Confiance à l’ère du numérique

Sécurité et conformité des données au service de vos clients : comment bien positionner le curseur ?

Retrouvez les éclairages apportés par nos clients et experts lors de la conférence du 21 mai 2019

Abington ADVISORY

Les participants à la table ronde

Cori Cabistany, Directrice Juridique & Compliance Groupe

Sylvain Gorce, Directeur de la Sécurité des Systèmes d'information Groupe (au sein de la Direction des Risques)

Abdelkrim Boulkerch, Directeur des Systèmes d'Information

Julien Bizjak, Directeur associé – Responsable de l'activité « Cybersécurité et Confiance numérique »
en tant qu'animateur

La confiance numérique procure un avantage concurrentiel de plus en plus important et contribue directement ou indirectement au développement du chiffre d'affaires des entreprises

La contribution de la confiance numérique sur le business d'une entreprise est liée à son activité et à son positionnement.
Le « ROI » de la confiance numérique est donc difficilement calculable et lié à l'écosystème propre à chaque entreprise.

La confiance numérique est en train de devenir un critère de choix de plus en plus différenciant pour gagner des parts de marché, notamment dans un environnement de forte concurrence, que ce soit en B2B ou en B2C. L'enjeu est de pouvoir rassurer le client en toutes circonstances.

L'enjeu se pose également en matière d'image de marque, l'actualité médiatique ayant tendance à largement relayer l'impact d'un incident (cyberattaque, sanction CNIL, ...).
A ce titre, la cybersécurité et la transparence sont essentielles, notamment dans un contexte d'accroissement des cyberattaques, qui profitent de l'ouverture des réseaux imposée par la course à la digitalisation et à l'innovation technologique.

La confiance numérique contribue à la valorisation de l'entreprise en cas de fusion/acquisition

Le niveau de confiance numérique contribue à maximiser la valeur d'une entreprise ou, en cas de faiblesses avérées, augmenter son exposition aux risques et, in fine, diminuer sa valeur.

Ces éléments sont directement utilisés lors des négociations avec les investisseurs dans le cadre des travaux de « due diligence » d'une opération financière.

Elle contribue également dans la valorisation du « patrimoine Data » des entreprises

Toute démarche de confiance numérique impose de connaître et de maitriser son SI et les données associées.

Cette maitrise permet au « patrimoine Data » d'être un véritable actif, sur lequel les entreprises vont pouvoir développer une nouvelle stratégie et de nouveaux services.

La confiance numérique d’une entreprise repose sur 3 grands axes

Axe 1 : Adaptation & Anticipation : Cartographier et réduire les risques

La confiance numérique doit être raisonnable et progressive en :

- S'alignant sur les activités métiers les plus critiques de l'entreprise, un dispositif de paiement par exemple
- Prenant en compte l'exposition de l'entreprise : sites Web, populations nomades dont les commerciaux, …

Porter une attention particulière sur les prestataires

- Les prestataires (infogérants métiers/IT, fournisseurs cloud) doivent être pris en considération dans la démarche de confiance numérique de l'entreprise
- Les cyber attaquants peuvent en effet cibler ces acteurs pour au final rebondir sur leurs « vraies cibles »
- A ce titre, et selon la criticité des prestataires pour les métiers, il s'agit dès le début d'un appel d'offres, d'intégrer les exigences de confiance numérique et inclure (voire dans certains cas, négocier) des clauses contractuelles adaptées (audit, demandes de droits d'une personne, …)

Axe 1 : Adaptation & Anticipation : Cartographier et réduire les risques

L'objectif est d'avoir une approche pragmatique s'appuyant sur plusieurs outils

/ L'inventaire de l'ensemble des réglementations à satisfaire (sectorielles, protection des données, …)

/ L'analyse de maturité en matière d'hygiène informatique mise en avant par l'Agence Nationale de Sécurité du SI (ANSSI) dans son guide éponyme

/ La réalisation d'une cartographie des risques « boite à outils » s'appuyant sur des référentiels reconnus en la matière (EBIOS, ISO 27005, …). Cette analyse de risques doit également être réalisée en continue lors des projets : « *security / privacy by design* »

/ La construction d'un plan projets pluriannuel pour renforcer cette maturité et réduire les risques identifiés en déployant les actions associées

Axe 2 : Détection & Réaction : Réagir à une attaque / crise / contrôle

La prévision de toutes les attaques est impossible

Pouvoir détecter et savoir gérer les attaques est encore plus important que de pouvoir s'en « échapper » :

/ Il convient alors d'adapter le plan de continuité et de reprise d'activité afin que le risque cyber soit pris en considération (et non pas principalement une destruction physique du Système d'Information)

/ Ce plan doit notamment inclure une activité en mode dégradé permettant de s'isoler d'Internet et de ses menaces.

