N° 01/2013

recherches & documents

Février 2013

Enquête sur la sécurité numérique des entreprises

Bruno Gruselle *Maître de recherche, Fondation pour la Recherche Stratégique*

FONDATION pour la RECHERCHE STRATÉGIQUE

WWW.FRSTRATEGIE.ORG

Édité et diffusé par la Fondation pour la Recherche Stratégique
4 bis rue des Pâtures – 75016 PARIS

ISSN : 1966-5156
ISBN : 978-2-911101-71-7
EAN : 9782911101717

SOMMAIRE

Introduction

Cette étude rassemble les résultats des entretiens menés avec une vingtaine de directeurs de sécurité de grands groupes français industriels, gestionnaires de réseaux ou fournisseurs de service[1]. La grille de question utilisée se trouve en annexe.

La notion de sécurité numérique, employée dans l'ensemble de cette étude, rassemble deux domaines distincts :

- **La sécurité des systèmes d'information** à proprement parler : il s'agit de protéger les systèmes et les logiciels contre l'ensemble des menaces susceptibles d'en affecter le fonctionnement.

- **La protection et la sécurité des données stockées sur des supports numériques** : celles-ci doivent être protégées contre des tentatives de vols ou de toute compromission dans la mesure où elles affectent le fonctionnement de l'entreprise ou de ses diverses fonctions ou systèmes.

Ces deux facettes sont généralement traitées par les entreprises dans un ensemble ou, du moins, de façon coordonnée, même si la protection des données tend généralement à se rapprocher de la protection du patrimoine.

Cette étude ne fournit délibérément pas (peu en tout cas) de données chiffrées sur les réponses des personnes rencontrées. S'agissant d'entreprises dont les domaines d'intérêt économique sont relativement diversifiés, de tels chiffres – qui ne pourraient d'ailleurs être obtenus que par une véritable enquête conduite par un institut de sondage – manqueraient sans doute quelque peu de cohérence.

Nous distinguerons dans l'ensemble du rapport trois types d'entreprises afin de rattacher certains éléments de réponse à leur contexte économique :

- ➥ Les entreprises de service dont le principal produit économique est un service rendu aux consommateurs (financier, communications, transports, etc.),

- ➥ Les gestionnaires de réseaux qui sont responsables du fonctionnement d'une infrastructure au niveau national ou local, voire international (eau, électricité, etc.),

- ➥ Les opérateurs industriels qui conçoivent et produisent des biens matériels ou non.

Les questions posées se concentrent sur trois principales problématiques :

- ➥ La perception par l'entreprise des risques numériques et de ses vulnérabilités actuelles et futures par rapport à ceux-là,

- ➥ L'organisation du groupe en matière de sécurité numérique, la politique dans le domaine et les moyens qui y sont consacrés,

[1] Dans certains cas, les personnes rencontrées étaient accompagnées du responsable de la sécurité des systèmes d'information du groupe.

- L'influence et le rôle du cadre légal et réglementaire sur les activités de sécurité numérique du groupe considéré en distinguant les contraintes nationales et celles spécifiques des pays étrangers qui s'imposent aux sociétés opérant au niveau international.

Avant de rentrer dans les détails des résultats des entretiens, quelques éléments généraux peuvent être relevés :

- Pour ce qui concerne la perception des menaces, il convient tout d'abord de distinguer ce qui relève du bruit de fond : des attaques permanentes mais dont les conséquences sont limitées, autant financièrement que techniquement. Les tentatives de *phishing*[2], le balayage (*scanning*) de sites mis en ligne pour en découvrir les vulnérabilités sont quotidiennes et généralement sans conséquences majeures pour l'entreprise,

- Outre ces attaques quotidiennes, dont on verra qu'elles peuvent exceptionnellement produire des effets importants, il existe des événements rares qui s'avèrent généralement dimensionnant pour la structuration des politiques de sécurité numérique des entreprises,

- La place des outils numériques est considérée par tous comme devenue incontournable. Elle s'étend encore dans le domaine de la production mais également des services, en particulier pour des activités de paiement ou de connectivité,

- Les investissements réalisés pour assurer la sécurité des systèmes d'information et de l'information numérique sont très difficiles à évaluer. En effet, de nombreux systèmes qui participent à ces fonctions ont d'autres rôles qui ne relèvent pas de la sécurité. De façon générale, les personnes rencontrées indiquent que les budgets de sécurité numérique représentent une fraction des investissements de sécurité de l'ordre de quelques pourcents. Ils soulignent que ces efforts financiers sont limités par rapport à l'impact de la matérialisation de certains risques majeurs.

[2] Mails frauduleux destinés à piéger le lecteur afin qu'il transfère des fonds vers un malfaiteur.

Perception par les directeurs de sécurité des risques et des vulnérabilités numériques de l'entreprise

Les directeurs de sécurité reconnaissent que les risques numériques sont critiques pour l'entreprise

De façon générale, les personnes rencontrées indiquent que les risques numériques existent et pèsent parfois lourdement sur le fonctionnement de la société. Dans l'ensemble, ils font une différence entre le bruit de fond permanent composé d'attaques de faible intensité et des agressions majeures qui visent plus particulièrement leur groupe. Ces dernières structurent, aux yeux de tous les directeurs rencontrés, la politique et les moyens consacrés à la protection numérique de l'entreprise mais les premiers peuvent, même si cela est rare, avoir des conséquences sur le fonctionnement des groupes.

Ces constats montrent indéniablement que le risque numérique et le besoin de répondre à son évolution par des adaptations de la fonction de sécurité sont pris en compte de façon consciente par les structures qui ont cette responsabilité. Nous sommes arrivés – à quelques très rares exceptions près – à un stade qui se trouve au-delà de la prise de conscience, souvent décrite comme indispensable à la fin de la décennie 2000, pour entrer dans une phase de connaissance plus précise des risques et des vulnérabilités.

Cette situation amène les entreprises concernées à considérer les vulnérabilités à partir de leurs activités et des métiers qui les sous-tendent en abandonnant (progressivement) une perspective générale.

Un bruit de fond constant dont les conséquences, le plus souvent limitées, peuvent parfois s'avérer significatives

Les entreprises rencontrées sont soumises directement à de très nombreuses attaques journalières avec un impact plus ou moins fort sur leurs opérations. Comme l'indique quelques uns des directeurs de sécurité rencontrés, plusieurs dizaines, voire centaines d'attaques visent chaque jour les entreprises. Il peut s'agir de tentatives d'escroquerie (type *phishing* plus ou moins sophistiquées) ou d'attaques utilisant des logiciels malveillants visant les sites web des entreprises ou leurs réseaux. Plusieurs directeurs de sécurité notent le développement d'actes de fraude conduits dans le cadre d'opérations ciblées combinant de l'ingénierie sociale et des actions plus classiques (envois de faux mails, de faux FAX, faux coups de téléphone...).

Les sites Internet sont très attaqués (10 à 100 attaques/seconde souvent automatisées) même si les effets de ces attaques sont très limités en termes opérationnels. C'est effectivement un exploit très recherché de montrer que l'on a piraté/attaqué le site de certaines entreprises. Certains de nos interlocuteurs soulignent que les sites internet sont d'abord attaqués en fonction de la visibilité ou de l'exposition médiatique de l'entreprise.

Les tentatives d'intrusion – en particulier celles visant les fonctions externes de certaines entreprises de service (portail, service de mail, etc.) – sont le plus souvent conduites par des robots.

Comme le remarque l'une des personnes rencontrées, la protection des sites internet coûte très cher alors que les effets matériels des attaques réussies sont souvent nuls.

Les sites Internet sont également scannés de façon souvent automatique pour en découvrir des failles. Il s'agit alors pour les acteurs malveillants de les exploiter en tant que portails potentiels vers des systèmes mieux protégés ou vers des données confidentielles ou des opérations dont le piratage est une source potentielle de profit. Une des personnes rencontrées indique que son entreprise a été victime d'une cartographie de son architecture SI menée depuis un site Internet de confiance rattaché au réseau interne de l'entreprise. Il souligne qu'il existe de trop nombreux points d'entrée souvent difficiles à surveiller efficacement.

S'agissant du *phishing* et des fraudes visant les collaborateurs, l'une des personnes rencontrées indique qu'elle considère qu'il existe toujours quelques salariés qui feront l'erreur de se laisser piéger : ce taux incompressible d'erreur devrait être pris en compte dans les solutions de sécurité correctives mises en place et il faut en effet être en mesure d'assister les collaborateurs qui ont été piégés, une fois que l'incident est passé.

Quelques unes des personnes interviewées rappellent que les attaques de « bruit de fond » visent également les réseaux de communication interne des entreprises – c'est-à-dire les réseaux téléphoniques ou data privés utilisés par les entreprises –[3] et peuvent causer des préjudices financiers ou économiques. Dans ce cas, c'est le fournisseur de service qui porte l'essentiel des conséquences.

Les attaques visant directement la réputation de l'entreprise sont relativement peu citées par les personnes rencontrées. Trois d'entre elles indiquent cependant devoir faire face à des actes malveillants organisés visant spécifiquement sa réputation.

Mais plusieurs autres entreprises rencontrées – en particulier, celles intervenant dans le secteur des services, notamment bancaires, d'assurance ou de télécommunication – soulignent que les attaques numériques réussies font peser sur elles un risque de réputation important. La nouvelle d'une attaque réussie peut grandement réduire la confiance des clients dans la protection des données personnelles que les entreprises peuvent détenir : cette perte de confiance peut se traduire par des effets économiques et/ou financiers importants.

En termes de bruit de fond, on peut distinguer plusieurs périodes :

- Entre 2000 et 2004 : les vulnérabilités sont essentiellement techniques et il s'agit pour les agresseurs avant tout de pénétrer les grands comptes le plus vite possible afin de voler n'importe quelle information monnayable. Pour les entreprises, la fréquence des attaques dépend pour une grande partie de la visibilité publique. Certaines se trouvent en première ligne et doivent faire face à des attaques potentiellement très efficaces. Elles doivent développer des solutions efficaces rapidement. Pour les autres, finalement, les réponses sont simples : il suffit

[3] http://en.wikipedia.org/wiki/Private_branch_exchange#Private_branch_exchange

d'appliquer les correctifs que les premiers ciblés mettent en place pour combler les vulnérabilités et limiter ainsi les conséquences d'une attaque du même type.

- Entre 2004 et 2008 : le développement du crime numérique (*cybercrime*) s'appuie sur la professionnalisation des acteurs et leur organisation au sein de groupes dont l'objectif est avant tout de tirer profit de leurs actions. Cela équivaut finalement à une dématérialisation des approches mafieuses dont l'objectif est de voler ce qui peut se revendre, en ciblant les entreprises ou les salariés vulnérables.

- Depuis 2008 : de nouvelles menaces se développent de type APT – *Advanced Permanent Threat* – qui ciblent une entreprise en particulier. Les APT sont des attaques ciblées contre une entité (économique ou politique) et conduites par un groupe criminel, politique ou un gouvernement pour cartographier puis pénétrer ses réseaux afin d'y dérober des données ou des informations. Elles sont généralement plus difficiles à détecter car elles s'accompagnent de signaux faibles et laissent peu de traces. Ces attaques associent souvent des actions numériques – développement d'un code malveillant, recherche de failles – à d'autres opérations (ingénierie sociale) : il s'agit généralement de démarches relativement intelligentes et complexes.

Elles visent quelques collaborateurs pour passer sous les filtres de *spam* et afin d'obtenir le « click » qui permet de déclencher la propagation d'un virus (un cheval de Troie..). Le risque comportemental est présent et on ne peut l'annuler : il y aurait trop de paramètres à prendre en compte. Les antivirus sont quant à eux inopérants ce qui rend difficile de trouver des solutions efficaces.

L'utilisation du bruit de fond pour dissimuler des attaques furtives s'avère être une autre évolution préoccupante. Elle met du reste en lumière le rôle clef que jouent les moyens et les outils de détection mis en place par les entreprises dans leur sécurité numérique.

