LA NOUVELLE
revue du courtage

ÉDITION RÉGIONALE NORD

SEPTEMBRE 2024 #16

Mini site du Collège PLANETE CSCA Nord | www.planetecsca.fr/planete-csca/organisation-gouvernance/college-nord/

La parole du Président

Chères consoeurs, chers confrères,

C'est l'heure de la rentrée et bien malin celui qui peut nous éclairer sur notre avenir même à court terme.

Dans un contexte politique plus qu'incertain et avec les inquiétudes que cela engendre il est urgent pour notre profession de garder la tête froide et de se concentrer sur nos fondamentaux : qualité de l'expertise, accompagnement de nos clients et volonté de s'inscrire dans le temps long.

Depuis 2 mois et la fin des élections beaucoup de choses sont dites, beaucoup de promesses intenables. La réalité est que quelle que soit la couleur politique du Gouvernement, PLANETE CSCA doit rester un interlocuteur incontournable vis-à-vis des pouvoirs publics dans les discussions. Et à l'heure où l'incertitude règne, les corps intermédiaires, dont nous faisons partie, sont plus que jamais indispensables au bon fonctionnement économique et démocratique du pays.

> ***À toutes et tous je vous souhaite une bonne rentrée.***

Nos échanges réguliers avec nos ministères de tutelle, nos élus de tous niveaux, nos autorités de contrôles ou les compagnies d'assurances se veulent constructifs, dans l'intérêt de nos clients et visent à la pérennité de notre écosystème.

L'heure des renouvellements approche et la dernière chose dont ont besoin les courtiers et leurs clients est d'une confusion politique et économique.

Gageons que chacun reprenne ses esprits et que le sens des responsabilités prenne le dessus.

À toutes et tous je vous souhaite une bonne rentrée.

Avec toute ma sympathie. ●

Jean-François Cousin

Président PLANETE CSCA Nord

LA GESTION DES RISQUES CYBER : assurance, prévention, intervention et bonnes pratiques

Entretien avec Augustin Salmon, responsable du développement commercial et du courtage pour Stoïk en région Nord et région parisienne, et Thibault Carré, directeur cybersécurité chez Inquest, entreprise de conseil, filiale de Stelliant, leader français du service à l'assurance.

Dans un monde de plus en plus numérique, les entreprises doivent faire face à des menaces croissantes en matière de cybersécurité. La question n'est plus de savoir si tel ou tel va être victime d'une attaque cyber mais plutôt, quand.

Cet article fait suite à la présentation de deux experts du domaine aux adhérents du collège Nord en mai dernier. Augustin Salmon de Stoïk et Thibault Carré d'Inquest, récapitulent tout ce qu'il faut faire ou ne pas faire pour une bonne gestion des cyber-risques, les solutions d'assurance, et les meilleures pratiques de prévention et d'intervention.

Deux approches complémentaires en cybersécurité, un but commun.

Stoïk : l'assurance cyber proactive

Stoïk propose une offre complète comprenant une police d'assurance cyber, une plateforme de prévention du risque en continu, et une gestion de sinistres internalisée. Le produit d'assurance est distribué par ses courtiers partenaires qui peuvent ainsi accompagner leurs clients dans la gestion de leur risque cyber tout au long du contrat de manière proactive. Stoïk se concentre sur une relation en continu avec ses courtiers partenaires et propose des services de cybersécurité complémentaires en fonction du niveau de risque de leurs clients.

Inquest : Des interventions ponctuelles

Inquest propose des services de réponse à incident et de conseil en cybersécurité. Par exemple, Inquest propose des audits et accompagnements cyber, des exercices de gestion de crise, des sensibilisations et formations. Inquest intervient également en réponse à un incident et une gestion de crises cyber, notamment dans le cadre de contrats d'assurance. Leur approche est plus centrée sur des interventions spécifiques plutôt que sur une relation continue.

Leur but commun : œuvrer pour l'amélioration du niveau de sécurité.

Les prérequis pour contracter une assurance cyber

Pour souscrire une assurance cyber, les entreprises doivent démontrer un niveau minimum de sécurité. Ces exigences se regroupent en trois principales catégories :

Sauvegarde et résilience

La sauvegarde des données est cruciale en cas d'attaque de type ransomware. Les entreprises doivent s'assurer que leurs sauvegardes sont fréquentes, sécurisées et testées régulièrement. Une bonne sauvegarde doit être isolée du système principal pour éviter qu'elle soit également compromise en cas d'attaque.

