N° 457 MAI 2016

MENSUEL

le Bulletin de l'ilec

Ceci n'est pas une newsletter

SOMMAIRE

Cybersécurité : impératifs et opportunités

Penser, classer, assurer

Quelques entreprises de grande consommation ont pris pleinement conscience des menaces qui planent sur elles et sur leur secteur en matière de cyberattaques. Mais beaucoup négligent encore les risques, ou ne les appréhendent que sous l'angle des coûts, plutôt que sous celui de la création de valeur.

Entretien avec Alain Juillet, président du Club des directeurs de sécurité des entreprises (CDSE)[1]

Le CDSE compte-il des entreprises de PGC ?

Alain Juillet : Ce club réunit cent dix grandes entreprises industrielles, financières ou autres, au nombre desquelles Danone, Fromageries Bel, L'Oréal, LVMH, Michelin, Nestlé. Mais la grande consommation et surtout l'agroalimentaire y sont sous-représentés, alors que nous apportons une vraie contribution à la gestion de la sécurité, étant à la charnière entre le public et le privé.

La cybersécurité et son écosystème sont-ils bien appréhendés par les entreprises de PGC ?

A. J. : Beaucoup de dirigeants ont du mal à en comprendre l'ampleur et les enjeux. Cela reste pour eux un problème d'antivirus à l'entrée de l'ordinateur. Cette relative cécité me rappelle celle d'il y a quelques dizaines d'années devant la finance et la comptabilité : de gros investissements ont été réalisés par les directions des systèmes d'information, comme hier par les directions financières, sans réelle prise en compte des questions de sécurité. Quand une crise survient, il leur est difficile de reconnaître les failles d'investissements élevés qu'elles ont recommandés. Le même phénomène a provoqué la création de l'audit, pour contrôler la gestion. Les spécialistes cyber n'ignorent pas les problèmes, mais ils ne maîtrisent pas leur complexité dans le domaine de la sécurité, et surtout ils ne peuvent se condamner en reconnaissant leurs erreurs.

Quelles sont les pires menaces ?

A. J. : Le piratage de données (fichier clients, formules en R&D, plans d'action…), les escroqueries (« au président », substitutions de factures ou de virements…) et les chantages (attaques contre les *Scada*, systèmes de contrôle et d'acquisition de données permettant le contrôle à distance des installations techniques). Les piratages sont quotidiens et le fait de *hackers* qui pillent les fichiers ou détournent des documents. L'escroquerie au président coûte cher aux petites et aux grandes entreprises (480 millions d'euros détournés depuis trois ans en France). Michelin a avoué en avoir pâti, mais en général les entreprises restent muettes –

(suite page 2)

Éditorial

L'affaire de tous

Quelque cinq cents millions d'euros de pertes depuis trois ans, en France, pour la seule escroquerie au président, des entreprises rançonnées au bord de la faillite, des emplois menacés… Sans compter celles qui ne parlent pas, de peur de perdre leur réputation auprès de leurs clients, fournisseurs et consommateurs. Entreprises, attention, danger ! L'heure n'est plus à l'espionnage industriel aux manières de barbouzes mais aux attaques de cyberpirates, qui pillent le capital immatériel de l'entreprise, attirés par les données, or blanc du XXe siècle. Ne pas protéger les leurs, c'est, particulièrement pour les entreprises de grande consommation, risquer de perdre rapidement une réputation acquise de longue date, ainsi que des consommateurs soucieux de la sécurité et de l'usage de leurs données personnelles.

Le phénomène ne semble pas encore perçu à son vrai degré de danger par la plupart des entreprises, même si certaines ont commencé à prendre conscience des enjeux. Il oblige à repenser leur gestion à l'aune de la responsabilité de chacun dans l'entreprise, car il en va de son emploi et de celui des autres.

Il n'échappe plus à l'État que le partenariat public-privé a un grand rôle à jouer. L'atteste le Forum international de la cybersécurité, créé à l'initiative de la Gendarmerie et qui a réuni cette année 5 500 participants de 80 pays, ce qui en fait la référence en matière de sécurité et de confiance numérique au niveau européen. Un encouragement, pour les entreprises qui furent pionnières en marketing, à l'être de nouveau en orientant la cybersécurité vers la création de valeur.

Jean Watin-Augouard

>> *suite de la page 1*

jusqu'au jour où des petites déposent le bilan. Les cyberpirates entrent dans l'entreprise et y demeurent en moyenne plus de deux cents jours, pour identifier les fichiers, les codes, les programmes de travail ; et quand ils sont prêts, l'attaque dure quelques secondes.

Enfin le chantage, la recherche d'une rançon sous la menace de détruire l'outil industriel dans une usine, prend de l'ampleur, depuis la première qui visa l'usine atomique de production d'uranium de Natanz en Iran. Un virus placé dans le pilotage des machines altère leur vitesse de fonctionnement de manière brutale et aléatoire, et c'est le chantage à sa complète mise en œuvre, qui détruirait l'usine. Les entreprises de PGC sont les plus exposées à cette menace.

Et les attaques les plus fréquentes ?

A. J. : Les plus fréquentes sont les escroqueries au président, mais les piratages de fichiers augmentent, d'autant plus qu'ils n'intéressent pas que les concurrents. Les plus dangereuses, et nous n'en sommes qu'au début, sont les attaques Scada. Le détournement d'information par des employés aussi est courant : des salariés en place ou quittant l'entreprise vendent à des concurrents ou emportent programmes, plans, brevets, fichiers ; il est facile de sortir des données sur clé USB ou par transfert. Les lois françaises empêchant certains contrôles, il faut trouver un juste équilibre, en accord avec les partenaires sociaux. Ajoutons que certains concurrents français ou étrangers n'hésitent pas à recourir à l'espionnage. La plupart des entreprises de PGC n'ont pas pris conscience des enjeux et sont donc mal ou peu armées.

Qui du terroriste mafieux, de l'« hacktiviste », du concurrent jaloux ou du salarié licencié est le plus actif en matière de cybermenace ?