Néanmoins, comme le souligne l'une des personnes rencontrées, le risque viral permet de maintenir un niveau de vigilance élevé. Les codes malveillants agissent finalement comme des rappels à l'ordre pour les entreprises qui doivent leur permettre de maintenir leurs moyens et leurs politiques de sécurité à jour.

Si l'essentiel des entreprises rappelle que ce « bruit de fond » produit des effets numériques souvent réduits (par exemple, l'indisponibilité de quelques machines non vitales pendant quelques heures), les attaques virales sont susceptibles de causer des dégâts importants ou durables dans certains cas :

- Un des responsables note que des événements survenus à l'été 2012 montrent que des attaques peuvent conduire à la destruction simultanée de plusieurs dizaines de milliers de machines au sein d'une entreprise.[4]

- Un autre rappelle que le périmètre des systèmes d'information a tellement augmenté que l'on ne peut pas tout surveiller utilement et en permanence. Pour certains groupes opérant dans le domaine du service, des centaines de milliers de terminaux mobiles sont connectés en permanence au réseau et constituent autant de points d'entrées. Dans ces cas de figure, le système est donc très étendu, les

[4] AFP, *Saudi oil giant fixes network after cyber attack*, 29 août 2012

signaux des attaques faibles et les volumes d'information générés sont extrêmement importants (e.g. plusieurs dizaines de Go par jour).

- Les attaques détectées montrent aussi que le principal problème est la complexité du système d'information : le nombre et la diversité des systèmes et des applicatifs ont explosé. Les problèmes de mise à jour sont difficiles à gérer. Dans certaines branches, des activités de nature différente peuvent se cumuler au niveau même des postes de travail utilisateurs (administration, calcul, opérations complexes/recherche dans des domaines variés) ; ce qui peut parfois s'accompagner d'une diversification de systèmes d'exploitation (Linux, Windows, MacOS) et donc des applicatifs embarqués.

- Dans le même ordre d'idée, un autre interlocuteur note que la volumétrie des attaques a augmenté avec la montée en puissance d'Internet en France et mondialement. Pour ce dernier les entreprises ont eu à faire à des coups de semonces appuyés : ceux qui ont fonctionné ont visé les réseaux les plus exposés, c'est-à-dire connectés à Internet. **On assisterait donc aux prémisses d'une période caractérisée par des crises numériques majeures.** Cette situation résulte de l'utilisation par les Etats et certains acteurs économiques de l'espace numérique pour parvenir à des objectifs politiques ou stratégiques (obtenir des informations, saboter des outils de production, etc.)

- Les réseaux isolés sont encore relativement peu attaqués même si les épisodes DuQu/Stuxnet/Flame montrent qu'ils ne sont pas imperméables du fait des risques à partir d'appareils de mobilité (USB, disque dur portable). Les cas *DuQu/Stuxnet/Flame* montreraient pour certains responsables de sécurité que l'arme cyber se développe en tant qu'outil manié par les Etats. Il existe en conséquence un risque de voir cette menace percoler vers le reste du Monde : les méthodes, logiciels et bibliothèques d'attaque pourraient être utilisés par des acteurs malveillants non étatiques contre les vulnérabilités qui existent ou se développent, notamment, au sein des entreprises. On assistera probablement à terme à une migration de ces codes malveillants dans le bruit de fond.

A la lumière des informations recueillies lors des entretiens, il apparaît que le risque numérique a été amené à évoluer depuis l'apparition des premiers virus dans les années 1990. Les personnes rencontrées ont exprimé de façon relativement générale leur préoccupation face à ce phénomène. On peut distinguer trois grandes périodes :

1990 - 2000 : Dans les années 1990, les attaques informatiques sont essentiellement le fait de spécialistes de l'informatique cherchant à montrer leur compétence en piratant des sites ou des serveurs très protégés, appartenant généralement aux agences de sécurité ou de défense.

2000-2008 : L'exploitation des compétences techniques des *hackers* « pour la gloire » a cédé la place à une véritable criminalité numérique, professionnalisée et spécialisée, visant à dégager des profits essentiellement matériels pour des organisations criminelles. La cybercriminalité s'est illustrée, dans un premier temps, par l'apparition puis l'augmentation de cas d'attaque de sites Internet marchands, de vente de produits contrefaits jusqu'à la mise à disposition de moyens d'attaques Internet. Les pirates se

sont regroupés en cellule et se sont répartis le travail criminel.

Depuis 2008 : Outre la poursuite du phénomène de cybercriminalité, l'espace numérique est devenu un domaine d'intervention pour les Etats, des groupes à caractère politique revendicatif et certains acteurs économiques pour conduire des opérations visant à saboter les moyens de production ou les réseaux, obtenir des informations ou des données sensibles et mettre en cause la réputation des cibles.

L'insécurité numérique résulte-t-elle principalement des comportements des collaborateurs ?

La question de la place des comportements des salariés dans le développement des risques numériques soulève des réactions parfois divergentes chez les personnes rencontrées. On peut distinguer globalement *deux écoles de pens*ée :

- **Comme le souligne l'une des entreprises, un des problèmes vient de l'existence d'atteintes internes, volontaires ou non.**

La diffusion d'informations propriétaires via les blogs, les forums ou encore les réseaux sociaux (FB, *twitter*) peut entraîner des conséquences dramatiques pour l'entreprise : il s'agit rarement d' « attaques » organisées au sens propre même si parfois des groupes peuvent se rassembler pour contester la politique de l'entreprise. Parmi les autres problèmes cités par quelques uns des interlocuteurs, la poursuite du dialogue avec d'anciens camarades (de faculté, d'école, de travail) qui peuvent utiliser le savoir obtenu pour leur société.

La gestion des réseaux sociaux est d'autant plus problématique que l'entreprise se montre permissive sur leur utilisation par les employés. Le développement des médias sociaux créés des craintes particulières quant au ciblage des salariés par des actions d'ingénierie sociale (*social engineering*). De fait, ces actions sont souvent citées comme une préoccupation grandissante par les entreprises.

Les malfaiteurs utilisent habilement un mélange de moyens de communication classiques et numériques pour se faire passer pour des membres du comité exécutif et obtenir des virements bancaires. Comme le rappellent plusieurs interlocuteurs, il ne s'agit pas à proprement parler de criminalité numérique mais elle s'appuie sur le recours à certains outils indispensables aux entreprises pour fonctionner.

L'enjeu de sécurité est de créer une forme de discipline efficace et de mettre en place des politiques contraignantes (ce qui est difficile en France).

- **Dans le même ordre d'idée, la problématique de la gestion d'une politique de type « *bring your own device* » (BYOD) se pose souvent en termes d'encadrement des comportements des utilisateurs.**

Si les personnes interviewées constatent la montée en puissance du BYOD – qui est portée à la fois par les dirigeants mais surtout par les jeunes collaborateurs en particulier dans le domaine commercial –, la subissent ou l'accueillent comme une opportunité

économique pour l'entreprise, toutes cherchent à en encadrer la généralisation dans leur groupe.

L'irruption du BYOD dans l'espace professionnel consacre, pour la plupart des personnes rencontrées, le brouillage des frontières grandissant entre la sphère privée et professionnelle – déjà constatée pour l'utilisation et la généralisation des réseaux sociaux ou encore des processus de co-création ou de coopération virtuelle – et conduit irrémédiablement à poser le problème de la ségrégation des espaces numériques et des données.

On arrive *in fine* à une situation paradoxale. Comme le souligne un de nos interlocuteurs, ces phénomènes créent en effet plus de vulnérabilités mais accroissent également la productivité des collaborateurs. De fait, il est devenu difficile d'isoler les équipes du monde extérieur alors que c'est la solution souhaitable[5] : le numérique partout (et de plus en plus interconnecté) crée des failles béantes qui sont exploitées à l'envie par les concurrents.

Un autre interlocuteur fait remarquer que, d'une part, on offre de plus en plus de solutions technologiques aux collaborateurs et que, d'autre part, on restreint de plus en plus ses accès et les droits qu'il a de s'en servir (ex. ségrégation Internet et intranet de plus en plus poussée).

➟ **La fragilité comportementale aurait, selon les tenants de cette école, de nombreuses sources : méconnaissance, manque d'info, de formation, négligence, naïveté.**

L'un des interlocuteurs souligne que plusieurs ingrédients se mélangent pour renforcer le risque humain : un contexte économique et social difficile, l'ego et la vanité des gens qui les amènent à agir sans mesurer les conséquences (en particulier à livrer publiquement des informations), un mélange d'insouciance et d'incompétence et parfois, des difficultés d'appropriation des nouvelles technologies.

Pour autant certains reconnaissent que le risque provoqué par le trop de connaissances est aussi réel : les spécialistes qui ont dû être recrutés pour faire fonctionner des SI de plus en plus complexes utilisent souvent leurs compétences pour contourner les mesures de sécurité mises en place. Quelques-unes des personnes interrogées évoquent d'ailleurs un risque spécifique concernant les administrateurs informatiques qui résulte de leur trop grande confiance dans leur compétence couplée à des comportements à risque et des accès à de nombreux systèmes et données. L'un de nos interlocuteurs souligne que l'un des problèmes spécifiques avec les administrateurs est que leurs droits de gestion leur offrent des capacités à affecter les systèmes mais également les données qui sont stockées ou sauvegardées.

[5] Certaines personnes soulignent toutefois que l'isolement « numérique » des équipes est parfois pratiqué sur des projets très sensibles.

- **D'autres responsables de sécurité considèrent que l'intervention humaine crée une part incompressible de risque avec laquelle il faut pouvoir composer.**

Au-delà de ce constat, les sociétés qui interviennent dans le domaine des services considèrent que l'émergence de nouvelles formes d'usage des outils numériques (on revient au BYOD mais pas seulement) est incontournable et qu'augmente avec elle la part du risque humain. L'utilisateur veut pouvoir faire beaucoup de choses en ligne, très vite. Cela nécessite de proposer des applicatifs qui répondent aux besoins sans remettre en cause la sécurité des connexions et des données échangées. Il faut donc développer des solutions de sécurité des produits/applicatifs utilisés par les clients ce qui est complexe.

L'émergence de nouveaux acteurs numériques sur le marché du service (notamment financier, cf. *paypal*), qui ne sont parfois pas soumis aux mêmes contraintes que les entreprises traditionnelles en termes de régulation, s'avère également être une forte tendance qui est source de défi en termes de sécurité (pour le client comme pour les sociétés concernées).

On irait donc d'une logique de forteresse vers une logique d'aéroport et il faut vivre avec cette ouverture et évoluer rapidement en ayant conscience des problèmes de sécurité.

Au-delà du risque qu'il ferait courir à l'entreprise, l'utilisateur est aussi un moyen pour l'entreprise de détecter des attaques qui visent son système d'information. Comme le souligne l'une des personnes rencontrées, les informations remontent soit au travers de la veille (zataz.com) soit du fait des utilisateurs. Il s'agit donc pour les responsables de la sécurité de proposer des outils intéressants pour amener les gens à la sécurité sans les forcer. Il en conclut que la démarche de sécurité doit être intégrée aux projets de la société car on ne peut pas (plus ?) imposer de choix.

Ces deux approches sont moins contradictoires qu'il n'y paraît. Elles illustrent en effet le paradoxe de l'évolution des usages numériques : facteur indispensable du développement économique de l'entreprise (accès à l'information en permanence et partout, aide à la gestion ou au traitement des tâches, facilité de coopération..) et source de vulnérabilités qui, si elles ne sont pas forcément nouvelles, peuvent se trouver accrues par le manque d'encadrement. Pour prendre un exemple, l'usage des réseaux sociaux par les collaborateurs et les salariés font, selon la plupart des entreprises, l'objet de mesures d'encadrement plus ou moins contraignantes. Pour autant, plusieurs d'entre elles soulignent que leur entreprise développe des outils sociaux internes destinés à favoriser les échanges entre les collaborateurs, l'adhésion aux valeurs de l'entreprise ou simplement la communication entre les salariés.

