GUIDE DES RISQUES CYBER IFACI 2.0

LES QUESTIONS DE L'AUDITEUR ET DU CONTRÔLEUR INTERNE

2020

LE MOT DU DÉLÉGUÉ GÉNÉRAL

Les risques cyber tiennent une place particulière au sein de la cartographie des risques. Année après année, ils figurent parmi les toutes premières préoccupations des managers et de leurs dirigeants. L'édition 2020 de Risk in Focus, le palmarès européen des risques les plus importants pour les directeurs d'audit interne, le confirme une fois encore. Cette spécificité du risque cyber tient sans doute à son origine, tant humaine et organisationnelle que technique, qui le rend plus transversal et plus diffus que d'autres dont les causes sont plus aisément circonscrites.

C'est donc en toute logique que les adhérents de l'IFACI souhaitent en permanence améliorer leurs connaissances et leurs pratiques dans ce domaine. En 2018, l'IFACI a publié le guide « cyber-risques: enjeux, approches et gouvernance » dont l'objectif était, au plan de l'organisation comme de la méthode, de définir les fondamentaux du traitement du risque cyber. La deuxième étape consistait, pour les auditeurs et les contrôleurs internes, à détailler la méthode.

C'est ainsi que, supervisé par Guy-Philippe Goldstein, les adhérents de l'IFACI ont conjointement produit ce guide 2.0. De nombreux apports et soutiens ont contribué à augmenter encore sa qualité. Je remercie ici tout particulièrement Fabien Caparros et Yann Tonnelier (ANSSI), Vincent Maret (KPMG), Thierry Delville (PwC) et Maxime Cartan (Citalid) qui ont chacun participé à la rédaction de ce document.

Un risque complexe et évolutif comme celui que nous traitons ici doit faire l'objet d'une surveillance permanente. C'est l'esprit qui guide cette initiative depuis deux ans. Au-delà, ce projet illustre la capacité des adhérents de l'IFACI à se mobiliser dans le temps, autour d'une réflexion qui sert toute la communauté des auditeurs et des contrôleurs internes.

Je les en remercie sincèrement.

Philippe Mocquard
Délégué Général

TABLE DES MATIÈRES

INTRODUCTION

UN GUIDE DES CYBER-RISQUES POUR L'AUDITEUR ET LE CONTRÔLEUR INTERNE

L'OBJECTIF

Le risque cyber constitue désormais l'un des tous premiers risques de l'entreprise. Dans son édition de janvier 2020, le baromètre du risque publié par Allianz faisait figurer pour la première fois le risque cyber à la première place des risques de l'entreprise (39% des réponses), devant même le risque d'interruption d'activité – alors que le risque cyber n'était qu'à la 15ième place il y a juste sept ans (avec alors 6% des réponses) [1].

D'autres sources soulignent également cette prépondérance nouvelle. L'étude semestrielle du risque sur la place financière de la City de Londres, réalisé par la Banque d'Angleterre via un questionnaire auprès des cadres dirigeants financiers, décrit la même évolution. Là encore, il y a sept ans, moins de 5% des répondants seulement identifiaient le risque cyber comme un risque majeur pour leur organisation pour la place de Londres. Il est désormais, à la 2ième place des risques les plus importants, avec plus de 60% des répondants [2]. De même, dans la section « risques pour l'activité économique », le Global Risk Survey du World Economic Forum de Davos faisait figurer dans son édition de 2020 le risque cyber au 2ième rang – et au premier rang aux Etats-Unis, en Grande-Bretagne et en France [3].

Ce constat, déjà apparent en 2018, avait conduit à la réalisation d'un premier guide introductif par l'IFACI, qui traitait de manière généraliste à la fois de l'importance du sujet et de premières réflexions tant sur les référentiels que sur les questions de gouvernance. Afin d'aller plus loin, et au vu de l'importance toujours plus forte du sujet, il a semblé nécessaire de passer d'une réflexion large à une approche plus appliquée, et qui aide directement le public des auditeurs et des contrôleurs internes de l'IFACI.

1 Voir Allianz Global Corporate & Specialty, "Allianz Risk Barometer: Identifying The Major Business Risks For 2020", Janvier 2020
2 Voir Rapport sur site de la banque d'Angleterre (https://www.bankofengland.co.uk/systemic-risk-survey/2019/2019-h2). Le risque le plus important pour les cadres dirigeants de la City de Londres étant le risque politique propre à la Grande-Bretagne, c'est-à-dire Brexit.
3 Voir section "Risk of Doing Business", disponible à http://reports.weforum.org/global-risks-report-2020/survey-results/global-risks-of-highest-concern-for-doing-business-2020/#

LA DÉMARCHE

Pour s'assurer que ce guide 2.0 permettrait d'être directement utile aux auditeurs et aux contrôleurs internes, l'IFACI est parti de principes simples :

1. demander directement aux auditeurs et contrôleurs internes, via une enquête, les questions identifiés comme les plus importantes concernant les risques cyber (voir ci-dessous les résultats)
2. dans le contexte toujours évolutif du cyberespace, se concentrer sur les points les plus prioritaires plutôt qu'essayer d'apporter des réponses exhaustives
3. créer pour chaque question de petites équipes de travail, constituées des auditeurs et des contrôleurs externes : les mieux à même de répondre aux questions de leurs propres confrères.

Ces volontaires, dont on pourra retrouver une biographie à la fin de ce guide, ont également été épaulés par trois experts externes – Maxime Caritan de Citalid, Vincent Maret de KPMG et Thierry Delville de PwC – ainsi d'ailleurs que par les experts de l'ANSSI : Fabien Caparros, chef de la division chargée des méthodes de management de la sécurité numérique à l'ANSSI, et Yann Tonnelier, chef de bureau adjoint Management des risques cyber.

LES SUJETS PRIORITAIRES

Un questionnaire sur les questions les plus importantes que se posaient les auditeurs et les contrôleurs internes a été soumis aux membres de la communauté de l'IFACI. Il a été renseigné par 51 répondants. La population des répondants a été constitué essentiellement d'auditeurs (2/3) et pour environ 15% de contrôleurs internes (le reste étant constitué de consultants et conseils des auditeurs et contrôleurs internes). Les répondants venaient principalement d'organisations de plus de de mille employés (71%) dont en particulier des grands groupes de plus de 10.000 employés (43%).

Les demandes les plus fortes concernent des précisions sur les éléments / contrôles de base, les manières d'arriver à communiquer avec le top management sur ces questions cyber et la traduction du risque cyber en effets opérationnels concrets.

A contrario, sur cet échantillon, la demande a été moins forte sur les questions de vocabulaire a minima, liste de prestataires… même si cette demande est demeurée matérielle. In fine, ce sont les questions qui à la fois ont dépassé les 75% en termes d'intérêts cumulés (« Oui, assez intéressé » et « Oui, très intéressé ») et qui ont dépassés le 40% en termes d'expression la plus forte (« Oui, très intéressé ») qui ont finalement été retenues pour étude pour ce guide 2.0. La liste des questions retenues se trouve ci-contre (noté en bleu gris).

Fig.1. Questions-clés retenues pour étude pour le Guide 2.0

QUESTION	% TRÈS INTÉRESSÉ
Connaitre les fondamentaux techniques/ contrôles de base nécessaire à minima pour les équipes audit et de contrôle interne	73 %
Sensibiliser le top management, et avec quels types de tableau de bord	68 %
Identifier les impacts opérationnels concrets du risque cyber	65 %
Mesurer la maturité de l'organisation et son niveau d'exposition au risque cyber	62 %
Développer et évaluer une capacité de gestion de crise et de résilience cyber	61 %
Préciser le rôle de l'audit et du contrôle interne face aux autres experts internes en cybersécurité	57 %
Se tenir informé de l'évolution du risque cyber – y compris au niveau géopolitique	55 %
Sensibiliser les collaborateurs, et développer une « cyber-hygiène »	52 %
Prendre en compte le risque cyber dans les projets informatiques	41 %
Connaître le vocabulaire/jargon technique nécessaire à minima pour l'auditeur et le contrôleur interne	39 %
Sélectionner les bons prestataires	18 %

RÉSULTATS ET PROCHAINES ÉTAPES

L'ensemble des travaux réalisés par les différentes équipes de travail a été présenté en session plénière et ont donnée lieux à des fiches de synthèse ici présentes. Ces fiches doivent être lues comme une introduction à chacune de ces questions clés, et permettre aux auditeurs et contrôleurs internes une première orientation. Des compléments en termes de contenu et parfois d'outils Excel sont disponibles aux adhérents de l'IFACI sur Workplace.

Ces fiches sont donc l'expression de la réflexion des différentes équipes. Epaulés par les conseils listés plus haut, les équipes d'auditeurs & contrôleurs internes ont néanmoins gardé jusqu'au bout le contrôle rédactionnel et donc sont seules responsables des éléments posés ici. Il s'agit d'un parti pris. Face à une matière technologique terriblement large et changeante, embrassant des entreprises de tout type et conditions, il serait illusoire d'écrire dans le marbre ce qui pourrait être nuancé, ou changé, dans 24-36 mois. Ce guide se veut donc le reflet volontaire d'une première réflexion collective, avec tous ses avantages et ses défauts. Il reflète aussi une démarche particulière : il est un appel au questionnement et à la réflexion de tous, qu'ils convergent avec les idées présentées ici, ou bien au contraire qu'ils en divergent. Car, à la mesure de la matière, ce guide doit être vivant et évoluer.

Avis, exemples, réflexions sont donc les bienvenues de la part de l'ensemble des auditeurs et contrôleurs internes. Tout apport constructif permettra de faire progresser la communauté des membres de l'IFACI, tant le sujet, important et riche, doit encore incorporer variations, compléments ou même situations éventuelles de contre-indication. Au-delà de ce guide et de son matériel, c'est cette conversation qui permettra à la communauté des auditeurs et des contrôleurs internes de contribuer de manière efficace et dynamique à un risque en perpétuel évolution, qui menace les entreprises et même, parfois, les nations derrière les organisations qui la composent. A terme, ce guide, lui, devra devenir la somme des avis et questions dont tous les auditeurs et les contrôleurs internes sont « les héros ». Avec une logique sous-jacente de questionnement et de responsabilité personnelle, qui est finalement la plus importante face au cyber-risque.

Sans oublier bien sûr, avant que cette conversation ne démarre dans les pages suivantes, les efforts importants des vingt-quatre « éclaireurs », membres de l'IFACI, et qui ont apporté la première pierre à cet échange. Qu'ils trouvent ici l'expression des remerciements du reste de l'organisation de l'IFACI.

PARTIE I PREMIERS ÉCLAIRAGES D'EXPERTS

LE RISQUE CYBER : RÔLE DES DIRIGEANTS, DES AUDITEURS & DE LA GOUVERNANCE

*Le risque cyber est devenu un risque majeur pour l'entreprise. Yann Tonnelier rappelle qu'il implique le dirigeant – enjeu de la question « **Sensibiliser le Top Management** ». Il souligne aussi l'importance de l'auditeur et d'une gouvernance avec un comité qui implique les trois lignes de défense – un point évoqué également dans la question « **Préciser le rôle de l'audit et du contrôle interne** ».*

Yann Tonnelier
Chef adjoint du bureau «Management des Risques Cyber» de l'ANSSI

Les organisations évoluent à l'heure actuelle dans un environnement instable et hyper réactif, marqué par la transformation numérique et des contextes économique, politique et géopolitique en mouvement permanent. En parallèle, la menace évolue tout aussi rapidement dans ses formes et ses modes opératoires.

