ifaci
institut français de l'audit et du contrôle internes

Cyber-risques :
Enjeux, approches et gouvernance

L'IFACI est affilié à
The Institute of Internal Auditors

« Les cyber-risques sont des tempêtes imprévisibles qui croissent toujours en intensité ; rien n'est plus efficace pour les affronter de manière pérenne qu'une alliance proactive entre une gestion anticipatrice du risque et un audit interne clairvoyant. »[1]

Carlos Ghosn
PDG et Président du Conseil d'Administration
de RENAULT-NISSAN MITSUBISHI Alliance

I- Cyber-risque : Enjeux & caractéristiques

La prise de conscience de l'importance du cyber-risque est très récente. Par exemple, au Royaume-Uni, l'enquête sur le risque systémique réalisée semestriellement par la Banque d'Angleterre auprès des cadres de la City de Londres ne fait ressortir le sujet de la cybersécurité comme important qu'à partir de 2014-2015, pas avant[2]. De manière plus générale, si jusqu'en 2012, le cyber-risque est peu cité dans les enquêtes mondiales auprès des directeurs généraux d'entreprises ou des experts, il entre constamment parmi les 10 premiers risques de l'entreprise et de l'environnement économique depuis, voire dans son top 3 à la dernière réunion du World Economic Forum de Davos[3].

Des coûts toujours plus élevés avec des impacts économiques et sociétaux significatifs

L'accélération des attaques, mais surtout l'alourdissement de leurs coûts, expliquent cette prise de conscience. Le géant américain de la distribution Target a annoncé que la cyber-attaque dont il a été victime fin 2013 lui aura couté 200 millions de dollars[4]. Son DSI et son PDG seront licenciés dans la foulée[5]. En juin 2017, la cyber-attaque NotPetya a coûté à Saint-Gobain près de 250 millions d'euros de chiffre d'affaires et 80 millions d'euros de résultat net[6]. La société Equifax va perdre, elle, plus d'un quart de sa valeur boursière suite à l'annonce d'une fuite de données en août 2017. Son RSSI, son DSI et son PDG seront licenciés. Au niveau sociétal, certaines études internationales récentes ont observé une baisse de la confiance client par rapport aux activités commerciales en ligne concernant les questions de cybersécurité, de véridicité et de respect de la vie privée[7]. Or, le maintien de la confiance client est crucial pour le développement des activités en ligne[8].

À l'origine du risque : la digitalisation des activités économiques et sociales…

L'augmentation du cyber-risque est parallèle à celle de la digitalisation de l'ensemble des activités humaines. Celle-ci aussi est très récente : ce n'est qu'à partir de 2007 que plus de 93 % de toute l'information transmise ou enregistrée par l'ensemble de l'humanité est retranscrite en 0 et en 1, c'est-à-dire en « numérique » via des moyens informatiques[9]. Cette explosion digitale s'accélère : dès 2020, plus de 70 % des habitants de la planète posséderont un smartphone[10]. D'autres types d'objets connectés devraient s'y ajouter : S'il n'y avait que 0,5 milliard d'objets connectés en 2004[11], ils devraient atteindre 20 milliards en 2020[12] et peut-être jusqu'à 1 000 ou 2 000 milliards construits au total d'ici à 2035.

Les bases techniques de cette transformation digitale posées à la fin des années 2000, elle finit par s'imposer économiquement dans la décennie qui suit. Marc Andreessen, fondateur de la société Netscape, note en 2011 que « le logiciel est en train de manger le monde[13] ».

En 2017, sept des dix plus grandes sociétés au monde par leur capitalisation boursière viennent du digital[14]. De manière générale, à lui seul, le secteur des technologies de l'information atteignait en 2017 plus de 22 % du total de la capitalisation boursière du S&P 500[15].

… et la complexité technique et humaine

Cette accélération technologique crée aussi de nouvelles complexités, empilant couches de services, de matériel ou de procédures, imbriquées dans l'organisation humaine qui les gère. De cette complexité non maîtrisée naît la vulnérabilité. Elle commence avec l'imbrication de lignes de code dont le volume explose. Ainsi, le noyau du logiciel Linux a vu le nombre des lignes de code qui le composent augmenter d'environ 800 % en dix ans[16]. Les logiciels des véhicules automobiles se composent aujourd'hui parfois de plusieurs dizaines de millions de lignes de code[17]. La complexité s'exacerbe aussi au niveau du réseau d'entreprise. La gestion des mises à jour est d'autant plus complexe qu'il est extrêmement difficile d'obtenir une vue à plus de 90 % - 95 % de l'ensemble des actifs sur le réseau, et que, pour les entreprises les moins aguerries, cette vue dépasse rarement les 80 %[18].

Cette complexité agit aussi sur les acteurs humains, responsables au niveau individuel face aux cyber-risques, et d'abord au plus haut niveau : celui de la direction générale et du conseil d'administration. Lors de la cyber-attaque contre Target, c'est l'absence de gouvernance adéquate et de rapidité dans l'exécution managériale au plus haut niveau qui a permis à l'attaque de se conduire jusqu'au bout. Pour tous les collaborateurs, une formation exhaustive face à la complexité des systèmes est nécessaire pour avoir les bons réflexes. Or, ce n'est pas suffisamment le cas. Résultat : 95 % des incidents sont liés à une erreur humaine[19].

Une définition du cyber-risque

Dans les cas cités plus haut, il y a cyber-risque parce qu'un risque « classique » de l'entreprise (risque de réputation, de continuité opérationnelle, de poursuite légale…) va être matérialisé à la suite d'une action malveillante utilisant les moyens digitaux, et pouvant exploiter une négligence humaine et/ou une vulnérabilité du logiciel ou du matériel. Ainsi, Equifax perd un quart de sa valeur car sa réputation commerciale est entachée par son incapacité à protéger les données personnelles contenues dans les fichiers que la société gère. Le marché anticipe également des poursuites judiciaires.