Les moyens mobiles cités comme une source spécifique de vulnérabilité

En amont du BYOD, se pose, pour la plupart des interlocuteurs rencontrés, la problématique de la sécurité et de la protection des moyens mobiles : systèmes de stockage (clef USB, disque dur portable), ordinateurs portables et terminaux mobiles (*smart phone*).

Les préoccupations sont essentiellement liées, soit aux conséquences de la perte ou du vol de machines en termes d'accès aux données ou aux informations stockées sur le disque, soit à l'introduction d'applications malveillantes sur les réseaux internes des entreprises. Ce dernier risque est spécifique à l'utilisation de systèmes de stockage mobile – en particulier les clefs USB – qui après avoir été infectés dans le cadre d'une utilisation privée sont introduits dans des ordinateurs professionnels liés aux réseaux de l'entreprise et peuvent ainsi les infecter. Le cas de l'attaque subie par le Pentagone en 2008 illustre assez bien la préoccupation des entreprises dans ce domaine. Il avait alors été infecté par un code malveillant (vraisemblablement un cheval de Troie) introduit sur le réseau protégé par le biais d'une clef USB[6]. Le secrétaire adjoint à la Défense, William Lynn, révèle en 2010 que ce logiciel espion pourrait avoir permis à une agence étrangère d'accéder à plusieurs milliards d'octets d'information, y compris des données classifiées[7]. Cette attaque, longtemps passée sous silence par les Etats-Unis, aurait accéléré la création du CYBERCOM. Il convient de souligner que trois ans après cette attaque, le Pentagone continuerait à nettoyer son système d'information des traces de ce virus.

La perte et le vol d'ordinateurs portables constituent également des sources importantes de préoccupation du fait des informations ou données qu'ils peuvent contenir ou du fait qu'ils peuvent permettre l'accès aux réseaux internes des entreprises. *A contrario*, les personnes rencontrées s'inquiètent généralement moins du vol ou de la perte de téléphones mobiles en particulier dans la mesure où ces derniers peuvent souvent être effacés à distance à la condition qu'il s'agisse d'engins fournis par l'entreprise.

Un spectre de vulnérabilités relativement constant mais qui dépend partiellement de la branche d'activité et des métiers

Les principales vulnérabilités des entreprises : les données et les informations, la résilience et la résistance des systèmes d'information

De façon très schématique, les systèmes d'information des entreprises d'assez grande taille peuvent se décomposer de la façon suivante :

- Un ou plusieurs réseaux internes dont la vocation est administrative : gestion des ressources humaines, messageries, contrôle de gestion, etc.
- Un ou plusieurs réseaux internes plus ou moins isolés (en interne comme vers l'extérieur) qui ont des fonctions liées aux métiers : production, développement/R&D, calcul, etc.
- Des pages Internet, dont les vocations sont diverses et qui peuvent constituer des portes d'entrée vers certains réseaux internes.

Cette décomposition permet de mieux comprendre le fait que les vulnérabilités numériques ressenties par les entreprises sont profondément liées aux secteurs dans lesquels elles interviennent. Elles sont également le fait de l'évolution rapide de la prégnance des systèmes informatiques dans les opérations des entreprises.

[6] Security and Defense Agenda, *A conversation on Cybersecurity with William J. Lynn III*, 15 septembre 2010

[7] Le Monde Informatique, *Les systèmes informatiques du Pentagone attaqués par une clef USB*, 26 août 2010

A.– Le risque informationnel

Comme le soulignent plusieurs personnes, on constate moins une aggravation des menaces – la plupart des codes malveillants s'avère le plus souvent basiques même si certains interlocuteurs estiment qu'on assiste à une amélioration des capacités des groupes malveillants – qu'une modification des activités numériques qui, en augmentant et en se diversifiant, amènent de nouvelles vulnérabilités pour l'entreprise. Brèche dans la confidentialité des informations et perte d'intégrité ou de disponibilité des systèmes critiques (surtout en cas de crise) sont les principaux risques à prendre en compte.

Ainsi, on peut distinguer trois principales catégories de vulnérabilités : sur les informations, sur les données et sur les systèmes d'information. Les deux premières sont relativement proches :

- **Les risques (de vol ou de diffusion) pesant sur les informations appartenant à l'entreprise qui sont stockées ou échangées sous format numérique**. Il peut s'agir d'informations techniques (y compris des brevets), technologiques, financières et économiques qui partagent la caractéristique d'être sensibles pour l'activité de l'entreprise. A ce titre, certains progiciels propriétaires critiques pour le fonctionnement de certains secteurs (calcul de probabilité dans le milieu des assurances par exemple) font partie des informations jugées vitales.

Les interlocuteurs qui insistent sur cette problématique l'expriment sous la forme de « fuite de savoir et de savoir-faire » et parfois de perte de patrimoine (même si cette notion ne couvre pas certains cas, comme par exemple la révélation d'information sur des activités économiques (fusion/acquisition)). Pour les entreprises concernées, il s'agit d'identifier le patrimoine sensible – qui s'ajoute éventuellement aux informations protégées par le secret de la défense nationale – dans un ensemble large d'informations afin de le protéger de façon plus efficace.

- **Les risques (de perte/vol, de diffusion ou de destruction) de données dont l'entreprise est dépositaire pour une tierce partie.** Ces données personnelles peuvent être de nature financière, de nature personnelles comme celles portant sur la santé voire même plus générales. La perte ou la destruction de ces données (par un acte ciblé ou non) peut avoir un impact très fort sur les opérations et sur la réputation d'une société, opérant par exemple dans le secteur financier et des assurances mais également pour les opérateurs de télécommunication qui sont soumis à des règles strictes de transparence sur la perte de données. Comme le souligne l'un des responsables interrogés, les données conservées peuvent être vitales pour l'entreprise car on ne peut pas les « refabriquer ».

Face aux risques « informationnels », l'un des interlocuteurs fait remarquer que la priorité est de conserver la confiance des utilisateurs/clients dans une situation où la détection des intrusions et de l'accès non souhaité aux données est très difficile s'agissant non pas de vol avec disparition mais de copies illégales. Le risque informationnel dépasse du reste le seuil numérique puisqu'il s'étend à l'archivage physique des données, à l'édition papier ou encore aux courriers.

La question du suivi et de la protection est valable tout au long de la durée de vie de l'information et jusqu'à sa destruction éventuelle. La plupart des informations sont en effet sensibles pendant une durée généralement limitée (dans la mesure où leur

divulgation aurait un impact opérationnel important) et doivent être protégées spécifiquement.

Le risque informationnel se matérialise en particulier par le vol ciblé de données mais également par des intrusions silencieuses visant à piller l'ensemble des informations stockées sur les réseaux infectés. Quelques exemples d'intrusion ou de vol ont été donnés par les personnes rencontrées :

- Une attaque qui s'est déroulée en plusieurs phases :

  ⇒ dans un premier temps, tentative de cartographier le réseau en passant un site de confiance rattaché au système mais mal contrôlé,

  ⇒ Plus tard, intrusion silencieuse via le site d'une ancienne filiale encore connectée au réseau (serveur orphelin). Cette tentative (détectée) conduit à fermer les accès aux réseaux de l'entreprise pour reconfigurer l'ensemble de la base d'accès causant une interruption de disponibilité de plusieurs mois.

- Un collaborateur sort des informations sur lesquelles il travaille et les vend sur une plateforme Internet localisée aux Etats-Unis. Après enquête, ce collaborateur est identifié, le FBI alerté et l'action est qualifiée en infraction pénale : le collaborateur sera condamné à 18 mois de prison et 180 000 $ d'amende.

Le risque informationnel porte en creux la question du développement de l'offre de *cloud computing*, en particulier pour le stockage des informations et des données.

Comme pour le BYOD, la plupart des groupes soulignent que le développement de l'offre de *Cloud* conduit l'entreprise à réfléchir au gain économique qui peut être obtenu en transférant à un opérateur extérieur la responsabilité d'une partie des données. La réflexion se structure autour d'une logique de rationalisation des coûts plutôt qu'en termes de sécurité. En particulier, il est très difficile de justifier l'écart financier entre le recours à une solution interne (coûteuse) et l'utilisation d'une solution hébergée/opérée par un tiers.

Les interlocuteurs qui évoquent le *Cloud* soulignent souvent qu'il s'agit pour la sécurité d'accompagner des choix économiques même si certains rappellent que les entreprises font parfois le choix de ne pas externaliser le stockage des données précisément du fait de la sensibilité des informations et données qu'elles détiennent ou sur lesquelles elles travaillent. Au final, les problématiques de sécurité sont quand même prises en compte, puisque l'examen des solutions de *Cloud* externe est effectué par les entreprises sur des bases de disponibilité des informations, de maintien de confidentialité (en particulier vis-à-vis des services locaux) et de fiabilité du stockage.

B.– L'autre famille de risques porte sur les systèmes d'information

Une distinction est faite entre les outils bureautiques qui sont généralisés à l'ensemble de l'entreprise et destinés à équiper le plus grand nombre des collaborateurs et les outils de production ou de R&D, plus spécifiques. Parmi les problématiques mises en valeur par les personnes interrogées, il convient de souligner celles concernant la montée en

puissance des risques liés aux Systèmes d'information de pilotage de production (SCADA).

Beaucoup d'interlocuteurs soulignent leurs préoccupations tout en rappelant que les conséquences d'une action qui toucherait ces systèmes sont généralement d'abord de nature économique avant d'être physique (c'est-à-dire qui aurait un impact direct sur la sécurité des personnes ou des biens).

Dès lors, l'enjeu des réponses se pose plutôt en termes de capacités à se ***remettre rapidement*** d'une attaque réussie tout en fonctionnant dans l'intervalle en mode dégradé. Ceci nécessite d'ailleurs de pouvoir identifier rapidement la source de la défaillance et d'appliquer des correctifs en maintenant un bon niveau de production (ou de service). En creux, la résilience des processus informatisés de production soulève le problème de l'intégrité et de la disponibilité des systèmes d'information.

Comme le souligne l'un des interlocuteurs, ces risques montrent que les entreprises doivent être capables de détecter des signaux faibles dans un environnement complexe.[8] Pour certains secteurs, ces « processus industriels » peuvent être des applications mises à disposition des clients. La pression du « marché » peut, dans ce domaine, conduire à mettre des produits à disposition (en ligne) rapidement sans maîtriser toutes les sources de vulnérabilités.

On notera que certaines personnes interrogées rappellent qu'il existe des problématiques spécifiques liées à la résilience des systèmes financiers, en particulier ceux destinés à gérer des opérations financières en temps réels : l'impact d'une indisponibilité même momentanée peut être catastrophique pour certaines entreprises.

Enfin, il faut souligner que certains risques physiques (incendies, pannes...) peuvent avoir des conséquences numériques importantes et se traduire par l'indisponibilité d'un système (voire d'une fermeture de serveurs dans certains cas extrêmes) ou la nécessité d'opérer en mode dégradé.

Une aggravation due à l'évolution des comportements, aux structures des entreprises et de leur architecture numérique globale

Les risques mis en lumière sont généralement aggravés par des facteurs supplémentaires propres à leur taille et au fonctionnement des entreprises. S'agissant généralement de sociétés qui sont à la fois implantées sur des sites nombreux en France et à l'étranger et qui possèdent soit des filiales, soit des établissements, les problèmes de sécurité numérique peuvent être rendus plus aigus :

- **Par l'internationalisation de l'entreprise** qui conduit à gérer des niveaux de sécurité qui peuvent fortement variés entre les pays concernés, en particulier pour les Etats en développement. Ainsi, des choix locaux peuvent être effectués sans respecter les règles de sécurité ce qui nécessite parfois une intervention au plus haut niveau pour rétablir les standards de sécurité. Comme le souligne une des personnes rencontrées, les contraintes légales locales peuvent notamment obliger à utiliser localement des outils qui ne sont pas connus ou mal sécurisés.