A. J. : Les terroristes mafieux sont peu nombreux, même si des affaires de chantage ont déjà eu lieu avec des produits pollués. L'agro-alimentaire connaît ce problème depuis longtemps. En revanche, le *hacker* activiste n'en est qu'à ses débuts. Des personnes, pour des raisons idéologiques, défendent certaines causes de manière violente, comme en Grande-Bretagne certains de ceux qui veulent protéger les animaux contre leur usage dans les laboratoires, allant parfois jusqu'à des actes criminels.

Le salarié licencié n'a généralement pas pour ambition de faire du mal à l'entreprise, il veut tirer profit d'informations stratégiques en les vendant au plus offrant ou à la société dans laquelle il arrive, comme dans l'affaire Falciani avec UBS.

La cybersécurité serait-elle créatrice de valeur ?

A. J. : À n'en pas douter ! Les entreprises de PGC ont ainsi construit depuis longtemps un système de prévention des risques à base d'assurance. Or cela n'existe pratiquement pas en cybersécurité, car les entreprises ne l'ont pas encore intégrée à leurs réflexions. Quand elles devront assurer toute la partie cyber de leurs activités, elles s'apercevront qu'elle a une vraie valeur, en raison des primes demandées par les assurances. Et celles-ci vont exiger des règles strictes de sécurité. Aux États-Unis il y a 4 milliards de dollars de primes d'assurances dans la cyber, en France le montant est cent fois moindre.

Comme de responsabilité sociétale, devrait-on parler aussi de responsabilité sécuritaire des entreprises ?

A. J. : Absolument ! Quand Domino's Pizza, aux États-Unis, se fait voler quinze millions de fiches qui circulent sur le *dark web*, sa réputation en souffre auprès de ses clients, d'autant qu'ils sont attaqués individuellement avec demande de rançon à l'écran crypté. L'« e-réputation » dépend de la capacité de chacun à assurer sa propre sécurité.
Aux États-Unis, bien en avance, la fonction de directeur de la sécurité monte en grade, pour être présente dans les comités exécutifs. Avec l'entrée dans le cyberespace et la multiplication des risques, ces entreprises ont compris que les failles sécuritaires sont ce qui peut générer les plus grosses pertes. Il faut pouvoir les prévenir, les anticiper ou y faire face très vite. Qui en est capable ? Un directeur de la sécurité proche de la direction générale.

La protection d'une entreprise contre les cyber-risques est-elle du seul ressort du service informatique ?

A. J. : Non. De même que le comptable ne peut pas signer le chèque, de même le service informatique ne peut pas être seul chargé de la protection contre les cyber-risques. On ne peut pas être juge et partie. La cybersécurité est avant tout une question d'état d'esprit. Pour lutter contre les cyberattaques, il faut qu'à tous les niveaux chacun soit conscient des risques. Les salariés travaillant beaucoup chez eux, les clés USB, ordinateurs

portables et téléphones mobiles sont essentiels dans leur travail. Combien de clés USB plombées, d'ordinateurs pénétrés par un virus, de messages interceptés ? Il est urgent de sensibiliser les salariés. Une faille, c'est à terme un risque pour l'emploi dans une entreprise menacée.

Et les parties prenantes, les fournisseurs ?

A. J. : Oui, car lorsque une entreprise a mis des barrières efficaces à l'entrée, les attaques passent par les sous-traitants ; elle doit donc avoir une politique globale, passer des accords avec eux pour les amener à respecter ses règles de sécurité.

Votre recommandation majeure ?

A. J. : Le vrai problème concerne le secret et ce qu'on doit protéger. Chaque entreprise doit se poser la question de ce qu'il faut protéger et de ce qui ne mérite pas de l'être, car on ne peut pas tout protéger. Il faut identifier le niveau de secret, de 0 à 10, pour toutes les activités, du cœur du réacteur, auquel personne ne doit avoir accès, aux activités banales. Le niveau de cybersécurité ne peut pas être le même dans toutes les activités de l'entreprise, sous peine de coûter trop cher et d'être inefficace.

Les formations universitaires sont-elles adaptées aux enjeux ?

A. J. : Non, car la cybersécurité est un nouveau domaine. Il existe des écoles spécialisées, comme l'Epita, des formations universitaires et des organismes d'État comme l'Anssi, mais ils ne sont pas en nombre suffisant pour répondre à la demande. Il revient aux organisations professionnelles (Medef, CGPME, Ilec…) et aux CCI de sensibiliser leurs adhérents, car la cybersécurité est le grand enjeu des prochaines années. Pour les avoir bien connues, je pense que les entreprises de PGC ont un rôle important à jouer, car elles ont été, sur le plan du marketing, de la connaissance des clients ou de la création de produits, en avance sur les autres. Elles doivent être à la pointe de la cybersécurité.

La « Stratégie nationale pour la sécurité du numérique » présentée le 16 octobre 2015 marque-t-elle un engagement fort de l'État ?

A. J. : L'État a pris conscience du problème, car les premières victimes ont été ses services. L'Anssi, la DGSI, la gendarmerie et certains services de police font un excellent travail de sensibilisation et d'appui. Le secrétariat d'État au Numérique mobilise et coordonne beaucoup d'actions, mais l'État n'a pas les moyens de tout faire. Les organisations professionnelles et les universités doivent prendre le relais.

Qu'attendre du « Service de l'information stratégique et de la sécurité économique », créé le 29 janvier 2016 et rattaché à la Direction générale des entreprises ?

A. J. : À la différence de l'ancienne Délégation à l'intelligence économique qui avait surtout en charge la sensibilisation, la formation et la normalisation, objectifs globalement atteints, ce service a pour vocation d'être opérationnel, d'aider les entreprises à se défendre.

Propos recueillis par J. W.-A.