Les attaquants, d'une part, redoublent d'ingéniosité pour parvenir à leurs fins, en exploitant les relations de confiance entre les parties prenantes, causant des impacts imprévisibles et fulgurants. Dans certains cas, ces pratiques peuvent même être fatales aux organisations concernées.

D'autre part, la transformation numérique des organisations et leurs interconnexions croissantes avec leurs clients, fournisseurs et partenaires, ont fait évoluer le risque numérique qui pèse sur celles-ci.

Le risque numérique, qui était vu comme un risque technique il y a encore quelques années, doit dorénavant être considéré comme un risque majeur pour les organisations.

Si l'on devait proposer une définition contemporaine du risque numérique, elle pourrait inclure les caractéristiques suivantes :

- Le risque numérique est indissociable des nouvelles technologies exploitées par les organisations et des nouveaux usages proposés à leurs clients et partenaires.
- Lorsqu'il survient, le risque numérique peut anéantir l'organisation, notamment si les impacts n'ont pas été suffisamment anticipés.
- Enfin, le risque numérique engage la responsabilité du dirigeant dans sa gestion et son traitement car ses impacts concernent l'ensemble de l'organisation.

Il est clair qu'aujourd'hui, le dirigeant n'a pas d'autre choix que de maitriser le risque numérique au même titre que les autres risques majeurs de son organisation. A défaut, il engage la responsabilité sociétale de l'entreprise, sa responsabilité civile, voire son mandat de dirigeant. Cette responsabilité est notamment accentuée par les réglementations de sécurité numérique qui s'imposent aux organisations (RGPD, NIS, LPM, etc.).

Devant l'accroissement du risque numérique et sa propension à gagner toutes les activités de l'organisation, le dirigeant doit définir de nouveaux seuils d'acceptabilité du risque.
De plus, l'évolution et la transversalité du risque numérique oblige le dirigeant à reconsidérer son modèle de gestion des risques, de telle sorte que ce risque rejoigne les préoccupations stratégiques, économiques et juridiques de l'organisation.

Pour acquérir cette vision globale des risques et veiller à ce que le risque numérique soit corrélé aux objectifs de l'organisation, un comité des risques doit être mis en place en s'appuyant sur l'ensemble des trois lignes de défense. Une attention particulière sera portée à sa capacité à s'affranchir des silos fonctionnels, métiers et opérationnels existants.

Les auditeurs et contrôleurs internes, qui forment cette troisième ligne de défense, sont des acteurs indispensables dans la maîtrise du risque numérique. Ils évaluent la réalité et l'efficacité des actions engagées, au regard de la stratégie de gestion des risques en place. Ils apprécient l'évolution des risques et s'assurent que la cotation ou quantification des impacts soit revue. Enfin, les auditeurs et contrôleurs internes font remonter les informations nécessaires aux risk managers et dirigeants pour qu'ils pilotent les risques en pleine conscience et en dégagent les tendances à venir.

De ce fait, ils participent pleinement au pilotage et à l'amélioration continue du modèle de gestion des risques. Ils fournissent l'assurance de l'efficacité du dispositif à l'équipe dirigeante de l'organisation.

Pour conclure, l'organisation ne peut que s'adapter à l'évolutivité du risque numérique. Il est indispensable que ses acteurs, qu'ils soient dirigeants, managers ou salariés, se saisissent du sujet et s'impliquent dans le modèle de gestion du risque numérique.

Les travaux menés par les contributeurs de l'IFACI et présentés dans ce guide en sont la preuve. Je les remercie pour les travaux menés et les encourage à poursuivre leurs réflexions dans cette voie.

GÉRER LE RISQUE CYBER : OBJECTIFS ET APPROCHES

Le risque cyber s'inscrit dans le cadre général de la gestion du risque, comme le rappelle Maxime Cartan. Pour l'entreprise, il s'agit d'identifier le plan d'action le plus rentable. Afin de le calculer rapidement, à chaque évolution de l'entreprise, on peut prendre en compte plusieurs facteurs, rassemblés sous l'acronyme « Chain ». Ces éléments introduisent en particulier les questions des « ***Impacts opérationnels concrets du risque cyber*** *» et de la nécessité de «* ***Mesurer la maturité et l'exposition au risque*** *», approfondis dans le document.*

Maxime Cartan
Co-fondateur et Président de Citalid Cybersécurité

Le risque cyber fait partie du top 2 des risques auxquels font face les organisations. Cependant, sa gestion reste une équation difficilement soluble.

Premièrement, dans un contexte de transformation digitale massive, les organisations font face à des menaces toujours plus intenses, omniprésentes, protéiformes et qui évoluent vite. Pour y répondre, elles disposent d'initiatives et de moyens internes qui œuvrent trop souvent en silos, et d'une offre pléthorique de produits cyber complexes, onéreux et couvrant des pans de sécurité distincts. Cette couche tactique est trop souvent décorrélée de la couche stratégique, en raison d'univers et de langages différents. Point d'orgue de tout cela : comme tout acte d'investissement, leurs budgets sont scrutés et restent sous tension.

Cet état des lieux débouche sur un constat inévitable : il n'est économiquement pas viable d'espérer pouvoir couvrir tous les scénarios de risque cyber à 100%. Les organisations doivent donc basculer dans une logique d'arbitrage : quels sont les risques qu'elles vont accepter, au regard du faible impact économique encouru ? Quels sont ceux à fort impact, qu'elles doivent réduire prioritairement ? Lesquels transférer, par exemple à un cyber-assureur ? Aucun choix n'est mauvais, et ils peuvent même être combinés : chaque organisation se doit d'avoir une réponse différenciée et contextualisée à ses scénarios de risque, selon leurs fréquences et impacts financiers.

Pour y parvenir, les décideurs ont besoin d'être guidés dans leurs choix. Ils ont besoin d'un GPS qui indique où ils se situent exactement par rapport à la menace, la destination à atteindre en termes d'exposition financière au risque cyber, et par quel chemin y parvenir. Il est possible de filer cette métaphore : un GPS calcule automatiquement le chemin le plus court et le plus rapide, c'est-à-dire ici le plan d'action le plus efficace et rentable.

De surcroît, qui dit menace mouvante et actions menées pour s'en protéger, dit nécessité de recalculer le positionnement de l'organisation et le chemin à emprunter de façon dynamique. Enfin, ce GPS ne peut fonctionner que si les décideurs bénéficient d'une vision « cockpit » centralisée et quantitative, afin de faire correspondre automatiquement l'ensemble des efforts internes et solutions de sécurité aux menaces les plus pertinentes, et de concevoir le programme d'investissement optimal.

Afin de rendre possible cette approche innovante, les auditeurs et contrôleurs internes de l'IFACI ont très bien identifié les objectifs à relever. Ce travail effectué avec eux, en particulier autour de plusieurs questions clés [4], reflète ce que j'observe au quotidien sur le marché. À cet effet, et de manière à bien identifier et évaluer les risques cyber, on peut proposer aux organisations le « GPS » décrit ci-dessus, qui se résume via l'acronyme CHAIN :

- Contextualiser la menace et son évolution (facteurs techniques, géopolitiques, économiques, ...);
- Harmoniser son évaluation afin de pouvoir établir des priorités ;
- Anticiper la fréquence et les impacts opérationnels de chaque scénario de risque ;
- Investir dans le meilleur «mix» défensif pour réduire ou transférer son exposition au risque ;
- Notifier les instances stratégiques dans un langage adapté, notamment en leur présentant le ROI de leurs investissements.

C'est en combinant tous ces éléments que les couches tactiques et stratégiques peuvent être décloisonnées de manière objective et transparente, en cohérence avec la menace.

4 En particulier les questions suivantes, traitées dans ce document : Evolution du risque cyber ; Impacts opérationnels concrets du risque cyber ; Sensibiliser le top management ; Mesurer la maturité et l'exposition au risque

CYBER : LES QUESTIONS CLÉS POUR LES CONSEILS D'ADMINISTRATION

Vincent Maret
Partner KPMG France
Cybersecurity and Privacy

*Quelles sont les questions clés que doivent se poser les conseils d'administration – et donc que doivent examiner les auditeurs ? Vincent Maret en fait le tour ici, en mettant en avant des points importants tels que, entre autre, la question de l'évaluation de l'organisation – développé dans « **Mesurer la maturité de l'organisation** » ; reprendre les bases de gestions de la donnée, comme rappelé dans « **Connaitre les fondamentaux techniques/contrôles de base nécessaire** » ; ou encore se mesurer de manière dynamique, y compris par rapport à ses compétiteurs – un point qui complémente « **Se tenir informé de l'évolution du risque cyber** ».*

Les conseils d'administration et les comités d'audit ont pleinement pris conscience que des cyberattaques pouvaient avoir des impacts majeurs pour les entreprises, et au-delà pour l'écosystème et la société. Cette prise de conscience a été nourrie par des multiples exemples d'incidents ayant frappé des entreprises, et par des analyses telles que celles du rapport du Forum de Davos qui classe les risques cyber parmi les plus impactants et les plus probables.

En outre, de multiples parties prenantes (clients B2B, B2C, partenaires, citoyens, régulateurs, etc) ont aujourd'hui des attentes élevées, ce qui rajoute à la pression .

Les conseils d'administration et les comités d'audit se saisissent donc du sujet, et posent des questions aux directions générales. Par exemple :

- Qui dans notre entreprise est en charge de la cybersécurité ? comment sommes-nous organisés ? le sujet est-il traité au bon niveau ? les interactions avec les métiers sont-elles suffisantes ?
- Quels sont nos actifs informationnels critiques ? quels sont les scénarios de risques associés ? avec quels impacts et quelles probabilités ?
- Comprenons-nous nos points de vulnérabilité ? quels processus sont en place pour améliorer notre résilience face aux cyber-menaces ?

- Avons-nous identifié les lois et règlements qui nous concernent en matière de cybersécurité et de protection des données personnelles ?
- Est-ce que nous prenons suffisamment en compte la cybersécurité et la protection des données personnelles dans nos projets de transformation ? le développement de nos nouveaux produits et services ?
- Les collaborateurs de l'entreprise, à tous les niveaux, sont-ils conscients des risques cyber ? sont-ils formés et mobilisés pour contrer les risques cyber ?
- Sommes-nous en mesure de détecter les cyber incidents ? de réagir efficacement en cas d'attaque ? quel est notre degré de résilience face aux attaques cyber ?
- Est-ce que l'un de nos partenaires ou fournisseurs peut nous mettre en danger ?
- Comment pouvons-nous évaluer l'efficacité de nos investissements en matière de cybersécurité ?
- Nos pairs sont-ils en avance sur nous ? Si oui, cela leur donne-t-il un avantage business ?

En conséquence, les directions d'audit interne sont de plus en plus sollicitées pour aider à répondre à ces questions, et elles considèrent que la cybersécurité est aujourd'hui le premier sujet sur leur agenda (cf. étude Etude « Risk in Focus 2019 » de l'ECIIA).

Il est donc important que les auditeurs internes disposent de guides et de référentiels pour auditer efficacement les différentes dimensions liées à la cybersécurité au sein de l'entreprise.