Le risque de réputation commerciale est celui qui affecte le plus durement la valeur des entreprises. Son impact suite à des cyber-attaques, mesuré sur les marchés pour les entreprises cotées, peut atteindre 1/5ème de la valeur d'entreprise[20] – mais parfois plus, si un client important supprime sa relation commerciale avec l'entreprise défaillante : la société américaine Heartland Payment Services a ainsi perdu 70 % de sa valeur suite à une fuite de données menaçant sa relation avec Visa[21]. Au niveau interne, l'impact sur la réputation pourrait également jouer sur la marque employeur et le coût de rétention ou de recrutement[22].

Au-delà de la réputation : les nouveaux territoires du cyber-risque

Les imbrications à la fois techniques et légales créent de nouveaux risques judiciaires ou administratifs. En 2015, la FTC (Food and Trade Commission) aux Etats-Unis a, pour la première fois, imposé à la chaîne hôtelière Wyndham d'adopter un programme de cybersécurité suite à des fuites de données en 2008 et 2009[23]. Dans l'Union Européenne, la réglementation RGPD en vigueur depuis mai 2018 impose une responsabilité de l'entreprise en cas de fuite de données, même si celle-ci est le fait d'un sous-traitant.

Les risques sur la continuité opérationnelle de l'activité sont aussi de plus en plus nombreux. Par exemple, la prise de contrôle de caméras de vidéo-surveillance dans le tunnel du mont Carmel en Israël en 2013, a forcé au blocage du tunnel et provoqué plusieurs jours d'embouteillages. L'attaque NotPetya aurait contraint le transporteur danois Maersk à subir des retards et des annulations d'une valeur de 300 millions de dollars et à rebâtir une large partie de son réseau informatique en quelques jours[24].

Des risques sur la sûreté des utilisateurs commencent également à se faire jour. Certains exemples issus de l'essor des objets connectés ou de l'informatique industrielle, comme la prise de contrôle à distance de voitures Jeep Cheerokee en 2014 ou la révélation qu'une cyber-attaque en 2017 ciblait des installations pétrochimiques en Arabie Saoudite avec l'objectif d'un sabotage industriel cherchant à faire des victimes parmi le personnel[25], montrent que cette nouvelle informatique appliquée implique désormais la capacité avérée de blesser ou de tuer via une cyber-attaque, potentiellement sur une grande échelle.

II- Approches pour l'analyse des cyber-risques

La gestion des cyber-risques de l'entreprise est une activité complexe, avec une composante technique, humaine et organisationnelle. Afin de pouvoir l'aborder sous toutes ses facettes, il est utile de partir de références permettant d'apporter principes et idées afin de couvrir à minima les questions essentielles.

Le présent document ne propose pas un cadre de règles préétablies, mais une suite d'éléments clés issus pour certains de modèles de référence, afin que chaque entreprise puisse établir par la suite le cadre le plus approprié à sa situation – qu'il s'agisse de sa taille, de son industrie, de sa stratégie & business model, de son appétence au risque, de sa vision et même de ses valeurs éthiques.

En tant que tel, ce document constitue aussi une introduction à des modèles reconnus au niveau international et national - en particulier : *OECD Principles for Digital Security Risk Management (OCDE, 2016); Framework for Improving Critical Infrastructure Cybersecurity (National Institute of Standards and Technology, 2017); The CIS Critical Security Controls for Effective Cyber Defense (Center of Internet Security).* On pourra également intégrer le Guide d'hygiène informatique (ANSSI, 2017), ou le cadre *COBIT 5 Framework* (ISACA, 2016)[26].

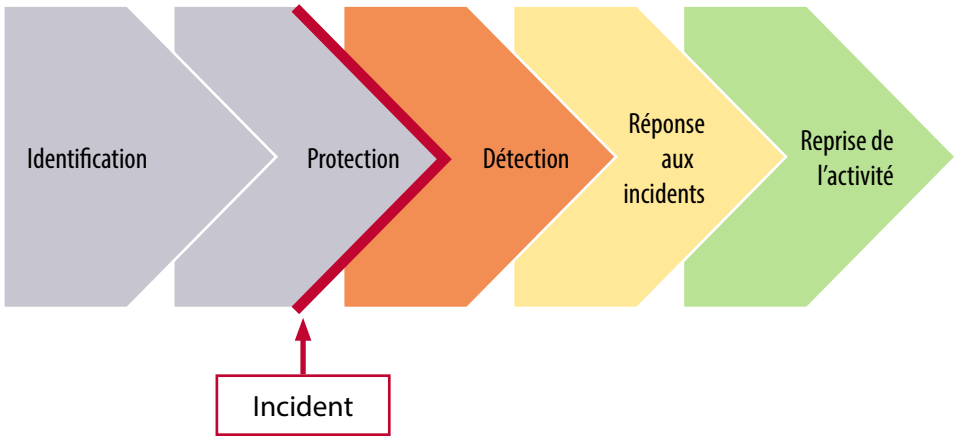
Les éléments ici posés s'appliquent qu'il s'agisse d'entreprises B2C ou B2B. Ils prennent en compte également la réalité de l'entreprise étendue, avec ses nombreuses parties prenantes. Ils ont été décomposés en deux blocs (voir schéma page suivante) :

- Les activités, souvent gérées au niveau opérationnel, liées au traitement des incidents de cybersécurité avant leur survenance, puis après. Il est à noter que la survenance d'un incident, quelle que soit sa taille, est approchée comme évènement certain : le but des activités avant la survenance de l'incident n'est pas son interdiction absolue, mais la minimisation de sa fréquence et son impact avec un objectif *in fine* de résilience de l'organisation.
- Les principes généraux transverses qui se retrouvent dans chacune de ces activités. Leur respect et animation est, le plus souvent, du fait du niveau de la gestion du risque plutôt que du niveau opérationnel. La bonne application de ces principes doit permettre à l'organisation de plus rapidement faire preuve de résilience face aux cyber-risques.