1. Auteur de Gérer les risques criminels en entreprise : stratégies et comportements pratiques *(De Boeck éditeur, 2012), Alain Juillet a dirigé des entreprises avant d'être directeur du renseignement à la DGSE, puis haut responsable à l'intelligence économique, rattaché au Premier ministre. Il est aujourd'hui conseiller au cabinet Orrick.*

Négligence et crédulité, lit du cybercrime

Dans la majorité des cas, les escroqueries ou les atteintes à la réputation peuvent être anticipées et neutralisées par la sensibilisation et l'acquisition de réflexes de bon sens.

Entretien avec Xavier Leonetti, directeur du service intelligence économique de la gendarmerie nationale.

Comment faire de la cybersécurité une opportunité pour les entreprises ?

Xavier Leonetti : Offrir des solutions de cybersécurité aux salariés dans leur vie de tous les jours est une opportunité : il s'agit de définir les menaces qui pèsent sur leur patrimoine personnel (numéro de compte bancaire, identité numérique, réputation…), de les sensibiliser à la protection de leurs données personnelles pour qu'ils acquièrent des réflexes de sécurité, qu'ils utiliseront ensuite dans leur vie professionnelle.
En partant d'exemples de la vie courante, la cybersécurité se résume à des actes de bon sens : en premier lieu du principe enfantin « je ne parle pas aux inconnus ». Sur Internet, tant de personnes communiquent directement à des inconnus leurs identifiants, mots de passe, numéros de comptes ! Donneraient-elles ces informations à un inconnu qui les aborde dans la rue parce qu'il porte l'uniforme d'un opérateur télécom, d'une banque ou d'une assurance ? Comme on le constate sur les réseaux sociaux à la veille des vacances scolaires, de nombreuses personnes communiquent des informations sur leur vie privée. Auraient-elles envie de distribuer dans la rue des tracts expliquant qu'elles s'apprêtent à partir en vacances, laissant leur appartement vide pour plusieurs jours ?
Cette approche pédagogique est déterminante, au regard de la typologie des cyberinfractions, dont 90 % sont des escroqueries ou des atteintes à la réputation ; le véritable piratage ne concerne qu'une part infime des attaques. La plupart des atteintes reposent sur la confiance des internautes et sur leur crédulité. L'enjeu pour l'entreprise est de développer les outils informatifs et préventifs, généralement peu coûteux, qui permettront de lutter contre neuf menaces sur dix.
Cela acquis, la protection du patrimoine de l'entreprise devient une opportunité. En matière de prévention des escroqueries au faux virement par exemple (lorsque un escroc se fait passer pour un dirigeant de l'entreprise et ordonne un versement financier à l'étranger), la sensibilisation des salariés chargés de la comptabilité ou des finances a permis en 2016 de réduire considérablement le nombre de cas : celui des tentatives d'escroqueries est désormais supérieur à celui des infractions réellement constatées.

En quoi la cybersécurité peut-elle être créatrice de valeur ?

X. L. : La sécurité n'est jamais un gain, mais une absence de coût. En matière d'escroquerie au faux président, la mise en œuvre d'un dispositif de sensibilisation et de prévention a permis d'éviter en 2015 plus de 90 millions d'euros de préjudice. Cet argent est une capacité d'investissement préservée, une source de compétitivité et de croissance.

Le financement de la cybersécurité oblige-t-il à une réallocation des ressources de l'entreprise ?

X. L. : Il s'agit de financer des dispositifs de lutte contre l'intrusion dans un système automatisé de données. Ce piratage

représente moins de 10 % des cyberinfractions constatées, mais ces actions, menées par des groupes ou des États, visent le plus souvent des intérêts stratégiques, publics ou privés.
Par conséquent, les outils de lutte ne s'adressent pas a priori au grand public, mais à la grande entreprise, à un opérateur d'importance vitale, ou à une jeune pousse qui développe des innovations stratégiques. Les outils publics d'accompagnement et d'investissement contribuent au développement de solutions de cybersécurité « fabriquées en France ». Dans le même sens, des consortiums public-privé, sur le modèle de celui créé entre le ministère de la Défense et Orange, permettent de mutualiser les ressources et les compétences. Ainsi, les entreprises disposent d'offres françaises de cybersécurité, que ce soit en matière d'informatique en nuage ou de lutte contre les piratages. En la matière, une liste d'entreprises labellisées est disponible sur le site de l'Anssi.

Faut-il tout contrôler ?

X. L. : La sécurité et le sentiment d'insécurité relèvent principalement de facteurs humains. Un dispositif de sécurité doit être accepté par les salariés, ou il sera perçu comme intrusif, attentoire aux libertés ; là encore, la pédagogie est au cœur de la prévention. En outre, un dispositif de sécurité doit être proportionné aux menaces. Il s'agit de trouver un point d'équilibre entre les enjeux de sécurité et les modes de travail et de vie internes.

L'État a-t-il pris la mesure de la menace pour tous les secteurs ?

X. L. : Au ministère de l'Intérieur, un « cyberpréfet » est chargé de coordonner les dispositifs de prévention et de lutte contre les cybermenaces. Pour l'accompagner, la police et la gendarmerie disposent de services spécialisés, comme le centre de lutte contre la criminalité numérique (C3N) de la gendarmerie, en mesure de lutter contre toutes les formes de cybercriminalité. Les enquêteurs de ce service détectent les nouveaux comportements ou les nouvelles techniques adoptées par les cybercriminels. Ils développent des moyens de lutte, par exemple l'application pour téléphones permettant de détecter les piratages de terminaux de paiement des grands magasins. C'est une course technologique entre le gendarme et le cybervoleur.
La police nationale dispose aussi de services et d'enquêteurs spécialisés. Ainsi, police et gendarmerie proposent un service public de cyberproximité sur l'ensemble du territoire. Une personne ou une entreprise peut directement solliciter un commissariat ou une brigade locale. Sur Internet, le site *Interieur.gouv.fr* propose plusieurs solutions de signalement en ligne avant plainte.

Quelles formes de coopération peuvent être envisagées entre les entreprises et l'État ?

