Colloque de la Chaire de Cyberdéfense et Cybersécurité « Economie de la Cybersécurité »

Paris – le 14 novembre 2016

Optimisation des dépenses et cyber-assurance

Pierre-Luc REFALO
Groupe Capgemini
Directeur - Conseil Stratégique Cybersécurité

Aborder la dimension économique de la cybersécurité peut sembler une gageure dans un pays qui aime peu l'économie pour des raisons « éducatives », et la sécurité pour des raisons « culturelles ». L'initiative de la Chaire de Cyber Défense et Cyber Sécurité de St Cyr – Sogeti – Thalès est donc une excellente opportunité pour aborder le sujet de manière globale et pluri disciplinaire.

Ce document (voir aussi la présentation sur le site de la Chaire) se concentre sur la question des coûts et des dépenses qui permettent de réduire des (cyber) risques, de les optimiser, voire de s'appuyer sur une assurance « cyber ». Il reste exploratoire et traduit la vision d'un « praticien-cherchant » qui n'est ni chercheur, ni sachant.

Depuis 40 ans, les Etats, puis les entreprises et également les individus ont progressivement intégré un ensemble de mesures organisationnelles, juridiques, comportementales et techniques. Toutes ont un coût et ont permis le développement d'un marché (très atomisé mais en phase de concentration).

La finalité est désormais de créer de la valeur directe et indirecte (innovation, emploi et formation, transformation numérique et services en ligne de confiance, réduction de pertes en cas d'attaque, etc.).

Nous devrions d'ailleurs parler davantage de sécurité numérique que de cybersécurité[1].

Désormais, l'enjeu n'est pas de protéger le Système d'Information d'une organisation (face à des menaces externes) mais de permettre le développement de ses activités en intégrant le numérique au cœur de la stratégie. La sécurité et la confiance numériques sont très liées. Et si elles génèrent des coûts, elles doivent surtout être considérées comme des facteurs de compétitivité et de développement économique. *Il faut donc bien - ou mieux - dépenser*[2].

La question de la « mesure » est donc majeure. Mais sait-on, déjà, mesurer la sécurité ? Non !
La sécurité n'est pas la conformité. Et la sécurité n'est jamais absolue, totale. Coexistent en effet :

- *une « bonne » sécurité* : basée sur l'évaluation des risques, transparente et peu contraignante, intégrée en limitant les surcoûts, éthique et s'appuyant sur des contrôles / preuves,
- et *une sécurité « réelle »* : ciblée sur les enjeux majeurs - pour les Etats, entreprises et individus - mesurable en relation avec les risques / incidents, s'appuyant en premier lieu sur l'humain, visible et opérationnelle en apportant des résultats.

Mesurer la « sécurité » repose en définitive sur 3 paramètres :

[1] Voir « La sécurité Numérique de l'Entreprise – L'effet papillon du hacker » Eyrolles - 2012

[2] Ces sujets ont été traités en 2011 au sein d'un Groupe de travail du Cercle Européen de la Sécurité que l'auteur de ces lignes a eu le privilège de piloter et dont certains enseignements sont repris.

- les risques – le pourquoi : scénarios, impacts, statistiques,
- la maturité – le quoi/comment : mise en œuvre effective de bonnes pratiques
- et bien sûr, les coûts - le combien (gestion analytique et financière, de l'amont à l'aval en incluant les incidents).

Le champ des dépenses en cybersécurité, qui est devenu très vaste (voir tableaux en annexe) s'adresse à l'IT (systèmes de gestion), l'OT (systèmes industriels) et l'IoT (objets connectés). Le coût des mesures de sécurité n'est d'ailleurs pas systématiquement identifiable, ni mesurable à quelque niveau et dans quelque contexte que ce soit.