Principes généraux transverses

- ... **Exhaustif** (actifs humains, organisationnels & techniques déployés ou en production)
- ... Priorisé par niveau de **valeur en risque**
- ... Nourrissant des **boucles d'apprentissage**
- ... Piloté par une **mesure permanente**
- ... En communication avec **toutes les parties prenantes**

Chaîne d'activité avant/après incident



Principes généraux transverses

1. Être exhaustif dans l'ensemble des éléments couverts par les activités de cybersécurité

La cybersécurité s'applique à un champ très vaste d'éléments dans l'entreprise :

- En tout premier lieu : les acteurs humains, qu'ils soient pris dans leur dimension fonctionnelle & hiérarchique, dans leur adhésion à la politique générale de gestion de l'entreprise, voire dans les dimensions personnelles ou interpersonnelles.
- Les systèmes techniques en activité, incluant : actifs techniques (appareils, applications, réseaux), jeux de données[27], procédures formelles ou règles informelles.
- Les systèmes techniques qui ne sont pas encore actifs ou qui doivent être modifiés[28].

2. Centrer l'approche de cybersécurité sur l'analyse de la valeur d'entreprise en jeu

Pour l'entreprise, l'importance de la cybersécurité réside dans la défense de la valeur économique. Elle doit donc être analysée d'abord et avant tout à cette aune.

- Le cyber-risque doit être intégré à la politique d'Enterprise Risk Management qui doit aller jusqu'à l'impact sur la valeur d'entreprise. À maturité, un lien est établi entre,

d'une part, la cartographie « classique » des risques (ex : risque de réputation, risque sur la continuité des opérations, etc.) et, d'autre part, la cartographie des risques cyber qui constituent une nouvelle courroie de transmission de ces risques « classiques »[29].

- La capacité de gestion de crise[30] doit aussi être évaluée : elle impacte le coût final de l'incident.
- La réduction du risque peut inclure un transfert partiel du risque via assurances.
- L'analyse économique doit permettre de dégager également des opportunités de création de valeur en particulier sous un angle compétitif de mieux-disant de cybersécurité qui pourront intéresser les autres parties prenantes, y compris les actionnaires ayant une vue de long terme et pour lesquels la qualité des opérations joue un rôle primordial[31,32].
- La synthèse économique de ces éléments de risques, mais aussi d'opportunités, doit permettre une meilleure définition de l'appétence au risque de cybersécurité.

3. Être adaptatif dans la mise en place de la politique de cybersécurité

Apprentissage et adaptation continus sont nécessaires dans des environnements incertains, en constante évolution. C'est précisément l'une des caractéristiques de l'environnement de la cybersécurité. D'où les actions suivantes :

- Favoriser une politique d'apprentissage continu, incluant culture du test et de l'erreur, mesure des actions, inclusion dans une base de connaissance et diffusion.
- Privilégier la mise en place de procédures itératives, en jouant sur les phénomènes de diffusion naturelle qui renforcent les apprentissages[33].
- Développer la résilience « cyber » de l'organisation par une politique de « chocs » volontaires (entretenus par exemple par des tests non annoncés, ou par des exercices de simulation)[34].

4. Mesurer l'action et résultats pour apprendre et optimiser

Un système de mesures permet d'évaluer objectivement les apprentissages *(principe #3)* et donc de les favoriser, en s'inspirant des points suivants :

- Privilégier le développement de métriques simples afin de mesurer le plus grand nombre de phénomènes le plus souvent possible.
- Favoriser une politique de tests non annoncés plutôt que de « pointage » des situations afin d'obtenir les mesures observées les plus justes.
- Idéalement, lier / corréler les mesures aux impacts potentiels sur la valeur de l'entreprise.
- Comme cité plus haut, utiliser les mesures dans le cadre de l'instruction de boucles d'apprentissage, et le développement d'une culture d'adaptation et de résilience.

5. Être capable de communiquer avec les autres parties prenantes de « l'entreprise étendue » à fin de bonne intégration dans l'écosystème de cybersécurité

La communication est une dimension clé de la cybersécurité et de la gestion de crise. Elle devra inclure :

- les intervenants internes, qu'il s'agisse des métiers, des employés et bien sûr des structures de management et de gouvernance ;
- les différentes parties prenantes externes[35], dont à minima :
  - les clients et les associations de consommateurs, dont les opinions établiront la sévérité de l'impact sur la réputation de l'entreprise, ainsi que d'autres corps intermédiaires[36] influant sur la réputation de l'entreprise ;
  - les fournisseurs et les acteurs financiers[37] ;
  - les autorités de tutelle en cybersécurité et autres responsables judiciaires.

Cadre d'analyse pré-incident / incident

Au-delà des principes transverses d'analyse, on doit inclure des principes d'analyse des activités de cybersécurité spécifiques aux phases « avant incident » et « pendant / après incident ». Les principes décrits ci-dessous sont inspirés du *Framework for Improving Critical Infrastructure Cybersecurity (National Institute of Standards and Technology, 2017)*[38].

Cadre « pré-incident »

6. Identification

Les activités d'identification analysent la surface d'attaque de l'entreprise, dans le cadre de ses caractéristiques propres, en termes de gouvernance, politique de risque, etc.

- Identification de l'ensemble des actifs gérés, y compris les données (voir *principe #1*).
- Compréhension de l'environnement économique de l'entreprise.
- Compréhension de la gouvernance de l'entreprise.
- Développement de l'analyse et de la stratégie de gestion du risque[39]. En rapport avec les objectifs ainsi posés, un reporting du niveau de maturité de l'organisation au regard des cyber-risques devra être développé.

