Pierre-Luc **RÉFALO**

La sécurité numérique de l'entreprise

L'effet papillon du hacker

EYROLLES

Une approche innovante de la sécurité numérique

Dans une société hyper concurrentielle, les entreprises dépendent très fortement de leurs systèmes d'information et d'Internet. Confrontées à de multiples attaques cybercriminelles, elles doivent relever le défi de la sécurité numérique. Mais alors :

- Comment démêler les questions sociologiques des évolutions technologiques et des enjeux juridiques ?
- Quels sont les risques majeurs et comment évaluer les menaces pour mieux se protéger ?
- Comment peuvent s'adapter les décideurs ?
- Comment doivent évoluer les pratiques de management en termes de gouvernance et d'économie de la sécurité globale ou d'implication des utilisateurs ?

Cet ouvrage analyse l'ensemble des démarches et outils indispensables pour un management innovant de la sécurité numérique. Il apporte aussi aux entreprises les clés pour une meilleure protection de l'information sensible dans un environnement complexe. Son approche stratégique est avant tout pragmatique, pour permettre de mieux maîtriser les risques numériques et d'anticiper les cyber-attaques.

Créateur et dirigeant d'entreprises, **Pierre-Luc Réfalo** est conseil-expert en sécurité numérique auprès des entreprises. Il a été représentant au G8 et à la Commission européenne sur le cybercrime, la signature électronique et la vie privée. Il est membre du Comité de pilotage des Assises de la sécurité et des systèmes d'information et auteur des Livres bleus publiés à cette occasion depuis 2004.

barbaryourte.com | Photo de couverture : phovoir.fr

Code éditeur : G55525
ISBN : 978-2-212-55525-7

La sécurité numérique de l'entreprise

L'effet papillon du hacker

Groupe Eyrolles
61, bd Saint-Germain
75240 Paris cedex 05

www.editions-eyrolles.com

ISBN : 978-2-212-55525-7

Pierre-Luc RÉFALO

La sécurité numérique de l'entreprise

L'effet papillon du hacker

EYROLLES

Sommaire

Avertissement

Cet ouvrage n'aborde pas la question de la sécurité des systèmes d'information (SSI) de manière conventionnelle. L'approche n'est ni stratégique, ni technique ou opérationnelle, ni méthodologique voire juridique. Elle se veut pragmatique et surtout tactique. Elle s'appuie sur mes vingt ans d'expérience dans le domaine. Je poursuis les réflexions et les travaux présentés dans *Sécuriser l'entreprise connectée*[1] en 2002.

Centré sur l'entreprise, le propos n'exclut pas l'État et l'Europe et encore moins les individus (professionnels de la sécurité, dirigeants, managers, informaticiens, salariés, étudiants et citoyens). Chacun trouvera, je l'espère, des éléments qui l'intéresseront dans son contexte propre et selon son niveau de connaissance et d'appétence pour le sujet.

Le contenu s'appuie essentiellement sur les Livres bleus des Assises de la sécurité et des systèmes d'information auxquels j'ai eu l'honneur de participer depuis 2004. Ces travaux ont été menés en trois grandes phases : une phase d'exploration et d'introspection en trois temps a traité le *management stratégique des cyber-risques* (2004), *les indicateurs et tableaux de bord en sécurité SI* (2005), *les grands défis des professionnels de la sécurité SI* (2006). Puis, une phase d'ouverture et de découverte en deux étapes a étudié *les pouvoirs en sécurité/sûreté* (2007) et *la sécurité globale* (2008). Enfin, une phase de maîtrise et de professionnalisation en deux étapes a analysé *la culture des risques informatiques/informationnels* (2009) puis *la dimension économique de la sécurité des systèmes d'information* (2010).

Les questions de nature socio-économique abordées en 2009 et 2010 ont été approfondies dans le cadre d'un groupe de travail sur la fonction sécurité SI (SSI) et sur l'économie de la SSI mis en place depuis juin 2010 au sein du Cercle européen de la sécurité et dont les principaux enseignements seront également repris. En 2011, nous avons enfin transcendé l'ensemble de la dialectique autour d'une question de fond sur le secret et la confidentialité à l'ère du numérique.