Les assureurs se positionnent avec prudence sur le risques cyber

/ Les assureurs peuvent demander de fortes garanties sur le niveau de sécurité minimal à avoir

/ Le cyberespace inclut des « Cyberguerres » qui peuvent constituer des clauses d'exclusion en cas d'incident ou des sinistres subis par les organisations

Axe 3 : Amélioration & Préparation : Simuler une crise et contrôler le niveau de confiance obtenu

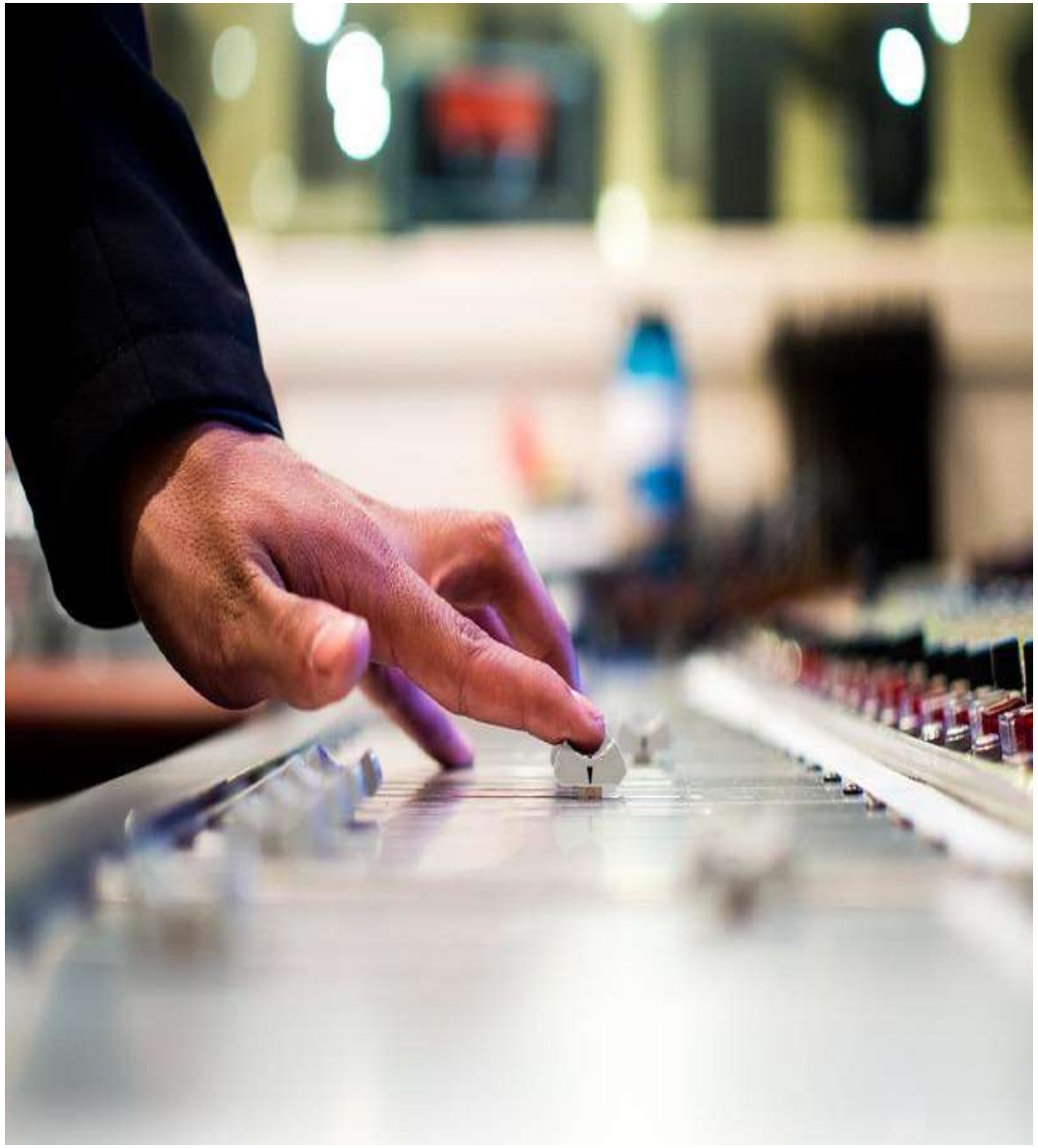
Les mesures essentielles à contrôler

/ La gestion des identités et des habilitations au SI, dont les accès à droits étendus (administrateurs…)