7. Protection & Prévention

Les activités de protection « pré-incident » doivent permettre de préparer l'entreprise à limiter les risques de cybersécurité, mais également, sous un angle de résilience, à pouvoir les absorber et à réduire les effets une fois qu'ils seront avérés. Elles incluent :

- Actions de prise de conscience et formation de l'ensemble des intervenants, dans le cadre d'une politique de prévention des cyber-risques qui pourra prendre la forme de cours, exercices et tests, jeux & simulations, etc.

- Politique de contrôle des accès.
- Politique de sécurité des données.
- Processus & procédures de protection de l'information (y compris dans le cadre du cycle de vie du processus de développement) incluant plan de continuité d'activité et plan de reprise d'activité, définis en mettant en particulier en avant les procédures renforçant la résilience de l'entreprise en cas d'incidents avérés (ex: back-up).
- Maintenance de ces processus et procédures – incluant également la politique de mise à jour de l'ensemble des actifs (en prenant en compte le *principe #1 d'exhaustivité*).
- Gestion des technologies de protection – pouvant inclure les technologies d'interdiction (ex : firewall) mais aussi les technologies de déception protective incluant des leurres sophistiqués.

Cadre d'analyse durant et après l'incident

8. Détection

Activités de détection des opérations cybercriminelles alors qu'elles sont en cours. On peut noter :

- Détection des anomalies et implications, en distinguant la détection des non-conformités et des vulnérabilités de celle des attaques exploitant ces non-conformités et vulnérabilités.
- Observation permanente des conditions de cybersécurité.
- Test et maintien des procédures de test.

9. Réponse aux incidents

Ensemble des activités en réponse aux incidents qui, à nouveau, doivent être vues tant sous un angle d'interdiction d'une extension de l'activité malveillante que sous un aspect de résilience, c'est-à-dire de maintien d'une activité à minima en cas d'infection / intrusion cybercriminelle :

- Exécution du plan de réponse aux incidents.
- Communication avec les parties prenantes cybersécurité internes et externes.
- Opération d'analyse de l'incident.
- Activités de remédiation, y compris les activités permettant la poursuite même en mode dégradé des processus fondamentaux de l'entreprise.
- Amélioration des procédures par prise en compte des leçons déduites de l'incident.

10. Reprise de l'activité et/ou résilience de l'activité

Ensemble des activités techniques et opérationnelles permettant de maintenir une activité même en mode dégradé et/ou de reprendre l'activité en cas d'interruption liée à l'attaque :

- Exécution du plan de reprise de l'activité, pouvant inclure les activités comprises dans le cadre de la réflexion de résilience pour l'entreprise.
- Amélioration des procédures par prise en compte des leçons de la reprise de l'activité.
- Communication et coordination opérationnelles avec toute partie prenante interne & externe.

Socle à minima offerts par les contrôles de base

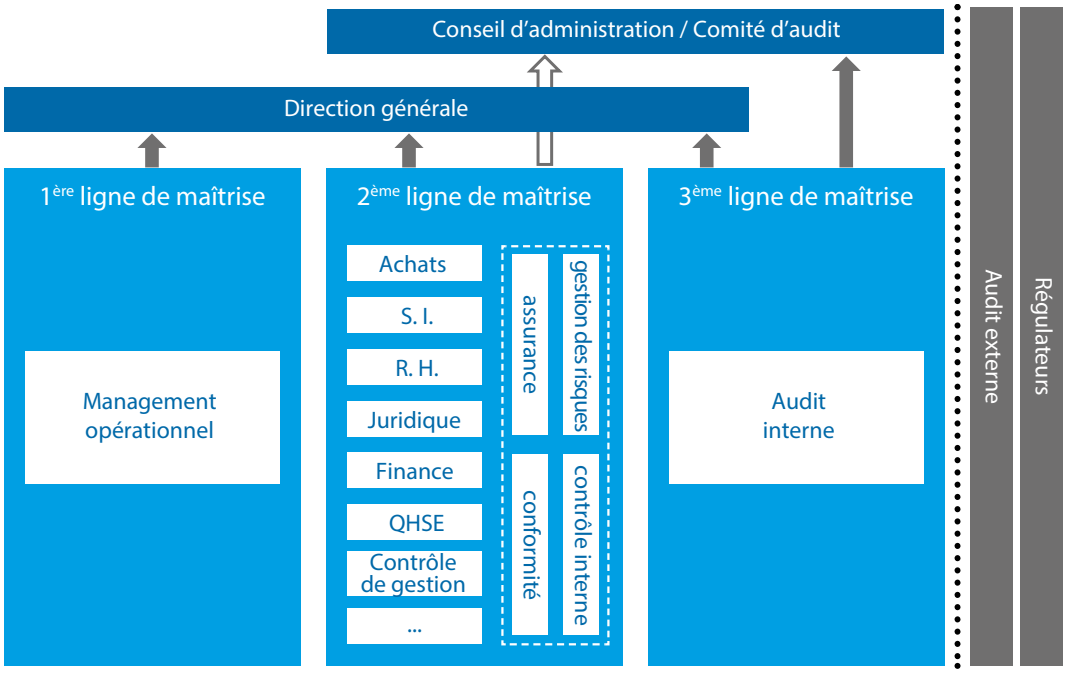
À ces dix principes peuvent se superposer 20 contrôles de base, listés en Annexe 1. Ils servent de points d'entrée à minima ou pour une organisation qui doit partir de zéro et doit prioriser ses premières étapes. Ils reprennent les dix principes énoncés plus haut, en particulier sur les aspects préventifs *(principe #7)*, détectifs *(principe #8)* ou correctifs *(principe #9)*.