[8] Nous reviendrons sur ce point dans le chapitre suivant.

Par ailleurs, pour certaines entreprises, l'internationalisation se traduit par la création de partenariats (ex. *joint ventures*) nécessitant de mettre en place des moyens de préserver le savoir-faire, l'expertise et l'expérience propriétaire. Pour certaines coopérations, il faut pouvoir cloisonner efficacement les réseaux concernés et mettre en place des accords intergouvernementaux solides.

De façon plus générale, la gestion de l'entrée et de la sortie des filiales du groupe (au gré des achats et ventes) peut créer des problèmes spécifiques si elle prend mal en compte les connexions entre les réseaux de ces entreprises et ceux du groupe. Il peut ainsi apparaître des points d'entrée mal maîtrisés potentiellement utilisables pour des actions malveillantes.

➥ **Par la diversité des métiers** qui sont représentés dans l'entreprise (facteur à rapprocher de la différence entre la culture des établissements et celle propre à l'échelon central) qui peuvent conduire à un effet d'atomisation des systèmes d'information et d'inflation des applications utilisées (voire dans certains cas de figure, des systèmes d'exploitation).

Si la plupart des entreprises déploient des solutions unifiées pour la bureautique classique, certaines doivent gérer en plus des systèmes dédiés aux métiers. Le risque spécifique à ces systèmes dédiés est aujourd'hui relativement bien maîtrisé dans la mesure où ils sont généralement séparés des réseaux administratifs et sont donc moins vulnérables à des attaques qui seraient conduites depuis Internet par le truchement de ces derniers.

Mais plusieurs personnes rencontrées soulignent la tendance très forte à l'interconnexion des réseaux qui conduirait à accroître le risque pesant sur les métiers spécifiques (production, R&D, finances...). Quelques personnes ont rappelé que leur entreprise était à la fois fortement informatisée et possédait un réseau s'étendant au niveau mondial et parfois interconnecté avec celui des autres entreprises du même secteur ou des sous-traitants.

Plus spécifiquement sur les SCADA, l'un des interlocuteurs a indiqué que pour les systèmes industriels de connexion, il existait une pression grandissante pour les connecter avec l'extérieur, soit pour du *reporting* en temps réel (par exemple exploitation des données des SI indus par logiciels SAP de contrôle de gestion des activités au niveau entreprise[9]), soit pour pouvoir reconfigurer rapidement une chaîne de production. De la même façon, les sous-traitants informatiques souhaitent pouvoir accéder à distance aux systèmes pour en assurer le dépannage ou le maintien, y compris l'application de correctifs. Le risque portant sur les systèmes industriels est donc considéré par de nombreuses entreprises comme s'aggravant rapidement. Il nécessite une prise en compte spécifique, en particulier si l'on considère la possibilité que des logiciels malveillants (de type *DuQu*, *Stuxnet*) soient introduits même pour les systèmes déconnectés du réseau. La tendance à une connexion plus importante (avec les réseaux bureautiques) ne fait qu'accroître les possibilités de voir un système infecté par un logiciel malveillant qui transiterait par les machines à caractère administratif. Comme le souligne

[9] *SAP applications, built around their latest R/3 system, provide the capability to manage financial, asset, and cost accounting, production operations and materials, personnel, plants, and archived documents.*

certains interlocuteurs, la généralisation des solutions commerciales (*off-the-shelf*) pour l'équipement des réseaux industriels tend à accroître les risques de voir des virus développés spécifiquement pour les infecter.

➟ **Par l'évolution des comportements des utilisateurs** qui est l'un des importants facteurs contribuant à l'introduction rapide de nouveaux moyens plus ou moins bien sécurisés dans l'entreprise (en particulier le phénomène BYOD cf.supra).

Pour plusieurs personnes rencontrées, l'évolution des comportements oblige les responsables sécurité à s'adapter pour accompagner des changements qui sont portés en interne par ses populations.

Il faut ainsi gérer des comportements venus de l'extérieur qui s'impriment sur le fonctionnement de nos systèmes d'information. Il en résulte parfois des difficultés à maîtriser l'environnement.

Pour autant, plusieurs interlocuteurs soulignent que le risque comportemental n'est pas forcément dimensionnant s'agissant de populations qui peuvent être plus facilement sensibilisées aux problèmes liés à leur utilisation des outils et des données numériques.

Les menaces futures (e.g. Advanced Permanent Threats) : quelles perceptions ?

Quelques-unes des sociétés rencontrées ont été victimes d'intrusions informatiques de grande ampleur visant (en général) à des vols de données et des activités d'espionnage.

Dans la mesure où elles sont par nature silencieuses, ces intrusions soulèvent la problématique de la détection. Dans certains cas, celle-ci se fait par hasard mais elle révèle toujours l'existence de failles souvent en termes d'organisation de sécurité (il ne s'agit pas forcément d'un problème de moyens). La détection peut conduire à totalement arrêter tout ou partie du système informatique de l'entreprise pendant plusieurs jours, voire plusieurs semaines.

L'origine de ces attaques constitue en soi l'objet de nombreuses questions. La possibilité que l'absence de détection ne soit pas synonyme de l'absence d'intrusion a parfois été mise en avant par les interlocuteurs.

Le développement d'une forme de guerre économique fondée sur le domaine numérique ne fait pas de doute pour certaines des personnes rencontrées qui rappellent l'existence d'efforts étatiques significatifs entrepris par certaines puissances mondiales. Ainsi, l'une d'entre elles estime que les entreprises – plutôt d'ailleurs celles évoluant dans des secteurs de forte concurrence internationale – sont attaquées et pénétrées quotidiennement dans le but d'obtenir et de voler des informations. Il s'agit d'attaques majeures conduites par des acteurs de très haut niveau : c'est organisé, c'est persistant et cela fait partie d'une stratégie plus générale visant à piller les entreprises avancées (leurs compétences, leurs technologies et leurs capacités d'organisation).

Quasiment toutes les entreprises indiquent que la capacité de détection (d'une attaque, d'un vol de données, d'une action d'espionnage) s'avère être au cœur de la problématique de sécurité numérique. Face à cette question, la réponse la plus structurée se fonde sur le constat qu'une entreprise ne peut pas se prémunir contre tous les risques

informatiques et qu'il s'agit de faire des arbitrages économiques pour protéger les « ressources numériques critiques de l'entreprise ». L'identification de ces dernières se trouve finalement au cœur de la démarche des entreprises en matière de sécurité numérique.

Architectures de sécurité numérique mises en place

Le constat relativement partagé entre les entreprises sur l'importance de la sécurité numérique – des informations, données et des systèmes – conduit à s'interroger sur les organisations mises en place et les mesures et moyens consacrés à répondre à des défis qui sont à la fois de plus en plus présents et dont les conséquences (économiques, réputationnelles, humaines, etc.) sont toujours plus graves.

Parmi les questions qui ont été posées pour essayer de mieux comprendre l'action des entreprises rencontrées, l'enquête a soulevé celles concernant les coûts et investissements consacrés à la sécurité numérique.

De façon générale, les interlocuteurs ont indiqué ne pas pouvoir précisément fournir de données sur ce point du fait de la fongibilité des investissements. Sur les aspects matériels et logiciels, il semble effectivement difficile de faire la part des budgets participant plus ou moins directement à cette fonction. On notera toutefois que les entreprises possèdent généralement un réseau de correspondants « sécurité des systèmes d'information » (SSI) dont le rôle est directement de s'assurer de la mise en œuvre des mesures de politique de sécurité, du suivi de celle-ci et du soutien aux utilisateurs pour les questions relatives à la protection des moyens numériques de l'entreprise.

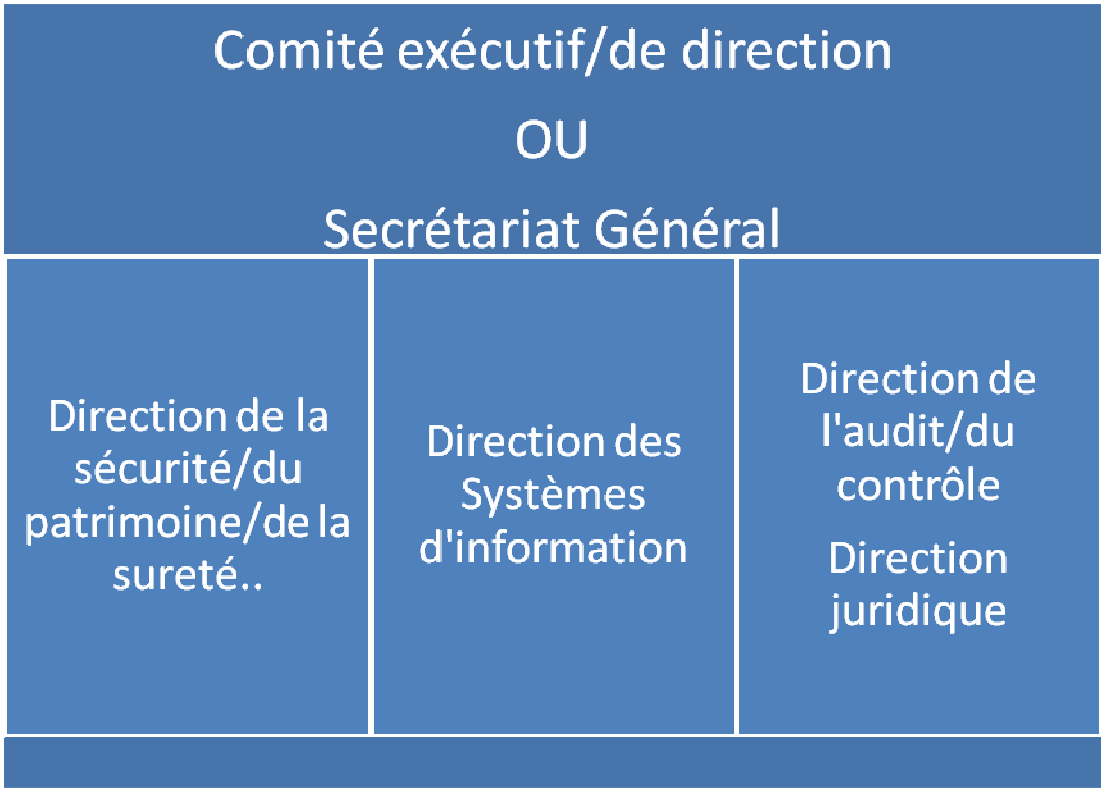

Figure 1 : Plusieurs directions interviennent plus ou moins directement dans la fonction sécurité numérique des entreprises

Enfin, il convient de souligner, à l'instar d'une des personnes rencontrées, que les structures mises en place sont avant tout là pour permettre de gérer des incidents graves ou des crises. ***Au quotidien les choses s'organisent en fonction des rapports qui peuvent exister entre les gens qui participent à la sécurité*** : il faut avoir une démarche de sécurité comparable conceptuellement à celle de la qualité ; c'est-à-dire maîtriser la chaîne et savoir détecter les problèmes et les contrôler. Il convient également de remarquer que le RSSI est souvent mal perçu et peu écouté : c'est un excellent technicien mais généralement un piètre tribun.

Structuration de la fonction sécurité numérique

Responsabilité de la sécurité numérique au sein du groupe	Nombre de sociétés concernées	Notes
Sous la direction d'un RSSI	7 (30%)	Le plus souvent au sein de la DSI
Sous la responsabilité de la direction de la sécurité	12 (52%)	Dans certains cas existence d'une direction de la sécurité numérique
Pilotage par un organisme transverse	4 (12%)	Cet organisme peut choisir des directions pour mettre en œuvre la politique

Figure 2 : Trois principaux schémas d'organisation
de la sécurité numérique ont été mis en lumière

La question du positionnement et du rôle de la fonction « sécurité numérique » se pose ou s'est posée à l'ensemble des entreprises rencontrées. Comme l'a noté l'une des personnes rencontrées, cette question est directement liée à la nature même des risques « informatiques » qui concernent autant le patrimoine « informationnel » de l'entreprise que les moyens systémiques qui participent à son fonctionnement.