LE CYBER-RISQUE : LES ASPECTS HUMAINS ET ORGANISATIONNELS SONT FONDAMENTAUX

Thierry Delville

Associé chez Pwc France, ancien Délégué ministériel aux industries de sécurité et à la lutte contre les cyber-menaces

*Le risque de cybersécurité nait de facteurs humains, porté par la malveillance - ou la maladresse des collaborateurs, rappelle Thierry Delville. La réponse nécessite donc un effort sur la culture et les comportements, méritant différents moyens – un point important approfondi dans « **Sensibiliser les collaborateurs** », y compris dans les exercices de crise, également abordés dans « **Développer et évaluer une capacité de gestion de crise** ». Enfin, il faut prendre en considération les partenaires externes de l'entreprise, fournisseurs de produits ou de services logiciels – peut-être en s'inspirant des approches justement développées pour « **Prendre en compte le risque cyber dans les projets informatiques** ».*

La cybersécurité est-elle un sujet principalement technique ? A l'évidence la réponse est non. Les travaux menés par l'IFACI mettent en évidence l'importance qu'il faut accorder à la sensibilisation des collaborateurs et à des règles qui n'ont pas vraiment changé au fil des dernières décennies (ce retour aux fondamentaux chers aux praticiens du rugby).

La menace vient surtout de l'intérieur. Bien entendu, il existe une part de malveillance mais l'inattention et la maladresse sont la cause de bien des incidents qui prennent ensuite une ampleur considérable.

La culture d'entreprise face au risque cyber est souvent à l'image de la culture globale face aux autres risques de sécurité qu'ils soient physiques ou logiques. C'est bien par un travail en profondeur qui part du rappel des règles essentielles d'hygiène en cybersécurité (dont l'ANSSI a d'ailleurs très justement établi les principes sur son site en 42 mesures) que l'on peut atteindre un résultat tangible.

La sensibilisation du personnel par différents moyens (formation, jeux, campagnes thématiques, exercices de crise…) constitue un des premiers points à adresser suivi d'un autre qui concerne les dirigeants lesquels doivent, s'ils ne le sont pas encore, se sentir pleinement concernés par ce sujet. Une grande majorité de dirigeants ne savent pas comment sont organisées et surtout localisées leurs data.

Au-delà de la réponse technologique, qu'il faut inscrire dans une stratégie et un plan d'investissement en ligne avec les enjeux de protection de l'entreprise, la protection de l'information doit faire l'objet d'une véritable réflexion en profondeur. Quelles sont mes informations sensibles ? quelles sont celles sans lesquelles je ne fonctionne plus du tout ? celles dont la divulgation remet en cause toute la stratégie et le développement ? qui accède à quoi et pourquoi ?… c'est par une approche méthodologique mais d'abord par des réflexions simples que l'on arrive à mettre en place une démarche qui portera ses fruits dans la durée.

Protéger ses informations repose globalement sur la confiance que l'on place dans son système, ses collaborateurs, les partenaires ou encore les tierce-parties… c'est aussi une réflexion à avoir dans et hors l'entreprise. Le sujet de la protection des agents en mobilité mérite une attention toute particulière pour qui souhaite exporter.

Enfin la confiance en ses prestataires doit se mériter et s'éprouver… régulièrement … on voit bien souvent un décalage important entre l'image que l'on se fait d'une solution acquise ou d'un service (dès l'instant où le seul critère de choix n'a pas été le prix auquel cas on en a souvent pour « son argent ») et la mesure à postériori entre la performance souhaitée et la réalité observée.

Ce guide très bien fait et dont il faut saluer la sortie, tant sont importantes les initiatives qui concourent à l'élévation générale du niveau de maturité des entreprises, rappelle une règle qu'il faut toujours avoir à l'esprit : « la solidité d'une chaîne dépend du maillon le plus faible ». C'est bien dans une démarche globale de sécurisation des entreprises qu'il faut s'inscrire durablement.

PARTIE II SYNTHÈSE SUR NEUF QUESTIONS CLÉS

CONNAITRE LES FONDAMENTAUX TECHNIQUES/CONTRÔLES DE BASE NÉCESSAIRE À MINIMA POUR LES ÉQUIPES AUDIT ET DE CONTRÔLE INTERNE

Olivier Meyer, Vétéa Lucas & Olivier Sznitkies

Introduction & Enjeux

Afin d'aider les organisations à renforcer leur maitrise des risques liés à la cybersécurité, de nombreuses initiatives publiques, associatives ou privées ont publié différents référentiels de bonnes pratiques en matière de cybersécurité. Ces référentiels (par exemple COBIT, ISO27k, PCI DSS, FDA, LPM/PASSI, ENISA) sont d'une très grande qualité mais requièrent souvent une maîtrise technique n'en facilitant pas l'approche aux non-spécialistes.

Plus récemment, de nouvelles initiatives (par exemple CIS20, Guide d'Hygiène d'Informatique de l'ANSSI) ont choisi d'avoir une **visée plus didactique** en se focalisant sur un nombre de **contrôles incontournables** considérés comme prioritaires.

L'objectif de cette fiche est de **mieux faire connaitre aux auditeurs et contrôleurs internes ces référentiels de contrôle de base** et les aider à mieux cerner les fondamentaux techniques sous-jacents pour leur permettre de contribuer en tant que seconde et troisième lignes de maîtrise à une meilleure gestion des risques liés à la cybersécurité dans leurs organisations.

[...] Il apparaît nécessaire que les auditeurs généralistes aient une bonne compréhension des objectifs et enjeux des règles et contrôles de base décrits dans le CIS20 et le Guide d'Hygiène Informatique de l'ANSSI[...]

Grands principes

Aperçu du Guide d'Hygiène Informatique de l'ANSSI

Le guide de l'ANSSI propose 42 « règles de sécurité simple » couvrant les domaines suivants :

- Sensibilisation et formation,
- Connaissance du système d'information,
- Authentification et contrôle des accès,
- Sécurisation des postes de travail,
- Sécurisation des réseaux,
- Sécurisation de l'administration du système d'information,
- Gestion du nomadisme,
- Maintien à jour du système d'information,
- Supervision, audit et réaction.

Pour chacune des règles, l'ANSSI propose un système de maturité (« Standard / Renforcé ») permettant d'identifier, pour chaque organisation, ses priorités d'action.

Aperçu du CIS20

Le CIS20 propose 20 domaines de contrôles permettant aux organisations d'évaluer et améliorer leur niveau de maitrise du risque cyber.

Le CIS20 propose, en outre, une appréciation du niveau de priorisation des contrôles au vu de la taille et de la sensibilité de l'entité à protéger reconnaissant qu'une PME d'une dizaine de personnes ne peut pas mettre en œuvre les mêmes moyens de protection qu'une multinationale de plus de 50 000 personnes.

Bonnes pratiques

Le tableau ci-après présente une vue synthétique des principaux domaines de contrôle à mettre en œuvre selon le CIS20 avec une évaluation de la technicité requise selon une échelle à trois niveaux :

- **Initiale : un auditeur avec une culture générale informatique** pourra adresser les objectifs de base du domaine en s'appuyant sur les ressources informatiques de l'organisation,
- **Intermédiaire : un auditeur avec une spécialité informatique** pourra couvrir les points clés de ces domaines,
- **Avancée : seul un spécialiste de la cybersécurité** sera à même de vérifier l'existence d'un niveau de contrôle adéquat sur ce domaine.

DOMAINE	OBJECTIF DU CONTRÔLE	TECHNICITÉ REQUISE POUR L'AUDITEUR
Inventaire et contrôle des équipements matériels	*S'assurer que seuls les équipements autorisés peuvent accéder au réseau de l'entreprise et que les équipements non autorisés sont identifiés et bloqués*	Initiale
Inventaire et contrôle des systèmes logiciels	*S'assurer que seules les applications autorisées puissent être exécutées, et que les applications non autorisées soient identifiées et/ou que leur installation soit bloquée*	Intermédiaire
Gestion des vulnérabilités	*S'assurer de la mise à jour continue de l'identification, l'évaluation et la réduction des vulnérabilités pour minimiser les opportunités d'attaques*	Intermédiaire
Contrôle des accès aux comptes « à privilèges » étendus	*S'assurer de la bonne utilisation, allocation et configuration des accès administrateurs sur les équipements informatiques et les applications*	Intermédiaire
Sécurisation des configurations matérielles et logicielles	*S'assurer d'une bonne gestion de la configuration de la sécurité des équipements et d'un bon processus de gestion des changements afin de prévenir l'exploitation de toute vulnérabilité*	Intermédiaire
Mise en œuvre, surveillance et analyse des journaux d'activité	*S'assurer de la collecte, la gestion et l'analyse des journaux d'activité afin de détecter, comprendre ou rétablir les systèmes en cas d'attaque*	Intermédiaire
Protection des messageries et des navigateurs web	*S'assurer du bon niveau de protection de l'entreprise en réduisant les opportunités d'attaque des utilisateurs au travers des navigateurs internet ou des systèmes email*	Intermédiaire
Défense antivirus/antimalware	*S'assurer de l'utilisation optimale d'outils automatisés pour la mise à jour, l'identification et la correction des codes malveillants pour prévenir l'installation, la propagation et l'exécution de*	Initiale
Contrôle du réseau via la limitation des ports, protocoles, et services	*S'assurer d'une bonne gestion (identification, contrôle et correction) de l'utilisation opérationnelle des ports, protocoles et services réseaux pour minimiser les opportunités*	Avancée
Capacité de reprise de données	*S'assurer de la capacité à restaurer dans un délai raisonnable les informations et processus critiques de l'organisation*	Initiale
Sécurisation des configurations réseaux	*S'assurer de la bonne configuration et de la bonne gestion des changements de l'infrastructure réseau de l'organisation*	Avancée
Défense périmétrique	*S'assurer de la détection, prévention et correction de tout flux d'information entre différentes zones du réseau qui pourrait avoir un impact sur la sécurité*	Avancée
Protection des données	*S'assurer que des processus et des outils sont en place pour prévenir l'exfiltration massive de données et pour assurer la confidentialité et l'intégrité des données sensibles*	Intermédiaire
Accès contrôlés sur la base du « besoin d'en connaître »	*S'assurer que les accès aux ressources et informations sensibles sont limités aux personnes ou systèmes qui en ont l'autorisation*	Intermédiaire
Contrôle des accès « sans fil »	*S'assurer que les réseaux sans fil soient sécurisés de manière appropriée via l'utilisation de processus et d'outils pour contrôler les points d'accès*	Intermédiaire
Surveillance et contrôle des comptes	*S'assurer d'une bonne gestion du cycle de vie des comptes utilisateurs sur les systèmes et applications, de leur création à leur suppression*	Intermédiaire
Implémentation d'un programme de formation/sensibilisation	*S'assurer de l'identification des compétences nécessaires pour garantir la protection de l'entreprise et développer des plans pour définir et implémenter des formations en*	Initiale
Sécurité des applications	*S'assurer de la gestion de la sécurité au travers du cycle de vie des applications pour prévenir, détecter et corriger les failles de sécurité*	Intermédiaire
Gestion et réponse aux incidents	*S'assurer de l'existence de processus de réponse aux incidents pour gérer, contenir et éradiquer les cyber-attaques*	Initiale
Test de pénétration et simulation d'attaque	*S'assurer de la solidité des défenses via la simulation d'attaques informatiques*	Avancée

Conclusions/Recommandations/Plan d'action

Un auditeur généraliste ne sera souvent pas capable d'auditer efficacement l'ensemble de ces contrôles de bout en bout et **devrait recourir à des spécialistes de l'audit IT ou de la cybersécurité en fonction du niveau d'assurance requis**. Néanmoins, compte tenu du niveau de risque lié à la cybersécurité, il apparaît **nécessaire que les auditeurs généralistes aient une bonne compréhension des objectifs et enjeux** des règles et contrôles de base décrits dans le CIS20 et le Guide d'Hygiène Informatique de l'ANSSI. Les Directions de l'Audit Interne pourront utilement s'assurer que leurs équipes sont correctement formées sur ces sujets.