---

1. Éditions d'Organisation, octobre 2002 (disponible en e-book).

À l'issue de ces huit années de travail, l'ensemble des documents représente près de 400 pages d'analyses, de questionnements et de recommandations qui restent, pour beaucoup, d'actualité et qui sont repris, mis à jour ou approfondis.

Préambule

« Lorsque le passé n'éclaire plus l'avenir,
l'esprit marche dans les ténèbres. »

Alexis de Tocqueville

L'effet papillon du hacker

19 mars 1999, Washington – 9 heures heure locale.

Un jeune Américain de 18 ans, Jay Satiro, est arrêté par le FBI pour s'être introduit frauduleusement sur le réseau d'AOL. Les préjudices sont estimés à 50 000 dollars malgré un discours rassurant du porte-parole sur l'absence d'impact pour les clients. Pour lui, l'intrusion « *... should mean absolutly nothing for AOL members*[1] ». Quelques instants plus tard, l'AFP répercute l'information en France. Cet événement va entraîner des conséquences qui n'auraient peut-être jamais permis l'écriture de ces lignes.

Vers 17 heures à Paris, un courriel de la vice-présidente d'AOL en charge des questions de sécurité m'informe qu'elle ne pourra venir à Paris pour assurer la conférence d'ouverture du Forum Eurosec organisé par XP Conseil, à l'époque, leader du conseil en sécurité des systèmes d'information. J'ai rencontré Tatiana quelques mois plus tôt dans le cadre des échanges avec mes homologues au sein des actionnaires de Cegetel (devenu SFR) qui m'employait à l'époque. Je lui propose de venir en France lors de la prochaine conférence Eurosec. Mariée à un Français, elle ne dit pas non ! Coup dur pour les organisateurs car il faudra d'urgence trouver un remplaçant sur un thème qui reste d'actualité : « Adapter la sécurité aux priorités de son entreprise ». Cette ouverture internationale avec un acteur majeur d'Internet était très attendue. Petite gestion de crise où tous les scénarios sont étudiés. Tatiana me propose bien de faire l'intervention à sa place avec sa présentation. Problème : Cegetel est actionnaire minoritaire d'AOL France et quelle légitimité aurais-je à porter la parole d'un leader américain de l'Internet ? Et traduire ou transposer le discours *AOL worldwide* dans le contexte français sonnerait sans doute un peu faux.

1. « ... n'aurait absolument aucun impact pour les membres d'AOL. »

À 19 heures la solution est trouvée, en accord avec la direction de la communication, la DRH et ma hiérarchie : j'assumerai la conférence d'ouverture en tant que directeur du programme sécurité de l'information de Cegetel. Il me faut maintenant élaborer un discours. Nous sommes vendredi soir, et demain toute la famille est à la maison pour fêter les 3 ans de mes filles. Nouveau dilemme : est-ce que je prépare mon intervention au bureau ou à la maison en pleine réunion familiale ? Après discussion avec mon épouse, le choix est vite fait : pas de travail ce week-end ! Je me lance donc dans la préparation d'une intervention délicate mais au demeurant intéressante.

Vers 22 heures, je quitte la Défense en taxi. Quinze minutes plus tard, un chauffard de 18 ans lui aussi, roulant à 140 km/h sur le périphérique, nous percute par l'arrière. Bilan : un mort, deux blessés graves et moi plus légèrement malgré un double coup du lapin. La lumière qui s'éteint par deux fois. Mais elle est revenue ! Je sors du taxi alors que le moteur prend feu. Après une heure de soins sur le tarmac avec un périphérique bloqué, puis deux heures aux urgences d'Antoine-Béclère à Boulogne-Billancourt, je rentre chez moi, un hématome au front et une minerve pour soutenir mes cervicales. Il est 2 heures du matin. La vie est belle (malgré tout) ! Lundi matin, j'assumerai l'ouverture d'Eurosec 1999…

L'humain : clé de toute question de sécurité

L'acte « criminel » du pirate américain l'a-t-il vraiment été ? Est-il à l'origine de la mort de ce chauffard de la route ? Nul ne le sait vraiment. Ce qui est sûr, c'est qu'il aura engendré cinq situations d'urgence voire de crise : pour AOL d'abord avec une enquête rondement menée avec le FBI. Pour les organisateurs d'Eurosec aussi, obligés de revoir leur programme à la dernière minute. Pour Cegetel également, contraint de trouver une solution de remplacement. Pour moi, au cœur des discussions, devant traiter un conflit familial potentiel et me préparer à assumer une intervention publique trois jours plus tard devant 200 professionnels de la sécurité. Pour la sécurité civile enfin, qui répondra efficacement à ce drame de la route, tant psychologiquement que médicalement.