En d'autres termes, le risque numérique concerne autant les directions informatiques des entreprises que les directions de la sécurité.[10] Cette réalité transparaît dans l'ensemble des entretiens que nous avons réalisés : ces deux entités sont plus ou moins associées dans le traitement de la protection des systèmes d'information au sein des entreprises. Il convient de noter à ce stade que nous avons pu discuter généralement avec le directeur de la sécurité (ou son représentant) parfois accompagné du responsable de la sécurité des systèmes d'information du groupe.

[10] Nous n'entrons pas ici, délibérément, dans un débat sur le fait de parler de sûreté ou de sécurité. De façon générale, nous parlons de la direction qui a pour fonction la protection de l'information et, plus généralement, des opérations au sein de l'entreprise.

On peut distinguer, à la lumière des entretiens, plusieurs principes d'organisation des entreprises en matière de sécurité numérique. Les choix réalisés sont influencés par le vécu en matière d'incident mais également par la structuration de l'entreprise et par sa perception de ses vulnérabilités. Dans certains cas, la décision de choisir certains types d'organisation peut être prise de façon à améliorer la visibilité de la direction responsable auprès du comité directeur ou exécutif de l'entreprise ou pour permettre son pilotage (direct ou non) par un membre de celui-ci. Les rattachements organiques de la fonction « sécurité numérique » sont également le résultat de choix concernant l'accès des responsables aux échelons décisionnaires de l'entreprise.

Il existe, de façon schématique, ***trois types de structuration de la fonction sécurité numérique*** :

- un rôle central donné à la direction des systèmes d'information,
- le pilotage de la direction de la sécurité,
- la mise en place d'un fonctionnement collégial – rassemblant plusieurs directions intéressées – qui s'accompagne éventuellement de la création d'une entité chargée de diriger la politique de sécurité numérique de l'entreprise.

La sécurité numérique est parfois de la responsabilité de la direction informatique

Sur les 23 sociétés rencontrées, 7 confient exclusivement la responsabilité de la sécurité numérique à un responsable central de la sécurité des systèmes d'information (RSSI). Celui-ci est parfois rattaché à la direction des systèmes d'information (DSI) mais il peut se trouver dans certains cas sous les ordres d'un autre directeur ou membre du comité exécutif (par exemple le secrétaire général). Il convient de souligner que, dans quelques cas, le périmètre de responsabilité est parfois réduit à la seule protection des moyens informatiques englobant les informations et données qui peuvent y être stockées mais excluant celle du patrimoine immatériel de l'entreprise. Dans quelques cas, ce RSSI « groupe » coordonne son action avec celle du directeur de la sécurité, mais ce dernier se trouve alors cantonné à un rôle d'appui plutôt que de coordonnateur.

Le RSSI, quelle que soit sa position au sein du groupe, s'appuie en général sur une équipe centrale plus ou moins importante ainsi que sur un réseau de responsables et de correspondants – celui-ci comprend en général au moins une personne désignée par entité appartenant à l'entreprise – dont le rôle est à la fois de prendre en compte les consignes et prescriptions mais également de faire remonter le cas échéant des informations ou des alertes vers le responsable central.

La logique de ce choix tient au fait que la sécurité des SI est considérée avant tout comme une activité de gouvernance, à prépondérance technique, dont la fonction est de participer au pilotage des projets informatiques des entreprises concernées mais également de remplir des rôles de prescripteur et d'assistant aux métiers pour la gestion de leurs moyens.

A.– Le rattachement à la DSI en question

La question du rattachement à la DSI occupe souvent la réflexion des personnes rencontrées en particulier pour les entreprises concernées par ce modèle. L'une d'elles s'interroge d'ailleurs sur la direction vers laquelle sa société doit aller : soit une direction sécurité absorbant la SSI, soit la continuation du modèle séparé sécurité-SSI. Elle insiste également sur le fait que le problème tient au fait que la fonction SSI possède une véritable spécificité technique alors que le directeur/responsable de la sécurité est avant tout chargé de la gestion politique/stratégique des questions de protection.

L'un des cas rencontrés est particulièrement intéressant dans la mesure où, si le responsable central de la sécurité des systèmes d'information appartient à la DSI, les membres du réseau RSSI de l'entreprise sont eux rattachés aux directions des risques. Selon la personne interrogée, cette situation permet d'éviter que ces derniers ne soient soumis aux aléas de la gestion des systèmes mais place également le RSSI central dans une position où il peut arbitrer entre les besoins des différents échelons. Ainsi, la dichotomie entre direction informatique et sécurité est gérée à un niveau subsidiaire mais permet effectivement de prendre mieux en compte la dimension sécuritaire de la gouvernance des systèmes d'information.

Il convient du reste de souligner que, au-delà de l'articulation entre les aspects de pure sécurité et ceux relatifs à la gestion des questions techniques, l'une des problématiques importantes tient à la prise en compte des aspects sécurité dans la conduite des projets informatiques des entreprises. Pour certaines des personnes rencontrées, les responsables sécurité sont avant tout considérés comme des obstacles aux progrès des programmes. Ils doivent donc autant que possible s'intégrer dans les équipes plutôt que d'agir comme prescripteurs au début et des censeurs à la fin des travaux afin, si possible, de proposer des solutions adaptées aux enjeux.

Ainsi, comme le souligne l'un des interlocuteurs, la notion de RSSI est une aberration car il faut concevoir la sécurité comme tout autre fonction et pas comme un métier à part. On doit faire évoluer pour intégrer la sécurité dans les besoins de tous les projets et pas comme une contrainte externe portée par une direction qui intervient en dernier ressort.

B.– Des groupes de coordination interservices peuvent parfois être mis en place

Dans l'un des cas, l'entreprise fait chapoter la fonction de responsable de la sécurité informatique par un comité qui rassemble, sous la direction du secrétaire général, les directions fonctionnelles qui interviennent sur ces problématiques : DSI, direction juridique, ressources humaines, communication, sécurité, etc.. Ce type d'organisation permet essentiellement de prendre en compte les préoccupations des différents acteurs et de définir puis de coordonner la politique du groupe en matière de SI.

Comme dans de nombreux autres cas, cette politique est approuvée par le comité exécutif avant de s'imposer dans l'entreprise sous la conduite, en l'occurrence, du responsable SI et de son réseau.

C.– Pour certaines entreprises, la problématique de la sécurité des SI est (relativement) nouvelle

La création d'un poste ou d'une fonction dédiée à la sécurité des systèmes d'information s'avère récente pour quelques-unes des sociétés rencontrées. De façon générale, cette décision tardive s'explique par le fait que la menace était considérée comme faible soit parce que l'exposition (informatique) de l'entreprise ne faisait pas craindre d'attaques ou d'actes malveillants – par exemple, dans la mesure où les moyens informatiques de l'entreprise étaient très limités ou peu vulnérables – soit parce qu'elle n'était pas assez connue pour se considérer comme une cible possible.

Pour ces entreprises, le choix de créer un poste ou une fonction RSSI s'insère dans une volonté de protéger des moyens informatiques/réseaux nouveaux en cours de mise en place et pour lesquels une interruption de service aurait des conséquences potentiellement désastreuses. L'évolution générale de la menace – par exemple, au travers d'un transfert depuis une autre activité pour ce qui concerne les grands réseaux d'infrastructure – peut également être à l'origine de la création d'une nouvelle fonction RSSI.

La sécurité numérique comme co-responsabilité de la direction de la sécurité et de la DSI

Dans la plupart des entreprises rencontrées (12 sur 23), la sécurité numérique se trouve sous la tutelle partagée de la direction de la sécurité et de la DSI ou du RSSI. Pour l'essentiel, la direction de la sécurité, qui rend compte directement à la direction générale ou au comité exécutif, a un rôle de synthèse, de standardisation et d'évaluation des risques (avec prise en compte des aspects numériques). Sur ces bases, elle est chargée de ***définir des politiques de sécurité*** (ou des schémas directeurs) ***qui sont validées par le COMEX ou le DG***. Elle ne possède en revanche ni les moyens matériels ni les ressources humaines pour mettre en œuvre et vérifier la réalisation de ces politiques. Elle agit donc comme un maître d'ouvrage alors que la direction des systèmes d'information se positionne comme maître d'œuvre en matière de sécurité numérique.

Ainsi, la DSI et/ou le RSSI sont chargés (1) de participer à l'évaluation des risques et (2) de la mise en œuvre de la politique de sécurité déclinée aux questions relatives aux systèmes d'information. Comme pour le schéma d'organisation précédent, ni le RSSI « groupe », ni la direction de la sécurité n'ont de moyens propres suffisants pour assurer la mise en œuvre de la politique et l'investissement des moyens. Tout au plus, le RSSI de niveau central s'assure que certaines mesures clefs font l'objet d'une généralisation dans l'ensemble du groupe (typiquement, déploiement d'un antivirus unique, etc.). Il revient donc aux responsables de la SSI au niveau des entités locales (filiales, établissements) de s'assurer de la mise en œuvre. Ce réseau sécurité des systèmes d'information (qui est plus ou moins lié au réseau des responsables sécurité) s'avère donc être, pour les grands groupes considérés, le maillon critique du fonctionnement de la politique de SSI.

Or, comme le souligne plusieurs des personnes rencontrées, les besoins de sécurité sont souvent en concurrence avec d'autres postes économiques. Ainsi, la sécurité devient de plus en plus entrepreneuriale : elle se développe au sein de l'entreprise en fonction des contraintes des métiers, en exploitant des ressources limitées et en se fixant des

objectifs. Au final, il ne s'agit plus de tout protéger à des niveaux équivalents – cela serait trop coûteux – mais de faire des choix. Ces derniers sont pris par les responsables de métiers, voire dans certains cas, au niveau des entités élémentaires (business unit, laboratoire, bureau d'études) si celles-ci sont en charge de leurs budgets.

L'un de nos interlocuteurs indique que son entreprise envisage la ***création d'un pôle interne centralisé d'expertise en sécurité numérique*** mais une telle démarche suppose une cartographie précise des compétences existantes au sein du groupe.

Si le découpage maître d'ouvrage/d'œuvre s'applique dans l'essentiel des cas, il existe des spécificités selon que l'entreprise concernée fait face plutôt à un risque à caractère informationnel ou des vulnérabilités matérielles et/ou informatiques. Ainsi, dans le premier cas, le rôle de la direction de la sécurité est prépondérant et la DSI intervient plutôt en soutien (matériel ou intellectuel). *A contrario*, pour les entreprises pour lesquelles la continuité d'activité informatique est critique, la direction de la sécurité prescrit mais le RSSI est l'acteur fonctionnel pour la mise en œuvre et le suivi des actions. Enfin, dans les entreprises qui ont des responsabilités en termes de sécurité humaine, la direction de la sécurité est responsable de la fonction de protection face au risque de matérialisation physique des menaces informatiques.

La vérification de la mise en œuvre peut revenir à la direction de la sécurité ou à celle chargée de l'audit et du contrôle qui peuvent ponctuellement faire appel à des opérateurs extérieurs, par exemple pour des tests d'intrusion. De façon générale, l'existence d'un contrôle de conformité confronte les plans et mesures spécifiés par l'échelon central avec les réalités économiques des unités élémentaires ou celles des entités régionales. En d'autres termes, des écarts par rapport aux standards sont tolérés si : (1) ils sont justifiés par des choix économiques et (2) ils ne portent pas sur des éléments de sécurité considérés comme obligatoires par la politique (par exemple : chiffrement des disques durs, présence de l'antivirus). Certaines des personnes rencontrées jugent toutefois que le manque de contraintes (comme celles qui peuvent peser sur le secret de la défense nationale) conduit à donner un poids plus important aux problématiques d'économies de préférence à celles de sécurité.