Note : des éléments complémentaires sont disponibles sur le dossier Workplace, à l'adresse : https://bit.ly/30vvghf

COMMENT SENSIBILISER LE TOP MANAGEMENT ET AVEC QUEL TABLEAU DE BORD

Gustavo Bohlen, Gilles Brunet & Marie-Hélène Laimay

Introduction & Enjeux

Enjeux généraux

- Assurer le « tone at/from the top » de l'entreprise en matière de sécurité et la mobilisation des ressources humaines, financières et techniques pour obtenir et mettre en place des mesures adaptées (de sensibilisation, d'investissements et coûts).
- Promouvoir la visibilité sur les points essentiels et maintenir la mobilisation sur les sujets de cybersécurité.

Menaces

- Pour faire face à l'hétérogénéité des organisations et aux menaces évolutives et multiformes, les pratiques de sensibilisation doivent **s'adapter à la culture de l'entreprise**, à l'activité/environnement de l'entreprise et au degré d'exposition cyber.
- En l'absence d'implication du top management et de choix budgétaire clair et continu pour gérer les risques de cybersécurité, la **capacité de résilience voire la survie de l'entreprise est en question**.
- L'incapacité du top management à expliquer sa politique de cybersécurité au Conseil, aux actionnaires, aux acteurs financiers peut entrainer une **perte de crédibilité et une fragilisation financière** de l'entreprise (chute du cours de bourse, de l'activité).

En cas de [...] langage trop technique, l'audit interne devra traduire en langage Business, opérationnel et financier les incidents identifiés pour que le Top management puisse comprendre et agir en connaissance de cause.

Grands principes

- Ce n'est plus une histoire de techniciens, mais un enjeu qui a des impacts concrets pour l'entreprise. Par exemple, la chaine de production de l'entreprise pourrait se voir à l'arrêt suite à une attaque, **les coûts du risque deviennent quantifiables**.
- Les actions de sensibilisation sont assurées par la 1ère ligne de défense (opérationnels) et la 2ème ligne (CI, RSSI, RM, ...) et complétées par le reporting de la troisième ligne (Audit Interne) sur le niveau de risque (alerte, coopération entre 1ère, 2ère et 3ère ligne)
- En cas de manque de maturité dans la communication des 1ère et 2ème lignes, de langage trop technique, l'audit interne devra **traduire en langage Business, opérationnel et financier** les incidents identifiés pour que le Top management puisse comprendre et agir en connaissance de cause.
- Le niveau d'abstraction est souvent très élevé, et les managers ne sont pas formés à ces éléments. Articuler et diminuer la distance entre l'élément technique, précis et lointain et l'impact de l'intrusion, qui cause de vrais dégâts
- **Éviter le cercle vicieux** : Manque de moyens (humains, outils) et de compétence (expertise) qui est un premier risque, mais aussi la « root cause » de l'absence d'identification des risques cybersécurité dans la cartographie globale des risques de l'organisation ce qui entraine un manque de moyens et compétences dédiés.
- L'Audit Interne peut être confronté au déni et à la réticence du Top management. Il devra directement sensibiliser le Top Management et les organes de gouvernance à travers des **exemples concrets et des alertes**.

Bonnes pratiques

L'audit interne dans son rôle de troisième ligne de défense effectue à la fois la revue des politiques menées par la première et la deuxième ligne de défense ; et assure également une fonction de conseil auprès du management notamment dans le cadre d'un effort de sensibilisation directe, souvent incarné par l'échange entre l'auditeur et la direction générale et divers membres du comité d'administration ou du comité d'audit. Ces deux dimensions sont détaillées ci-contre dans le cadre de l'effort de sensibilisation.

1. S'assurer que les actions de sensibilisation sont soutenues de manière continue par les premières et deuxièmes lignes de défense.

   a) Par la présence d'une fonction Directeur sécurité ou RSSI dans l'entreprise et de comités sécurité. Ce RSSI doit idéalement communiquer les points suivants :
      - L'évolution des menaces plus que sur le nombre d'attaques/incidents ;
      - Les conséquences potentielles identifiées sur le Business et les atteintes à la stratégie (y compris l'impact financier) ;
      - Prendre en compte les informations / évaluations externes :
        - Agences de notation Cybersécurité et Financières
        - ANSSI
        - Incidents graves survenus dans d'autres entreprises

   b) En impliquant le Management des risques, au travers de ses outils spécifiques :
      - Matrice de risque : contenant l'évaluation du risque cyber **dans la cartographie globale des risques**, combinée avec une cartographie détaillée des risques cybersécurité.
      - Comité des risques : présentation de la synthèse des risques et des plans d'action.

   c) Par le renforcement du rôle du Contrôle Interne dans le dispositif de contrôle cybersécurité :
      - Par la réalisation de rapports de contrôle interne domaine IT et cybersécurité.
      - Par l'évaluation du niveau de maturité SMS (Système Management de la Sécurité) par entités de l'organisation / vs évaluation des risques.
      - Par la réalisation de revues régulières du dispositif de Contrôle Interne sécurité (auto-évaluation).

2. L'Audit Interne sensibilise directement le top management et organes de gouvernance
   - En insistant sur la **responsabilité du Top Management** et en présentant les impacts financiers et d'image.
   - En communiquant des rapports de missions d'audit cybersécurité réalisés dans cadre du

plan annuel.

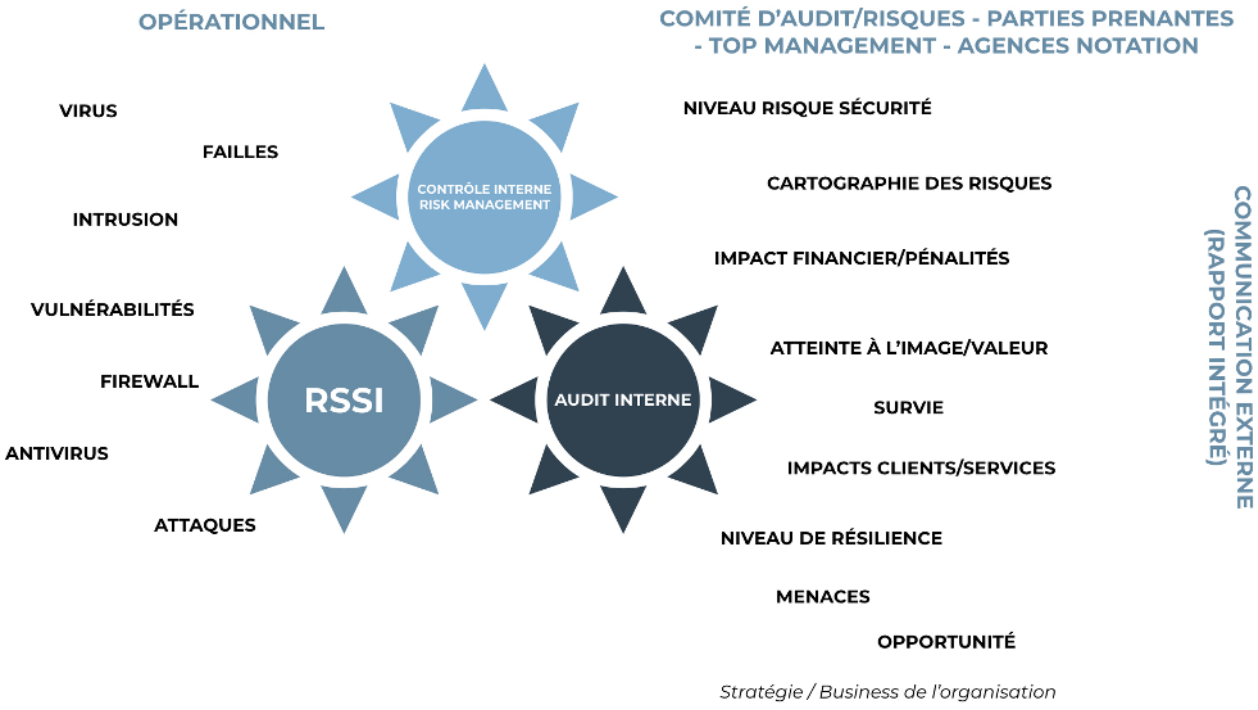
- En démontrant l'impact de l'exploitation de failles et vulnérabilités (test audits, si possible en temps réel).
- En réalisant une synthèse des points de faiblesses observées à une **fréquence annuelle ou tous les six mois (ISO27002)**
- En présentant régulièrement (**au moins 2 fois par an**) ou exceptionnellement en Comité d'Audit des résultats des missions cybersécurité.
- En communiquant directement avec le top management, y compris par voie d'alertes si nécessaire.

3. Utiliser un Tableau de Bord avec des KPI adaptés

   Point d'attention : limiter / adapter le nombre d'indicateurs pour avoir le plus d'impact possible

   - Niveau risque cyber (évalué aux bornes de l'organisation)
   - Dépenses sécurité : (Capex/Opex) IT security / (Capex+ Opex) IT cible Gartner 6,2% (quand la maturité est présente)
   - Taux de sensibilisation du personnel à la Cybersecurité
   - Taux d'équipement en moyens bureautiques sécurisés (Chiffrement postes de travail, PKI, …)
   - Taux d'avancement du plan de renforcement de la sécurité (organisationnel et technique) y compris sur les volets contractuels et juridiques (entreprise étendue)
   - Nombres attaques/incidents détectés : **nb pers impliquées, durée, impact, coûts**
   - Détails de la mise en œuvre et l'évolution des plans d'amélioration.
   - Points critiques et mesures entreprises/à entreprendre.
   - Niveau contractuel – Exigence d'audit et conformité pour les sous-traitants. Le numérique est une chaine de confiance, l'incident arrive par le maillon faible.

2ème et 3ème ligne comme traducteurs d'éléments techniques en langage compréhensible par le Top management



Note : des éléments complémentaires sont disponibles sur le dossier Workplace, à l'adresse : https://bit.ly/30vvghf

IDENTIFIER LES IMPACTS OPÉRATIONNELS CONCRETS DU RISQUE CYBER

Xavier Guiffard & Mathias Lorilleux

Introduction et Enjeux

L'identification d'impacts opérationnels concrets permet tout d'abord d'établir une meilleure gestion du risque car elle permet de classifier les risques et donc de prioriser les actions, les contrôles clés et les dispositifs de défense à mettre en œuvre pour s'en prémunir. Cette démarche permet d'établir une vision transverse de la menace dans l'entreprise. Elle est clé en l'absence d'évaluation précise et fiable de la réalité externe de la menace dont la visibilité reste très réduite et/ou partielle. Elle constitue donc l'un des fondements de la capacité de résilience de l'organisation face à un risque quasi-systémique, pouvant aller des rançongiciels à propagation mondiale [5]; au vol de données [6]; ou encore au détournement d'actifs financiers, comme par exemple dans le cas du cyber-braquage de la Banque Centrale du Bangladesh en 2016 pour 63 millions de $. Les impacts indirects peuvent être très lourds, incluant le risque réputationnel ou encore l'impact sur la valeur de marché : Dans 40% des incidents majeurs, les dommages feront chuter le cours des actions de 20% en moyenne après 12 mois [7].

Enfin, c'est l'analyse des impacts opérationnels concrets qui permet la bonne appréhension de la menace cyber par le métier et/ou par les instances dirigeantes afin notamment de lutter contre le manque de culture et la perception inadéquate des risques Cyber, eux-mêmes facteurs de vulnérabilité.

Il s'agit de déterminer des impacts potentiels théoriques en fonction des conséquences sur la vie de la société (survie menacée, fonctionnement très dégradé, fonctionnement dégradé, impact sur les marges).