« Comparaison n'est pas raison », mais l'analogie peut aider à comprendre les tendances. Par exemple, la sécurité routière (des frais d'apprentissage et d'examen, aux radars en passant par les airbags, ABS, conduite assistée et ceintures, etc.) démontre depuis 40 ans les impacts des mesures en termes de réduction des morts sur les routes. La sécurité aéroportuaire permet également de bien comprendre en quoi et comment les mesures d'anticipation, de prévention / protection et détection / réaction permettent de réduire les risques (accidents et erreurs comme fraude et malveillance, voire terrorisme) en intégrant « security / privacy / safety », le matériel, l'immatériel (données) et l'humain. *Que coûte la sécurité numérique d'un aéroport « digital », avatar de l'entreprise numérique construite sur des « plateformes » ?*

Historiquement, les professionnels ont eu du mal à définir leur « budget » sécurité pour le SI interne. Certains avouant même qu'ils ne souhaitaient pas connaître et encore moins communiquer sur leur « budget », de peur qu'il soit réduit … L'indicateur clé, connu des professionnels, est le fameux « entre 4 et 10% du budget IT ». Mais que met-on au numérateur et au dénominateur ? Et il leur faut désormais le faire en incluant les enjeux et les risques « business » liés au numérique. Très peu le font …

Face à la complexité, l'important est de disposer d'un modèle. Capgemini / Sogeti structure le sujet en 3 domaines (Organisation / Protection / Supervision) et 5 piliers (Infrastructures, Terminaux, Applications, Identités/Accès, Données). Sur cette base, nous pouvons, quel que soit l'environnement numérique, identifier près de 50 points d'évaluation des coûts … A appliquer aux SI internes de gestion, aux systèmes industriels (usine / supply chain) et désormais aux objets connectés ; le tout s'appuyant sur des plateformes « cloud » quel que soit le modèle.

Sur cette base, la mesure de ce qui peut l'être a peu de sens dans l'absolu (données brutes) car l'influence de la taille et du secteur d'activité voire du contexte de l'organisation est très marquée (conjoncture, stratégie d'investissement vs charges de fonctionnement, Comité de Bâle pour les banques, traitements de données sensibles / personnelles, etc.). Il convient donc d'élaborer des indicateurs relatifs ou « ratios »[3].

Quelques chiffres et ordres de grandeur constatés :

- Les mesures de prévention / protection représentent environ 85% des dépenses contre 15% pour la détection / réaction. Un rééquilibrage est en cours et devrait s'accélérer.
- Le marché des solutions techniques (outils) et les services (conseil, services managés) s'est progressivement équilibré (50/50) alors que pendant longtemps les technologies se situaient autour de 60%. Les pratiques d'outsourcing devraient poursuivre cette tendance.
- Les dépenses de sensibilisation des collaborateurs se situent entre 3 et 25 € par employé et par an (en fonction de la taille de l'entreprise).
- Les dépenses d'outils de protection du poste de travail se situent entre 5 et 30 € par poste (en fonction de la taille de l'entreprise).

[3] Cf. White paper des Assises de la Sécurité 2011

- Les équipes de pilotage (Gouvernance) comprennent en moyenne 2 professionnels pour 1000 employés (mais 0,2 professionnels pour les très grandes structures au-delà de 20000 employés)

De manière générale, les plus petites entreprises paient plus (par employé) que les grandes…

Dans un marché en croissance (entre 5 et 10% selon les domaines et parfois plus dans certains pays), l'ensemble de ces dépenses, fondamentales, n'apparaissent au final pas « suffisantes » pour réduire le risque à un niveau cohérent avec l'augmentation de la menace (les pertes liées à la cybercriminalité sont évaluées en centaines de milliards de dollars) et de la pression réglementaire (nationale, internationale et sectorielle). A l'inverse, une étude d'Atlantic Council et Zurich Insurance (Sept. 2015[4]) tend à démontrer que les bénéfices de la transformation digitale (économies, fluidité, réactivité, etc.) s'équilibrent avec les coûts induits par la sécurité inhérente aux exigences des utilisateurs, consommateurs ou des régulateurs. N'atteint-on pas certaines limites ? Ne risque-t-on pas un effet « ciseau » ? C'est une question majeure pour les 5 prochaines années.