/ Le découpage du SI en zones (cloisonnement des réseaux) et le filtrage des flux de données entre ces zones selon des critères précis (types de flux, émetteurs, destinataires…)

/ La supervision du SI et la détection des incidents / attaques potentiels

/ La réalisation de tests d'intrusion (ou encore d'audits « red team ») visant à évaluer le niveau de sécurité des applications / services, en priorité exposés sur Internet



Axe 3 : Amélioration & Préparation : Simuler une crise et contrôler le niveau de confiance obtenu

Le déploiement d'un tableau de bord

Le tableau de bord doit être en lien avec :

/ la maturité
/ les actions à déployer
/ les risques de l'entreprise, en s'appuyant sur des indicateurs « intelligents » et limités en nombre

En complément de la prise de décision, cela permet également de communiquer en interne et de préparer le changement de culture à instaurer auprès de l'ensemble des parties prenantes

La préparation est irremplaçable et permet d'être coordonné en cas de contrôle par une autorité

/ La centralisation de la documentation et des « preuves » à fournir

/ L'identification des acteurs qui répondront aux questions et leur formation sur les éléments de langages à tenir

Abington ADVISORY

Ces 3 axes génèrent des actions qui viennent alimenter le programme de transformation de l'entreprise.

Ces actions :

Sollicitent de multiples compétences et positionnements au sein de l'organigramme (direction générale, managers, collaborateurs)

/ Pour un niveau de confiance raisonnable et progressif en lien avec l'écosystème de l'entreprise (clients, concurrents, sous-traitants, partenaires, autorité de contrôle, réputation …)

S'appuient sur de l'accompagnement au changement

/ Pour renforcer la culture et faire évoluer les comportements
/ Ce changement de culture s'opère inévitablement en deux temps :
- En prenant conscience de l'importance du sujet et des attendus des acteurs selon leur rôle dans l'organisation
- En accompagnant l'évolution du comportement au quotidien et l'exemplarité du management

bakertilly STREGO

KBRC ORATIO AVOCATS

Notre offre « Cybersécurité & Confiance numérique »

NOTRE OFFRE CYBERSÉCURITÉ & CONFIANCE NUMÉRIQUE

Nos objectifs

Accompagner les Directions SI, Cybersécurité, Risques, Juridiques et Métiers (Marketing, Commerce, RH…) dans:

- La **cartographie** de leurs risques Cyber et Conformité (RGPD/GDPR*, LPM**, NIS***…) et la construction d'un **plan projets priorisé**
- Le déploiement des projets visant à **renforcer** les dispositifs Cyber et Conformité en lien avec **l'évolution des attaques, les nouveaux usages** des outils et la jurisprudence
- **En cas d'attaque**, l'analyse de la situation, la **reprise** de l'environnement impacté et le retour opérationnel

Nos expertises de bout en bout

Management Cybersécurité & Confiance numérique
Risques, Fonctions, Feuille de route, Processus, Tableaux de bord, Changements

Urbanisation SI / Cybersécurité
Architectures, Applications, Bases de données, Systèmes, Réseaux, Terminaux

Juridique
Audit et renforcement contractuel
Litiges / contentieux

Simulation d'attaques & Contrôles
Audit techniques et organisationnels
Tests d'intrusion / audits « red team »
Campagnes de *phishing*
Mise en situation d'équipes

Nos clients

Des **clients renommés** de taille et de secteurs d'activité variés qui nous renouvellent leur confiance (événementiel, prévoyance, distribution, services, industries…)

Notre équipe

15 consultants (certifiés CISM, CISA, ISO 27001, ITIL, …) au sein d'une équipe pluridisciplinaire d'Ingénieurs en cybersécurité et de Juristes IT

6 avocats expérimentés en protection des données pour le conseil juridique et le contentieux

Votre contact

Julien BIZJAK
Directeur associé

16 rue Monceau, 75008 Paris, France
Mobile : +33 6 74 34 27 68
E-Mail : julien.bizjak@abingtonadvisory.com

* RGPD / GDPR : Règlement Général européen sur la Protection des Données

** LPM : Loi de Programmation Militaire

*** Directive NIS : Directive "Network and Information Security"