X. L. : Les enjeux de cybersécurité pour l'État et les entreprises se rejoignent souvent. Par exemple, contre la radicalisation sur Internet, des dispositifs de prévention et de sensibilisation sont mis en œuvre dans les entreprises, à partir de guides et de conseils prodigués par les services de l'État. Contre les piratages ou escroqueries, les services du ministère de l'Intérieur travaillent étroitement avec les entreprises et les fédérations professionnelles, afin de connaître leurs besoins et les menaces dont elles font l'objet. À la direction de la Gendarmerie nationale, la section intelligence économique territoriale agit en partenariat avec la CCI France ou la CGPME, afin d'offrir aux entreprises des outils de sensibilisation et de diagnostic.

Données personnelles, danger

Les bases de données sur les consommateurs peuvent devenir le cauchemar des entreprises, si elles ne sont pas protégées.

Entretien avec Christophe Bouguereau, maître de conférences associé en marketing relationnel, université Bretagne Sud IUT[1]

Toute entreprise a-t-elle un « patrimoine informationnel » ? Comment est-il valorisable ?

Christophe Bouguereau : Le patrimoine informationnel, défini comme l'ensemble des informations accessibles à l'entreprise et potentiellement utiles à son activité, ne peut se voir au travers du prisme comptable que dès lors qu'on lui attribue une valeur économique. Or l'information ne se valorise que lorsqu'elle devient connaissance, qu'elle est traitée. Si le problème de l'accès ne se pose plus – aujourd'hui même une TPE peut générer ou obtenir de très nombreuses informations –, la volumétrie et les temps d'analyse conduisent à de nouvelles interrogations, notamment sur la rentabilité des temps associés à ces chantiers.

Les outils de « relation client » (coupons de réduction, cartes de fidélité…) sont-ils protégés des prédateurs de données ?

C.B. : Oui et non. Les éditeurs de solutions sont forcément très attentifs aux questions de sécurité, les solutions en mode SaaS (logiciel en tant que service) proposent même des hébergements locaux, dans le pays de leur client, afin de le rassurer, mais aussi de se mettre en conformité avec les lois nationales. Par exemple, le donneur d'ordre peut exiger des audits de sécurité, ou certains hébergements de données peuvent être soumis à des agréments (autorités de santé par exemple).
Cependant, quelles que soient les barrières techniques, la multiplicité des points d'accès rend les fuites probables. C'est parce que les donneurs d'ordres ou les fournisseurs en sont conscients qu'un maximum de garde-fous sont déployés. Chaque situation doit être analysée en termes de bénéfice et de risque. L'hyperprotection existe, mais elle a un coût.

Les données personnelles des consommateurs réunies dans les bases de données sont-elles suffisamment sécurisées ?

C.B. : Pas toujours. Surtout lorsque les bases sont en cours de création et les processus en cours de formalisation. La définition du rôle des différents acteurs peut rendre accessibles des données à des personnes qui ne devraient pas pouvoir les consulter.

Bien sûr, il y a des piratages de bases, on imagine des génies de l'informatique qui cassent les codes, mais c'est plus souvent la négligence qui ouvre les données à des tiers. Les mots de passe cachés sous les claviers, réunis sur des pense-bêtes adhésifs ou dans des fichiers « password.xls » rendent bien des bases de données accessibles à n'importe quel stagiaire ou individu de passage sur le réseau de l'entreprise.

Quelles bases de données sont le plus exposées : celles des marques, ou des prestataires ?

C.B. : Il n'y a pas de réponse catégorique. La première serait

de dire qu'une base hébergée en interne bénéficie d'un maximum de sécurité ; dans les faits ce n'est pas toujours le cas. Par méconnaissance des procédures, par une sensibilisation insuffisante des salariés, la marque peut se mettre en difficulté, alors qu'un bon contrat engagera formellement le prestataire sur les aspects de sécurité.

Comment définir la sensibilité des données et les niveaux de sécurité ?

C.B. : Deux réponses simples. D'abord, en se conformant à la loi ! Ensuite, par la capacité à donner de la valeur à la donnée ; valeur économique bien sûr, mais surtout valeur en termes d'avantage concurrentiel.

1. Aussi fondateur de MDC (Maison du client), société d'expertise en stratégie client.

Savoir tenir le bouclier du droit

Actif primordial de l'entreprise, le patrimoine informationnel ne peut être juridiquement protégé que si les réglementations sont connues et appliquées, et les instruments juridiques en place. Une responsabilité du chef d'entreprise.

Par Myriam Quéméner, magistrat, docteur en droit

Le patrimoine informationnel des entreprises de grande consommation, comme de tous les secteurs majeurs, n'est pas à l'abri de cyberattaques, comme en témoigne, en 2014, l'affaire du distributeur Target, victime du vol des données bancaires de quarante millions de clients. En 2015, un pirate avait trouvé le moyen de diffuser le son d'un film porno dans l'enceinte d'un magasin de cette même chaîne, visant à atteindre son image.

Ces sociétés détiennent un trésor comprenant les données clients et fournisseurs, du savoir-faire, des brevets, des bases de données. Ces informations[1] sont diverses, certaines peuvent entrer dans une ou plusieurs catégories juridiques et sont protégeables à ce titre. La protection des données personnelles est ainsi au cœur d'enjeux essentiels, puisque la valeur d'une société se juge à sa capacité de résister à des cyberattaques[2]. Les préjudices pour un piratage sont importants, comme le montre Axa[3], dans un cas où un vol de données sur un site de vente de meubles a conduit Google à l'inscrire sur liste noire, à une perte de chiffre d'affaires de 30 000 euros pour deux semaines de blocage, et à une inestimable perte financière due à la baisse de confiance des clients[4].