5 Voir par exemple les rançongiciels WannaCry et NotPetya en 2017, ou LockerGoga en 2019
6 Voir par exemple les fuites de données dont ont été victimes Yahoo ou Target en 2013, Sony Pictures Entertainment en 2014, Equifax en 2017, ou encore Marriott/Starwood en 2018
7 Source PwC France 2019

Grands principes

L'évaluation des impacts concrets du risque cyber doit être fondée sur la cartographie des processus et des ressources clés de l'entreprise. Il s'agit d'identifier les éléments clés nécessaires à l'accomplissement de la mission de l'entreprise et les différents types d'impact possibles :

- Disponibilité (outil de production, service…),
- Confidentialité (informations…),
- Intégrité (information, produit, service…),
- Traçabilité (chaine de production, information, demande…),
- Direct (activité immédiate de l'entreprise)
- …ou Indirect (réputation, valeur de marché…).

La classification des effets pour l'entreprise en cas de perte, altération, indisponibilité de ces processus ou ressources est **indépendante du niveau ou du type de menace éventuelle**. Il s'agit de déterminer des impacts potentiels théoriques en fonction des conséquences sur la vie de la société (survie menacée, fonctionnement très dégradé, fonctionnement dégradé, impact sur les marges).

- Il est nécessaire de considérer l'écosystème dans l'élaboration des scenarii de risque en intégrant les parties prenantes externes (clients, fournisseurs, partenaires, administrations). Le rôle de l'organisation dans la supply chain doit être clairement identifié, tout comme sa place éventuelle dans les «infrastructures essentielles».
- Il faut évaluer la vraisemblance du risque et ne pas chercher à établir sa fréquence car, en matière de probabilité d'occurrence du risque cyber, il est difficile de se fonder sur des données exogènes (absence de données fiables et exhaustives qui permettraient de quantifier une menace, les données statistiques à posteriori ont des périmètres d'analyse spécifiques et/ou hétérogènes…).

Bonnes Pratiques

1. Évaluer le champ des possibles sur la base d'une analyse métier :
   - La détermination des impacts concrets du risque cyber doit commencer, comme pour tous les autres risques exogènes (naturels par exemple), par une analyse des **processus et ressources critiques pour l'entreprise** :
     - Chaine de production
     - Secrets industriels
     - Base de données clients
     - Expertise…
   - Une classification des effets pour l'entreprise en cas de perte, altération, indisponibilité de ces processus ou ressources :

ÉCHELLE	CONSÉQUENCES
CRITIQUE	SURVIE MENACE
GRAVE	FONCTIONNEMENT EN MODE TRÈS DÉGRADÉ
SIGNIFICATIVE	FONCTIONNEMENT EN MODE DÉGRADÉ
MINEURE	IMPACT SUR LES MARGES

2. Prévoir des situations et évaluer des scenarii au croisement de la gravité pour l'entreprise, de la conformité des processus / ressources concernées et des typologies de menaces.
   Il faut considérer que **tout peut arriver** et envisager les situations les plus critiques au regard :
   - Du niveau de conformité des processus et/ou ressources concernées pour la gestion du risque cyber, notamment à travers les référentiels existants :
     - Normes (ISO 27000…)
     - Bonnes pratiques (PSSI, recommandations de l'ANSSI…)
     - Règlementation (RGPD, LPM, Directive NIS…)

- D'une macroanalyse des menaces potentielles selon les **types d'attaquants potentiels** et leurs motivations éventuelles :
  - Individu isolé (interne notamment) qui veut se « venger » de l'entreprise ou qui cherche simplement à s'amuser
  - Hacktiviste avec une démarche politique
  - Cyber-terroriste qui veut atteindre un système et ou attenter à la sécurité des personnes
  - Concurrent qui souhaite porter atteinte à la performance de l'entreprise ou voler des données sensibles
  - Cybercriminels qui recherchent le profit financier
  - Entité étatique qui vise à prendre le contrôle ou à perturber le fonctionnement d'organismes vitaux

3. Évaluer la vraisemblance du risque liée à un scenario en **établissant des scenarios opérationnels** qui reflète le degré de faisabilité ou de possibilité que l'une des actions de l'attaquant aboutisse à l'objectif visé.

4. Combiner la vraisemblance du risque à la gravité des impacts pour estimer le niveau de risque et en déduire la stratégie de traitement adéquate.

Note : des éléments complémentaires sont disponibles sur le dossier Workplace, à l'adresse : https://bit.ly/30vvghf

MESURER LA MATURITÉ DE L'ORGANISATION ET SON NIVEAU D'EXPOSITION AU RISQUE CYBER

Jean-Paul Parisot, Tatiana Postil & Frederic Vilanova

Introduction & Enjeux : pourquoi l'évaluation de la maturité [8]

- **Favoriser une prise de conscience collective et active** en cybersécurité.
- Mieux identifier, comprendre et évaluer les travaux et contrôles effectués par le Contrôle Interne, le RSSI, le DSI, l'Architecte Réseaux et Systèmes.
- Diffuser les bonnes pratiques en cybersécurité, les mieux adaptées à la maturité de l'organisation.

Il faut « utiliser un outil d'évaluation de la maturité de l'organisation en cybersécurité qui soit de préférence simple, synthétique et pratique ».

Grands principes

Principes fondateurs

- **Évaluer la gouvernance et la pratique de la SSI** en termes de conception des procédures/ contrôles et d'effectivité de leur mise en œuvre.
- **Utiliser un ou plusieurs référentiels adaptés en matière de maîtrise des risques de cybersécurité** pour déterminer son niveau de risque (voir détails dans « bonnes pratiques »).
- Utiliser un outil d'évaluation de la maturité de l'organisation en cybersécurité qui soit de préférence simple, synthétique et pratique .

Facteurs de risques

- **Absence de politique formalisée de Sécurité des Systèmes d'Information** (SSI)
- **Absence de mise en œuvre effective des procédures prévues en interne et externe à l'organisation** (sous-traitants, travail à distance...)

8 On notera que cette évaluation de la maturité s'opère dans un cadre plus général, comprenant la nécessité pour l'auditeur d'être au rendez-vous du risque cyber pour un risque perçu comme important par les entreprises

- **Absence de fonction de Responsable SSI** (RSSI interne ou externalisée) ou difficultés d'appréciation sur la maturité de la SSI de l'organisation (en voie vers des certifications ISO 27001 / 27002 / 27701 ? etc...)
- **Insuffisante perception des cyber-risques par le COMEX**
- **Hétérogénéité des organisations** (nature de l'activité économique, degré d'exposition aux menaces, risques géopolitiques, etc...) rendant difficile la comparaison des niveaux de maturité

Bonnes Pratiques

Quelles bonnes pratiques adopter ? On peut évoquer trois approches fondamentales pour examiner la maturité de l'organisation.

1. Prise en compte des risques numériques dans les enjeux métiers

Critères

- Inscription des risques numériques (technologiques et cyber) dans la gestion globale des risques de l'entreprise.
- Mise en place d'une politique et d'une organisation de gestion des risques, couvrant les processus critiques de l'entreprise.

Facteurs de risque

- Manque de capacité de l'entreprise à faire face aux risques cyber sur les applications majeures, les infrastructures clés et les données critiques.
- Désintérêt ou manque de partage dans le domaine des risques numériques.
- Défaut de soutien ferme et clair du Conseil d'Administration et de la Direction Générale.

2. Utilisation d'un ou plusieurs référentiels adaptés en matière de maîtrise des risques

Critères

- Utilisation des contrôles proposés en CIS Critical Security Controls for Effective Cyber Defense (Center of Internet Security), complémenté du Guide d'Hygiène Informatique de l'ANSSI [9]
- Utilisation d'EBIOS RM (ANSSI) pour appréhender les risques cybersécurité.
- Communication en Direction en fonction des objectifs de ces référentiels pour montrer la progression en couverture des risques et en maturité de traitement.

9 D'autres référentiels sont possibles : ISO 27001 pour définir un Système de Management de la Sécurité de l'Information (SMSI) ; COBIT 2019 pour appréhender la Direction des Systèmes d'Information (vision générale: Govern, Plan, Build, Run, Control) ; COSO ERM

Facteurs de risque

- Absence de référentiel pertinent en maitrise du SI et de la cybersécurité
- Absence de contrôles type CIS
- Dettes méthodologiques ou techniques lourdes empêchant de mettre à jour les systèmes rapidement (investissements insuffisants en interne ou chez les prestataires sous-traitants)

3. Disposer d'un outillage adapté

Un **premier outil (formalisé sur Excel)**, est proposé à titre d'exemple d'instrument **facile à mettre en œuvre pour évaluer de façon préalable la maturité de l'organisation en matière de risques cybersécurité**

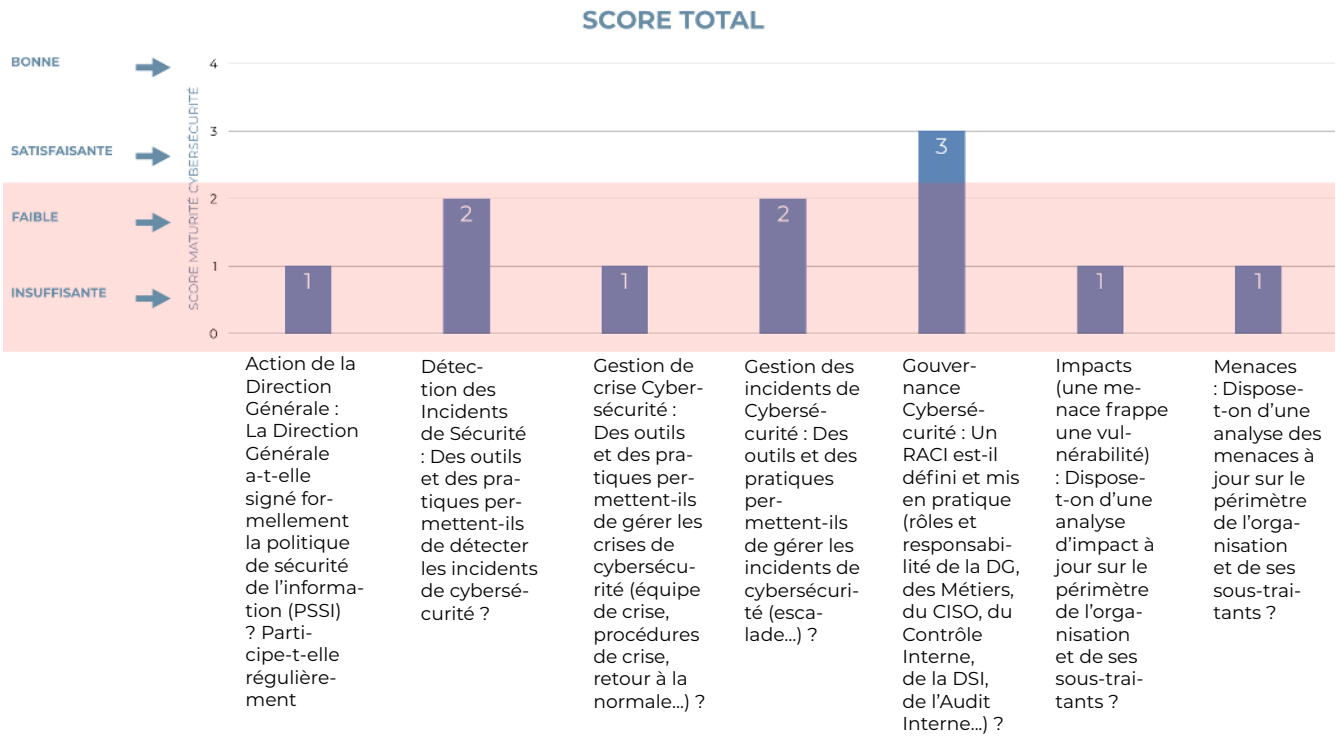
- voir détails sur **dossier workplace** à l'adresse : **https://bit.ly/30vvghf** et exemple sur la page suivante. Il peut être structuré autour des 10 questions suivantes :