A.– Les relations avec les services de l'Etat

Il paraît utile de souligner que dans la majorité des cas, la Direction de la sécurité est chargée des contacts institutionnels dans le domaine de la sécurité sans pour autant avoir de relations exclusives avec certains d'entre eux. Elle a ainsi en charge les aspects communication en particulier vers l'extérieur, qu'il s'agisse des services de l'Etat, y compris d'ailleurs les enquêteurs dans le cadre de commissions rogatoires, des Douanes ou de la Direction centrale du renseignement intérieur, ou des autres entreprises.

Les relations avec les services responsables en matière numérique, notamment l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la Commission nationale de l'informatique et des libertés (CNIL), peuvent se révéler un peu plus complexes.

- Si la relation avec la CNIL est en général bien cadrée – du fait de la prise en compte des obligations réglementaires ou légales qui pèsent sur l'entreprise – le contact avec l'ANSSI est parfois plus compliqué. Pour certains des interlocuteurs, l'agence est encore trop peu réactive et s'intéresse encore trop aux grands comptes liés à l'Etat plutôt qu'à l'ensemble du tissu économique.

- Dans les situations de gestion de crise, ils estiment relativement inutile de se rapprocher de l'agence même si, une fois la crise réglée, un dialogue paraît nécessaire.

- Une majorité des personnes rencontrées note cependant une amélioration de la capacité de l'ANSSI à intervenir dans les dossiers d'actualité ou encore à diffuser des alertes critiques. Ils attribuent ces améliorations aux efforts de l'agence pour renforcer ses équipes et sortir du cadre imposé précédemment par son statut de direction centrale.

B.– La question (délicate) de la déclinaison des principes de sécurité dans l'ensemble de l'entreprise

Le niveau d'organisation à l'échelon central donne une image relativement incomplète de la structuration de la fonction sécurité numérique au sein des groupes rencontrés. En effet, pour la majorité d'entre eux, ils rassemblent plusieurs dizaines d'entités locales ou de filiales qui sont parfois réparties dans de nombreux pays et sont responsables individuellement de leur sécurité.

La mise en œuvre concrète de la politique de sécurité numérique décidée au niveau central – y compris le contrôle – se heurte dans les faits aux situations spécifiques de ces entités, notamment, comme nous l'avons vu, les moyens dont elles disposent, leur culture d'entreprise, les métiers dans lesquels elles exercent, voir même, les endroits où elles sont implantées. De la même façon, la taille même des entreprises concernées conduit à des effets importants d'inertie : les changements fréquents d'orientation sont dans les faits irréalisables alors même qu'il faut prendre en compte un contexte de sécurité évoluant rapidement.

Certains groupes sont également confrontés à la problématique de la jeunesse relative de leur constitution. Ils peuvent même dans certains cas appartenir à des conglomérats plus importants et rassembler des entités anciennes très autonomes. Dans un des cas rencontrés, la fusion se fait progressivement depuis 10 ans et doit prendre en compte le problème ***de convergence des systèmes d'information et d'harmonisation des logiques de sécurité.***

Pour certaines des personnes rencontrées, il est donc essentiel de mailler l'entreprise de correspondants locaux de sécurité – dont le rôle englobe la veille et l'alerte – et d'essayer d'amener l'ensemble à un niveau cohérent minimal de prise en compte des questions de sécurité numérique. La direction de la sécurité tient alors un rôle opérationnel en soutien des entités, pour la formation et l'assistance technique. Elle doit aider au déploiement des solutions de sécurité qu'elle prône pour faciliter leur fonctionnement au niveau des entités du groupe.

Au-delà de la problématique, importante, de la mise en œuvre harmonieuse des politiques de sécurité numérique, de nombreuses entreprises appliquant ce schéma ou l'un des deux autres font face à des difficultés spécifiques aux intervenants extérieurs (prestataires, sous-traitants).

La direction de la sécurité numérique confiée à un groupe collégial

Dans quelques cas (3 sur 23), la direction de la politique de sécurité numérique est confiée à un groupe collégial qui est chargé de réunir l'ensemble des intervenants concernés (juridiques, communications, informatique, sécurité, audit...). Il convient de souligner que, si elles ne font pas forcément appel à un collège ayant des attributions de direction, plusieurs entreprises fonctionnant selon les schémas précédents mettent également en place des groupes d'échange ou de travail permettant de réunir de façon périodique les principaux acteurs de la sécurité numérique de l'entreprise.

Dans le schéma collégial, le groupe valide et pilote les analyses de risques et les politiques de sécurité qui déclinent les mesures à prendre pour aborder les problématiques identifiées. Il convient de souligner que dans plusieurs schémas précédemment identifiés, il est commun que l'effort d'analyse du risque soit conduit de façon collégiale, en associant d'ailleurs également les responsables des principaux métiers.

La mise en place de ce type de fonctionnement prend en compte trois éléments :

- la sécurité numérique concerne de nombreux acteurs au sein de l'entreprise, le directeur de la sécurité et le RSSI en font partie mais leur mission est davantage de s'assurer de la réalisation des plans que de les définir seul. Une évolution de ce type part du constat selon lequel les risques informatiques doivent être comparés avec les autres facteurs afin d'établir leur importance relative. Sur cette base, le groupe propose des options stratégiques, mais le choix (la décision finale) revient au comité exécutif qui porte les risques et aux branches métiers.

- une instance de haut niveau a paru nécessaire pour animer un réseau de sécurité cohérent qui rassemble les acteurs techniques (appartenant à la DSI) et les responsables locaux ou régionaux de la sécurité (appartenant à la direction de la sécurité). Son rôle est donc de faciliter l'échange d'information avec les échelons opérationnels dans un sens pour la remontée d'informations et l'alerte, et dans l'autre, pour la prescription de mesures de sécurité. Il est également chargé d'assurer la transmission des informations critiques aux autorités de l'entreprise à des fins autant pédagogiques qu'opérationnelles.

- Le contrôle de la réalisation des mesures de sécurité devrait être conduit sous la responsabilité d'un « collège » qui ne participe pas directement à cette mise en œuvre. Dans l'ensemble des cas dans lesquels cette collégialité existe (sous une forme aussi structurée qu'un comité de la sécurité des systèmes d'information), la fonction de contrôle s'opère avec un soutien extérieur. L'un des interlocuteurs souligne cependant qu'il convient de ne pas trop déléguer le contrôle car cela doit rester une démarche interne, l'autonomie de l'analyse étant cruciale.

Dans ce schéma d'organisation, les directions conservent leurs fonctions et leurs attributions opérationnelles. Le rôle du collège est avant tout d'examiner les risques de façon périodique plus ou moins fréquente et si nécessaire d'orienter la stratégie de l'entreprise. Dans l'un des cas, le collège se réunit de façon très fréquente pour procéder à une évaluation « dynamique » des risques numériques. Cette notion d'évaluation et de réorientation permanente est loin de faire l'unanimité des personnes rencontrées. Toutefois, certaines considèrent comme indispensable une évolution rapide de la

posture de sécurité comprenant une réorganisation très fréquente de la fonction et des retouches permanentes de la politique.

Dans un cas rencontré, il existe par ailleurs un ***collège qui est chargé de façon informelle et ponctuelle d'examiner les incidents numériques importants***. Il rapporte à la direction générale et peut proposer des orientations. Il sert également à effectuer des retours d'expérience afin de progresser sur les sujets. Par exemple, cette entreprise déclare vouloir travailler sur la préservation des « scènes de crime numériques ». Ce comité permet d'avoir une vision et de développer une doctrine homogène pour le groupe. Cela peut se traduire par des notes d'information ciblées pour répondre à un risque tendanciel.

A.– Le cas spécifique de la création d'une Direction de la sécurité numérique

Dans un des cas, l'entreprise a effectué le choix de créer une direction chargée de la sécurité numérique c'est-à-dire de la protection des données et informations dématérialisées et celle des systèmes d'information. La nouvelle direction est séparée de la direction des systèmes d'information dans la mesure où il s'agit clairement de séparer le maître d'ouvrage et le maître d'œuvre.

Cette direction est chargée de trois missions spécifiques :

- Participer à la maîtrise d'ouvrage et assister au développement et au déploiement des moyens informatiques,
- Renforcer la gestion/maîtrise des risques : définir la cartographie des risques, établir une politique de sécurité numérique,
- Renforcer les actions de contrôle et d'audit.

Cette direction est donc rattachée au contrôle général du groupe qui rapporte au président. Elle s'appuie sur deux outils :

- Au niveau local un réseau d'officiers de sécurité de zone qui déclinent la politique de sécurité numérique. L'entreprise met également en place des coordinateurs de la protection de l'information dont le rôle est de coordonner la zone avec les actions transverses de l'entreprise : ils doivent identifier les données sensibles, les risques métiers et s'assurer que les dispositifs en place sont conformes au besoin.
- Une cellule de sûreté économique, sorte d'observatoire (qui n'a pas pour vocation à coordonner) qui comprend le DSN, le directeur de la sûreté, le directeur éthique et évaluation des risques. Ce collège partage les retours sur les événements incidents internes et externes. Il n'a pas de rôle prescriptif même s'il peut proposer des pistes d'amélioration ou d'évolution et pousser ces propositions vers le Comité des Risques ainsi que vers les membres du Comité Exécutif concernés auxquels il rend compte périodiquement de ses travaux.

Politique et moyens dédiés à la sécurité numérique

La prise en compte des risques numériques au travers des organisations mises en place par les groupes rencontrés montre que ces éléments constituent une préoccupation centrale en termes de sécurité.

Cette réalité se concrétise également dans les efforts réalisés par ces entreprises pour imposer à tous les utilisateurs l'emploi de certains moyens et outils permettant d'obtenir un niveau de sécurité minimal commun. Outre le déploiement de solutions de protection contre les codes malveillants, les firewalls ou encore les logiciels de filtrage du courrier ou de blocage de sites, on retrouve dans beaucoup d'entreprises : le chiffrement des sessions, celui des disques durs, l'utilisation de *token* physiques d'identification pour les sessions, la mise en place de filtres sémantiques pour le choix des mots de passe ou encore la sauvegarde automatique des données. Certaines entreprises ont d'ailleurs mis en place ces mesures de sécurisation des sessions bureautiques de façon à être interopérables avec les filiales et les fournisseurs de service qu'elles emploient.

L'une des personnes interrogées souligne que l'un des défis de sécurisation est de faire venir les utilisateurs à la sécurité plutôt que de les obliger à appliquer des mesures qu'ils ne comprennent pas ou qu'ils trouvent inutiles, voire incompréhensibles. Il faut pouvoir intégrer le plus en amont possible la sécurité comme un métier (un besoin) parmi d'autres plutôt que de passer son temps à en faire (avec le contrôle) une question trop spécifique. Par exemple, le poste de travail bureautique doit allier la convivialité, l'ergonomie, l'efficacité et la sécurité. Les collaborateurs doivent participer à la sécurité de façon naturelle et l'entreprise doit tirer le meilleur parti des solutions qui existent pour rendre ce réflexe naturel (essayer autant que possible d'intégrer dans les produits : chiffrement de disque dur sous *windows 7*, protocoles de chiffrement des connexions sans fil ou de contrôle de connexion, sauvegarde des données, etc.).

La question de la lisibilité de la politique de sécurité au niveau des collaborateurs se pose dans certaines entreprises. Ainsi, l'un des interlocuteurs a indiqué que les documents de référence dans ce domaine peuvent être trop nombreux (ou trop denses) pour que les collaborateurs les assimilent et en appliquent efficacement les principes. Le problème du « corpus documentaire » doit trouver une solution au travers de la rédaction de guides pratiques qui mettent en valeur les notions de base élémentaires. D'autres documents simples, comme des codes de conduite ou de bonnes pratiques sont également rédigés et distribués par certaines entreprises. De nombreux groupes font également signer à leurs collaborateurs des chartes pour l'utilisation des systèmes d'information et l'usage des données ou des informations dématérialisées.

Dans le même ordre d'idée, quelques entreprises s'interrogent sur la manière de *gérer les entrées/sorties* des collaborateurs mais également des filiales en termes de sécurité numérique.