Vie professionnelle, vie publique, vie privée se sont entrechoquées en l'espace de cinq heures ce soir de mars 1999 parce qu'un pirate informatique s'intéressait de trop près aux données personnelles des clients d'AOL. Ou pour son « *quart d'heure de gloire* », prédit par Andy Warhol dans les années 70 ? Pour son frère : « *Jay is a genious !* » Pour d'autres ce n'est pas si sûr…

Cet événement m'a fait beaucoup réfléchir sur le sens de l'engagement et sur les métiers de la sécurité des systèmes d'information. Entre Tatiana qui mène l'enquête avec le FBI et moi qui dois intervenir lors d'une conférence pour expliquer que la sécurité n'intéresse les dirigeants que si elle s'inscrit dans une logique « business », l'écart semble gigantesque. Approche « secrète » de l'enquête d'un côté, « publique » d'une action de communication de l'autre. Gravité d'une gestion de crise d'un côté, action de promotion et de formation lors d'une conférence professionnelle de l'autre. Eh bien non : car tout est lié !

La globalisation : source d'une complexité croissante et de risques grandissants

À la fin du siècle dernier déjà, la question de la *sécurité globale* était posée et largement débattue dans le cadre des réunions du G8 sur la *cybercriminalité* où je représentais Vivendi Universal au sein de la délégation française. L'informatique, les réseaux, Internet sont au cœur du développement de la société de l'information et toute atteinte à des infrastructures critiques peut avoir comme origine et/ou comme cible des ordinateurs, des réseaux, des services en ligne ou des données sensibles.

À l'époque, les systèmes financiers, les transports, l'énergie et les télécoms sont les quatre domaines les plus critiques. Les terroristes, les pédophiles et les pirates de musique sont surtout dans la ligne de mire. Une convention « Cybercriminalité » du Conseil de l'Europe sera d'ailleurs signée en 2001 par une trentaine de pays rejoints en dix ans par une petite vingtaine seulement. Les enjeux : pénalisation des « cybercrimes » et coopération judiciaire internationale pour arrêter les criminels. Une approche étatique et juridique, certes nécessaire mais surtout répressive, sur le long terme (pour sa mise en œuvre) et qui ne répond à l'évidence pas aux enjeux culturels et sociaux voire économiques.

2002 : les messages clés de *Sécuriser l'entreprise connectée*

En 2002, je quittais Cegetel/SFR après quatre ans d'une expérience d'une grande richesse en plein boom des télécoms mobiles. Sans prétention – car le contexte s'y prêtait –, j'ai parfois l'impression d'avoir eu la chance de pouvoir faire, avec les équipes de l'opérateur privé, autant si ce n'est plus, en quatre ans, que certains RSSI en dix ans. Je prends alors mon bâton de pèlerin pour m'engager sur le volet éducatif. Je crée Comprendre et Réussir, non sans avoir livré à la profession un premier ouvrage, *Sécuriser l'entreprise connectée*, qui demeure à bien des égards d'une grande pertinence. Dans la conclusion, je proposais aux lecteurs, professionnels de la sécurité et décideurs, dix orientations[1] que je reprends ici.

1. *Sécuriser l'entreprise connectée*, *op. cit.*, p. 360-362.

Dix orientations possibles

Revenez aux fondamentaux

Cette première orientation, énoncée en 2002, fait étrangement penser au *back to basics*[1] de Patrick Pailloux, directeur général de l'ANSSI[2], lors de la séance de clôture des Assises de la sécurité en octobre 2011. La sécurité est un mal nécessaire ! Chaque individu se passerait de ses contraintes et de ses coûts. La réalité nous oblige malgré tout à être acteur. Pourquoi ? Tout simplement parce que deux enjeux majeurs doivent animer en permanence les démarches : la protection des libertés individuelles, notamment la vie privée, et la protection du patrimoine et des biens nous obligent à être des acteurs responsables. Être responsable signifie se déterminer au niveau de l'art de la gestion des risques. Est-ce qu'on privilégie la maîtrise des vulnérabilités dans une approche « qualité » ou est-ce qu'on s'attache davantage aux menaces en veillant aux potentialités et aux réalités des attaques et des fraudes ?

