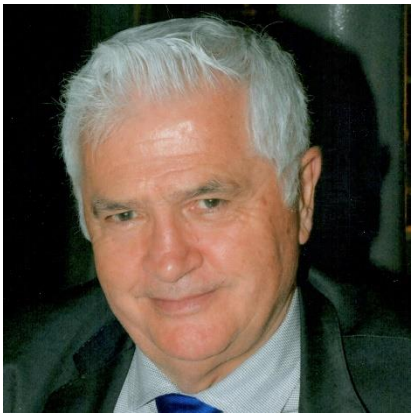
Vers une nouvelle gouvernance de la cybersécurité



Bernard BARBIER
Membre de l'Académie des Technologies
Président de BBCyber SAS

Une approche systémique de la maitrise du risque numérique dans l'entreprise
La sécurité 360° de l'entreprise

La cybercriminalité, une situation dramatique[1]

En début 2021 la menace de la cybercriminalité, du cyber espionnage, ou de la cyber destruction contre les entreprises, les collectives locales, les hôpitaux, est devenue extrême. Le coût pour l'économie est évalué mondialement à plusieurs milliers de milliards de dollars. La Cyber est devenue le premier ou le deuxième risque que les entreprises doivent gérer. C'est un risque très nouveau, très immatériel que les entreprises ont du mal à appréhender et à maitriser.

Pourquoi une telle situation ?

Depuis l'aube de l'humanité, toute innovation peut également être utilisée à des fins négatives. La nouveauté de la cybernétique est que son usage est aisément accessible à tous les niveaux, depuis l'individu isolé jusqu'aux organisations les plus élaborées, qu'elles soient officielles, gouvernementales, clandestines ou mafieuses. La lutte en est rendue plus complexe. Elle doit prendre en compte simultanément l'ensemble de ces niveaux d'autant plus que l'attribution de l'attaque et l'identification de l'agresseur sont difficiles, même si les grands groupes mafieux ont des « signatures » techniques spécifiques. On assiste à un phénomène aggravant, celui de groupes de pirates cyber qui se mettent désormais ouvertement sur le marché. Ils sont prêts à vendre leur service au plus offrant, État comme entreprise, en vendant le « ransomware as a service » (RaaS), c'est-à-dire à la fois les portes d'entrée dans les entreprises ou institutions ciblées et les outils pour récupérer et blanchir la rançon.

Un nouveau défi : la cybercoercition[2]

La cyberattaque est devenue une arme utilisée par plusieurs pays pour provoquer des tensions permanentes qu'on peut qualifier de coercition. Ces tensions sont diverses mais elles sont provoquées par deux phénomènes très inquiétants. Le premier est l'attaque généralisée

[1] The Hidden Costs of Cybercrime (mcafee.com)
[2] Cybercoercition : un nouveau défi stratégique : Le Monde Publié le 28 janvier 2020, Face aux cyberattaques, la France doit se doter d'une capacité de dissuasion autonome, écrivent Bernard Barbier, (ex-DT de la DGSE), Edouard Guillaud (ex-CEMA) et Jean-Louis Gergorin (ex-Quai d'Orsay)

conduisant à des versements de rançon. L'autre phénomène, considérée comme un acte de guerre, est la cyberattaque contre des infrastructures critiques, entreprises et services collectifs. C'est le risque évoqué par Guillaume Poupard, directeur général de l'ANSSI, lors du Forum international de cybersécurité en 2019. Il a révélé l'existence de pré positionnements d'implants logiciels, par des Etats, au sein d'infrastructures critiques, pouvant être activés ultérieurement pour saboter celles-ci.

La porosité entre les groupes cyber mafieux et certains Etats a des conséquences dramatiques pour les entreprises : le niveau technique de certains attaquants est comparable à celui des Etats. L'opération réussie contre l'éditeur de logiciel SOLARWINDS pourrait avoir des conséquences très graves : certains codes sources de Microsoft ont été volés, les armes offensives utilisées par FIREYE pour tester la sécurité des entreprises, ont été volées. Face à cette situation critique c'est l'évolution globale de notre société de plus en plus numérique qui est menacée. L'exemple des hôpitaux est très marquant : la numérisation de leurs activités les a rendus vulnérable, sans qu'une organisation de cyberdéfense appropriée, des moyens humains et les budgets suffisants soient mis en place, mais surtout sans aucune réelle prise en compte du risque cyber.

Actuellement le réflexe classique des directions informatiques c'est d'empiler des outils de protection en ayant la fausse illusion d'être protégé.

Une évolution historique : de la ligne Maginot informatique vers l'aéroport des données

En France la réglementation a d'abord été imposée dans un objectif de protection de l'information classifiée (Instruction 900 du 20 juillet 1993). Les grands principes reposaient sur la protection grâce à des barrières logiques et physiques (trois barrières physiques pour la protection des informations classifiées). Cette culture réglementaire reposant sur la protection conduisait à construire « une ligne Maginot » numérique. C'était une obligation de moyens qui a marqué la culture SSI des entreprises.