III- Gouvernance des trois lignes de maîtrise à l'heure des cyber-risques

1. Rappel des grands principes

La notion de « trois lignes de maîtrise », développée au niveau européen par un partenariat entre l'ECIIA et FERMA, constitue une approche reconnue et privilégiée pour développer les activités d'Entreprise-wide Risk Management (ERM) où la direction générale se retrouve au cœur du dispositif de maîtrise globale des risques. En particulier, cette approche définit des tâches et responsabilités spécifiques à chaque ligne de maîtrise[40] :

- des activités de contrôle définies et mises en œuvre par les opérationnels, permettant, entre autres, la maîtrise des activités au jour le jour ;
- un dispositif structuré et coordonné par la deuxième ligne de maîtrise, constituée des services fonctionnels responsables de domaines d'expertise et des fonctions dédiées à l'animation du dispositif global de maîtrise des risques (fonctions de gestion des risques, de contrôle interne, d'assurance, de conformité...) ;
- une évaluation globale et indépendante du dispositif conduite par la troisième ligne, assurée par la fonction d'audit interne indépendante et rattachée au plus haut niveau de l'organisation. Elle fournit, à travers une approche fondée sur le risque, une assurance globale aux instances de surveillance et à la direction générale de l'organisation.



2. Adapter rapidement la gouvernance à la maîtrise des risques cyber

- Le modèle des trois lignes de maîtrise doit pouvoir s'adapter à tous les types de risques nouveaux qui sont en train d'émerger : nouveaux risques environnementaux / climatiques ; nouveaux risques politiques ; nouvelles approches sur la RSE et le développement d'externalités positives-négatives ; et donc aussi risques cyber. À date, la délinéation des rôles au titre de bonne gouvernance qu'implique le concept des trois lignes de maîtrise ne semble pas devoir être remise en cause par l'un de ces risques.
- Cependant, le risque cyber pose un problème particulier en termes de vitesse d'adaptation, que l'on retrouve également d'ailleurs dans la création de valeur digitale, en raison de multiples caractéristiques particulières à l'environnement cyber/digital :
  - nouvelle importance de compétences strictement techniques, ou difficiles à acquérir rapidement, alors même que les talents peuvent se trouver en situation de pénurie ;
  - approches sécuritaires particulières, propres à la sécurité dans les systèmes d'information, dont l'originalité (via la mise en place spécifique de procédures, technologies, personnel, culture) a parfois du mal à s'acclimater aux structures existantes – avec un écho ici aux difficultés plus générales de transformation digitale rencontrées dans certaines entreprises ;
  - accélération de la transformation digitale en parallèle avec l'augmentation rapide du risque cyber, et sa très grande évolutivité qui ne permet plus à l'entreprise de pouvoir prévoir sereinement son rythme d'adaptation à ce nouveau risque.
- Afin de répondre à cette problématique d'adaptation accélérée, particulière à l'univers cyber, tout en maintenant le principe invariant des « trois lignes de maîtrise » et les équilibres entre ses trois composantes, une solution transitoire est proposée : celle de la constitution d'un « comité d'adaptation aux cyber-risques », qui permettrait d'accélérer conjointement l'adaptation des trois lignes de maîtrise au risque de cybersécurité. Cette solution temporaire se rapproche de ce qui s'observe sur les questions de la création de valeur dans le domaine digital, avec l'émergence de la fonction de *« Chief Digital Officer »,* souvent perçue comme temporaire, mais nécessaire pour accélérer la transformation de l'entreprise dans le cadre d'une évolution non linéaire de son activité.

3. Principes structurant du Comité d'adaptation aux cyber-risques

a. Le Comité a pour mission d'accélérer l'adaptation aux cyber-risques, c'est-à-dire faire atteindre à l'ensemble des trois lignes de maîtrise un niveau de maturité satisfaisant en matière de cyber-risques. Ce niveau satisfaisant doit pouvoir être identifié de manière objective sur des critères explicites (voir point suivant). Lorsque ce niveau sera atteint, ce comité pourra être dissout : la dissolution signifiera donc auprès des différentes parties prenantes de l'entreprise que celle-ci considère qu'elle a atteint un niveau de maturité satisfaisant. Ce comité pourra être composé de représentants des fonctions IT, RH, Com-

munications, Finance, Juridique, Gestion du risque ainsi que du RSSI (responsable de la sécurité des services informatiques) et du DPO (délégué à la protection des données).

b. L'organisation pourra s'inspirer des critères suivants lui permettant de définir pour elle-même si elle a atteint un niveau de maturité satisfaisant :

- La cartographie des risques « traditionnels » de l'entreprise (par fonction, par métier) trouve une traduction précise dans la cartographie des nouveaux risques cyber (et vice-versa).
- Pour les actifs existants, l'évaluation du risque cyber est dynamique (en fonction de l'évolution de la surface d'attaque de l'entreprise et des menaces externes) et valorisée en terme d'impact sur la valeur totale d'entreprise.
- Pour les actifs en développement, les processus d'innovation de type « transformation digitale » prennent en compte au plus tôt le risque cyber, évalué de manière dynamique et valorisé sur la valeur totale d'entreprise : ce risque dans l'innovation est donc pris en compte au plus tôt, dans le cadre d'applications de processus « *security by design* ».
- En interne, la direction générale et le conseil d'administration évaluent de manière fréquente et régulière les conditions de cybersécurité de l'entreprise, de son environnement et de la concurrence, sur la base des cartographies de risques définies plus haut. Ils vérifient également l'adéquation des ressources humaines disponibles pour la cybersécurité.
- L'ensemble des procédures, personnels et technologies de l'entreprise sont soumis de manière permanente à des tests et simulations de cybersécurité qui évaluent le niveau de résilience et actualisent la valorisation dynamique de la cartographie des risques – tout en identifiant les apprentissages les plus pertinents.
- Qualité (volume, fréquence, précision) de la communication avec les tiers (régulateurs, agences de notation, assureurs, clients, partenaires) sur le risque de cybersécurité.