Pilotez par objectifs…

… en adaptant en permanence les structures. La sécurité informatique nous a appris à cibler les objectifs en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité. Ce paradigme doit être revu : plus que de disponibilité, c'est d'accessibilité et de performance ; plus que d'intégrité, c'est d'authenticité, de fiabilité, d'utilité, voire de pertinence ; plus que de confidentialité, c'est de propriété et de partage qu'il convient désormais de parler. Pour les domaines historiques, ce sont donc plus des questions de qualité que de sécurité qui nous intéressent aujourd'hui. Que reste-t-il alors des risques informatiques ? En quoi consiste désormais la cybersécurité ? Est-ce de la véritable gestion de risques ou bien de la qualité ? Est-ce bien investir ou ne pas dépenser ?

---

1. Dans son discours de clôture des Assises de la sécurité 2011, le directeur général de l'ANSSI avait dénoncé une « *sécurité cache-sexe* » et « *essentiellement technique* » par manque de respect de principes fondamentaux (« *règles d'hygiène élémentaires* ») par les informaticiens. Voir www.ssi.gouv.fr.
2. Agence nationale à la sécurité des systèmes d'information. Rattachée au Premier ministre au sein du SGDNS (Secrétariat général à la Défense nationale et à la sécurité).

Élaborez plusieurs politiques…

… en clarifiant les objectifs et les cibles. Si l'on a longtemps parlé de politique de sécurité, il convient désormais d'élaborer des politiques s'appuyant sur une charte d'entreprise et des guides de bonnes pratiques et de management. Ces derniers reposeront utilement sur les standards internationaux émergents. Les divergences d'intérêts et la complexité des contextes obligent à réduire le champ d'action des politiques à des enjeux précis, des activités ou des entités dûment identifiées.

Revoyez les moyens d'action…

… en vous recentrant sur le facteur humain. Les professionnels structurent les plans d'action en termes de prévention et de protection et, plus rarement, de détection et de réaction. […]

Ouvrez-vous à l'environnement et à ses risques

L'entreprise et l'administration ne sont plus des sanctuaires. Un domaine sensible comme la sécurité doit vivre sa révolution et s'ouvrir aux partenaires et aux concurrents. Partager sur ses bonnes et mauvaises expériences possède des avantages et des inconvénients. Les premiers dépassent désormais largement les seconds. Pouvoir disposer de retours d'expérience de tiers, de chiffres et de statistiques fiables et globaux nécessite que les entreprises, les offreurs, les associations et l'État coopèrent intelligemment.

Repensez les architectures techniques

Prenez des risques ! Les moyens actuels sont trop complexes et trop nombreux. Concentrer les mécanismes qui s'adressent aux infrastructures, aux services et aux contenus et préparer les plates-formes « cryptographie » et « contrôle/surveillance » sont les véritables enjeux. […]

Investissez dans les hommes

Les entreprises devraient pouvoir consacrer 10 % de leur budget de logiciels et matériels en formation de leurs collaborateurs. En fait, il serait plus intelligent de dépenser autant en formation qu'en moyens techniques. [...]

Responsabilisez trois acteurs

L'essentiel est de savoir qui, en interne ou en externe, anticipe sur l'émergence des risques, élabore les règlements pertinents et conçoit les solutions adaptées. [...]

Sous-traitez tout ce qui n'est pas stratégique

Le marché offre pratiquement tous les services possibles aux entreprises. Elles ont tout intérêt à se retourner vers des prestataires de qualité et expérimentés. [...]

Préparez-vous au pire

Quoi que nous fassions, les fraudeurs et pirates auront toujours un temps d'avance. Ils disposent désormais au sein de groupes organisés, parfois d'essence criminelle, de moyens importants et d'une motivation très forte. Se préparer au pire consiste avant tout à identifier des scénarios d'incidents types et à mettre en place des processus de gestion de crise formels et opérationnels.

