Dans certains cas, ce type de risque a pu provoquer leur faillite. La question « Quand et combien va nous coûter une cyberattaque ? » est un sujet d'actualité que doivent affronter et traiter les Comités de direction.

Pourquoi la cyber est aussi un enjeu d'image ?

"It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently." La formule de Warren Buffet résume assez bien la situation ; et les deux dernières attaques de ransomware ont démontré :

> L'immédiateté et la rapidité de la diffusion de l'information par les pirates qui sont aussi des experts de la communication,

> L'effet amplificateur, l'impossibilité de contenir l'information, l'absence de frontières, la rapidité de la viralité de l'information sur le piratage,

> « L'irréalité » du dommage : difficile de faire un point sur la situation pour présenter des faits.

Pour plus d'informations, contacter :
Agnès Bonnet - Directrice Responsabilité civile
Tél. : 01 58 86 78 47 - agnes.bonnet@verlingue.fr

Comment aborder la cybersécurité ?

Dans un monde idéal, les entreprises auraient des ressources illimitées leur permettant d'instituer des mesures de sécurité tout en poursuivant leur croissance et leurs programmes d'innovation. Loin de cette utopie, l'élimination des risques semble de plus en plus inenvisageable. C'est le réalisme qui prédomine et le concept de cyber-résilience qui vise le financement couplé du niveau raisonnable de protection et de la réparation des cyber-préjudices. Encore faut-il identifier les priorités…

Quelles solutions d'assurance ?

Selon PwC, moins de 5 % des entreprises françaises disposent d'une cyber-assurance. Il s'agit ici de compléter les couvertures traditionnelles par une solution dédiée capable de garantir l'indemnisation des dommages subis et causés suite à une atteinte à la disponibilité des systèmes d'information, leur intégrité ou la confidentialité des données. Deux domaines doivent être garantis :

> Les Dommages et Pertes pour les incidents subis et leurs conséquences sur son activité,

> Les Responsabilités pour indemniser les préjudices par ses clients et fournisseurs.

Les retours d'expérience démontrent que l'indemnisation seule ne suffit pas ; il faut pouvoir agir très vite. Aussi, cela implique que les dirigeants puissent disposer de différents services d'assistance et avoir accès à un panel d'experts en gestion de crise (informatique, juridique et perte d'image). C'est par la cohérence des actions entre les équipes de Direction et la Direction des Systèmes d'Information, la sensibilisation et la formation des collaborateurs et enfin la mise en place d'une stratégie de cyber-résilience que les dirigeants pourront préserver leurs systèmes et data, et optimiser la protection de leur entreprise.

PAROLE D'EXPERT

Jonathan Uzan, Directeur Cyber Defense chez Onepoint, répond aux questions de Verlingue Infos.

À l'instar des récentes attaques mondiales, doit-on craindre une explosion des cyberattaques ?

« Ces 10 dernières années, ce qui ne représentait jusqu'alors que des menaces à la marge ciblant essentiellement des systèmes à données stratégiques (campagnes d'activisme politique, de déstabilisations étatiques...) s'est déporté avec beaucoup d'opportunisme vers les secteurs de l'économie classique. Il n'est plus tant question de briser un système avec qui l'on est en désaccord mais plutôt de gagner férocement de l'argent. Une mutation qui a sans doute connu sa traduction médiatique la plus forte lors de l'attaque WannaCry. Le grand public, et avouons-le quelques chefs de grandes entreprises aussi, découvraient comment des pans entiers d'activité pouvaient être paralysés, puis rançonnés. Des attaques à distance, anonymisées, sans transporteur, sans receleur, depuis des pays sans extradition, et la possibilité pour les mieux organisées d'en blanchir les fonds directement en crypto-monnaies (Bitcoin). Le volume d'attaques augmentera nécessairement. Il ne faut pourtant pas en avoir peur. Il n'y a là rien qui ne puisse être surmonté lorsque l'on y est correctement préparé. »

Comment les entreprises françaises sont-elles organisées ?

