futuribles
INTERNATIONAL

Entreprises et cybersécurité à l'horizon 2020

cigref
Réseau
de Grandes Entreprises

Synthèse de l'étude

menée en 2013-2014

Le CIGREF s'est associé à Futuribles International pour mener cette étude, avec la participation et les contributions de grandes entreprises.

Elle a été réalisée en souscription. Les résultats complets sont donc réservés aux entreprises contributrices.

Cette synthèse présente les principales recommandations formulées au sein de l'étude globale.

Directeurs d'étude : Cécile Wendling puis François de Jouvenel,
et Nicolas Mazzucchi
Conseiller scientifique : Olivier Kempf

Association Futuribles International • 47 rue de Babylone • F-75007 Paris
Tél. + 33 (0)1 53 63 37 70 • Fax + 33 (0)1 42 22 65 54
E-mail mailto:mbprivey@futuribles.com• Site Internet www.futuribles.com

Pascal BUFFARD
Président du CIGREF

Le mot du Président du CIGREF

Construire une vision des enjeux stratégiques et des défis managériaux auxquels sera confrontée l'entreprise à l'horizon 2020, telle est l'ambition de notre dernière publication. Parmi ces 9 enjeux et défis, la maitrise des nouveaux risques numériques est au cœur de la transformation numérique de nos entreprises.

Investir pour préserver la sécurité et la compétitivité

S'il s'agit avant tout de tirer parti du numérique pour augmenter la compétitivité des entreprises, les risques numériques doivent dès lors être considérés à l'aune de la stratégie. La sécurité numérique fait partie intégrante du plan numérique de l'entreprise. Si l'on admet que la sécurité des flux est fondamentale pour la compétitivité des entreprises, l'investissement dans la sécurité des systèmes d'information devient alors une véritable priorité.

Redéfinir la création de valeur

La numérisation du business amène le système d'information à être directement impliqué dans la chaîne de valeur. Avec la « servicisation » et l'ouverture des entreprises sur leur écosystème, la fonction SI est incontournable pour assurer, non seulement la convergence et la cohérence du système d'information, l'agilité et l'innovation mais surtout sa sécurité !
Force est de constater que les entreprises ne disposent quasiment plus de fonctions essentielles indépendantes du système d'information : dès lors, toute faille majeure peut se transformer en une grave crise tant pour l'image que pour la performance opérationnelle, synonyme dans les deux cas de destruction de valeur.

Sensibiliser

En matière de sécurité, les entreprises doivent travailler à la fois sur les aspects techniques, mais également sur la formation, la sensibilisation des dirigeants et l'information des collaborateurs sur les risques liés au numérique et à ses usages. Le CIGREF mène de nombreuses actions en ce domaine :

- Création d'une formation (labélisée par l'ANSSI) « Sureté des usages numériques » avec l'INHESJ
- Développement d'un serious game « *Keep an Eye Out* »
- Information des Administrateurs de sociétés sur les risques numériques en collaboration avec l'IFA.
- Participation au groupe de travail de l'ANSSI dans le cadre du Plan 33 sur la cyber sécurité.
- Création d'un Cercle « Cyber sécurité » ouvert aux Dirigeants de nos entreprises.

Anticiper

Telle est notre dernière contribution : **Entreprises et Cyber sécurité à l'horizon 2020** !
Nous avons mené cette étude prospective avec Futuribles international en y associant plusieurs entreprises et organisations durant l'année 2014.
Notre but était d'anticiper les « futurs possibles » de nos environnements dans le but de mieux concevoir nos stratégies de cyber sécurité. Il ressort des 6 scénarios globaux de l'étude une série d'enjeux et de recommandations transverses liés aussi bien à l'organisation interne des entreprises qu'à leurs relations avec les parties prenantes.

Affirmant notre rôle de « *carrefour d'informations, de réflexions et d'échanges sur l'entreprise dans le monde numérique* », Le CIGREF est heureux de mettre à disposition de tous, ce document de synthèse. Il servira de base à l'organisation d'un prochain colloque sur ce thème.

Paris, février 2015

SYNTHÈSE DE L'ÉTUDE

Les risques cyber évoluent vite, obligeant les entreprises et les administrations publiques à réagir sur des temps très courts. Néanmoins, une approche uniquement réactive des questions de cybersécurité est préjudiciable à la mise en œuvre de stratégies efficientes sur cette question.

L'étude réalisée par Futuribles International a pour ambition de replacer les enjeux de cybersécurité dans une perspective systémique et stratégique de moyen terme qui soit utile à la mise en place de stratégies de réduction des risques à différentes échelles (États, entreprises, individus). Le but de cette étude est donc de proposer aux organismes qui y ont participé une vision claire et documentée des évolutions possibles de leur environnement d'ici 2020 qui leur soit utile pour concevoir leurs stratégies de cybersécurité.