L'un des incidents rencontrés par l'une d'entre elle – la pénétration du réseau interne grâce au réseau d'une société n'appartenant plus au groupe – conduit à s'interroger sur les conditions dans lesquelles on accompagne techniquement et juridiquement les aléas de la vie d'un groupe. Cette problématique se rapproche de celle portant sur la gestion de la confidentialité des informations sachant que – en dehors des documents et informations protégés par le secret de la défense nationale – le cadre juridique portant sur le statut des données (non personnelles, cf. supra) manipulées par les (ex)collaborateurs est parfois mal connu, et que les mesures permettant de mieux le maîtriser n'ont pas été toujours prises. Cette difficulté complique les efforts que peuvent entreprendre certaines sociétés pour procéder à la « classification » des informations qu'elles détiennent. Cette question s'étend d'ailleurs également à l'utilisation de ces données/informations par des fournisseurs ou des tiers intervenant au profit de

l'entreprise. Au final, les éléments contractuels doivent être suffisamment précis pour englober la responsabilité du sous-traitant à un niveau équivalent à celui des sociétés appartenant au groupe. Ainsi, quelques entreprises affirment cadrer les sous-traitants au travers d'une politique contractuelle très contraignante sur la sécurité, le maintien de la confidentialité des informations ou encore la continuité d'activités.

En l'absence d'un cadre juridique clair, un interlocuteur souligne que les logs des connections des employés sont difficilement utilisables dans le cadre d'enquêtes internes même sous la responsabilité d'un service spécifique et sur la base de raisons légitimes. Ce n'est pas aux responsables de la personne mise en cause de conduire sa propre enquête et c'est cela qui rend l'enregistrement des logs acceptables par les salariés.

L'une des personnes interrogées souligne toutefois que la tendance est plutôt à la clarification des textes de loi ou des règlements, parfois d'ailleurs sous la contrainte juridique ou réglementaire (type loi Sarbanes-Oxley). A ses yeux, le renforcement des dispositions sur la protection des données personnelles doit être considéré à ce titre comme une évolution positive. Le cadre juridique – quand il est clair et précis – s'avère en fait être d'une grande aide et simplifie le travail de sécurisation[11].

Vers un isolement physique ou logique des équipes de projet travaillant sur des programmes critiques

La sécurité des informations patrimoniales (compétences, savoirs et savoir-faire spécifiques à l'entreprise) et, dans une moindre mesure, des données personnelles, doit prendre en **compte la tendance actuelle à la coopération en ligne entre des sites géographiquement distants**. Il peut s'agir de co-développement entre des entreprises appartenant à une même *joint venture*, de travaux de R&D menés dans plusieurs laboratoires ou simplement de projets conduits par des équipes situées dans des établissements différents.

Cette situation conduit quelques-unes des entreprises à réfléchir aux moyens de mieux protéger les informations qui transitent ainsi :

- Il peut s'agir d'isoler (y compris géographiquement) quelques équipes qui travaillent sur des projets jugés stratégiques en fonction de la stratégie de l'entreprise, de l'investissement lié au projet (donc des retombées économiques attendues) et de la démarche qui le sous-tend (projet structurant pour l'avenir). Mais la bulle n'est pas que numérique ; elle doit comprendre une part de sécurité physique, sociale et doit être régulièrement testée pour voir si elle reste sûre.

- Une autre entreprise qui capitalise sur son empreinte géographique relativement limitée, indique que tous les nouveaux projets font d'abord l'objet d'un rassemblement physique des équipes pendant plusieurs mois avant, éventuellement, de séparer les participants dans leurs établissements d'origine.

- De fait, l'apparition de solutions permettant de séparer au niveau logique des environnements de travail a été citée, en particulier par les entreprises ayant une importante activité de recherche-développement, comme un progrès notable permettant d'apporter des débuts de réponse à ce problème. Enfin, le

[11] Pour plus d'éléments sur cette question, cf. infra.

cloisonnement des accès fait partie de la politique de certaines entreprises. Il vise à limiter ce qu'une personne peut obtenir comme données en termes d'accès physiques comme logiques.

Quelques entreprises ont créé des centres d'opération

Pour l'instant, seules 4 des entreprises rencontrées (17%) possèdent ou sont sur le point de créer un centre d'opération qui a pour vocation à être disponible de façon continue. Si pour l'essentiel, ces centres sont dédiés à la sécurité numérique, dans au moins l'un des cas, il a été précisé que sa fonction couvrait de façon plus générale les incidents ayant un impact sur l'entreprise en termes de sécurité. Certains groupes, qui ne possèdent pas forcément une telle organisation, considèrent que le réseau de SSI a vocation à produire une veille permanente et à alerter en temps réel l'échelon central sur les incidents les plus graves.

Les fonctions et attributions de ces centres d'opération sont plus ou moins étendues :

- *A minima*, les centres d'opération sont chargés d'assurer la veille sur les incidents de sécurité et d'alerter (l'échelon central et les responsables locaux) en cas de détection d'une intrusion ou d'un événement grave.
- Ils peuvent en outre participer aux travaux sur l'évaluation des risques ou aux réflexions sur les retours d'expérience. Il communique alors avec (1) le dispositif des responsables locaux de la sécurité des systèmes d'information et (2) avec le groupe ou le collège qui pilote la politique de SSI du groupe.
- Pour un des groupes rencontrés, le centre participe au déploiement global des solutions de sécurité, à la gestion des mises à jour et du fonctionnement. Il peut également soutenir des entités en cas de problèmes et participer à la gestion de crise. En revanche, il n'a pas vocation à participer à la veille sur les menaces.

Si les centres d'opération sont généralement dirigés et armés par la direction de la sécurité, il existe au moins un cas de figure dans lequel une entreprise envisage de sous-traiter cette fonction à un opérateur extérieur et de la délocaliser dans un pays tiers.

Les centres opérationnels ont parfois vocation à être les précurseurs ou les porteurs d'une fonction de ***suivi et de détection des signaux faibles*** susceptibles de se transformer en risques pour l'entreprise, son patrimoine ou ses clients. Quelques entreprises ont mis en place ou envisagent de le faire, une politique qui se fonde autant sur la planification/préparation face à la matérialisation de risques détectés par cette technique qu'à des efforts visant à se doter de moyens de conduite de crises.

La sensibilisation et la formation sur la sécurité numérique sont l'une des priorités des entreprises

La formation et la sensibilisation sur les questions de sécurité numérique semblent être pratiquées par l'ensemble des entreprises concernées, même s'il existe des niveaux d'efforts et d'investissement variables. L'importance donnée à ces politiques de formation est évidemment davantage prononcée pour les entreprises qui considèrent que la vulnérabilité « humaines » est importante.

Pour autant, comme le souligne une des personnes rencontrées, il faut noter l'existence de deux tendances antinomiques : d'une part, on ne peut pas tout miser sur l'utilisateur et il faut concevoir la sécurité en imaginant que l'utilisateur va faillir. D'autre part, les failles ou les attaques importantes (en particulier les APT – *Advanced Persistent Threat*) sont le plus souvent détectées par les utilisateurs. Il est donc indispensable de faire de l'information, de la sensibilisation et de la formation.

Par ailleurs, au-delà des moyens déployés – dont on peut *a minima* noter qu'ils peuvent être relativement importants quand il est nécessaire d'atteindre tous les collaborateurs de l'entreprise et qu'ils comprennent souvent des outils de *e-learning* – se pose la question de l'adaptation des messages et des formations aux populations visées. La moitié environ des entreprises rencontrées (11 sur les 23) affirment chercher à adapter les formations aux métiers qui sont concernés. La plupart s'appuie pour conduire leurs campagnes sur la direction de la communication et parfois sur d'autres directions de l'entreprise (juridique). Plusieurs font appel aux services de l'Etat, en particulier à la Direction centrale du renseignement intérieur, pour effectuer des sessions de formation.

La formation et la sensibilisation des informaticiens, singulièrement des administrateurs de réseaux, sont pour quelques entreprises une priorité. Elles doivent permettre, comme le souligne l'une des personnes rencontrées, d'éviter que ne s'installe dans ces populations qui sont en première ligne en termes de sécurité une trop grande confiance. De la même façon, plusieurs entreprises soulignent la prise en compte d'un objectif de sensibilisation des décideurs (comité exécutif ou « top management »). Bien entendu, il faut s'adapter aux difficultés propres à cette population. Un de nos interlocuteurs indique qu'il peut être utile de s'appuyer sur des incidents récents pour faciliter la transmission de messages.

Pour une majorité des entreprises rencontrées, il existe deux niveaux de formation : directement après le recrutement qui permet généralement de présenter les risques, la politique de sécurité mise en place et les outils de l'entreprise. Ensuite, dans le cycle de vie de l'employé, se déroule des modules spécifiques sur les SI et leur sécurité.

Le recours à des campagnes d'information à vocation universelle a aussi été pratiqué durant les dernières années par quelques entreprises. Leur développement est conduit en en coopération avec la direction de la communication et associe la direction dont l'exemplarité en la matière est jugée absolument indispensable par plusieurs interlocuteurs.

Dans un des cas rencontrés, l'entreprise a ainsi engagé un programme mondial de sensibilisation à la protection de l'information avec du *teasing* (1 semaine), puis une journée ludique et pédagogique au niveau central (vidéos, *serious gaming*, conférences). Des outils ont été fournis aux filiales pour monter des campagnes du même type. Depuis lors, il semblerait que la remontée d'information soit meilleure et on assiste à la mise en place d'un véritable « civisme d'entreprise » : le collaborateur devient un acteur de la sécurité et en tant que tel il doit être soutenu dans sa démarche de sécurité. Cette notion de responsabilisation des collaborateurs est souvent décrite comme un enjeu clef des efforts de formation et de sensibilisation.

L'une des personnes rencontrées considère d'ailleurs que les supports actuels ne sont pas adaptés car trop statiques (ça n'intéresse personne). Or, il s'agit d'expliquer et de convaincre les collaborateurs pour changer de culture : il faut pouvoir montrer,

communiquer intelligemment sur la sécurité comme savent le faire les Anglais : être convaincant et faire « sexy » mais également utiliser les références culturelles de la société (ex. sécurité physique des banques). Il souligne qu'il faut aussi, pour être efficace, pouvoir manier le bâton aussi bien que la carotte. La difficulté en la matière est avant tout juridique : même si les salariés signent souvent des chartes d'utilisation des moyens informatiques, ces dernières sont rarement opposables.

La question se pose enfin de mesurer effectivement l'efficacité de ces efforts. Si certains indicateurs peuvent offrir des informations utiles, c'est le cas par exemple pour le niveau de perte/vol des ordinateurs portables, il demeure difficile d'imaginer des métriques suffisamment pertinentes pour répondre à cette question.

Eléments de réflexion sur la problématique des ressources affectées à la sécurité numérique

Plusieurs facteurs font qu'il est difficile de préciser ce que représente réellement l'investissement des entreprises en matière de sécurité numérique (fongibilité des efforts, pénétration sécurité physique/numérique, activités de l'entreprise et métiers impactés...). Cependant, on peut schématiquement aborder la question sous deux angles : celui des moyens humains consacrés à la fonction « sécurité des systèmes d'information » et celui de la part du chiffre d'affaires (voir du budget de fonctionnement de la direction des systèmes d'information) investie dans les moyens déployés.

S'agissant des moyens humains consacrés à la sécurité des systèmes d'information, les groupes rencontrés ne fournissent pas toujours de données précises. Toutefois, à la lumière des informations fournies qui distinguent l'échelon central et le réseau SSI/sécurité, la fonction occupe à temps plein quelques dizaines de personnes pour des entreprises qui emploient généralement plusieurs milliers de salariés. Si l'on ajoute les correspondants sécurité des métiers, les membres des réseaux SSI dont la sécurité numérique n'est pas la fonction principale, on arrive à plusieurs centaines de personnes qui participent à la mission.