« La France nourrit des ambitions solides sur le numérique depuis les années 2000. Des moyens technique et humain importants ont été déployés afin de préserver nos souverainetés digitales. Des acteurs stratégiques, bien que privés, comme certains grands opérateurs financiers, de l'énergie ou encore du transport ont pu bénéficier de la protection opérationnelle des Agences de l'État. Dont acte. Quid des entreprises ne faisant pas partie de cette liste classée confidentielle d'un peu moins de 250 grands opérateurs ? Et bien c'est un corpus normatif qui devrait permettre d'harmoniser l'ensemble des recommandations au niveau européen et pour l'ensemble des entreprises ayant à manipuler des données électroniques. LPM, GDPR, des sigles mais aussi autant de moments d'introspection, d'opportunités de repenser infrastructures digitales et sécurité. Oui mais voilà. Les entreprises françaises se trouvent rapidement dépassées par ces nouvelles obligations, parfois pesantes, souvent vécues comme des contraintes financières, ralentissant métier et flux de travail. Rien ici qui ne prenne en compte les besoins et les réalités de la compétition commerciale. Chaque entreprise française, par ailleurs, vit une histoire numérique qui lui est propre. Souvent construite dans l'urgence, sur quelques solutions généralistes proposées par les grands players de la défense et d'une exigence en ressources techniques et humaines hors de toute proportion possible. Déployées improprement depuis toujours, ces solutions sont à présent au mieux totalement obsolètes, au pire elles sont un poids que les entreprises ne font plus que subir. Les choses pourraient pourtant se passer bien différemment. »

Le cyber n'est-il pas un sujet de gouvernance pour les entreprises ?

« Le cyber est intrinsèquement un sujet de gouvernance. Les entreprises françaises devraient à présent être assez matures pour démystifier des mots comme hacking ou piratage, et ré-aborder leurs infrastructures sous un angle nouveau. Nous avons trop longtemps approché la sécurité des systèmes par le biais technique, dur, obscur, parfois même inquiétant, où tout ne serait qu'encryption, feux et urgence. La sécurité totale vantée par les vendeurs de solutions n'existe pas. Il est maintenant temps que le métier, accompagné d'experts, se réapproprie son destin numérique. Qu'il définisse sur mesure quantité et qualité de risque digital qu'il encourt, qu'il tolère, et celui qu'il ne pourra jamais se permettre. Il pourra alors y mettre en face les contre-mesures proportionnées les plus justes. La menace se nourrit d'immobilisme, nous le constatons tous les jours dans les entreprises que nous auditons, nous avons ainsi acquis cette conviction forte que le métier doit être le moteur du choix cyber et, se désincarcérant de la contrainte, gouverner. C'est à cette frontière, entre innovation et cyber-décision, que se trouve véritablement la sécurité de nos entreprises. »

Rapide état des lieux avant de nouvelles réformes

La protection sociale a occupé une large place dans les débats de la dernière campagne électorale. Les constats et les impératifs sont largement partagés quant au traitement du déficit de la branche maladie ou à un meilleur accès aux soins. Et la Sécurité sociale qui n'a cessé de complexifier sa nomenclature, continue de transférer de la charge aux complémentaires (cf. les annonces récentes du Projet de loi de finances). Elle reste éloignée d'une partie de la réalité des pratiques médicales et des coûts subis par les assurés (ex. des actes médicaux non reconnus par la Sécurité sociale).

Le candidat Emmanuel Macron avait pour sa part commencé à dévoiler la feuille de route de son quinquennat : prise en charge des prothèses dentaires, lisibilité des contrats complémentaires santé, développement de la prévention... Des objectifs auxquels de nombreux Français peuvent naturellement souscrire et pour l'atteinte desquels, il faudra probablement accepter de changer de paradigme.

Dans ce contexte, le renforcement « Sécurité sociale / organismes complémentaires » constitue un chantier majeur. Un meilleur partage des rôles, une fluidité accrue des échanges de flux, des innovations technologiques… généreront à coup sûr des bénéfices perceptibles par les Français.