INTITULÉ	DÉTAIL
Q1 - Vulnérabilités (surface d'exposition)	Dispose-t-on d'une analyse des vulnérabilités à jour sur le périmètre de l'organisation et de ses sous-traitants ?
Q2 - Menaces	Dispose-t-on d'une analyse des menaces à jour sur le périmètre de l'organisation et de ses sous-traitants ?
Q3 - Impacts (une menace frappe une vulnérabilité)	Dispose-t-on d'une analyse d'impact à jour sur le périmètre de l'organisation et de ses sous-traitants ?
Q4 - Design des procédures	Les procédures relatives à la cybersécurité sont-elles définies (rédaction de la procédure, KPI, etc.) ?
Q5 - Effectivité des procédures	Les procédures relatives à la cybersécurité sont-elles mises en oeuvre régulièrement (quotidiennement, hebdomadairement, KPI alimentés...) ?
Q6 - Gouvernance Cybersécurité	UN RACI est-il défini et mis en pratique (rôles et responsabilité de la DG, des Métiers, du CISO, du Contrôle Interne, de la DSI, de l'Audit Interne...) ? *[Note Matrice RACI - R(Responsible), A(Accountable/Supervision), C(Consulted), I(Informed)]*
Q7 - Détection des Incidents de Sécurité	Des outils et des pratiques permettent-ils de détecter les incidents de cybersécurité ?
Q8 - Gestion des incidents de Cybersécurité	Des outils et des pratiques permettent-ils de gérer les incidents de cybersécurité (escalade...) ?
Q9 - Gestion de crise Cybersécurité	Des outils et des pratiques permettent-ils de gérer les crises de cybersécurité (équipe de crise, procédures de crise, retour à la normale...) ?
Q10 - Action de la Direction Générale	La Direction Générale a-t-elle signé formellement la politique de sécurité de l'information (PSSI) ? Participe-t-elle régulièrement aux points de gouvernance Cybersécurité ?

Chaque question reçoit une réponse sur une échelle de 1 à 4 (plutôt que 1 à 5, qui risque une accumulation de notes sur la position médiane, « 3 », et évite de prendre position).

NIVEAUX	SCORE	MATURITÉ GLOBALE
INITIALISÉ	1	MATURITÉ GLOBALE TROP FAIBLE
FORMALISÉ	2	MATURITÉ GLOBALE ASSEZ FAIBLE
MANAGÉ	3	MATURITÉ GLOBALE SATISFAISANTE
OPTIMISÉ	4	MATURITÉ GLOBALE TRÈS SATISFAISANTE

Les scores peuvent par la suite être pondérés selon le type d'entreprise (PMI/PME ou ETI/GE). Il en résulte un score global entre 1 et 4 qui permet d'avoir une première appréciation générale du niveau de maturité de l'entreprise. Une représentation graphique permet de ventiler les notes de maturité sur la plupart des questions et donc de mieux identifier les zones prioritaires d'amélioration. (voir exemple ci-contre).



Cet outil quoique sommaire permet néanmoins rapidement de communiquer avec les Métiers, la DSI, le RSSI et la Direction Générale en matière de maturité de l'organisation au regard des cyber-risques. À l'utilisateur d'affiner les questions et les pondérations pour l'adapter au contexte de son organisation.

Exemple – analyse de la maturité d'une Entreprise

QUESTIONS	POIDS POUR VOTRE ORGANISATION	QUESTIONS	ÉVALUATION POUR VOTRE ORGANISATION	SCORE BRUT	SCORE PONDÉRÉ	Poids conseillés ETI/GE	Poids conseillés PMI/PME
Q1	2	**Vulnérabilité (surface d'exposition)** Dispose-t-on d'une analyse des vulnérabilités à jour sur le périmètre de l'organisation et de ses sous-traitants ?	Formalisé	2	4	2	1
Q2	2	**Menaces :** Dispose-t-on d'une analyse des menaces à jour sur le périmètre de l'organisation et de ses sous-traitants ?	Initialisé	1	2	2	1
Q3	1	**Impacts (une menace frappe une vulnérabilité) :** Dispose-t-on d'une analyse d'impact à jour sur le périmètre de l'organisation et de ses sous-traitants ?	Initialisé	1	1	1	1
Q4	1	**Design des procédures** Les procédures relatives à la cybersécurité sont-elles définies (rédaction de la procédure, KPI, etc...) ?	Initialisé	1	1	1	1
Q5	2	**Effectivité des procédures** Les procédures relatives à la cybersécurité sont-elles mises en oeuvre régulièrement (quotidiennement, hebdomadairement, KPI alimentés...) ?	Initialisé	1	2	2	1
Q6	1	**Gouvernance Cybersécurité :** Un RACI est-il défini et mis en pratique (rôles et responsabilité de la DG, des Métiers, du CISO, du Contrôle Interne, de la DSI, de l'Audit Interne...) ?	Managé	3	3	1	1
Q7	2	**Détection des Incidents de Sécurité :** Des outils et des pratiques permettent-ils de détecter les incidents de cybersécurité ?	Formalisé	2	4	2	2
Q8	2	**Gestion des incidents de Cybersécurité :** Des outils et des pratiques permettent-ils de tracer et de gérer les incidents de cybersécurité (escalade...) ?	Formalisé	2	4	2	2
Q9	2	**Gestion de crise Cybersécurité :** Des outils et des pratiques permettent-ils de gérer les crises de cybersécurité (équipe de crise, procédures de crise, retour à la normale...) ?	Initialisé	1	2	2	1
Q10	2	**Action de la Direction Générale :** La Direction Générale a-t-elle signé formellement la politique de sécurité de l'information (PSSI) ? Participe-t-elle régulièrement aux points de gouvernance Cybersécurité ?	Initialisé	1	2	2	2
10	17						
QUESTIONS	POIDS						

TOTAL	25
SCORE	1
Maturité globale trop faible	

1,4705882
35 Check

DÉVELOPPER ET ÉVALUER UNE CAPACITÉ DE GESTION DE CRISE ET DE RÉSILIENCE CYBER

Arnaud Burin des Rozier, Jean-François Charbonnier & Vincent Maret

Introduction : Enjeux & Menaces

Un Directeur Général sait aujourd'hui qu'il sera sans doute confronté un jour à une crise cyber. Celle-ci pourra prendre la forme de **l'indisponibilité du SI** pour plusieurs semaines, entraînant un arrêt de la production, des ventes, etc. Elle pourra porter sur les **données de l'entreprise** – qu'il s'agisse d'une fuite massive de données ou d'un chiffrement des fichiers avec demande de rançon. Elle pourra correspondre à une **fraude**, à de **l'espionnage industriel**, ou entrainer la destruction de l'appareil de production.

***Cybercrise** : crise déployée via le réseau internet mais également dont les conséquences sont spécifiques à internet (rapidité et globalité de diffusion, difficulté de détection des attaques, technicité de l'attaque, etc.).*

Les crises cyber ont certaines **spécificités** par rapport à des crises non-cyber :

- Une crise cyber peut être furtive et l'on peut mettre des mois à la détecter (vol de données)
- Elle peut frapper simultanément toutes les géographies / métiers d'une entreprise (contrairement à une crise sanitaire ou à un incendie par exemple)
- Elle peut avoir un temps de propagation de l'ordre de quelques dizaines de minutes
- Elle peut avoir des causes très techniques, peu compréhensibles par des non-spécialistes
- Elle peut impacter la gestion de crise (ex. en rendant indisponible les moyens de communication)
- Des exemples récents (NotPetya) ont montré qu'aucune organisation ne peut se prévaloir d'une protection absolue et que les Plan de Continuité d'Activité « traditionnels » ne constituent qu'une partie de réponse à la crise

La gestion de **crise cyber est un sujet de COMEX et de Direction Générale** car en cas de crise, l'actualité montre que c'est le DG qui monte au front (et qui dans certains cas est démis de ses fonctions). Les régulateurs commencent à exiger des mesures liées à la gestion de crise.

Grands Principes

Le premier principe d'une gestion de crise cyber efficace est de **comprendre et d'accepter qu'une telle crise surviendra**, quels que soient les efforts pour en prévenir la survenance. L'enjeu est donc que la crise cyber soit traitée de manière à entrainer le minimum d'impact sur l'entreprise, en favorisant la poursuite de l'activité métier, même en mode très dégradé, et en visant une reprise d'activité nominale dans les meilleurs délais. C'est ce qu'on appelle la **résilience**.

***Résilience**, du latin resilio, littéralement «sauter en arrière», d'où «rebondir, résister».*

En outre, des procédures sont prévues pour que l'entreprise survive et poursuive son activité même en mode très dégradé dans le cas où le SI n'est plus disponible pendant plusieurs jours ou semaines (scénario « âge de pierre », principe de « **rusticité** »).

***Rusticité** est la sobriété indispensable pour le retour à la normale lorsque pourvu d'outils dégradés - mais efficaces face à une crise.*

Il convient donc de se préparer en conséquence, en mettant en place les **fondamentaux** d'un dispositif de gestion de crise :

- Une organisation de gestion de crise, avec une description des rôles et responsabilités (COMEX, métiers, DSI, SSI, cellules de crise), des procédures (playbook) de déclenchement, gestion et clôture de la crise et un personnel sensibilisé et formé, et des outils de gestion et de communication utilisables même quand l'IT est indisponible
- Des procédures pour poursuivre l'activité métiers même si le SI est indisponible

- Des procédures pour poursuivre l'activité métiers même si le SI est indisponible
- Des simulations et scénarios de crise impliquant les différents échelons de l'entreprise
- Des analyses post-mortem permettant d'identifier les causes de la crise et les améliorations à apporter
- Une mise à jour fréquente du dispositif en fonction des incidents survenus et de l'évolution des processus métiers

Bonnes pratiques

1. Des éléments sont en place pour se préparer à la crise :
   - Rôles et responsabilités liés à la gestion de crise définis (COMEX, métiers, IT, sécurité, cellules de crise, etc.)
   - Procédures de gestion de crise cyber (playbooks) définies, mises à jour régulièrement publiées, accessibles par les acteurs, et connues par eux
   - Acteurs de la gestion de crise formés, connaissant leurs rôles et responsabilités, ainsi que comment accéder aux outils et aux procédures, et ensemble du personnel informé et sensibilisé
   - Outils de gestion de crise en place, avec un contenu (annuaire, procédures, etc.) à jour et utilisables même si le SI de l'entreprise est détruit (publication sur Internet, accessible via BYOD [10])

2. Des procédures dégradées sont prévues en cas d'indisponibilités de l'IT :
   - Plan de gestion de crise prévoyant les cas où le SI est totalement ou en partie détruit (scénarios de type NotPetya)
   - Études spécifiques réalisées pour identifier les dépendances en cas de destruction de l'IT (annuaire, téléphonie, réseau, sécurité des bâtiments, etc.)
   - Procédures de gestion de crise spécifiques pour guider les métiers dans les actions à réaliser à très court terme en cas de destruction de l'IT
   - Eléments nécessaires à l'exécution de ces procédures disponibles sur site (annuaire papier, chèque, PC/téléphone de secours, etc.)
   - Plan de communication incluant des éléments sur la conduite à tenir face à une crise cyber