UNE PROBLÉMATIQUE STRATÉGIQUE

L'appréhension du cyberespace par les entreprises relève souvent d'une dimension technique confiée aux DSI et RSSI. La place centrale que prend le cyberespace dans la vie de chacun comme dans le *business* des entreprises conduit à placer cette problématique au cœur de la vie des entreprises, en dépassant la seule approche technique.

Plusieurs éléments semblent centraux dans cette problématique de la cybersécurité des entreprises :

— Le rôle qui est accordé aux données dans les entreprises, qu'il s'agisse d'une question de stockage, de protection ou de valorisation.

— La place des utilisateurs au cœur des préoccupations liées à la cybersécurité en entreprise : qu'il s'agisse des collaborateurs de l'entreprise, de ses clients ou de ses partenaires, les utilisateurs jouent un rôle majeur dans l'appréhension du cyberespace et constituent le premier maillon de la chaîne de risque comme de protection.

— Enfin, la question de la conflictualité dans le cyberespace, depuis la cyberguerre, tant décrite mais non encore advenue, jusqu'au terrorisme, en passant par l'« hacktivisme » et la cybercriminalité en plein développement, touche de plus en plus les entreprises.

Le croisement des problématiques technologiques, sociales, politiques et économiques amène à envisager l'entreprise comme acteur dans un contexte étendu, en interaction avec de nombreux autres (utilisateurs, États, mafias, hacktivistes, lanceurs d'alerte, etc.). Il est donc nécessaire d'analyser les interactions entre ces différentes variables pour comprendre les évolutions potentielles du cyberespace et être à même de formuler des recommandations adaptées aux situations envisagées. Ce travail devrait permettre aux entreprises d'accroître leur compréhension de l'écosystème cyber, d'anticiper les changements à venir et donc de gagner en marge de manœuvre. Ainsi, elles auront la capacité de devenir des acteurs du cyberespace et d'établir une cyberstratégie globale.

UNE APPROCHE SYSTÉMIQUE ET PROSPECTIVE

Du fait de la multiplicité des éléments qui peuvent avoir des conséquences sur le cyberespace, aussi bien humains que techniques, organisationnels ou géopolitiques, celui-ci paraît pouvoir évoluer dans de nombreuses directions. La démarche prospective suivie

dans cette étude a permis d'identifier et d'étudier les principales variables susceptibles d'avoir une influence cruciale pour l'avenir de la cybersécurité des entreprises, puis de construire des scénarios d'évolution qui illustrent le champ des évolutions possibles. Ces scénarios dressent un panorama structuré des grandes tendances et des multiples incertitudes inhérentes à l'avenir du cyberespace. Ils constituent des cadres utiles à l'évaluation des stratégies de cybersécurité et à la conception de stratégies cyber efficientes.

Vingt-deux variables ont été jugées déterminantes pour appréhender les avenirs possibles de la cybersécurité des entreprises. Elles ont toutes donné lieu à un travail de réflexion prospective étayé permettant de révéler leurs possibilités d'évolution.

Ces variables relèvent de trois composantes principales : « Menaces », « Vulnérabilités et opportunités » et « Environnement extérieur ». Les composantes « Menaces » et « Environnement extérieur », qui touchent aux aspects externes à l'entreprise, ont permis d'analyser les différents déterminants sur lesquels les entreprises ont peu de marges de manœuvre, mais auxquels elles doivent pouvoir s'adapter. La composante « Menaces » s'articule autour des acteurs non commerciaux comme les États ou les groupes criminels, mais comprend également les phénomènes naturels et les aléas climatiques qui peuvent bouleverser l'appréhension du cyberespace par les entreprises. La composante « Environnement extérieur » analyse les différentes évolutions possibles du cadre législatif ou de la technologie. Elle a permis d'appréhender les évolutions globales du cyberespace qui peuvent avoir de lourdes conséquences pour les entreprises, qu'il s'agisse d'une évolution spatiale vers des pays pour l'instant peu connectés, de changements dans la gouvernance d'Internet, ou encore de ruptures dans le marché de la sécurité informatique. La composante « Vulnérabilités et opportunités », quant à elle, a permis de saisir les différentes problématiques directement liées à l'entreprise, dans son organisation interne comme dans ses liens avec des fournisseurs immédiats de solutions. Sur la base d'entretiens menés au sein des entreprises membres de l'étude, les questions de la place de l'informatique dans la structure, de l'appréhension du cyberespace et des éléments qui lui sont liés comme le stockage des données ou le nomadisme des utilisateurs, ont été abordées selon une grande série de paramètres pour les comprendre aussi finement que possible.