Authentification et accès

Avec l'augmentation des connexions à distance, notamment depuis la pandémie de Covid-19, il est essentiel que ces accès soient sécurisés. Cela inclut l'utilisation de VPN et l'authentification multi-facteur (MFA) pour protéger les accès sensibles.

Défense et surveillance

Un bon antivirus régulièrement mis à jour est indispensable. De plus, les entreprises devraient envisager l'utilisation d'EDR (End Point Detection and Response) pour identifier et bloquer à distance en cas de comportements anormaux et des systèmes de surveillance comme les SOC (Security Operations Center) et les SIEM (Security Information and Event Management).

Sensibilisation des équipes

L'erreur humaine est souvent à l'origine des incidents cyber. Il est donc crucial de former et sensibiliser les équipes à travers des formations régulières, des campagnes de phishing et des simulations de gestion de crise.

Des audits de sécurité

Des scans externes et internes, ainsi que des tests d'intrusion (Pen tests), permettent de vérifier la robustesse des systèmes et d'identifier les vulnérabilités potentielles.

Gouvernance

La documentation des plans de continuité d'activité, des plans de reprise et des plans de gestion de crise est essentielle. Cela permet de réagir de manière organisée et efficace en cas d'incident. Il est également important de comprendre et de se conformer aux réglementations en vigueur, comme le RGPD.

Intervention et gestion de crise

Quand malgré tout, l'attaque cyber est là, un certain nombre de phases se succèdent qu'il faut bien appréhender.

- *Phase1 : Réactivité*

En cas d'incident, la première étape consiste à alerter et mobiliser les ressources nécessaires pour contenir la crise. Cela implique souvent l'activation de contrats d'assistance et la mise en place de mesures pour empêcher la propagation de l'attaque.

- *Phase 2 : Maintien de la confiance*

Il est crucial de sécuriser les systèmes d'information et de comprendre l'attaque. Cela peut nécessiter des investigations numériques approfondies pour identifier comment l'attaquant a pénétré les systèmes et quelle est l'étendue des dommages.

- *Phase 3 : Rétablissement*

Cette phase implique la restauration des systèmes à partir des sauvegardes et la mise en place de mesures pour prévenir de futures attaques. La communication interne et externe est également importante pour maintenir la confiance des parties prenantes.

- *Phase 4 : Apprentissage*

Après la crise, il est essentiel d'analyser l'incident pour en tirer des leçons et améliorer les mesures de prévention, les outils en place et les réponses apportées.

En bref

La cybersécurité est un domaine complexe et en constante évolution. Les entreprises doivent être proactives pour prévenir les incidents et être prêtes à réagir efficacement en cas de crise. Que ce soit à travers des solutions intégrées comme celles de Stoïk ou des interventions spécifiques comme celles d'Inquest, ou encore en mêlant les deux, il est crucial de comprendre les risques et de mettre en place des mesures de prévention appropriées. ●

Événement

LE PALMARÈS RÉGIONAL DES TROPHÉES PLANETE CSCA

Le 31 mai dernier, le collège Nord a organisé la remise de ses Trophées régionaux. Ces Trophées, décernés en fonction des votes des adhérents, valorisent les relations existantes entre assureurs et courtiers.

Retrouver les résultats nationaux dans le cahier national

IARD

MARCHÉ DES ENTREPRISES

	1ER	2E	3E
DISTRIBUTION MULTICANAL	AXA	ALLIANZ	ABEILLE ASSURANCES
DISTRIBUTION COURTAGE	AIG	QBE	CHUBB

MARCHÉ DES PARTICULIERS ET DES PROFESSIONNELS

	1ER	2E	3E
DISTRIBUTION MULTICANAL	AXA	ASSURANCES MUTELLES DE PICARDIE	GENERALI
DISTRIBUTION COURTAGE	AIG	QBE	CHUBB

ASSURANCES DE PERSONNES

MARCHÉ DES ENTREPRISES

	1ER	2E	3E
DISTRIBUTION MULTICANAL	AXA	SWISS LIFE	GAN
DISTRIBUTION COURTAGE	VERALTI	ALPTIS	REPAM

MARCHÉ DES PARTICULIERS ET DES PROFESSIONNELS

	1ER	2E	3E
DISTRIBUTION MULTICANAL	SWISS LIFE	ALLIANZ	GENERALI
DISTRIBUTION COURTAGE	VERALTI	AFI ESCA	REPAM

RISQUES SPÉCIAUX

1ER	ALBINGIA
2E	HELVETIA
3E	BEAZLEY

"COUP DE COEUR"

ASSURANCES MUTUELLES DE PICARDIE