10 Bring Your Own Device

3. Le dispositif est testé via des simulations de crise impliquant les différents échelons de l'entreprise
   - Exercices de gestion de crise cyber organisés au moins annuellement
   - Exercices impliquant les cellules de gestion de crise, l'IT, mais aussi le COMEX et les métiers
   - Exercices basés sur des scénarios basés sur l'univers des risques cyber pouvant concerner l'entreprise
   - Exercices simulant notamment la réaction à une crise cyber dans des conditions de destruction de l'IT (utilisation de BYOD)
   - Exercices faisant l'objet d'un compte-rendu intégrant des propositions d'amélioration

4. Des analyses post-mortem sont réalisées pour identifier les causes de la crise et les améliorations à mener dans la gestion de crise, qui :
   - Permettent d'identifier les causes de la crise, et les axes d'amélioration à mettre en œuvre pour empêcher la survenance d'une autre crise ou au moins en atténuer l'impact
   - Donnent lieu à des recommandations portant notamment sur le dispositif de gestion de crise et les scénarios à couvrir
   - Alimentent une base de connaissance et d'amélioration en continue, gage de réactivité en cas de crise

---

*Après chaque crise cyber majeure, une **analyse post-mortem** est réalisée par l'Audit Interne et ses conclusions sont présentées au Comité d'Audit.*

---

5. Le dispositif est mis à jour en fonction des incidents survenus en interne ou dans d'autres entités et de l'évolution des processus métiers, pour l'adapter aux évolutions du contexte, prenant en compte :
   - Les retours d'expérience concernant les incidents cyber et les crises internes ou externes
   - La vulnérabilité des SI et l'évolution des menaces et des règlementations
   - L'évolution de la surface d'exposition de l'entreprise du fait des évolutions de processus métiers, d'organisation, de technologies

Une liste de questions clés sur 6 rubriques peut être téléchargée dans le **dossier workplace** également à l'adresse suivante : **https://bit.ly/30vvghf**. Un extrait sur la communication de crise cyber est présenté ci-contre.

Développer une capacité de gestion de crise et de résilience cyber : Feuille de route Audit Cyber-Crise

(Extrait – voir totalité des 6 rubriques sur le **document Workplace**)

NUMÉRO	CHAPITRE	QUESTIONS D'AUDIT INTERNE	BONNES PRATIQUES OBJECTIFS (OBTENIR L'ASSURANCE RAISONNABLE QUE...)
A01a	A - IMPLICATION DE LA GOUVERNANCE	1. Le conseil d'administration a-t-il défini son approche de supervision du dispositif de gestion du risque de cyber-attaques ? A-t-il confié, le cas échéant, la mission de suivi à un de ses comités ?	- Dans le cas où la mission est confiée au comité d'audit, ce dernier communique les résultats de ses travaux lors d'une séance du conseil d'administration.
A02a	A - IMPLICATION DE LA GOUVERNANCE	2. Existe-t-il des tableaux de bord relatifs à la gestion des risques technologiques et cyber pour le COMEX et conseil d'administration ?	- Il existe un dispositif d'évaluation de la maturité en cyber-sécurité.
A03a	A - IMPLICATION DE LA GOUVERNANCE	3. La capacité de réponse à la cyber crise est-elle évaluée ?	- Des simulations de mises en situation sont effectuées régulièrement.
A04a	A - IMPLICATION DE LA GOUVERNANCE	4. Le conseil d'administration s'est-il assuré de la protection des informations critiques et des actifs stratégiques matériels et immatériels à protéger en priorité (s'agissant de données)	- Un plan de protection est mis en oeuvre.
A05a	A - IMPLICATION DE LA GOUVERNANCE	5. Le conseil d'administration s'assure-t-il que les programmes de formation de l'entreprise intègrent les nouvelles sources de vulnérabilité à la cyber-criminalité ?	- Les programmes de formation de l'entreprise (internes ou externes) sont adéquatement intégrés dans les SI et la communication interne de l'entreprise.
A06a	A - IMPLICATION DE LA GOUVERNANCE	6. L'exigence de cyber-sécurité est-elle traitée au bon niveau dans les arbitrages concernants les SI sur les plans techniques, ressources humaines et gouvernance ?	- La cyber-sécurité est un élément stratégique pris en compte au démarrage de projets SI.
A07a	A - IMPLICATION DE LA GOUVERNANCE	7. Le conseil d'administration s'informe-t-il quant à l'organisation et aux ressources allouées au dispositif de cyber-sécurité, y compris l'existence d'un responsable de la sécurité des systèmes d'information (RSSI) ?	- Le planning du conseil d'administration intègre un volet IT qui prend en compte la responsabilisation / délégation à un CRI (Chief Risk Officer).
A08a	A - IMPLICATION DE LA GOUVERNANCE	8. Le management s'implique-t-il dans la cyber-sécurité ?	- La cyber-sécurité n'est pas un sujet tabou. Il est correctement appréhendé par le management dans son quotidien avec ses équipes.
A09a	A - IMPLICATION DE LA GOUVERNANCE	9. Le dispositif de prévention et de détection des cyber risques, y compris la gestion des conséquences d'une cyber-attaque, est-il présenté par le management au conseil d'administration ?	- Lors de communications (semestrielles ou quadrimestrielles) au conseil d'administration, le volet gestion des risques prend en compte le volet cyber-risque évoqué.
A10a	A - IMPLICATION DE LA GOUVERNANCE	10. Le conseil d'administration examine-t-il le déploiement du dispositif de lutte contre les cyber-attaques au sein de l'entreprise ?	- Il existe une cellule de gestion de crise.
A11a	A - IMPLICATION DE LA GOUVERNANCE	11. Le conseil d'administration s'assure-t-il de l'élaboration d'un processus de vérification du fonctionnement du dispositif de cyber-sécurité ?	- Il existe un audit technique indépendant réalisé en matière de cyber-sécurité.
A12a	A - IMPLICATION DE LA GOUVERNANCE	12. Le conseil d'administration examine-t-il le processus de remontée des cas de cyber-attaques ?	- Les cas de cyber-attaques et les simulations sont répertoriées et étudiées. Ils font l'objet d'améliorations futures sur les systèmes.
A13a	A - IMPLICATION DE LA GOUVERNANCE	13. Le conseil d'administration s'assure-t-il de la mise en oeuvre d'un programme d'amélioration continue, afin de s'adapter à l'évolution des modalités des cyber-attaques ?	- L'évolution des modalités des cyber-attaques est correctement prise en compte en utilisant les « 7 Quality Basics » et « Amélioration Continue ». En tant que garant de l'amélioration continue, le Département Qualité s'assure de la bonne conduite de ce processus avec les parties prenantes des risques cyber.
A14a	A - IMPLICATION DE LA GOUVERNANCE	14. Les risques majeurs pouvant amener à une situation de crise sont-ils identifiés et font-ils l'objet d'une coordination cohérente entre les différents acteurs (SI, fonctionnels, opérationnels, dirigeants).	- La cyber-crise est un élément spécifiquement abordée lors de brainstorming de création de matrice de risque (risk mapping).

RÔLE DE L'AUDIT ET DU CONTRÔLE INTERNE VIS-À-VIS DES AUTRES EXPERTS INTERNES EN CYBERSÉCURITÉ

Michel Archaud & Bruno Lechaptois

Introduction & Enjeux

L'enjeu global est de fournir l'assurance au management et à la gouvernance que ce risque est (raisonnablement) maîtrisé avec efficacité. Pour cela, l'entreprise va s'appuyer sur différentes fonctions qui lui permettent d'assurer et de bien coordonner sa protection **au sein de chacune des trois lignes de maîtrise, entre ces trois lignes, et avec la gouvernance**.

Les managers, les experts et notamment le RSSI –(Responsable de la Sécurité des Systèmes d'Information), cela peut être également une fonction dédiée, mais aussi le contrôle interne et l'audit interne, doivent donc travailler de manière concertée avec des rôles bien définis permettant de donner à l'entreprise une confiance raisonnable quant à la maîtrise de ce risque.

Ceci doit conduire à définir des règles et à s'assurer de leur bonne application. **Tous les membres de l'entreprise, doivent être acteurs de cette protection**, qui doit aussi prendre en compte les parties prenantes avec lesquelles l'entreprise entretient des relations et s'assurer qu'elles s'intègrent bien dans cette protection.

Quelle que soit la taille de l'entreprise, il est nécessaire de mettre en place un fonctionnement adéquat pour se prémunir de ce risque.

Les acteurs du processus de cybersecurité (managers, experts en cybersécurité, qualiticiens, contrôleurs internes et auditeurs internes), au sein des 3 lignes de maîtrise vont être conduits à travailler ensemble. [...] Tel que décrit dans le guide IFACI Cyber-Risque 1.0, un comité de pilotage des risques cyber est une bonne pratique à considérer.

Grands principes

La cybersécurité, processus transversal à forte spécificité technique, doit permettre de répondre à un risque majeur pour les entreprises, quelle que soit leur taille. Les acteurs de ce processus (managers, experts en cybersécurité, qualiticiens, contrôleurs internes et auditeurs internes), au sein des 3 lignes de maîtrise vont être conduits à travailler ensemble et il est important de préciser leur rôle en tenant compte des grands principes suivants :

- Un cadre utile et de référence suggère un découpage clair entre 1ière , 2ième et 3ième ligne de maîtrise. La 1ière ligne concerne les actions et processus de cybersécurité directement engagées par exemple par la DSI. La 2ième ligne intègre le Responsable de la Sécurité des Systèmes d'Information (RSSI) qui va développer une politique de cybersécurité et vérifier qu'elle est appliquée à la fois par la DSI et par le reste de l'organisation – tant le rôle et les actions de l'ensemble des utilisateurs de l'entreprise sont également fondamentaux pour assurer un bon niveau de cybersécurité. La gestion intégrée de la cybersécurité doit ainsi être intégrée à la gestion de risque de l'entreprise. Cependant, ce cadre n'est pas ou ne peux pas être toujours respecté. Il doit constituer néanmoins une référence.
- Des profils d'experts en cybersécurité sont proposés en exemple sur le site de l'ANSSI ; suivant la situation de l'entreprise et notamment sa taille, les actions peuvent être pilotées avec des experts internes ou externes
- L'audit interne et le contrôle interne doivent apporter à la gouvernance de l'entreprise l'assurance d'un pilotage effectif et pérenne de la cybersécurité, et notamment s'assurer que **le pilote du processus Cybersécurité bénéficie bien de moyens proportionnés**, et **de la collaboration des services concernés pour maîtriser les risques**
  - Selon les cas, le contrôle interne vérifiant, avec le soutien des experts et les managers opérationnels, **l'existence d'un dispositif raisonnable et efficient** permettant l'identification et le traitement des déficiences
  - L'audit interne, s'appuyant sur la vision du contrôle interne, comme sur les acteurs de l'entreprise, s'assurant que **les risques élevés sont identifiés** et **des réponses actées par le management**.

- Les interactions entre ces acteurs doivent être régies par une gouvernance pérenne (qui prend la suite des modalités d'adaptation telles que décrites dans le **guide IFACI Cyber-Risque 1.0**) : un comité de pilotage des risques cyber est une bonne pratique à considérer. Ce comité de gouvernance fournit un cadre de référence partagé par une correcte représentation des 3 lignes, et doit avoir un agenda détaillé permettant de revoir les risques, valider les décisions, avec un suivi des actions et des responsables. Chaque fois que possible, il doit être piloté par un responsable de la

Cybersécurité, ou en l'absence par la DSI. Il doit comprendre les principales fonctions de l'entreprise, en fonction des risques concernés.prise, en fonction des risques concernés.

