La Sécurité des Systèmes d'Information a échoué ?

La Sécurité Numérique doit réussir !

Par Pierre-Luc REFALO (Novembre 2012)

Cet article présente quelques éléments majeurs développés dans l'ouvrage « La Sécurité numérique de l'entreprise » paru aux Editions Eyrolles.

« La sécurité numérique n'est pas un autre nom de la sécurité informatique. Elle s'adresse aux usages, non aux systèmes et s'inscrit très étroitement dans le champ de la sécurité globale. »

En 10 ans, le numérique a bouleversé la société et le monde de l'entreprise. Et depuis 20 ans, les questions de Sécurité des SI ont été abordées de manière très technique et méthodologique, souvent éloignée des stratégies et des activités « métiers ». Nous sommes à la fin d'un cycle et le secteur doit évoluer de manière forte.

Dans un univers global, incertain et hyper-complexe, la Sécurité des SI doit sans doute, sans que ce soit paradoxal, effectuer un saut créatif tout en revenant sur ses fondamentaux. A défaut, elle pourrait « éclater » et s'intégrer d'un côté à la sécurité/sûreté dans une approche « cyber-défense » (infrastructures critiques) et « protection du patrimoine » (informations stratégiques), d'un autre, à la gestion des risques liés aux usages et à la dématérialisation (identités numériques, données à caractère personnel et vie privée, signature et preuve électroniques). Dans les deux cas, les questions de « conformité » prennent encore plus de poids. Mais être conforme, n'a jamais signifié être sûr ou sécurisé ! Il faudra faire des choix …

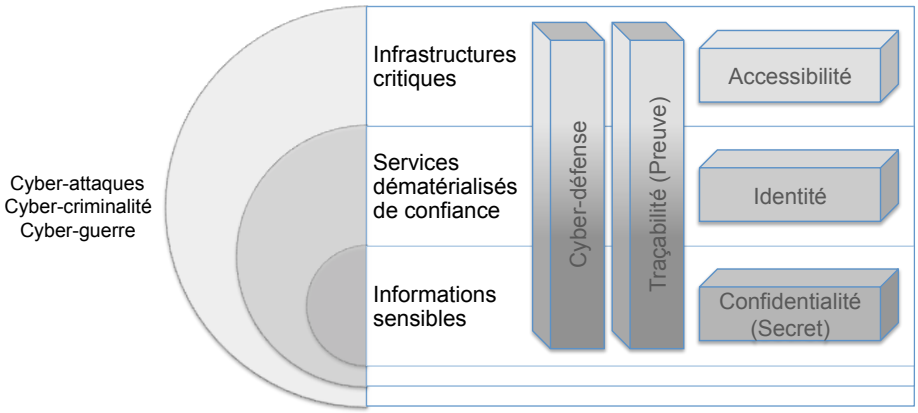
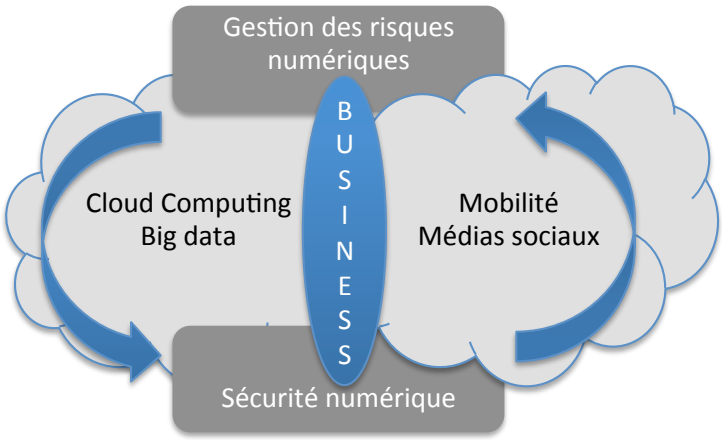


Schéma simplifié du champ de la sécurité numérique

Par exemple, les tentatives d'évolution de la Sécurité SI vers l'Intelligence Economique (veille, protection et influence), la sûreté de l'information et la protection du patrimoine (matériel et immatériel) restent inabouties et sont parfois dangereuses. Des affaires récentes sont à ce titre symptomatiques. Et dans le numérique, l'usage et le partage supplantent largement la propriété. Que faut-il donc vraiment protéger à l'ère du numérique, en particulier, en termes de secret et confidentialité ? Ainsi, l'émergence du Correspondant Informatique et Libertés crée autant de frictions que de synergies entre la protection de la vie privée (conformité à la loi) et le business d'une entreprise devenue « numérique » (développement économique). Pour faire simple, ***les véritables enjeux de la sécurité numérique se concentrent autour de 4 mots clés : identité, accessibilité, confidentialité et traçabilité*** (avec de manière sous-jacente les questions de secret et de preuve et pour certains, les enjeux de la cyber-défense). Ce domaine a son existence propre et continuera à se développer en apportant des services transverses, globaux et de plus en plus essentiels pour les entreprises et les administrations.