A partir des années 1995-2000, le Système d'Information des entreprises s'est ouvert sur l'Internet et le besoin de protection est devenu critique. Une isolation logique a été construite en utilisant des pare feux et les DSI ont commencé à se structurer en créant une nouvelle fonction : le (la) RSSI, le (la) Responsable de la Sécurité des Systèmes d'Information. Le (la) RSSI dirigeait une petite équipe au sein de la DSI, à l'origine essentiellement des experts réseaux qui étaient chargés de sécuriser et contrôler les frontières informatiques de l'entreprise entre le réseau interne, l'Intranet, et le réseau externe, l'Internet.

En France, à partir des années 2000, des grandes entreprises françaises ont subi des vols de données dans un objectif d'espionnage. Les menaces d'un déni de service massif bloquant des infrastructures informatiques critiques commençaient à apparaitre. La notion de « ligne Maginot informatique » protégeant les entreprises montrait donc ses limites. La défense du système d'information de l'entreprise ne repose plus uniquement sur des outils de protection, mais sur des outils de détection, et aussi sur la connaissance des menaces et des risques ; la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) a été inventée en 1995 pour les organismes et entreprises travaillant pour les Armées, et elle a

commencé à se généraliser pour toutes les entreprises à partir de 2005. Face aux menaces d'attaque informatique sur des infrastructures critiques[3], la France en 2008 et 2013, les Etats Unis en 2013, ont voté des lois qui obligent les Opérateurs d'Importance Vitale (OIV) à durcir et défendre leurs infrastructures informatiques et à se conformer à un référentiel strict, définissant des exigences techniques ou organisationnelles précises.

Cinq fonctions stratégiques sont définies : Identifier, Protéger, Détecter, Répondre et Récupérer. La sécurité du système d'information reposait traditionnellement sur la fonction Protéger. Des nouvelles compétences doivent être créées pour Identifier, Détecter et Répondre. La fonction Récupérer qu'on appelle Plan de Reprise d'Activité PRA est déjà couverte par la DSI mais souvent pas réellement testée.

Une approche systémique de la maitrise de leur risque numérique : « Bon Risk Appétit »

En 2020, la transformation numérique des entreprises a été accélérée par la crise sanitaire et le passage massif au télétravail : les processus classiques deviennent virtuels, le basculement très rapide vers des solutions de type SaaS pour la gestion des données de l'entreprise (Microsoft 365, TEAMS, ZOOM, SALESFORCE…).

La gestion et la maîtrise du risque numérique sont dorénavant clés pour l'entreprise.

Voici un rappel de mon analyse en fin 2014 :

« Au lieu de se murer, les organisations doivent développer un appétit sain pour le risque, en utilisant des outils intelligents pour détecter rapidement les intrusions et réagir en temps réel. En outre, la sécurité doit faire partie intégrante du cycle de vie des applications, et non une réflexion après coup. Une plate-forme numérique avec une sécurité intégrée permet de réaliser des nouvelles activités, plutôt que de les freiner. Le principe de base de « Bon Risk Appétit » (j'ai utilisé ce terme imagé Bon Appétit pour montrer l'importance d'apprendre à maîtriser le Risk) n'est pas d'éliminer tous les risques, une tâche impossible. Il s'agit de faire des affaires à un niveau de risque acceptable ».

Cette notion de « Bon Risk Appétit » est une approche systémique et elle est très bien adaptée à la complexité des entreprises. Tous les métiers de l'entreprise doivent apprendre à gérer et maîtriser leur risque numérique.

Deuxième élément clé de maîtrise du risque, la capacité de détection rapide des intrusions et de réaction en temps réel. Elle est complexe à déployer dans l'entreprise car elle nécessite des expertises très pointues qui n'existent pas dans celle-ci. Le SOC (Security Operation Centre) qui met en œuvre ces capacités, 24 heures par jour et sept jours sur sept, devient la tour de contrôle de la gestion du risque numérique. Cette tour de contrôle doit couvrir toutes les activités de l'entreprise et pas seulement la DSI. Elle est souvent externalisée par manque d'expertise interne (SOC managé).

La « Cyber Design Authority » : la qualification des applications est essentielle pour maitriser les risques numériques.