En attendant ces prochaines étapes, revenons sur trois évolutions importantes de la dernière législature :

Censure des clauses de désignation par le Conseil Constitutionnel (CC)

La décision du CC (juin 2013) est tout simplement structurante car elle souligne la liberté des entreprises de choisir leur assureur et contredit la pratique des clauses de désignation dans les accords de branche. Depuis, nombre d'entreprises ont fait le choix de quitter l'assureur auquel elles étaient jusqu'alors liées, en fondant leur décision sur le rapport coût / prestations, la qualité de gestion et les services offerts à leurs salariés.

Généralisation de la complémentaire santé

Depuis le 1er janvier 2016, la complémentaire santé s'adresse à tous les salariés. L'employeur, quel que soit son secteur d'activité ou son effectif est tenu de proposer et de financer à hauteur de 50 % le dispositif collectif et obligatoire mis en place. Dans son déploiement, le législateur a réussi à greffer une nouvelle dose de complexité entre les règles du « chèque santé » et ces dispenses d'affiliation pour lesquelles il convient d'adopter des process sécurisés.

Nouvelles règles pour le contrat dit « responsable »

Les règles applicables aux contrats frais de santé portent l'objectif d'influencer les comportements des assurés et des professionnels de santé. Leur non respect est lourdement sanctionné financièrement pour l'employeur et le salarié. La mise en œuvre de ces dernières normes (ex. plafonds de garanties) a des conséquences négatives en faisant progresser sensiblement les restes à charge sur les actes et honoraires des spécialistes (> 10 % tous postes de dépenses confondus). Les réponses à envisager doivent découler d'une analyse étayée des consommations médicales et de leur localisation (ex. Paris / Régions).

Quelles perspectives pour 2018 ?

L'objectif national de croissance des dépenses d'assurance maladie (ONDAM) est fixé à 2,3 % en 2018 par le Gouvernement. Ces vingt dernières années, les dépenses d'assurance maladie prises en charge par la Sécurité sociale ont progressé en moyenne de 3 % par an.

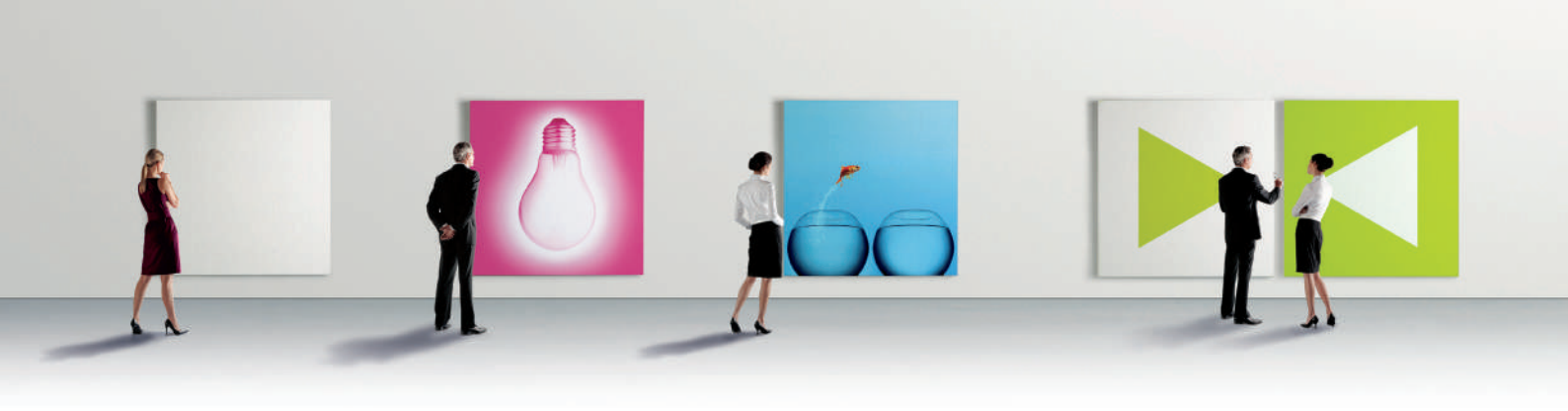
Dans cet environnement, la maîtrise des risques (incapacité de travail…) et le pilotage des régimes collectifs de prévoyance et de frais de santé demeurent un impératif afin de maîtriser les budgets alloués à la protection sociale.