Le secteur doit alors vivre ses *« aptations »* (transaptation ou exaptation, selon les cas, décrites par Pascal PICQ dans *« Un paléoanthropologue dans l'entreprise »* Eyrolles-2012) que certains ont déjà initiées : Il faudra donc évoluer en termes structurels (périmètres d'action et champs des responsabilités) et fonctionnels (acteurs et rôles), tout en tenant compte de l'histoire et de la culture de l'entreprise. Sinon, l'échec est assuré.

Globalement, ***une fonction « gestion des risques numériques » doit être clairement définie, de manière transverse, proche des métiers,*** et le cas échéant, hors des DSI. La responsabilité de la sécurité numérique (opérationnelle) doit alors être concrètement portée par les fonctions informatiques et les fournisseurs de services. La fonction transverse ne serait alors plus *« responsable »*. Elle apporte plutôt une *expertise* interne (et/ou externe) auprès des Directions RH, Finance, Juridique, Audit voire Risques et Sûreté, en étant plus proche des décideurs et des métiers. Les aspects stratégiques (menaces, technologies, relations gouvernementales), sociologiques (comportements, usages), réglementaires / normatifs (globaux, sectoriels), juridiques (contrats, engagements de services) et économiques (politique d'achat, assurance) sont suffisamment importants pour être abordés de manière coordonnée et plus transverse. Car à l'heure du *cloud computing*, de la mobilité, des médias sociaux et du *big data*, ***la sécurité numérique sera aussi de plus en plus intégrée dans des services globaux et souvent externalisée***. Au marché de répondre aux enjeux avec des engagements de moyens mais aussi parfois de résultat (protection des données à caractère personnel, infrastructures critiques, valeur probante de documents et de trace, etc.). Cette évolution sera très pragmatique et certainement sectorielle.



Gestion des risques numériques à l'heure du Cloud computing et de la mobilité

Il deviendra alors essentiel de fixer des limites aux pouvoirs (ex : du marché), à la réglementation (ex : pléthore et incohérence des textes) et à l'intégration (ex : des mécanismes et services de sécurité**).** Cette notion de « limites » s'est imposée au fil de la rédaction de l'ouvrage et elle synthétise l'approche « recentrée » qui est proposée. Tout d'abord, alors que l'on dénombre en France, plus de 20 associations, commissions et groupes de travail (autant utiles que légitimes) traitant plus ou moins de sécurité numérique, ***le secteur gagnerait à être mieux structuré autour d'instances plus représentatives des professionnels des entreprises***. Ils doivent être plus visibles et connus des pouvoirs publics et avoir plus de poids sur le marché. D'autre part, les *« politiques sécurité »* n'apportent plus grand chose, si ce n'est des référentiels d'auto-évaluation voire d'audit / conformité. Font-elles vraiment progresser la sécurité réelle à l'heure des normes ISO/IEC 2700x ? L'acculturation du management et des métiers (sur les usages et les risques) doit précéder la réglementation, au moins l'accompagner et non plus lui succéder. Tous les contenus, la pédagogie et les outils sont disponibles mais restent trop peu exploités. Enfin, sur l'intégration, on se situe plus sur le moyen / long terme. Comme pour la sécurité routière, on n'achètera plus les outils et services de sécurité qui seront intégrés dans des technologies de base, des offres d'opérateurs, d'hébergeurs et de plates-formes de service. Mais cela aura une limite qui remettra plus que jamais la sécurité réelle dans les mains de l'utilisateur. ***Le processus d'acculturation doit alors porter des messages forts de dissuasion (contrôles renforcés et indépendants) comme de motivation (indicateurs clairs et pertinents).***

L'auteur : *Créateur et dirigeant d'entreprise, Pierre-Luc REFALO possède plus de 20 ans d'expérience en Sécurité numérique et protection des informations. Homme de conseil, il fut aussi directeur du programme « Sécurité de l'information » de Cegetel / SFR (1997-2002) et représentant au G8 et à la Commission Européenne sur le cyber-crime, la vie privée et la signature électronique. Il accompagne depuis 10 ans ses clients dans l'évolution de la gouvernance des risques numériques et l'acculturation des acteurs. Il est membre du Comité de Pilotage des Assises de la Sécurité et des SI et auteur des Livres bleus publiés à cette occasion depuis 2004. Contact : plrefalo1063@gmail.com.*