Valoriser le patrimoine informationnel consiste à définir et à mettre en place des actions qui vont créer de la valeur. Il appartient au chef d'entreprise de gérer cet actif en se donnant les moyens d'identifier et de contrôler les catégories juridiques qui permettent de le protéger. À mesure que la valeur des données personnelles augmente, la conformité des entreprises avec les réglementations applicables devient un enjeu concurrentiel. Beaucoup ont compris que les données auront peu de valeur si elles ne sont pas collectées et traitées conformément aux réglementations applicables ; elles sont donc de plus en plus soucieuses de leur conformité.

Depuis les lois du 13 mars 2000 et du 21 juin 2004, le droit de la preuve électronique encadre l'archivage électronique, dont la problématique est posée par l'article 1316-1 du Code civil : « *sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ». Deux éléments en ressortent : l'identification et l'intégrité. Au niveau normatif, l'Afnor a publié en 2001 la norme Z42-013 et en 2005 la norme Z43-400 ; les normes ISO, NF ISO 15489-1 et FD ISO 15489-2 reprennent des notions similaires. Ces normes mettent en exergue les notions de disponibilité, d'accessibilité, de durabilité, d'intégrité et de confidentialité des données, ainsi que l'identification, l'authentification et la traçabilité.

Dans le patrimoine informationnel, l'archivage électronique n'est pas qu'un effet de la dématérialisation de l'archivage physique. Il faut aussi prendre en compte le cycle de vie des informations. La protection du patrimoine informationnel correspond aux risques entourant l'obsolescence des données. Lorsque la préservation et l'accès aux données sont garantis, il reste au chef d'entreprise à assurer la sécurité juridique des accès.

Un arsenal en évolution constante

La sécurité juridique du patrimoine informationnel passe par la protection des informations en elles-mêmes, par les droits de la propriété intellectuelle comme le droit d'auteur, le droit des bases de données, le droit des brevets, le droit des marques, le droit des dessins et modèles, la protection du savoir-faire, la protection du secret de fabrique, la protection des signes distinctifs (nom commercial, enseigne, dénomination sociale et nom de domaine), et par les mesures techniques de protection et d'information. Cette protection ne peut être que lacunaire dès lors qu'elle n'épuise pas tous les droits ni toutes les informations d'un patrimoine informationnel qui ne seraient pas couvertes par un droit spécifique.

Il existe des instruments juridiques intéressant d'une part la politique interne de sécurité, le rôle et les responsabilités du personnel concerné (DSI, RSSI et RSI), d'autre part la confidentialité des informations. À cet égard, il peut être conseillé à toute entreprise d'envisager la création d'une charte d'utilisation des communications électroniques, mais aussi l'insertion de clauses de confidentialité dans les contrats de travail, les règlements intérieurs et les contrats avec les tiers.

La responsabilité du chef d'entreprise peut être actionnée sur le fondement de la loi informatique et libertés en ce qui concerne les données à caractère personnel et la sécurité exigée. Sa responsabilité peut être aussi engagée sur le plan civil, en raison de fautes qui viendraient à être commises par un salarié. Enfin, certaines atteintes au patrimoine informationnel peuvent engager la responsabilité du chef d'entreprise sur le plan pénal, sur la base d'infractions d'accès frauduleux, ou d'atteintes volontaires à l'intégrité des données.

Concernant le vol de données immatérielles, après une réticence doctrinale affirmée et une insécurité juridique problématique, puisque certaines décisions avaient franchi le pas d'une timide reconnaissance du vol d'éléments immatériels[5], le législateur, par la loi du 13 novembre 2014 contre le terrorisme, a admis la répression de l'extraction de données, assimilée au vol, ce qui renforce la protection du patrimoine informationnel, notamment des entreprises de grande consommation. Le nouvel article 323-3 du Code pénal permet de réprimer une large gamme d'agissements frauduleux (extraction, détention, reproduction, transmission).

Formation et sensibilisation

Mettre en alerte constante les entreprises est essentiel à leur prospérité, et dans ce domaine la coopération public-privé prend tout son sens. Ainsi, la Direction centrale du renseignement intérieur et la gendarmerie[6] proposent dans le cadre de formations

des règles de bonne conduite pour limiter les dégâts causés aux entreprises, à leur image et à leur santé financière, et dans un deuxième temps pour asseoir leur pérennité sur de bonnes bases sécuritaires. De nombreuses associations regroupant des acteurs privés ont un rôle essentiel dans la sensibilisation à la culture numérique, par exemple dans le cadre du Cigref[7]. Autre exemple : le Club des directeurs de sécurité des entreprises (CDSE) et la DCPJ ont signé un protocole de coopération contre toutes les formes de fraudes et d'escroqueries d'envergure ou d'une particulière complexité.

Le Parlement européen a voté le 14 avril dernier la directive sur le secret des affaires[8]. Elle établit des règles visant à faciliter les recours juridiques des entreprises pour obtenir réparation du vol ou de l'abus de données relevant du secret des affaires. Les eurodéputés ont obtenu que la liberté d'expression et d'information soit protégée et que ces règles n'entravent pas le travail de la presse. Le même jour, ils ont adopté des dispositions sur la protection des données personnelles. Ce vote clôture quatre ans de travaux sur une réforme complète, composée d'un règlement général sur la protection des données personnelles et d'une directive relative aux transferts de données à des fins policières et judiciaires. Le règlement inclut des dispositions sur le droit à l'oubli et le consentement clair et explicite de la personne concernée, il prévoit des amendes allant jusqu'à 4 % du chiffre d'affaires mondial total d'une entreprise en cas de violation de ses dispositions. Il sera applicable dans tous les États membres courant 2018.

1. Olivier Hassid, « La protection des données au cœur de nos sociétés du XXIe siècle », Sécurité et stratégie 2014/2 (17), p. 1-2.
2. M. Van Den Berghe, Protéger le patrimoine informationnel de l'entreprise, Préventique n° 145, mars 2016, p. 19.
3. http://is.gd/yOXjpx.
4. Marcel Julien, « Entretien avec Alain Juillet et Jean-Pierre Vuillerme : l'entreprise face aux fuites d'informations. », Sécurité et stratégie 1/2011 (5), p. 17-26, http://is.gd/kG4UnS.
5. Olivier de Maison Rouge, « L'affaire Rose : une qualification audacieuse du vol de fichiers confidentiels dans un contexte d'espionnage économique », Sécurité et stratégie 1/2012 (8), p. 41-49, http://is.gd/Toe6gq.
6. ww.intelligence-economique-fc.orgl
7. www.cigref.fr.
8. http://is.gd/JyA59z.