c. À l'issue de la dissolution du Comité d'adaptation aux cyber-risques, plusieurs dispositions pourront être maintenues pour assurer la résilience de l'organisation :

- Poursuite continue de la politique de « tests et simulations permanents », qui doit permettre l'évaluation dynamique de la cartographie des risques cyber. Cette mise sous « tension permanente » est instruite de manière fréquente et régulière dans l'entreprise sans pour autant que les coûts directs ou indirects puissent constituer un préjudice compétitif. Elle permet de donner une visibilité sur l'état de la cybersécurité de l'entreprise aux intervenants financiers (assureurs, agences de notation de risques, organismes de crédit…) ou acteurs de la confiance (régulateurs, associations de consommateurs, etc.).
- La relation particulière entre le Responsable de la Sécurité des Systèmes d'Information et les services d'analyse et gestion des risques doit être maintenue afin de

poursuivre les liens nécessaires entre cartographie des risques de l'entreprise, cartographie des risques cyber et évaluation des risques cyber en rapport avec les impacts opérationnels sur l'entreprise. Cette relation doit être également maintenue dans le cadre de la diffusion de la connaissance, où le RSSI peut servir d'acteur de veille. De manière générale, il est rappelé que, quelle que soit sa taille, toute organisation devra posséder un responsable ou référent cyber-risque de manière permanente.

- Après dissolution, ce comité pourrait être réactivé dans la situation exceptionnelle d'un nouveau risque technologique correspondant à un changement disruptif et structurel de très grande ampleur, affectant l'ensemble du tissu économique et nécessitant une révision profonde des approches de sécurité[41].

Annexe & Notes

Contrôles CIS 20

Ces contrôles permettent d'assurer qu'un socle à minima d'une politique de cybersécurité a bien été établi. Ce point de « démarrage » correspond aussi à l'application du principe #3 « être adaptatif » au cadre d'analyse de la cybersécurité elle-même. Ces contrôles de base sont issus du *CIS Critical Security Controls for Effective Cyber Defense (Center of Internet Security)* qui pourra servir de document de référence. On pourra ainsi énoncer les contrôles suivants et les liens avec les principes décrits plus haut.

Ces contrôles sont listés par ordre décroissant d'importance, en soulignant l'importance primordiale des cinq premiers contrôles.

1. Inventaire des équipements autorisés et non autorisés (lié au principe #6, Identification).
2. Inventaire des logiciels autorisés et non autorisés (lié au principe #6, Identification).
3. Configurations sécurisées pour le matériel et les logiciels installés sur les équipements mobiles, ordinateurs portables, postes de travail et serveurs (lié au principe #7, Protection).
4. Analyse et remédiation des vulnérabilités de manière continue (lié aux principes #6 Identification, #8 Détection et #9 Réponse).
5. Utilisation contrôlée des privilèges administratifs (lié au principe #7, Protection).

À ceux-ci s'ajoutent 10 autres contrôles techniques « fondateurs » :

6. Maintenance, supervision et analyse des journaux d'audit (lié au principe #8 Détection, et #9 Réponse).
7. Politique de protection pour les emails et les navigateurs web (lié au principe #7 Protection).
8. Défense contre les maliciels (lié aux principes #7 Protection et #8 Détection).
9. Limitation et contrôle des ports, protocoles et services réseau (lié au principe #7 Protection).
10. Récupération des données (lié au principe #10, Reprise/résilience de l'activité).
11. Configuration sécurisée pour équipements réseaux (lié au principe #7 Protection).
12. Défense des frontières / périmètre (lié au principe #8, Détection).
13. Protection des données (lié au principe #7 Protection).
14. Contrôle des accès en fonction de la hiérarchie des droits et des besoins (lié au principe #7 Protection).

15. Contrôle des accès sans fil (lié au principe #7 Protection).
16. Supervision et contrôle des comptes utilisateurs (lié au principe #7 Protection et #8 Détection).

À ces contrôles, s'ajoutent d'autres contrôles d'ordre humain, organisationnel et concernant les procédures :

17. Analyse des compétences en sécurité et formation appropriée pour combler les lacunes de compétences (lié au principe #7 Protection).
18. Gestion du cycle de vie de tous les applicatifs de sécurité, développés en interne ou acquis auprès d'éditeurs (lié au principe #7 Protection).
19. Développement d'une politique globale de réponse et de gestion des incidents, incluant plans, rôles, formation, communication, gouvernance (lié aux principes #8 Détection et #9 Réponse).
20. Exercices d'alerte, de simulation, de tests d'intrusion permettant d'évaluer la qualité de l'organisation – hommes, technologies & processus (lié aux principes #9 Réponse et #10 Reprise de l'activité).

Notes

[1] « Cyber risks are like unpredictable storms of ever growing severity; nothing is stronger to weather them sustainably than a proactive alliance between anticipative risk management and farseeing internal audit ». Voir "At the junction of corporate governance and cybersecurity", p.4 publié par FERMA & ECIIA, 2017.

[2] Le cyber-risque n'est considéré comme important que par 1 % des répondants au 1er semestre 2013. Il est cité quatre ans plus tard par 51 % des répondants comme l'un des risques les plus importants pour la place financière de la City de Londres, en progression constante sur la période, et en deuxième position des réponses pour le plus grand risque majeur. Plus important encore : le risque de cybersécurité était désormais cité en 2ème position par 47 % des répondants comme étant le risque le plus difficile à gérer pour leur propre firme, à comparer avec une réponse de 1 % également quatre ans plus tôt – voir Bank of England Systemic Risk Survey, 1H 2017.