Au-delà des aspects budgétaires, la performance des dispositifs doit également être jugée sur leur bonne articulation par rapport aux spécificités économiques et sociales (âge moyen, structure des familles…) et sur la qualité de gestion dont bénéficient les équipes RH et les salariés.

Les régimes santé mettant en œuvre un socle collectif et des surcomplémentaires facultatives constituent aujourd'hui le modèle largement dominant, permettant d'apporter des réponses plus adaptées aux besoins des différentes familles.

Une réponse optimale consiste également à pouvoir proposer de nouveaux services (téléconsultation médicale, devis en ligne, réseaux de soins et programmes de prévention...) et de larges facilités digitales.

Les nouveaux collaborateurs portent attention à ces dispositifs qui constituent des éléments pour la compétitivité sociale de l'entreprise.



ACTUALITÉS

Verlingue accélère sa croissance européenne

Un an après l'acquisition d'Advantis (Zürich), Jacques Verlingue (Président) et Éric Maumy (Directeur Général) ont annoncé un partenariat majeur avec un leader du courtage d'assurance en Suisse : S&P Insurance Group (Lucerne).

À l'occasion du lancement de leur nouveau plan stratégique #2018, les dirigeants de Verlingue avaient annoncé l'ambition de poursuivre le développement de Verlingue en France tout en allant chercher de nouveaux territoires de croissance en Europe, avec l'objectif affiché de réaliser 2 opérations de croissance externe à l'international.

> *Verlingue poursuit son développement en Europe et confirme sa dimension internationale qui doit bénéficier à l'ensemble de nos clients. S&P Insurance Group est un leader du courtage d'assurance en Suisse avec une expertise pointue dans le management des risques auprès de grandes entreprises, d'ETI et d'institutions publiques de premier plan. Nous sommes très enthousiastes de commencer à travailler avec le management de S&P.* déclare Éric Maumy, Directeur Général de Verlingue.

WBN, 1er réseau de courtiers indépendants au monde

Verlingue a accueilli à Paris du 25 au 28 octobre la 57ème conférence WBN (Woldwide Broker Network), le 1er réseau de courtiers indépendants au monde avec plus de 500 bureaux sur les 6 continents.

Cette édition record a rassemblé près de 350 courtiers du monde entier pour échanger et travailler sur les programmes d'assurances internationaux.

4 jours d'ateliers techniques, de keynotes, de partages d'expériences en présence d'experts reconnus, de dirigeants d'assureurs français et internationaux et d'entreprises.

Verlingue recrute un Chief Financial Officer #2018

Dans le cadre de son projet d'entreprise #2018, Verlingue exprime ses ambitions de croissance en France et à l'international. C'est dans ce contexte que l'entreprise a annoncé le recrutement de Carl Toremans au poste de Chief Financial Officer.

Carl Toremans a plus de 20 ans d'expérience dans les domaines de l'audit, de l'industrie pharmaceutique et de l'agro-alimentaire sur les marchés internationaux, où il a acquis et développé une expertise pointue en pilotage de directions financières.

Directeur de la publication : Éric Maumy - Responsable de la rédaction : Benoît Le Corre - Imprimeur : Cloître Imprimeurs ZA Voie express RN 12 29800 Saint-Thonan - Date de parution et de dépôt légal : novembre 2017 - N° ISSN : 2106 - 5144
Siège social : 12 rue de Kerogan - CS 44012 - 29335 QUIMPER Cedex Tel 0 820 260 260 (0,118 € TTC/mn) Fax 0 820 209 242 / SAS au capital de 2 200 294 € / Code APE 6622 Z / Siren 440 315 943 RCS QUIMPER / Numéro ORIAS : 07000 840 - www.orias.fr - N° de TVA intracommunautaire FR 95 440 315 943 - Relevant du contrôle de l'ACPR (Autorité de Contrôle Prudentiel et de Résolution) 61 rue Taitbout 75009 PARIS [12.16].