Sécuriser pour gouverner

Si l'invulnérabilité est illusoire, l'identification des risques numériques demeure nécessaire, comme l'évaluation de leurs impacts sur l'activité de l'entreprise.

Entretien avec Guillaume Tissier, directeur général de CEIS, coorganisateur du Forum International de la cybersécurité (FIC)[1]

Comment une entreprise de PGC peut-elle se maintenir à niveau, face à la sophistication croissante des attaquants ?

Guillaume Tissier : Les entreprises de PGC sont exposées aux risques numériques au même titre que les autres. La première chose est d'évaluer ces risques. Ils diffèrent pour chaque entreprise, car ils dépendent de sa surface d'exposition. Plus elle est présente sur la Toile, plus elle est « numérique », plus elle est potentiellement vulnérable. Un système d'information invulnérable, ça n'existe pas. Il faut voir le problème en face, sans culpabiliser les entreprises. Toutes ont été ou seront un jour victimes d'une attaque informatique. En matière de criminalité informatique, la course entre le gendarme et le voleur est permanente. La différence se fera par la prise en compte des risques le plus en amont possible. Si les menaces sont réelles, il n'y a pas de fatalité.

Quels sont les « cyber-risques » ?

G. T. : Les risques informatiques sont de différents ordres : il y a le risque de panne, en raison d'un événement accidentel, et le risque de malveillance. Celui-ci consiste en risques traditionnels, que la transformation numérique et la dématérialisation des échanges ont accélérés (fraudes en tout genre, abus de confiance, diffusion de contrefaçons sur Internet…), et en risques spécifiquement liés au numérique, comme les attaques en déni de service, les vols de données ou les extorsions de fonds à l'aide de rançongiciels (logiciels malveillants qui prennent en otages des données personnelles). Dans tous les cas, ces risques peuvent avoir des conséquences lourdes en termes financiers : manque à gagner en chiffre d'affaires, coût de la remise en service, amendes en cas de mise en cause de la responsabilité de l'entreprise… Et en termes d'image de marque.

Après l'identification de ces risques, qui doit impliquer tous les métiers de l'entreprise, il s'agit d'évaluer leur impact potentiel en termes de disponibilité (d'un site de vente en lilgne, d'un système industriel…), d'intégrité (une modification de certaines données informatiques peut avoir des conséquences graves), de confidentialité (vol d'information) et de traçabilité.

Les entreprises doivent-elles conserver le contrôle de la cybersécurité en interne ou faire appel à des prestataires ?

G. T. : Le recours à des prestataires extérieurs qualifiés est recommandé. Seules les plus grandes entreprises disposent des moyens et de la taille critique pour mettre en place leur propre dispositif de sécurité. Et même dans ce cas, il est utile d'avoir un regard externe. Ces prestataires sont de différents types : prestataires spécialisés d'audit et de conseil, qui vont évaluer la sécurité de l'entreprise et analyser les risques, et entreprises de service, qui vont assurer au quotidien l'infogérance des systèmes d'information. Certaines ont développé des services de sécurité spécialisés, et mettent à disposition de leurs clients des divisions qui assurent la sécurité de l'organisation (SOC) et des centres d'alerte et de réaction d'urgence aux attaques informatiques (CERT). Arrivent aussi sur le marché des polices d'assurance spéciales, qui permettent aux entreprises de s'assurer contre certains risques liés aux systèmes d'information.

Est-il possible de conjurer l'asymétrie de la menace d'attaques transfrontières et anonymes ?

G. T. : La dimension transfrontalière de la cybercriminalité est un défi permanent. Certains États sont des paradis fiscaux, d'autres des paradis cybercriminels, qui tolèrent voire encouragent la cybercriminalité. Mais les choses progressent au plan international, de nombreux pays ont signé la Convention de Budapest, qui favorise les échanges d'informations. Récemment, l'Organisation de l'unité africaine a adopté la convention de Malabo, qui s'appliquera à terme aux pays africains.

Comment les entreprises peuvent-elles profiter sans risques de l'hébergement en nuage ?

G. T. : Il faut raisonner en termes de sécurité, et s'assurer que le

prestataire est compétent, car on a souvent affaire à une chaîne de sous-traitants dans laquelle un éditeur de « logiciel en tant que service » (SaaS) recourt à un hébergeur pour abriter ses serveurs. Mais il faut raisonner aussi en termes de maîtrise des données, car la sécurité n'est pas tout. Externaliser les données dont certaines sont sensibles est parfois indispensable, jamais anodin. C'est confier son patrimoine, parfois les clés de la maison, à un tiers, ce qui suppose qu'on ait confiance en lui. Et si l'on externalise des données sur les clients, cela engage triplement : vis-à-vis de l'entreprise (et des actionnaires), vis-à-vis des clients (responsabilité civile en cas de fuite), vis-à-vis de la justice, qui pourrait reprocher à l'entreprise une infraction en termes de protection des données personnelles.
Il faut donc bien évaluer les risques en amont, notamment en termes de législation applicable, et s'assurer que les conditions générales de vente du prestataire offrent certaines garanties. Nous travaillons avec l'association Cloud Confidence[2] à promouvoir un référentiel de confiance. Car en 2025, 80 % des applications professionnelles seront hébergées dans le Nuage. Mieux vaut accompagner le phénomène.

L'art de manipuler les personnes est-il un risque majeur ?