2002 : la cybersurveillance naissante

Au-delà de ces dix orientations dont beaucoup restent d'actualité tout en devant être révisées et actualisées, la principale conclusion de l'ouvrage se focalisait sur l'émergence de la *cybersurveillance*. Maître Yves Bismuth avait alors apporté un éclairage d'une formidable perspicacité.

« *La surveillance du réseau se déforme pour devenir une surveillance par le réseau. Ne pas y résister serait accepter une fausse liberté et une vraie atteinte à nos droits essentiels qui fondent notre identité humaine. Il est alors d'une importance cruciale de souligner que les droits fondamentaux de la personne humaine, énoncés à l'issue de la Seconde Guerre mondiale et à l'aube de l'ère de l'informatique, ne doivent pas être remis en question par une politique sécuritaire sans limites [...].*

Ainsi, l'entreprise, comme la société, devra faire, pour l'avenir et la sauvegarde de nos libertés, un choix fondamental entre un monde de défiance et un monde de confiance. Toutes les formes de clandestinité sont en effet à proscrire : celle de l'abus numérique par le salarié comme celle liberticide de sa surveillance déloyale. Chacun doit alors apprendre à prôner la jouissance paisible d'Internet. Mais il reste dès lors aux juges à explorer cette notion encore nouvelle en notre droit : celle du caractère raisonnable d'une attitude.

"Si tu es prêt à sacrifier un peu de ta liberté pour te sentir en sécurité, tu ne mérites ni l'une ni l'autre", *écrivait Thomas Jefferson.*

*Il est sûr que les chartes, droits et autres déclarations ne suffiront pas à nous préserver des dangers d'une information par trop libertaire : la mondialisation économique et financière, la globalisation des techniques, les flux transfrontières des données commandent le recours à l'éthique, une forme d'*habeas data *à l'échelon planétaire.*

Utopie, me direz-vous, mais il est parfois bon de s'en nourrir pour ne pas y succomber car alors, mais alors seulement, ne pourra se réaliser la prophétie de Paul Valéry : "Il faudra bientôt construire des cloîtres rigoureusement isolés, où ni les feuilles, ni les ondes n'entreront... On y méprisera la vitesse, le nombre, les effets de masse, de surprise, de contraste, de nouveauté et de crédulité. C'est là qu'à certains jours on ira, à travers les grilles, considérer quelques spécimens d'hommes libres[1]." »

1. Paul Valéry, *Regards sur le monde actuel.*

Par un heureux hasard, mon premier ouvrage se terminait par ces deux mots merveilleux : « *hommes libres* ». L'humain et la liberté, les deux idéaux pour lesquels il ne peut y avoir de sens dans tout combat, quel qu'il soit.

Je m'étais promis de poursuivre et de compléter ce premier travail, la maturité et l'expérience en plus. Je propose donc en 2012 *La sécurité numérique de l'entreprise*, un titre marquant à la fois une continuité (autour de l'entreprise) et une évolution majeure (le poids du numérique dans la société du XXI^e siècle).

2002-2012 : déjà dix ans…

En dix ans, les usages du numérique se sont démocratisés. Sous le double effet de la baisse des coûts et de l'avènement de la génération Y avide de *connectivité permanente* (réseaux sociaux et smartphones)[1].

En dix ans, de « connectée », l'entreprise est devenue « *numérique* ». Renforçant le pouvoir des métiers et des utilisateurs face à une direction des SI souvent jugée dépensière et aux projets/services parfois inopportuns. En parallèle, la *vulnérabilité* de l'entreprise s'est accrue par sa dépendance au numérique et les ouvertures de plus en plus larges allant jusqu'aux systèmes industriels et techniques reliés à Internet.

En dix ans, le marché de la sécurité numérique n'a pas connu les crises et s'est considérablement développé profitant sans doute plus aux éditeurs qu'aux prestataires. Entre offreurs « juges et partis » trop nombreux, des consolidations inévitables devront encore avoir lieu.