Ces différentes variables et les scénarios intermédiaires (microscénarios) construits sur chacune des trois composantes mettent en avant le caractère de plus en plus stratégique du cyberespace pour les entreprises. La volonté d'offrir un spectre large d'étude, depuis l'évolution géographique d'Internet jusqu'aux solutions de gestion de l'identité numérique, si elle rend l'analyse plus complexe, offre également un panorama global et systémique des évolutions du cyberespace, traduit, *in fine*, en six scénarios d'ensemble.

LES RECOMMANDATIONS

Il ressort des six scénarios globaux de l'étude une série d'enjeux et de recommandations transversales liés aussi bien à l'organisation interne des entreprises, qu'à leurs relations avec les parties prenantes.

- **Accompagner le changement du métier de RSSI** : dans la majorité de nos scénarios, le cyberespace occupe une place de plus en plus importante dans la société et donc dans les entreprises. Ainsi, les domaines de compétences des RSSI pourraient s'élargir. En effet, si l'ensemble des directions ou des services de l'entreprise intègrent une dimension cyber à leur activité, le RSSI pourrait voir s'ajouter à ses fonctions sécuritaires une dimension stratégique qui engloberait la cybersécurité, mais également la cyberdéfense et la mise en place d'une cyberstratégie économique. Le RSSI deviendrait ainsi le responsable de la stra-

tégie des systèmes d'information. Les questions de protection et de valorisation des données seraient au cœur de cette cyberstratégie. Ainsi, d'un service souvent cloisonné et parfois en marge des autres départements de l'entreprise, la SSI pourrait occuper une place plus centrale dans la stratégie et œuvrer de concert avec les autres services de l'entreprise. Il faut donc créer les conditions favorables à cette synergie et former les RSSI à ces compétences élargies.

◗ **Garder un contrôle de la cybersécurité en interne** : plusieurs des scénarios mentionnent une perte de contrôle totale ou partielle des entreprises sur leur propre cybersécurité, soit parce qu'elles n'ont pas les compétences pour la traiter en interne, soit parce qu'un acteur a pris une importance croissante et a acquis le monopole sur cette activité (on pense ici à Google par exemple). En outre dans un cadre où de nombreuses entreprises font appel à des prestataires externes pour leur cybersécurité, il appartient d'être particulièrement vigilant sur le choix de ces partenaires, d'autant plus que le marché apparaît dominé par des acteurs non européens (américains ou israéliens notamment) dont les liens avec leur État sont parfois marqués. Pour éviter ce genre de désagrément, les entreprises doivent multiplier les dispositifs leurs permettant de maîtriser la chaîne de valeur. Les entreprises peuvent travailler en collaboration avec les pouvoirs publics pour développer des solutions informatiques sécurisées et labellisées, mettre en place un système efficace de contrôle des infrastructures (audit) : pour cela, la collaboration avec des intermédiaires entre entreprise et État comme l'ANSSI est cruciale. Les offres de cybersécurité doivent être coconstruites par les entreprises et les États, elles doivent concerner l'ensemble de la chaîne de production afin d'inspirer de la confiance au client final.

◗ **Faire de la donnée un élément central de la stratégie des entreprises** : nous l'avons vu tout au long de nos travaux, la gestion de la donnée (protection et / ou valorisation) occupera une place cruciale dans les stratégies d'entreprises. Ainsi, les entreprises devront s'intéresser aux nouveaux métiers liés à la donnée (*chief data officer*, *data scientist*, etc.), réfléchir à l'insertion de ces nouveaux métiers dans leur organisation actuelle. Pour cela, elles devront créer un référentiel de compétences au sein de l'entreprise qui lui permettrait de chiffrer ses besoins actuels et à venir. La mise en place de ces nouvelles compétences au sein de l'entreprise pourrait lui permettre d'obtenir une cartographie précise de ses données mais également des différentes manières possibles de les valoriser ; ceci allant jusqu'à la transformation du *business model* de l'entreprise autour de ces dernières.

◗ **Mettre en place des plates-formes d'information et des outils d'alerte des agressions cyber** : dans le domaine du cyber, nous avons vu que les entreprises et les États travaillaient souvent de manière isolée à la détection et à la résolution des problèmes et des failles causées par les cyberagressions. La mise en place de plates-formes d'information communes entre entreprises d'un même secteur, mais également entre les entreprises et l'État, permettrait d'avoir une vision plus globale des cybercriminels, d'identifier plus facilement les données sensibles (celle qui sont recherchées par les cybercriminels), d'élaborer des systèmes de protection communs, d'améliorer la détection des agressions et de trouver plus aisément la source de ces agressions. Ces plates-formes aideraient également l'État à mettre en place une stratégie de cyberdéfense voire de cyberagression plus élaborée.