G. T. : De plus en plus. L'actualité plaide en ce sens. Non seulement la menace n'est pas théorique, mais elle est proche. Il y a quelques mois, une clinique de Boulogne-sur-Mer a été victime d'un rançongiciel et n'a dû son salut qu'à son dispositif de sauvegarde, qui lui a permis de remplacer les données qui avaient été chiffrées par les cybercriminels. Le nombre d'arnaques au président va croissant : une personne toujours bien informée téléphone, généralement pendant les vacances, au comptable d'une entreprise en se faisant passer pour le grand patron et demande un virement urgent…

Les comportements diffèrent-ils selon les générations ?

G. T. : Oui. Toutes les générations sont concernées par le phénomène, mais il y a des différences entre elles. Le comportement de la génération Y est paradoxal : un jeune sur cinq s'est déjà fait voler ses coordonnées bancaires, et ils se mettent à nu sur les réseaux sociaux avec des informations potentiellement exploitables par un tiers malveillant. Bien vivre avec le numérique, même quand on est né avec, n'est pas inné. Cela s'apprend.

1. www.ceis.eu ; www.forum-fic.com.
2. www.cloudconfidence.eu.

Nécessaire cryptage

Le stockage à distance n'offre de réelle sécurité contre les cyberattaques que si les données sont chiffrées.

Entretien avec Jean-Luc Louazon, directeur stratégie et développement, Forecomm (solutions de publication sur mobiles)

Comment garantir confidentialité et sécurité aux entreprises qui échangent quotidiennement des documents numériques ?

Jean-Luc Louazon : La solution la plus efficace, pour des documents sensibles, est le chiffrement : il permet aux entreprises de s'assurer que le document envoyé est protégé dans n'importe quel environnement par lequel il transite, sécurisé ou non, avant d'arriver à son destinataire. La solution BlueFiles[1] va plus loin, avec un chiffrement d'un bout à l'autre, qui permet d'échanger des informations sans jamais délivrer la version déchiffrée au destinataire (elle n'est que partiellement décryptée pour une lecture à la volée sur son ordinateur authentifié, et il ne peut en transmettre les droits de lecture).

Comment profiter d'un hébergement en nuage sans risques ?

J.-L. L. : Le *Cloud* est une infrastructure providentielle pour de nombreuses entreprises, car il augmente leur espace de stockage et facilite l'échange de documents hors de leur réseau interne, avec des partenaires ou des salariés en déplacement. Bien que de nombreux serveurs distants aient déjà subi une attaque, ils sont performants en termes de cybersécurité. Le principal problème des entreprises est qu'elles y stockent des données en clair. Si elles y sont à l'abri, rien n'empêche un employé ou toute personne ayant accès au dossier de les en sortir, sans autorisation. Le chiffrement évite ce problème, car une donnée chiffrée ne peut être consultée sans autorisation. Bien sûr, il doit s'inscrire dans la logique de travail de l'entreprise et être accessible aux employés.

La cybersécurité doit donc intégrer tous les salariés ? Et aussi les parties prenantes et les fournisseurs ?

J.-L. L. : Chaque employé informé des principaux risques de cybersécurité et de la meilleure façon de les éviter est une porte qui se referme au nez d'un pirate informatique. Il est essentiel de les impliquer tous dans la stratégie de cybersécurité : réunions, blog d'entreprise *ad hoc*, journées de formation, outils de cybersécurité, référentiel sur le degré de confidentialité des fichiers manipulés… Pourquoi investir dans de coûteux outils de cybersécurité si les partenaires, fournisseurs ou salariés utilisent les fichiers qu'on leur transmet dans des environnements non sécurisés ou contaminés (ordinateurs, serveurs ou mobiles) ?
Cependant, il n'est pas toujours facile ni possible de mettre en place un système d'échanges sécurisés adapté à chaque partenaire. Il faut alors considérer que chaque employé peut être une porte d'entrée pour un pirate : si l'entreprise n'est pas en mesure de protéger l'ensemble des « chemins » (serveurs, routeurs, wi-fi…) et des « portes » (ordinateurs, clés USB, mobiles.) par lesquelles circulent les données, sécuriser les fichiers lui assurera un niveau de cybersécurité acceptable pour un coût raisonnable.

Un meilleur contrôle de la cybersécurité passe-t-il par des plates-formes d'information communes entre entreprises d'un même secteur ?

J.-L. L. : Il passe forcément par la propagation d'informations à tous les acteurs d'un secteur, et à tous les niveaux de l'entreprise. La mise en commun d'expériences, de questions et de cas pratiques ne peut qu'aider les entreprises à appréhender et à gérer leur cybersécurité. Mais il est impossible de s'assurer que tous les partenaires utilisent les mêmes protocoles : personne ne peut se baser uniquement sur la confiance entre partenaires pour la sécurité de ses données ; il lui faut s'assurer qu'elles demeurent sa propriété, dans tous les cas.

Faut-il attribuer à la cybersécurité une direction spécifique ?

J.-L. L. : Il est préférable de rattacher la cybersécurité à la direction générale, qui sera en mesure de juger de sa mise en œuvre et de son efficacité dans sa globalité. En revanche, la mise en place d'un audit spécifique destiné à la vérification du bon déroulement des processus et de la remontée à la direction générale de situations ou de points bloquants est une option non dénuée d'intérêt.

1. www.mybluefiles.com.

Un contexte mouvant

L'économie s'ubérise, et le cyberdanger a de nouveaux visages, pour des données fragiles comme les numéros de cartes de paiement. Les meilleures technologies ne suffisent pas à les protéger.

Entretien avec Philippe Trouchaud, associé, cabinet PWC

Observez-vous une escalade dans le nombre de cyberattaques et dans leur degré de complexité ?

Philippe Trouchaud: Oui, en dépit d'un biais statistique – on mesure plus –, les attaques sur les sites industriels cette année ont connu un bond de 280 %. Il y a parfaite translation de la délinquance physique vers la cyberdélinquance. Ces attaques sont de surcroît toujours plus sophistiquées, furtives et scénarisées (appels téléphoniques avec l'imitation de la voix du président…). Les gens qui attaquent savent s'adjoindre les compétences financières ou fonctionnelles utiles à des opérations de trésorerie.