En dix ans, la profession a été submergée par de nouveaux textes plus ou moins directement liés à la sécurité numérique : piratage en ligne et droits d'auteur, sécurité intérieure, confiance dans l'économie numérique, données à caractère personnel, etc. Une tendance qui pose la question d'un « code du numérique » à vocation internationale comme pour le transport maritime ou le transport aérien.

1. Selon une étude du cabinet MacKinsey, l'économie numérique (liée au Web) a représenté en 2009 3,2 % du PIB français (60 milliards d'euros) et est montée à 3,7 % en 2010 (72 milliards d'euros). Elle devrait atteindre 5,5 % en 2015 (129 milliards d'euros).

En dix ans, à l'heure du *cloud computing* et de la mobilité, les professionnels en charge de la sécurité des SI sont parfois passés du « technicien » empêcheur de tourner en rond au « stratège » apporteur de solutions concrètes. Une évolution qui pose la question des définitions d'emploi et de la *professionnalisation* du secteur, finalement très peu et mal représenté *via* des structures associatives ou non vraiment trop nombreuses (voir conclusion).

En dix ans, la cybercriminalité s'est organisée et professionnalisée, passant du « ludico-cupide » au « stratégico-économique », dans une sorte de *cyberguerre* impliquant États, entreprises et individus, voire toute organisation. Une *économie parallèle* s'est structurée menaçant les équilibres fragiles des démocraties et influençant les centres de décision (finance, industrie, assurance, etc.).

En dix ans, la cybersurveillance s'est aussi développée, pour le meilleur (sanctions justifiées et accélération des enquêtes criminelles par exemple) et pour le pire (atteintes à la vie privée par exemple). Les démocraties sont confrontées à un autre terrible dilemme : se battre pour le respect des libertés individuelles ne fait-il pas, parfois, le lit du crime organisé et du terrorisme ?

Dans un tel contexte, comment sécuriser l'entreprise à l'ère du numérique ?

Introduction

« Être conscient de son ignorance, c'est tendre vers la connaissance. »

Benjamin Disraeli

Ne pas perdre le fil

En 2002, j'avais retenu en couverture le labyrinthe de la cathédrale d'Amiens (comment ne pas se perdre à l'ère de la cybersécurité naissante ?). J'avais aussi choisi une dialectique temporelle et chronologique (D'où venons-nous ? Où sommes-nous ? Où allons-nous ?). J'avais posé des questions et surtout proposé des orientations structurées. J'avais pris le parti d'une conclusion ciblée sur la *cybersurveillance* et abordant la question de l'amour à l'ère d'Internet. Pas si « fou » que ça, pour celui qui intègre l'éthique à la gestion des risques numériques. *La cyberéthique n'est-elle pas le chaînon manquant entre la cybercriminalité et la cybersurveillance ?*

Depuis dix ans, je me suis concentré sur la dimension humaine des risques numériques. J'ai poursuivi l'aventure de la sensibilisation/formation fortement ancrée dans *Sécuriser l'entreprise connectée*. J'ai accompagné des dizaines de directeurs et responsables de la sécurité, dans tous les secteurs d'activité. Je n'ai pas perdu le fil de la problématique qui reste globalement politique et organisationnelle, beaucoup plus que technique et juridique, sans oublier les dimensions économique et culturelle. Par exemple, *la globalisation et la consumérisation du numérique conduisent-elles à s'affranchir des questions culturelles (notion de propriété de l'immatériel par exemple) et économiques (valeur de l'information par exemple) ?*

Tous ces aspects seront abordés dans cet ouvrage.

Mais en 2012, l'approche est très différente. Le colimaçon de la présente couverture propose une trajectoire d'élévation, verticale, pragmatique, pas à pas. Elle n'exclut ni descentes ni régressions. Au-delà des questions qui subsistent pour beaucoup, je propose des réponses et exprime des convictions profondes, parfois risquées. La conclusion revendique une triple exigence autour du concept de limites. Limites des pouvoirs et enjeux de la professionnalisation/représentation du secteur, limites de l'approche

« politique » de la sécurité des SI et enjeux des processus d'acculturation, limites de l'intégration des mécanismes/services de sécurité et de leurs coûts avec une question clé : que restera-t-il de la sécurité numérique pour l'entreprise ?