[3] Voir World Economic Forum Risk Report 2017, ou encore PwC CEO Survey 2012-2017

[4] https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031

[5] https://www.theguardian.com/business/2014/may/05/target-chief-executive-steps-down-data-breach

[6] https://www.lemondeinformatique.fr/actualites/lire-saint-gobain-evalue-a-250-meteuro-les-degats-lies-a-l-attaque-notpetya-68955.html ou encore https://www.huffingtonpost.fr/2017/06/28/a-cause-de-la-cyberattaque-notpetya-des-salaries-mis-en-rtt-en_a_23005706/

[7] Voir par exemple l'étude IPSOS/CIGI pour United Nations Conference on Trade and Development (UNCTAD) sur 24 pays, parue en 2017, qui notait que 82 % des répondants étaient concernés par les atteintes en ligne à leur vie privée par les cybercriminels et que 74 % étaient « troublés » par les comportements des sociétés internet – cf. https://www.techrepublic.com/article/online-shoppers-are-losing-trust-in-e-commerce-study-finds/. Sur la question des activités de communication publicitaire en ligne, une étude Rakuten Marketing de 2017 pour la France, l'Allemagne, la Grande-Bretagne, l'Australie et les Etats-Unis notait que 83 % des 2500 personnes interrogées considéraient la publicité en ligne comme disruptive. 54 % des Français les associaient à une activité négative telle que celle des « *fake news* » – voir : https://digiday.com/marketing/global-state-consumer-trust-advertising-5-charts/

[8] Dans l'enquête IPSO/CIGI pour l'UNCTAD, seuls 12 % affirmaient faire confiance à Internet. Parmi le reste, 20 % faisaient moins d'achats en ligne en raison de leur manque de confiance, établissant un lien direct entre manque de confiance et dégradation du développement des activités en ligne. Cf. https://www.internetsociety.org/blog/2017/04/survey-paints-a-bleak-picture-of-the-current-state-of-trust-online/

[9] Martin Hilbert, University of Southern California, 2011. Cette explosion de données est liée au coût toujours plus réduit de captation et de traitement de l'information. Elle a été observée dans le domaine du calcul computationnel par l'un des fondateurs de Intel, Gordon Moore, qui a observé dès le milieu des années 1960, pour un prix égal, un doublement des capacités tous les 18 mois. Cette « loi », à peu près conservée au cours du dernier demi-siècle, trouve son pendant dans d'autres types d'applications.

[10] https://techcrunch.com/2015/06/02/6-1b-smartphone-users-globally-by-2020-overtaking-basic-fixed-phone-subscriptions/

[11] Exponential Organization, p. 31

[12] https://www.gartner.com/newsroom/id/3598917

[13] https://www.wsj.com/articles/SB10001424053111903480904576512250915629460

[14] Dont les trois plus grandes sociétés au monde : Apple, Alphabet et Microsoft – suivies d'Amazon et Facebook.

[15] http://siblisresearch.com/data/sp-500-sector-weightings/. Cette transformation des activités humaines et économiques ne semble pas devoir cesser. Aux Etats-Unis et en Europe de l'Ouest, la part de la publicité en ligne passe de 17-18 % à 31-32 % du total publicitaire de 2010 à 2016. En 2020, la publicité en ligne sera le premier secteur publicitaire au niveau mondial devant la TV, la radio et les médias papier. Le commerce en ligne va également continuer à très fortement augmenter. D'ici 2021, il devrait représenter 17 % du total des ventes au commerce aux Etats-Unis ; 20 % au Royaume-Uni ; et jusqu'à 33 % en Chine. Amazon en tire une croissance du chiffre d'affaires d'environ 25 % par an de manière continue et cela depuis au moins quinze ans. À ce rythme, Amazon devrait

dépasser le chiffre d'affaires de Walmart d'ici 4-5 ans. Les marchés anticipent déjà ces mouvements : Amazon est aujourd'hui valorisé à deux fois la valeur de Walmart.

16 Source Linux (Voir: http://eecatalog.com/embeddedlinux/2016/09/08/happy-25th-birthday-linux-a-short-history/).

17 Source Paladin Capital – présentation à Luxembourg PwC CyberDay, Octobre 2017.

18 Commentaire de Alain Bouillé, Président du CESIN (Club des experts de la sécurité de l'information et du numérique). Discussion avec l'auteur dans le cadre de l'étude (2018).

19 Source IBM Security Service 2014 Cyber Intelligence Index ; CompTIA 2015.

20 Voir article HBR France : https://www.hbrfrance.fr/chroniques-experts/2018/05/20164-valeur-de-lentreprise-a-lepreuve-cyber-attaques/

21 https://www.infosecurity-magazine.com/magazine-features/a-breach-too-far/

22 Par exemple, la société française TV5 Monde, victime d'une cyber-attaque sur ses systèmes de télédiffusion en 2015, verra les communications internes désorganisées pendant de longs mois, provoquant une atteinte réelle au climat de travail pour les employés. Voir : https://www.francetvinfo.fr/replay-radio/ils-ont-fait-l-actu/que-devient-tv5-monde-apres-la-cyberattaque_1784035.html

23 Cette obligation s'impose sans pour autant que Wyndham soit reconnue coupable. Voir : http://fortune.com/2015/12/09/wyndham-settles-data-breach-ftc/

24 https://www.theinquirer.net/inquirer/news/3025347/maersk-forced-to-reinstall-45-000-pcs-and-4-000-servers-following-notpetya-attack

25 https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

26 Il faut aussi noter que l'ensemble de ces cadres de référence peuvent s'interconnecter les uns avec les autres – et de nombreux travaux de cartographie sont d'ailleurs établis en ce sens. Il s'agit ici de souligner l'importance d'aller vers des standards communs qui permettront aux différents interlocuteurs (entreprises, éditeurs de logiciels, SSII, institutions de régulation…) , à terme, de mieux se comprendre afin de renforcer l'échange d'information, un point critique dans la lutte contre la cybercriminalité.