Les entreprises de PGC sont-elles plus touchées que d'autres ?

P. T.: Elles sont plus ciblées que d'autres, car la désintermédiation conduit de plus en plus ces entreprises à avoir des canaux de vente directe, à détenir des moyens de paiement. Or la première donnée fragile est le numéro de la carte bancaire. Et toutes ces entreprises se digitalisent pour améliorer la relation avec leurs clients. Elles sont conduites à détenir beaucoup de données personnelles sur eux. Le capital de confiance d'une marque peut être vite détruit en cas de cyberattaque.

Dans quelle mesure l'internet des objets, l'hébergement en nuage et la digitalisation augmentent-ils les cybermenaces ?

P. T.: Tout cela augmente mécaniquement l'exposition des entreprises. Hier n'étaient exposés que leurs centres de données ; avec la digitalisation même les murs d'un bâtiment peuvent avoir des capteurs. Target a connu aux États-Unis une cyberattaque par son système de climatisation ! Le *big data* amplifie les risques : un seul endroit virtuel réunit toutes les données…

Vis-à-vis de leurs clients, la cybersécurité est-elle pour les entreprises quelque chose dont elles ont à répondre, un aspect de la RSE ?

P. T.: C'est une tendance qui émerge aux États-Unis et qui va s'inscrire dans les règlements européens. Dès lors qu'une entreprise détient des données personnelles, elle a la responsabilité d'en garantir la sécurité. Cela deviendra une obligation de résultat.

La technique du cheval de Troie laisserait, dites-vous, 240 jours au pirate pour œuvrer sans être détecté ! Quelles alertes manquent aux entreprises ?

P. T.: Ces 240 jours sont une durée moyenne. Les attaques étant de plus en plus furtives, aucun indicateur ne peut les signaler. C'est la collation de signaux faibles qui permet de détecter les comportements anormaux. Moins de la moitié des entreprises ont un système d'alerte, il y a urgence pour les autres à s'équiper. Ce type d'équipement n'est pas comme une alarme de maison, il ne se déclenche pas au moment de l'attaque ; il faut apprendre à analyser les signaux faibles annonciateurs d'attaques.

Comment faire de la cybersécurité une opportunité pour les entreprises ?

P. T.: Toutes les entreprises font le même constat : les nouveaux entrants sur les marchés usent de nouvelles technologies résumées sous le terme d'ubérisation. Depuis trois ans, selon les études de PWC, tous les responsables des systèmes d'information entendent investir dans le digital, moyennant bien sûr des règles de sécurité. Investir pour contrer les nouveaux entrants en négligeant la sécurité ne sert de rien et détruit de la valeur.

Comment impliquer au mieux les salariés, les aviser des données à protéger, des risques d'intrusion, des erreurs à ne pas commettre (comme de recharger un téléphone mobile dans les hôtels, restaurants et salons professionnels ou se connecter à un wi-fi public) ?

P. T.: Il faut tenir un discours cohérent, expliquer que dans une entreprise les données sont des actifs qu'il faut protéger et qui n'ont pas vocation à être publiques. La jeune génération n'a pas la même vision que les seniors, plus vigilants, elle est habituée à échanger sur les réseaux sociaux sans contrainte ni limite. Elle n'est pas consciente de la chaîne de valeur de l'information. Il ne faut pas être dans l'interdiction, mais dans la démonstration des moyens de protection, et rappeler que la malveillance rôde toujours autour de l'entreprise.

Les formations universitaires consacrées à la cybersécurité permettent-elles de répondre à la demande ?

P. T.: Non, comme le soulignait en 2012 le rapport Bockel sur la cyberdéfense. On ne forme que quelques dizaines de spécialistes par an, il en faudrait des centaines, voire des milliers.

Quels profils manquent ?

P. T.: Il nous manque des gens capables de sortir du volet tout technologique, pour mieux appréhender les risques, et des statisticiens en mesure de comprendre les événements et d'avoir une vision du risque.

Dans votre livre[1], vous affirmez que la France dispose des atouts pour devenir le champion mondial des solutions de cybersécurité. Faut-il que la protection des entreprises françaises soit elle aussi française ?

P. T.: Les enjeux de souveraineté sont très importants dans la sécurité, particulièrement dans la cybersécurité. Faut-il pour autant le tout-français, je ne le pense pas, cela semble irréaliste sur le plan économique, nous n'avons pas la taille critique. Mais comme dans l'aviation civile, disposer de champions nationaux voire européens serait souhaitable.

Le Règlement général sur la protection des données de l'UE peut-il obliger les entreprises à intensifier leurs pratiques en la matière ?

P. T.: Oui, l'environnement réglementaire des entreprises va devenir de plus en plus pressant sur le plan européen, mais aussi en France du fait de la loi de programmation militaire, avec les OIV (organismes d'infrastructures vitales), dont l'objectif est de renforcer la sécurité des grandes infrastructures, et des données des clients consommateurs. Cela fait peser sur les entreprises des risques financiers de plus en plus importants et les oblige à progresser en maturité sur le sujet.

1. La Cybersécurité au-delà de la technologie, *Odile Jacob, 2016.*

Bulletin de l'Institut de liaisons et d'études des industries de consommation

Directeur de la publication : Richard Panquiault – Éditeur : Trademark Ride, 93, rue de la Santé, 75013 Paris (01 45 89 67 36, jwa@tmride.fr) – Rédacteur en chef : Jean Watin-Augouard – Secrétaire général de la rédaction et contact : François Ehrard (01 45 00 93 88, francois.ehrard@ilec.asso.fr) – Maquette et mise en pages : Graph'i Page (ividalie@orange.fr)

Imprimé par : SB Graphic, 38, rue Gay-Lussac, ZI de Mitry-Compans, 77290 Mitry-Mory – ISSN : 1271-6200

Dépôt légal : à parution – Reproduction interdite sauf accord spécial

www.ilec.asso.fr