◗ **Développer une veille sociétale** : nous avons vu dans nos scénarios que la société civile serait probablement amenée à jouer un rôle de plus en plus important dans le cyberespace. Les individus peuvent plus facilement comprendre et interagir avec les entreprises, mais ils ont aussi désormais des moyens de s'opposer frontalement à ces dernières en portant atteinte à leur image (atteintes à l'e-réputation), en mettant en place des systèmes économiques alternatifs hors des canaux des entreprises (économie de l'échange et du partage, monnaies alternatives, etc.). La nécessité pour les entreprises de mettre en place une veille

sociétale au sein de leurs structures afin de déterminer les grandes tendances et de gérer au plus près la relation avec les individus et les groupes, pourrait devenir un enjeu majeur dans les années à venir. Ainsi, les entreprises pourraient accroître leurs services liés à la veille, à l'intelligence économique, à la prospective. En ce sens, elles pourraient approfondir cet aspect avec l'ANSSI qui a un rôle d'alerte sur ces sujets.

- **Renforcer la législation européenne, notamment sur le stockage et la protection des données :** l'étude a mis en avant la place centrale que devrait prendre la donnée dans les années à venir eu égard à l'évolution du *business model* de certaines entreprises. Dans ce cadre, il apparaît important d'engager des actions de *lobbying* au niveau européen pour renforcer la règlementation sur ce point. En effet, la place prégnante des acteurs GAFA dans les services aux entreprises relatifs au stockage et à la gestion des données peut entraîner des dérives diverses s'il n'existe pas un cadre législatif strict. De la même manière que dans des pays comme la Russie ou la Chine, une obligation légale de stocker physiquement les données des entreprises européennes dans des serveurs positionnés sur le sol européen réduirait les incertitudes liées au caractère transatlantique des principaux acteurs.

- **Renforcement de la R&D** : la question de la dépendance technologique et de l'avance de certains pays en ce domaine est ressortie comme l'un des éléments prégnants de cette étude. L'avance prise par les acteurs américains — et le développement rapide des émergents dont la Chine avec Huawei et ZTE — amène à considérer la dépendance technologique des entreprises européennes comme un risque. En effet, depuis l'affaire PRISM, il a été prouvé que la coopération entre entreprises du secteur IT et État dans un but d'espionnage, y compris économique, était une réalité. Dans ce cadre, il apparaît nécessaire d'encourager le développement technologique en France et en Europe, non seulement au cœur des entreprises mais également en favorisant la naissance d'une base industrielle et technologique cyber, y compris via des *clusters* associant entreprises, État et centres de recherche.

- **Développer la culture cyber** : au cours de notre étude, les utilisateurs ont été un sujet récurrent. En effet, le déploiement de la cybersécurité en entreprise passe par le développement d'une profonde culture cyber au sein de l'entreprise mais également au sein de la société dans son ensemble. Ainsi, la formation à la sécurité informatique devrait être intégrée à l'ensemble des programmes scolaires. Par ailleurs, les entreprises et les pouvoirs publics devraient travailler de concert pour développer de nouvelles formations adaptées aux besoins cyber des entreprises. Cette coopération pourrait prendre la forme de pôles d'excellence, de *clusters* regroupant universités, centres de recherche et entreprises. Les entreprises devraient s'impliquer activement dans la formation en intervenant plus directement (cours, séminaires, colloques, etc.) et en agissant en partenariat avec les universités pour la définition des programmes de formation. Afin de susciter des vocations dans le domaine du cyber, les entreprises doivent également offrir des parcours de carrière clairs et attrayants. Au sein des entreprises, l'implication des salariés dans le domaine de la cybersécurité est également cruciale, les enjeux doivent être connus de tous et l'hygiène informatique doit faire partie des comportements à adopter en entreprise à tous les niveaux. Pour cela, la formation continue aux risques cyber ainsi que l'intégration active de la SSI dans les autres activités sont des pistes d'action que les entreprises peuvent commencer à mettre en place.

Cette étude replace les enjeux de cybersécurité dans une perspective systémique et stratégique de moyen terme. Elle n'atteindra son objectif que si les entreprises et les acteurs publics se saisissent de ces travaux pour nourrir leur propre réflexion stratégique de cybersécurité en intégrant la dimension du temps long.