27 Ex : données d'identification personnelle ; données générées par les applications ; données de mesures des activités internes…

28 En particulier: (a) Systèmes en cours de développement, qui doivent être idéalement développés selon des principes de « security by design », qu'il s'agisse du design utilisateurs et/ou des procédures d'utilisation qui doivent par exemple minimiser les risques de vulnérabilités, ou bien des tests du code en développement ; (b) Systèmes subissant remplacement ou mises à jour importantes – qu'il s'agisse du bon déploiement des mises à jour ou de la suppression effective d'anciens systèmes en analysant les impacts éventuels sur les systèmes existants.

[29] L'impact sur la valeur d'entreprise peut être déduit de ces liens entre risques « traditionnels » et « cyber-risques ». La valeur du dommage si le risque est réalisé sera liée à l'analyse des risques « classiques » – par exemple, le coût de réputation. La fréquence d'apparition du risque sera liée, elle, à l'étude de la fréquence des cyber-incidents. Cette étude devra être renouvelée afin de prendre en compte la rapidité des évolutions du domaine.

[30] Incluant la réponse et la reprise de l'activité, mais aussi actions de communications ou sanctions internes.

[31] On peut citer par exemple : via un impact compétitif positif – ex. : augmentation de la confiance client ; via une meilleure maitrise des coûts de cybersécurité ; via l'identification d'opportunités autour de l'information sur vulnérabilités & maliciels ; sur les savoir-faire développés pour détecter et remédier ; etc.

[32] À noter par exemple le courrier début 2018 de Larry Fink, dirigeant du fond BlackRock, à l'ensemble des sociétés dans lesquelles le fond a investi (voir https://www.blackrock.com/corporate/investor-relations/larry-fink-ceo-letter) ou bien la demande des fonds Jana Partners LLC et California State Teachers' Retirement System, actionnaires d'Apple, d'étudier l'impact des produits Apple sur les enfants (voir par exemple https://mashable.com/2018/01/07/apple-iphone-kids/#iy9jcBxhHOqj).

[33] Par exemple : (a) Mise en place itérative, étape par étape (éviter le « *big bang* » qui ne permet pas d'identifier rapidement les frictions de mise en place) – et appliquée en priorisant en fonction de la valeur en risque et des dépendances ; (b) Éviter la complexité dans les procédures – toujours chercher la simplicité (qui réduit le risque de vulnérabilités).

[34] Ces exercices permettent d'adresser la courbe d'apprentissage plus rapidement que si frappé par des évènements extérieurs incontrôlés.

[35] Il faudra prendre bien sûr aussi en compte les procédures et cadres d'interaction avec ces différents acteurs, y compris : (a) l'identification et le respect des cadres légaux et administratifs dans lesquels ces interactions doivent s'établir ; (b) l'identification des sources, fréquences et autres modalités de contact (y compris systèmes émergents d'échanges d'information).

[36] Syndicats, ONG, etc., mais aussi organismes représentatifs de la verticale industrielle.

[37] En particulier les assureurs – et les acteurs de l'écosystème émergent de la cyber-assurance.

[38] On pourra y adjoindre les contrôles soulignés dans *The CIS Critical Security Controls for Effective Cyber Defense (Center of Internet Security)* ainsi que ceux du Guide d'hygiène informatique (ANSSI, 2017).

[39] Pourra inclure une classification des actifs et données en fonction du risque, et permettre la mise en place de contrôles à minima en cas de risque identifié. Il conviendra, en effet, afin de concentrer son action et d'agir de manière adaptive (principes #2 et #3), de déter-

miner d'abord les actifs & données avec le plus grand facteur de risque et les politiques de gestion de ces risques en particulier. Dans le cadre évolutif de l'environnement de cybersécurité, il conviendra également d'établir une vision dynamique des mesures de sécurité avec tests et réévaluations fréquents.

40 Cf. les principes décrits dans le Document IFACI – AMRAE de 2013, « Trois lignes de maîtrise pour une meilleure performance ».

41 À titre d'exemples illustratifs, on pourrait évoquer l'émergence de nouvelles menaces liées à la diffusion de nouvelles capacités de calcul quantique alliées à l'intelligence artificielle auprès d'acteurs cybercriminels ; ou encore l'émergence d'un risque cyber-physique par l'utilisation de nano-drones permettant de nouvelles formes d'exploitation de vulnérabilités via la diminution de la défense par air-gap (isolement physique des systèmes, non connectés à de grands réseaux), etc.

Document rédigé par Guy-philippe Goldstein, Enseignant-chercheur à l'Ecole de Guerre Economique.

Remerciements

Pour leur contribution au sein du groupe de travail de l'IFACI :

Yann Boucraut, Directeur Central Contrôle Interne et Audit, Groupe Bouygues

Sylvie Sadones, Directeur Audit Interne Informatique, Groupe Renault

David Metivier, Head of Group Internal Audit for IT and operations, Sodexo

Vincent Maret, Partner, Cyber Security Services, KPMG Advisory

Pour leur relecture attentive et leurs conseils:

Philippe Trouchaud, Partner PwC France | Technology | Cyber Security & Infrastructure Leader

Alain Bouillé, Directeur de la Sécurité des Systèmes d'Information du Groupe Caisse des Dépôts, Président du CESIN (Club des experts de la sécurité de l'information et du numérique)

Danny Bren, Ancien Brigadier Général de l'Armée de Défense d'Israel, Commandant des Divisions de Cyber-Défense

Réalisation : Ebzone Communication (www.ebzone.fr)

IFACI - Institut Français de l'Audit et du Contrôle internes
98 bis, boulevard Haussmann - 75008 Paris
Tél. : 01 40 08 48 00 - www.ifaci.com