L'optimisation des dépenses doit donc s'engager avec plusieurs options potentielles qui ne s'appliqueront pas systématiquement, ni dans tous les contextes :

- Le rééquilibrage entre prévention / protection et détection / réaction (incluant l'anticipation)
- Le recours à des acteurs globaux (partenaires) dûment sélectionnés (au meilleur coût)
- Le développement de la sécurité « à la demande » limitant les investissements et lissant / modulant les coûts en fonction de volumes et de durées
- Et pour certains, l'externalisation des équipes dans un équilibre interne / externe à définir (encore souvent 50/50 dans les grands groupes) pour tenir compte des coûts élevés de recrutement et des tensions sur les salaires
- Et enfin, le recours à la cyber-assurance.

Ainsi, la cyber-assurance devient-elle plus qu'une option ? Une obligation ?

Les attaques, atteintes aux données personnelles / sensibles et infrastructures critiques, vols, fraudes, divulgations, etc. étant en augmentation constante, l'avantage reste (ra ?) à l'attaquant. La fuite en avant sur les dépenses de sécurité n'est sans doute pas la solution.

Les Etats-Unis ont, comme souvent, pris les devants (dès 2003 par l'Etat de Californie[5]). La déclaration d'une « cyber attaque » ou d'une fuite de données est obligatoire ; les impacts devant être dûment constatés et évalués. Les assurances, qui disposent de statistiques, ont construit des modèles financiers. En France, et plus généralement en Europe, les initiatives lancées en 2012-2013 n'ont pas donné les résultats escomptés. Appliquer des modèles US a des limites… Les capacités du marché sont désormais significatives (plusieurs centaines de millions d'euros) mais sans doute encore insuffisantes pour des cyber-attaques de grande ampleur (par exemple touchant les transports ou l'énergie).

Globalement, indépendamment des secteurs d'activité, le marché (hors individus) se structurerait en 4 grands domaines : les très grands groupes internationaux, le secteur public, les TPE pour qui la mutualisation peut être facilitée et les ETI avec des modèles à construire, sans doute au plan sectoriel. Les acteurs se cherchent encore en termes de contractualisation pour intégrer les risques « cyber » : adaptation de la couverture dommages,

[4] http://www.atlanticcouncil.org/news/press-releases/atlantic-council-zurich-insurance-report-finds-the-global-benefits-of-cyber-connectivity-expected-to-outweigh-costs-by-160-trillion-through-2030
[5] In 2003, California passed the Notice of Security Breach Act which requires that any company that maintains personal information of California citizens and has a security breach must disclose the details of the event.

responsabilité civile, fraude, risques informatiques, etc., voire création d'une police sur mesure (plus complexe à concevoir, plus simple à gérer).

En termes financiers, la question du risque maximum tolérable est posée et chacun peut avoir sa propre vision dans son contexte. Nous pouvons oser un ordre de grandeur[6] de 4 à 5% du chiffre d'affaire (ou du budget) étant difficilement supportable ou comme pouvant remettre en cause significativement l'activité d'une entreprise ou d'un organisme.

A ce titre, nous avons un cas concret pour expliciter les apports de la cyber-assurance : la société Target aux USA, victime d'une cyber-attaque ayant compromis ses systèmes de paiement et les données bancaires de ses clients. Son Directeur financier a dû s'expliquer devant le Sénat américain en février 2014. Benjamin Dean, de l'Université de Columbia a effectué une analyse[7] très détaillée de cette attaque, des impacts des fuites de données, des suites judiciaires et des aspects fiscaux. Au final, sur l'année 2014 la perte nette serait estimée à 0,1% du revenu, en raison notamment d'une réduction d'impôts significative liée à la baisse d'activité et d'une couverture d'assurance de 90M$...

Pour conclure, lier risques, maturité et coûts peut s'effectuer selon une échelle à 3 niveaux.