Tenir compte des évolutions structurelles majeures pour l'entreprise

Depuis dix ans, le contexte économique et social, politique et juridique, technologique et culturel a été profondément modifié. Le monde a sans doute changé en cinquante ans beaucoup plus que pendant les 200, 300 voire 500 années précédentes. Et l'informatique comme Internet n'y sont pas étrangers. Les effets de la globalisation touchent chaque individu, chaque entreprise, petite ou grande, dans son quotidien comme dans sa réflexion à court, moyen ou long terme. Pour soi-même, comme pour l'autre, le proche ou le prochain. Plus qu'une période de crise, nous vivons une phase de mutation planétaire. Souhaitons que l'individualisme de la société (américanisation) ne soit qu'apparent et parfois très trompeur. Et que l'idéal de la construction européenne, synonyme de paix et de démocratie, mais sous la contrainte de la puissance américaine et des ambitions chinoises, retrouve un nouveau souffle...

Concrètement, depuis dix ans, l'e-commerce et l'e-business sont devenus des réalités tangibles. L'e-administration et notamment l'e-santé se sont considérablement développées. Les e-loisirs (culture, jeux, paris, etc.) sont en plein essor. Microsoft, Apple et Google sont devenus des leaders de l'économie. Facebook, peut-être demain Twitter, regroupe(ront) plusieurs milliards d'internautes avides de partage et de connectivité permanente. Les smartphones et désormais les tablettes devancent les ventes d'ordinateurs portables à des coûts de plus en plus attractifs. Dorénavant, il faut être *on line* et l'information doit être *accessible*, en tout lieu, à tout instant et sur tout type de terminal[1].

1. Selon une étude de CISCO publiée en février 2012, le trafic mondial de données mobiles devrait être multiplié par 18 entre 2011 et 2016 (7,6 exaoctets par mois). Environ 10 milliards d'équipements mobiles seront connectés dont 2 milliards en *machine to machine*, soit plus que la population mondiale.

Pour l'entreprise, au-delà du phénomène bien concret de la globalisation, trois évolutions majeures ont dû être prises en compte.

- La *démocratisation d'Internet* et la *consumérisation du numérique* sont des sources d'opportunités et d'économies (*cloud computing*, dématérialisation, mobilité, médias sociaux, *big data*, etc.), mais aussi de nouveaux risques, plus stratégiques (dépendance accrue à l'informatique et au numérique et dissémination de l'information, etc.).
- La *pression réglementaire*, qu'elle soit de nature internationale, européenne ou nationale, pousse l'exigence de sécurité à une limite qui confine à l'excès. Plus que jamais les entreprises sont au cœur des risques numériques sous la double contrainte de l'Europe et des États comme des citoyens, salariés, parents, consommateurs, etc.
- Enfin, l'*intégration de la génération Y* (personnes nées entre 1975 et 1995) n'est pas sans conséquences sur la gestion de l'information (et sa confidentialité) et sur les usages du numérique (avec le concept du BYOD[1]). La jeune génération cohabite dans l'entreprise avec des baby-boomers qui ne sont pas tous en retraite et la génération X qui tient encore souvent les commandes.

Des orientations-questions aux convictions-réponses

Dépassant les questionnements et les orientations de 2002, je proposerai donc ici des réponses et exprimerai des convictions qui ne manqueront pas d'interpeller le dirigeant comme l'enseignant, le salarié comme l'étudiant, le parent-consommateur comme le salarié-citoyen. Centrant toujours la dialectique sur l'entreprise, ma réflexion n'omet ni l'État, ni l'Europe, ni l'individu.

M'appuyant sur les faits et des expériences concrètes, je structure la dialectique autour de la question centrale de la *gouvernance des risques numériques* qui conditionne tout le reste. Un bilan factuel de la décennie 2002-2012 alimentera une rédaction résolument pédagogique pour sortir

1. *Bring Your Own Device* : les employés sont invités à utiliser des outils de communication (ordinateurs portables, smartphones, tablettes) acquis pas leur soin pour les utiliser à des fins professionnelles.

de la complexité intrinsèque du domaine. De nouveaux modèles sont proposés dans le cadre de la *sécurité globale*. Certains principes fondamentaux, comme le *secret* et la *confidentialité*, sont revisités. Des modes de représentation exploitables sont proposés, sur les champs de responsabilités (gouvernance des risques numériques), la *culture des risques* (acculturation) et la *dimension économique* (pertinence et efficacité des dépenses).