Troisième élément clé : la sécurité doit faire partie intégrante du cycle de vie des applications. Dès l'expression d'un besoin d'une nouvelle

[3] L'Estonie, première cybervictime de Moscou (lemonde.fr)

application numérique, qu'elle soit louée en mode SaaS ou développée en interne ou externe, la sécurité doit être totalement intégrée dès le début au projet. Pour en faciliter la prise en compte, j'ai créé la notion de « Cyber Design Authority » qui est pilotée par un binôme entre le sponsor du projet (le métier, la BU demandeur d'une nouvelle application, l'IT) et le responsable cybersécurité. Cette « Cyber Design Authority » c'est une autorité d'accréditation visant à valider la prise en compte des mesures de sécurité et de protection des données pour tout nouveau projet, application, service. La « Cyber design authority » intervient sur toute la vie d'une application : dès l'expression du besoin en réalisant une analyse de risque, en définissant la cible de sécurité et les mesures techniques et organisationnelles pour réduire les risques à un niveau acceptable. Cette autorité doit entériner les choix techniques, conduire des audits techniques (pentest) avant la mise en production de l'application.

Une autre fonction stratégique clef : Identifier. Pour assurer sa sécurité l'entreprise doit connaitre les menaces externes et ses risques internes. Le besoin de connaissance des menaces nécessite de mettre en place une nouvelle fonction de type « renseignement-anticipation » : la CTI, Cyber Threat Intelligence. Cette fonction doit couvrir les menaces sur tout le périmètre de l'entreprise et pas uniquement la DSI. En général l'expertise CTI n'existe pas dans l'entreprise et celle-ci doit faire appel à un partenaire spécialisé dans ce domaine. La fonction CTI doit être organisée et intégrée dans une capacité d'Intelligence Economique (IE) afin de renforcer les moyens d'anticipation et de maitrise de l'information. En associant IE et CTI, l'entreprise se dote ainsi d'une très forte capacité de « renseignement-anticipation ».

Un pilotage centralisé et global de la sécurité-sureté opérationnelle de l'entreprise

Actuellement en France, beaucoup d'entreprises sont organisées de façon classique avec une direction sureté physique, une direction RH qui peut s'occuper de la sécurité des personnes, d'un (une) RSSI au sein de la DSI. La sécurité de la production et des produits est de la responsabilité des BU. Et pour certaines grandes entreprises une capacité d'intelligence économique « IE ». Ces entités sont disjointes et souvent très cloisonnées. Ce modèle devient totalement obsolète car il ne répond plus aux menaces et aux risques du numérique.
Un modèle efficace de la sécurité dans une grande organisation doit aller vers une approche holistique pour mieux anticiper, détecter, réagir et réparer face à des menaces sophistiquées. Ce modèle doit permettre le partage en temps réel de l'information, le partage du « renseignement », le partage de la connaissance des menaces, et de gérer globalement les crises et les menaces. L'objectif est de se concentrer sur tous les types de menaces pour permettre une réaction rapide et ainsi de créer une sécurité globale de l'entreprise (sureté physique, sécurité des personnes, sécurité de l'information, sécurité de la production, sécurité des produits).
C'est ce que j'appelle un cockpit sureté-sécurité 360° (la sécurité convergée)

Les grandes banques ou les grandes entreprises de défense ont changé radicalement leur organisation en créant une Direction de Sécurité-Sureté Globale (DSG), rattachée directement au PDG : Group Chief Security Officer.

Cette Direction Sécurité Globale couvre les fonctions de : Sécurité physique-contrôle d'accès,

Sécurité des personnes en particulier l'habilitation des personnes, Sécurité des fournisseurs tiers, Sécurité de l'information, Gestion du risque numérique, SOC (Security Operation Center), Gestion de crise , Reprise d'activité PRA, Maintien en condition opérationnelle de sécurité, Cyber Design Authority, Sécurité de la production, Sécurité des produits, Intelligence Economique IE et CTI, et la fonction DPO (responsable de la protection des données) doit être fonctionnellement partagée avec la direction juridique.

La DSI avec le (la) RSSI doit garder la fonction traditionnelle de Protéger et organiser la fonction Réparer. Les fonctions : Identifier, Détecter, Répondre, doivent être transférées (et souvent créées) dans la Direction de la Sécurité Générale (DSG). Cela permet une mutualisation d'expertise rare au sein de l'entreprise. Et surtout de bien séparer les responsabilités d'exploitant et de contrôleur. La séparation organisationnelle de ces responsabilités est fondamentale pour assurer une bonne gouvernance de la sécurité-sureté (ce qui est le cas dans le nucléaire, le transport aérien...). C'est au PDG d'arbitrer entre la DSI et la DSG : arbitrage sur les budgets et les investissements dans la sécurité, décision d'arrêter un système pour bloquer la propagation d'un MALWARE. Le PDG et le COMEX doivent être informés très régulièrement de la situation opérationnelle de la sécurité-sureté globale de l'entreprise.

En conclusion, les investissements dans la cyberdéfense ne doivent pas être considérés comme un passif, mais plutôt comme un actif de l'entreprise.