Le niveau Bronze (Baseline) est du ressort des équipes informatiques et du Responsable Sécurité du SI (RSSI, CISO) en incluant un responsable à la protection des données (CIL[8], DPO[9], CPO[10]). L'enjeu est de garantir la mise en œuvre uniforme de *« bonnes pratiques minimales et obligatoires»* au meilleur coût (en s'appuyant sur les normes et standards internationaux ou nationaux, des services managés à la demande, etc.). Afin surtout d'éviter le syndrome du maillon faible…

Le niveau Argent (Advanced) est à l'initiative des « métiers », en s'appuyant sur une fonction de Directeur des risques numériques (transverse, hors département informatique) et l'offre du marché (services) de plus en plus construite autour du Cloud. L'enjeu consiste, sur la base du niveau Bronze, à répondre aux exigences des clients et des régulations nationales ou sectorielles. Le financement étant - idéalement - intégré dans le modèle économique des métiers.

Le niveau Or (Premium) est du ressort des dirigeants et du Comité exécutif (et d'audit) avec, le cas échéant, le Risk manager. L'enjeu est de protéger les *« bijoux de la couronne »*, les actifs les plus critiques et de surveiller le respect des obligations réglementaires à fort impact médiatique, commercial ou juridique. Dans ce cas, le montant de l'investissement peut s'avérer « important », et doit être basé sur une analyse financière pointue, en lien avec l'assurance.

Les professionnels de la cybersécurité / cyberdéfense n'ont pas le choix qu'ils soient clients (secteurs privé et public) ou fournisseurs. Il leur faut intégrer plus fortement la dimension économique à leur champ de compétences. Un prérequis est de bien comprendre les modèles de coûts et d'assurance pour accompagner efficacement la transformation numérique des organisations publiques comme privées.

Le marché dans son ensemble devrait sans doute bénéficier, à terme, des obligations de notifications des cyber-attaques et des atteintes aux données …

[6] Exemple : pénalité prévue pour non-conformité à la réglementation européenne (GDPR)
[7] http://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570
[8] Correspondant Informatique et Libertés
[9] Data Protection Officer
[10] Chief Privacy Officer

ANNEXE

(types de dépenses selon le modèle Capgemini Sogeti)

ORGANIZATION		Internal	Out Sourced
Digital Risk Officer CSO / CISO / DPO office	Internal team (FTE) Correspondent network (FTE) Communication & Awareness (*) Community management Dashboard management (*)	✓	✓
Digital Risk Management	Risk analysis / matrix (*) Threat intelligence (*) Crisis management Cyber Insurance (*)		✓
Strategy & Planning	Strategy / Roadmap / Transformation Security & Privacy Program management Organization transformation		✓
Operations	Policies and procedures ISMS implementation / management (*) Training plan (*) Incident management & forensics	✓	✓
Assessment & Audit	Pen test (*) Vulnerability assessment (*) Code audit / Application security testing (*) Organization audit Compliance audit (*)	✓	✓

PROTECTION		HW	SW	Build / Run
Infrastructures	Firewalls, IDS, IPS, VPN Anti malware gateway NAC, Network segmentation, segregation Secure protocols, routing Hardware hardening	✓	✓	MSSP
End points	Security suite (FW, Anti malware, HIPS) Application management, Patch management IOCs discovery tool, remediation tool		✓	MSSP
User Id & Access	2FA device SSO & IAM Risk based authentication Privilege account management	✓	✓	MSSP
Applications	Secure coding lifecycle, OWASP review WAF, database firewall Security testing, pentesting Patch management Database hardening		✓	MSSP
Data	Laptop encryption Email encryption Tokenization & Data masking Data destruction Cloud encryption	✓	✓	MSSP

SUPERVISION		HW	SW	Build / Run
Infrastructures	Log management Sand boxing DNS supervision SIEM SOC CERT	✓	✓	MSSP
End points	End point Log management SOC	✓	✓	MSSP
User Id & Access	AD log management SOC	✓	✓	MSSP
Applications	Application log management Analytics and fraud management SOC	✓	✓	MSSP
Data	Data leak prevention SOC	✓	✓	MSSP