Sous l'aspect budgétaire, les retours sont assez cohérents des données sur les emplois consacrés à la sécurité numérique. On peut estimer qu'une part du chiffre d'affaires situé entre 0,5 et 2% est généralement affectée à la sécurité des systèmes d'information, soit entre 10 et 20% du budget de la direction informatique. Là encore, les personnes ayant fourni des informations chiffrées insistent sur le fait qu'il convient de mieux préciser le périmètre de la fonction avant d'être en mesure de proposer une estimation plus précise : faut-il inclure la protection physique des installations abritant des moyens informatiques ? Les efforts de protection des données ou encore les coûts indirects pour des équipements ou des investissements qui participent partiellement à la sécurité numérique ?

Conséquences pour les entreprises du développement des contraintes juridiques et légales

Selon le secteur dans lequel elles évoluent, les entreprises rencontrées sont confrontées à l'existence de dispositions juridiques et réglementaires. Parmi les mesures spécifiques, on peut notamment relever : celles portant sur la protection des données personnelles,

qui affectent pour l'instant les opérateurs télécom, celles portant sur la protection des opérations bancaires ou encore la vigilance des établissements financiers, les dispositions relatives à la protection du secret de la défense nationale et, enfin, les mesures spécifiques aux établissements d'importance vitale.

Il convient d'ajouter que la grande majorité des entreprises rencontrées sont soumises pour des raisons diverses à certaines des dispositions de la loi informatique et libertés. La plupart dispose d'ailleurs d'un correspondant CIL, qui est souvent le responsable SSI de l'entreprise.

Au niveau international et européen, globalement, on retrouve le même type de mesures qui peuvent être complétées le cas échéant par des textes portant sur le chiffrement des données, des dispositifs permettant la fouille aux frontières des moyens informatiques (portables) ou encore permettant à certaines agences d'accéder aux données stockées sur le territoire du pays concerné.

Ainsi, il existe un enchevêtrement de mesures légales ou réglementaires de sécurité, qui se déclinent au niveau national, européen et international. Certaines entreprises doivent littéralement suivre et gérer des dizaines de textes qui peuvent parfois créer des niveaux de contraintes économiquement ou techniquement ingérables : il existe parfois un risque, relevé par certains interlocuteurs, de voir la transcription de textes européens dans le système national conduire à des aberrations.[12]

Le « paquet télécom » de la Commission européenne créé de nombreuses obligations en termes de conservation et de protection des données personnelles, sur la continuité du service ou encore sur la transparence vis-à-vis de l'Etat et du public sur les incidents, en particulier les pertes de données. Sur ce dernier point, les opérateurs sont obligés depuis 2012 de rendre compte à la CNIL des incidents majeurs (ce qui laisse une marge d'interprétation). La CNIL décide des suites à donner qui peuvent comprendre des amendes et des processus d'information vers les clients concernés.

L'une des préoccupations partagées par plusieurs entreprises (du secteur des services aux personnes) est de voir les dispositions sur les données personnelles s'appliquer à leur activité. L'un des interlocuteurs souligne qu'elles conduisent dans les faits à handicaper les sociétés sérieuses – c'est-à-dire celles qui feront un effort pour se doter des moyens de détecter les vols de données et qui les rapporteront à la commission – par rapport à celles qui expliqueront ne pas avoir les moyens de détecter efficacement les vols.

L'une des questions qui découlent de la généralisation de cette mesure porte sur la différence entre le temps de la gestion administrative et judiciaire et celui de la gestion de crise. En clair, plusieurs entreprises considèrent qu'avant de déclarer aux autorités une perte de données, elles devraient d'abord pouvoir prendre (rapidement) des mesures correctives. Elles craignent que la transmission de l'incident conduise à une publicité qui interdirait effectivement une gestion sereine du problème au niveau interne alors même que le temps administratif/juridique est plutôt long.

[12] Cf. infra sur le paquet télécom.

Par ailleurs, quelques entreprises se sont interrogées sur la possibilité de rendre obligatoire l'utilisation de produits certifiés pour la protection des systèmes et des informations. Ainsi, les sociétés respectant la loi n'auraient pas, en cas d'incident ou d'attaque, à démontrer systématiquement avoir fait les bons choix en matière de sécurité. Un tel outil juridique permettrait d'éviter que certaines entreprises fassent totalement l'impasse sur la sécurité numérique – et notamment la protection des données personnelles – pour des raisons économiques.

Au fil des entretiens, il est apparu qu'il existe schématiquement deux approches des contraintes légales :

- La première consiste à prendre en compte les éléments existants et à les appliquer de façon mécanique en évitant des effets néfastes sur les opérations et le fonctionnement de l'entreprise. Certaines personnes indiquent que le cadre n'est pas forcément très pesant mais souvent trop peu adapté à la réalité des entreprises et de l'économie mondialisée pour être utiles ou efficaces.

- La seconde, qui est finalement assez répandue, consiste en une lecture relativement positive des contraintes réglementaires et juridiques ***à condition qu'elles soient claires et transposables de façon fonctionnelle*** (ce sur quoi ils rejoignent les premiers). Pour les personnes concernées, le développement du cadre légal et réglementaire permet (1) de pousser les équipes dirigeantes à adopter des mesures de sécurité qui sont par ailleurs jugées indispensables et (2) de faciliter la sensibilisation des collaborateurs et la mise en œuvre des politiques de sécurité.

  Comme le souligne l'une des personnes rencontrées, il faut appliquer les dispositifs légaux selon les contraintes locales. Elles lui apparaissent un peu insuffisantes en France par rapport aux Etats-Unis. L'Etat ne contraint pas réellement pas plus qu'il n'accompagne les entreprises en matière de sécurité numérique : aucune démarche d'ampleur sur la protection des travaux de recherche et développement, aucun effort de protectionnisme alors que certains pays mènent une véritable guerre commerciale (*dumping* accompagné d'actions d'espionnage systématiques).

  Autre problème relevé par l'un des interlocuteurs, **la coopération judiciaire internationale s'avère encore très insuffisante par rapport aux enjeux économiques liés à la cybercriminalité.** La convention de Budapest (2001) n'a pas été suffisamment ratifiée et peu d'efforts ont été entrepris pour harmoniser les législations nationales. La question de la « preuve numérique », par exemple, est abordée de façon différente par les Etats.

  Enfin, quelques personnes rencontrées se sont étonnées de l'absence d'un outil juridique qui permette **d'imposer un certain niveau de confidentialité aux informations non industrielles détenues par leurs entreprises** (de type secret des affaires).

Perspectives et recommandations

Cette enquête permet de mettre en valeur les efforts qui ont été entrepris par plusieurs grands groupes français pour prendre en compte les problématiques relatives à la sécurité numérique à la fois en termes d'évaluation de risque, d'organisation, de stratégie et de moyens.

Même s'il existe des différences d'approche, on peut estimer que les groupes rencontrés partagent une vision globalement cohérente de leur environnement et ont su prendre la mesure de leurs spécificités pour adapter leur politique.

Il resterait sans doute à savoir dans quelle mesure les dispositifs mis en place ou en cours de développement répondent efficacement aux menaces qui existent ou qui existeront bientôt. Sur ce point, on peut remarquer que la plupart des entreprises reconnaissent que la question de la détection des actions malveillantes s'avère être une question clef : les efforts de certaines entreprises sur le traitement des signaux faibles, ou encore la détermination à créer des dispositifs d'alerte et de gestion de crise témoignent du fait qu'il reste encore, du point de vue de nos interlocuteurs, beaucoup à faire.

Autre point important, il semble important de souligner que les systèmes d'information et les données qu'ils manipulent sont le plus souvent devenus vitaux pour les entreprises. Celles-ci peuvent fonctionner dans divers modes dégradés ou avoir les moyens de rétablir (plus ou moins rapidement) des réseaux attaqués, surveillés ou infectés, voire récupérer des données ou informations corrompues. En revanche, ces incidents peuvent avoir des conséquences, en particulier économiques, cataclysmiques pour une société. Le « vol » d'informations patrimoniales sur un projet en développement peut condamner un programme à la faillite, l'arrêt de fonctionnement d'une salle de marchés peut conduire des sociétés à la banqueroute.

De fait, tous les outils numériques existants tout comme ceux qui se déploient aujourd'hui (on pense au *Cloud*) ou se développeront demain (internet des objets) sont à la fois des sources de vulnérabilités pour les entreprises mais également des leviers fonctionnels, économiques et opérationnels incontournables.

En guise de conclusion, il paraît utile de relever quelques-unes des leçons qui peuvent être tirées des discussions que nous avons pu avoir avec les personnes rencontrées :

- **Les collaborateurs sont à la fois des sources possibles de vulnérabilités mais également l'un des remparts les plus importants** pour la protection des systèmes d'information et des données. Il est donc vital de pouvoir s'appuyer sur eux tout en reconnaissant que la plupart des menaces se matérialisent par leur biais.

- Quelle que soit l'organisation retenue pour piloter la politique de sécurité numérique, elle doit associer dans **un système collégial** les parties prenantes stratégiques (direction de la sécurité), techniques (direction des SI) et opérationnelles (audit, juridique, com., métiers...). Ce collège sert autant de

cénacle de réflexion sur les incidents rencontrés (pour le retour d'expérience) que de courroie de transmission entre le réseau SSI et les dirigeants de l'entreprise.

- A terme, il faudra envisager, en particulier pour les entreprises de R&D, de pouvoir **pratiquer l'isolement logique, voire physique des équipes travaillant sur des projets futurs.** Par ailleurs, l'intégration de la fonction sécurité numérique dans les programmes de développement pourrait se faire de manière comparable aux autres fonctions métiers.

- **La question du cadre juridique et de l'accompagnement des entreprises continue de se poser.** Les efforts des agences nationales, en particulier de l'ANSSI mais également de la DCRI, pour épauler les sociétés sont souvent cités en exemple. Les responsables rencontrés semblent souhaiter que le cadre juridique national continue de s'étoffer, tout en soulignant qu'il doit rester applicable et cohérent des impératifs économiques des entreprises.

Annexe 1 - Grille des questions

1. **Perception des principales menaces/risques** :

   - Votre société a-t-elle déjà été victime d'attaques numériques sur ses moyens, ses ressources humaines ou sa réputation ? Quelles en ont été les conséquences ?
   - Quelles vulnérabilités numériques votre société considère-t-elle comme les plus dimensionnantes/contraignantes pour son fonctionnement ?
   - Quelles menaces cyber existantes ou susceptibles de se développer préoccupent le plus votre société/groupe ?

2. **Structures de sécurité numérique** :

   - Quelle direction est responsable de la sécurité numérique au sein de la société ? Quelles sont sa place et son rôle dans la structure ?
   - Selon quels axes stratégiques (analytiques) avoir fait ces choix ?
   - Quelle est l'articulation entre sécurité numérique et sécurité générale dans la société ? articulation entre sécurité numérique et gestion des moyens cyber/informatiques ?
   - Quels développements futurs de la fonction considérez-vous comme essentiels/utiles pour répondre à l'évolution des menaces ?

3. **Moyens et politique de sécurité numérique** :

   - Quels sont les moyens matériels, logiciels et humains mis en place pour mettre en œuvre la politique de SN de votre société ?
   - Pouvez-vous décrire les politiques de formation et d'information choisies : finalités/objectifs, effets, évolutions nécessaires (selon vous) ?
   - Quelle est la part du budget de sécurité consacrée à la sécurité numérique : pouvez-vous détailler les principaux postes d'investissement ?
   - La direction chargée de la sécurité numérique interagit-elle avec le secteur public (FSI, Justice, ANSSI, autres ?) : comment qualifieriez-vous les relations et leur intérêt pour l'efficacité de la fonction sécurité numérique ?

4. **Questions réglementaires et légales** :

   - Le cadre réglementaire vous paraît-il adapté aux réalités du risque numérique aujourd'hui ?
   - Comment qualifieriez-vous son coût pour votre société par rapport aux bénéfices qu'il génère ?
   - Quelles évolutions considérez-vous comme souhaitables dans ce domaine ?