L'heure est à l'union des forces et des bonnes volontés pour une société numérique sortant de la défiance persistante de la cybersurveillance et du chaos bien réel de la cybercriminalité[1]. L'entreprise, acteur central du pouvoir au XXIe siècle, doit jouer pleinement son rôle comme garant du développement de la « *société de confiance* » chère à Alain Peyrefitte.

La sécurité numérique : vaste, immature et complexe

En 2002, j'avais fait remarquer l'absence de définition de « sécurité informatique » ou de « sécurité des SI ». J'avais proposé une définition pour « cybersécurité »[2] (version francisée de *cyber security* apparue en 2000) qu'on peut aussi traduire en « sécurité numérique ». L'Union internationale des télécommunications a proposé en 2010 : « ... *l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyber-environnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyber-environnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyber-environnement. Les objectifs généraux en matière de*

1. Notons cependant qu'en 2010, l'impact de la cybercriminalité était faible ou nul pour 54 % des professionnels interrogés par le Cercle européen de la sécurité, au sein de leur entreprise.
2. « Ensemble des activités techniques, juridiques et humaines visant à se protéger des risques de fraude et de piratage en ligne. »

sécurité sont les suivants : disponibilité, intégrité (qui peut englober l'authenticité et la non-répudiation), confidentialité. »

Cette définition reste très proche de la sécurité des systèmes d'information. Pourtant, des forums professionnels posent encore aujourd'hui la question de la différence entre *IT security* et *information security* ! Aucun intérêt pour certains, hyper-pragmatiques. Question de fond pour d'autres. Comment se comprendre si on ne met pas les mêmes idées et concepts derrière les mots ? Surtout lorsqu'on sait que tout a commencé il y a une trentaine d'années et qu'il est aussi question de fonctions, de professions ou de métiers qui doivent s'adapter en permanence et proposer des services ou des solutions…

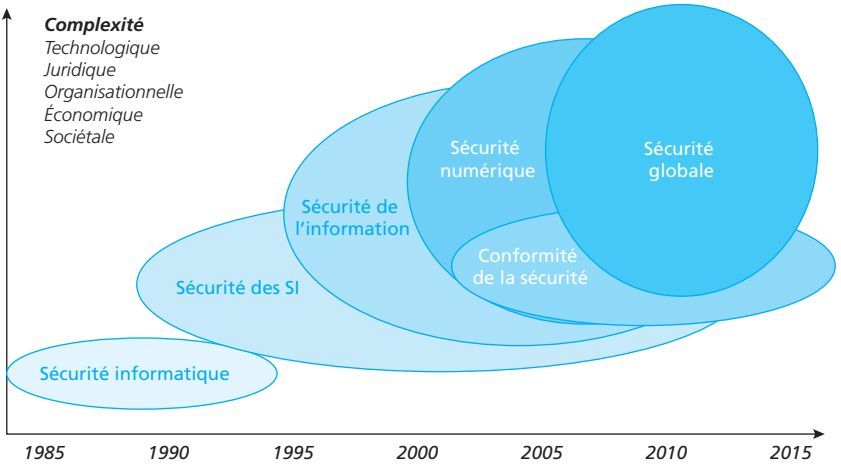

Figure 1. De la sécurité informatique à la sécurité numérique

Le champ que je propose d'investiguer doit évidemment être cadré tant le sujet est vaste, complexe et immature. Je m'explique.

Vaste : la sécurité informatique des années 80 n'a pas disparu mais elle s'est intégrée, fossilisée parfois dans un champ plus large, plus global qu'il faut bien appréhender. S'adaptant aux évolutions des technologies, aux nouveaux modes de gouvernance, comme aux nouvelles menaces, elle s'est progressivement interfacée plus étroitement avec des enjeux plus stratégiques (cyberguerre et cyberdéfense), très juridiques (vie privée, cybersurveillance, patrimoine immatériel) et aux connotations de plus en plus économiques (compétition, innovation, développement) et sociales (consommation, éducation, emploi).