Bonnes pratiques

En l'absence de RSSI : En dessous d'une certaine taille, notamment, les entreprises n'ont pas nécessairement mis en place une fonction de RSSI pour gérer les problématiques de sécurité informatique. En conséquence, **les rôles des différents acteurs peuvent être sensiblement partagés**, du fait notamment de l'absence d'une seconde ligne voir troisième ligne de maîtrise formalisée. Dans cette hypothèse, la tendance serait de faire assurer par les opérationnels les plus sensibilisés à cette problématique le rôle de RSSI. On peut notamment penser aux responsables infra (sécurité physique) et responsables réseaux (sécurité logique).

Dans cette fonction ils seraient alors challengés par leur hiérarchie (DSI) sur la mise en place et l'évaluation du dispositif, avec le soutien, quand il existe du Contrôle Interne. Cette organisation ne pourrait toutefois perdurer sans une assistance externe, sous la forme d'un soutien pour la fonction de RSSI, ce qui permettrait de renforcer la seconde ligne et surtout de formaliser la démarche (identification des risques et actions pour les réduire) ; il faut éviter que les opérationnels soient plus dans une approche de réponse à des risques non évalués que dans une **approche de planification/cartographie**.

Dans ces structures, l'audit interne, quand il existe, ne dispose pas des compétences nécessaires pour avoir une approche d'évaluation et d'amélioration du dispositif (en dehors des principes généraux). Une formation est possible mais il faut **envisager une assistance externe** pour structurer l'approche et la rendre cohérente avec l'organisation en place. Le rôle de l'audit interne pourrait alors être l'accompagnement à la mise en place d'une démarche auditable de détection/prévention et réponse, avec un risque non négligeable de perte d'indépendance si le soutien externe n'est pas **indépendant du soutien apporté à la seconde ligne de maîtrise**. Ce risque est toutefois à évaluer en relation avec le bénéfice lié à la formalisation de l'approche.

En présence du RSSI : Il est de la responsabilité du RSSI d'établir une **cartographie des risques de cybersécurité**, de définir les actions/plans d'actions pour maîtriser les risques les plus importants, et de suivre ces plans d'actions. Les fonctions audit et contrôle internes devront vérifier la présence d'une gouvernance adéquate (comité de gouvernance du risque cyber) et auront un rôle de support auprès du RSSI et de **courroie de transmission avec les autres services ou managers**.

S'il y a un dispositif séparé contrôle interne/ audit :

- Le contrôle interne doit apporter un soutien sur la mise en place et la maintenance d'un dispositif de cybersécurité efficient et raisonnable, notamment auprès des managers.
- L'audit va travailler à partir de cette cartographie pour s'assurer que les principaux risques ont été identifiés, et utiliser notamment les travaux du contrôle interne pour établir ses propres missions/ programmes de travail. **L'audit interne devra pouvoir utiliser une expertise externe si nécessaire pour documenter ses travaux**. Les travaux d'audit, bien que complémentaires aux actions du RSSI et du contrôle interne, devront **rester indépendants**.

S'il n'y a pas de dispositif séparé contrôle interne/audit, le responsable « audit/contrôle » devra identifier les points de faiblesse et amener les responsables à conduire les plans d'actions nécessaires. Dans cette tâche, l'audit devra pouvoir faire appel à une expertise externe selon les cas.

Une gouvernance adaptée : une bonne pratique est de mettre en place une gouvernance multifonctionnelle qui doit inclure les compétences et connaissances les plus larges de l'organisation. Cette gouvernance doit disposer d'un leadership fort et transversal, soit de la part de la Direction générale, soit par désignation d'un cadre dirigeant ayant une responsabilité transversale importante pour éviter de cloisonner les initiatives.

Dans ce dispositif, les trois lignes de maîtrise doivent être présentes ou représentées (processus de cybersécurité en 1ière ligne piloté directement par la DSI, politique de cybersécurité développé par le RSSI quand il est en présent et idéalement en 2ième ligne, responsable du contrôle interne, responsable de l'audit interne). Ce dispositif s'appuie sur une définition précise des missions des membres clairement identifiés, des réunions régulières avec des ordres du jour et des dossiers préparés, des comptes-rendus effectués et des actions suivies. La périodicité de réunion peut être trimestrielle et/ ou immédiatement en cas d'incident (sous forme de cellule de crise).

Note : des éléments complémentaires sont disponibles sur le dossier Workplace, à l'adresse : https://bit.ly/30vvghf

SE TENIR INFORMÉ DE L'ÉVOLUTION DU RISQUE CYBER – Y COMPRIS AU NIVEAU GÉOPOLITIQUE

Marjolaine Alquier-de-l'Epine, Christian Giangreco & Nelly Thieriot

Il faut avant tout retenir que la veille doit être personnalisée par le groupe ***c'est-à-dire adaptée à sa taille mais également à son domaine d'activité et à ses lieux géographiques d'activité*** *(à travers ses filiales notamment), et ce afin que la veille soit pertinente et proportionnée à ses besoins.*

Introduction & Enjeux

Se tenir informé de l'évolution des risques Cyber constitue un pilier important de la maitrise de ce risque pour les entreprises.
Les deux principaux enjeux résident dans :

- La connaissance, le suivi et la compréhension des menaces :
  - Quelles sont leurs origines : **géopolitique (les cyber-attaques d'États constituent une part significative des cyberattaques) ?** Un concurrent ? Un acte de fraude ?
  - Leur nature : le phishing reste à ce jour parmi les attaques les plus utilisées, le Ransomware, les attaques de déni de service, le spoofing (ou usurpation d'identité électronique) ...sont d'autres techniques sur lesquelles la sensibilisation et la veille sont nécessaires et pour lesquels les moyens de lutte diffèrent.
  - Leur évolution : **les techniques d'attaques évoluent très rapidement** de même que l'évolution des cibles.

- L'anticipation et l'évaluation des impacts afin de pouvoir appréhender le niveau de vulnérabilité de l'entreprise :
  - La prise en compte de l'exposition géographique est un enjeu majeur pour les entreprises. En effet, les entreprises organiseront leur veille et leur maîtrise du risque en fonction de leur présence géographique.
  - Également, l'exposition aux risques Cyber pour une entreprise varie considérablement en fonction de son utilisation de logiciels IT. Quels logiciels sont utilisés dans l'entreprise ? **Qui**

en sont les éditeurs ? Quel est leur degré d'ouverture / connexion avec d'autres systèmes ?

La veille doit permettre d'adapter la réponse de la société aux risques identifiés et de s'organiser en conséquence.

Grands principes

Une démarche de prévention du risque Cyber se construit en impliquant tous les acteurs concernés et en tenant compte des spécificités de l'entreprise (taille, moyens mobilisables, organisation, sous-traitance, co-traitance, intérim, filialisation, implantation géographique multiple, présence de tiers externes comme du public ou des clients, types de mission du personnel à l'étranger…).
Pour mettre en place une démarche de prévention, il est nécessaire d'avoir en tête que :

- La réponse se situe au-delà du service informatique
- Une communication ciblée doit être mise en place afin de partager l'information sur l'évolution du risque cyber avec le reste de l'entreprise
- **La communication doit être adaptée en fonction des menaces**

Pour mettre en place une démarche de prévention, il est nécessaire d'avoir en tête que la réponse se situe au-delà du service informatique

Bonnes pratiques

Quatre bonnes pratiques majeures sont à retenir dans la veille du risque cyber : la qualité des sources, l'existence de cartographie(s), la diffusion de l'information et les échanges avec les personnes en charge du risque géopolitique.

Qualité des sources :
Différents critères doivent être pris en compte avant d'utiliser une source :

- La source est-elle : identifiée, connue et reconnue, primaire ou secondaire ?
- Si la source est déjà utilisée, a-t-elle été challengée régulièrement (rapidité de changement, pertinence d'une situation à une autre) [11] ?

11 Exemple de sources : se reporter à la bibliographie en fin d'ouvrage

- Quelle est l'origine de la source (géographique par exemple) et sa pertinence aux regards des enjeux et risques identifiés par la société ?

En fonction des ressources de la société, il est possible d'avoir recours aux services de plate-forme spécialisées.

EXEMPLES DE SOURCES
ANSSI (FR)
WWW.MITRE.ORG (US)
HTTPS://CERT.LU
WWW.MISP-PROJECT.ORG (PROGRAMME DE DIFFUSION DE L'INFORMATION TECHNIQUE)
SOCIÉTÉS SPÉCIALISÉES DE VEILLE CYBER (ABONNEMENT À SOUSCRIRE), ÉDITEURS DE LOGICIELS

Cartographie :

La cartographie des risques, classique et normalement établie par la société, devrait également prendre en compte :

- Une cartographie **des risques cyber du point de vue SSI**, y compris une analyse des risques liés aux échanges avec les systèmes tiers ;
- Une cartographie des risques **cyber d'un point de vue géopolitique, en fonction des implantations et domaines d'activité de la société et de ses filiales**.

L'auditeur interne doit s'assurer que des plans d'action sont mis en place face à ces risques.

Diffusion de l'information

Un équilibre doit être trouvé quant au public visé (avec un flux différencié selon que le risque soit général ou spécifique), au niveau de détail de l'information diffusée (effort de vulgarisation) ainsi que de la fréquence de diffusion.

Par ailleurs, les personnes en charge de la veille doivent connaître le flux de transmission de l'information (destinataires, fréquences…) afin d'assurer une communication pertinente, notamment en cas d'urgence. Des outils d'aide à la diffusion existent qui peuvent aider l'entreprise à structurer sa démarche. Par exemple, OpenCTI de l'ANSSI, est un outil de gestion et de partage de la connaissance en matière d'analyse de la cybermenace (« Threat Intelligence »). Il permet de rendre plus intelligible et diffusable l'information.

Enfin, la diffusion de l'information doit également être possible depuis la base vers la direction (bottom-up) et peut être intégrée dans la routine sécurité (si celle-ci existe) ou communication de la société.

Échange avec les personnes en charge du risque géopolitique

Le risque cyber doit être une composante de l'analyse et de choix lors de toute implantation, directe ou indirecte à l'étranger. Cette composante doit être également prise en compte lors du choix de sous-traitants.

La composante géopolitique de l'analyse doit être alimentée régulièrement par des échanges avec les personnes en charge de la gestion de ces risques géopolitiques (mise en place de rituels) afin de s'assurer de la pertinence de la cartographie des risques ou des modifications à lui apporter. Ces échanges peuvent également amener l'entreprise à chercher de nouvelles sources de veille en cas de nouveaux pays ciblés ou impliqués dans le domaine d'activité de la société.

En conclusion, l'auditeur doit s'assurer que **les canaux de diffusion sont connus, alimentés et ce de façon pertinente et régulière**, tout en tenant compte du contexte propre à chaque entreprise (une entreprise intervenant dans le secteur de la Défense présente ainsi un niveau d'exposition plus élevé qu'un garage automobile). **Il doit également s'assurer que la veille n'est pas issue d'une source unique non challengée** et non adéquate au regard des enjeux de sa société.

Note : des éléments complémentaires sont disponibles sur le dossier Workplace, à l'adresse : https://bit.ly/30vvghf

SENSIBILISER LES COLLABORATEURS, ET DÉVELOPPER UNE « CYBER-HYGIÈNE »

Isabelle Boisbouvier, François Michaud & Marie-Line Tipret

Introduction & Enjeux

Un sinistre sur deux est le résultat d'un comportement inapproprié de la part d'un employé dû à une méconnaissance des risques, un défaut de formation, un usage inadapté des réseaux sociaux [1] [2]...
93% des sinistres en 2017 auraient pu être évités grâce à des pratiques basiques de cyber-hygiène [1] [3].

L'organisation doit chercher à développer un engagement de cyber-hygiène de la part de chacun car sensibiliser les collaborateurs, **ce n'est pas seulement les informer, mais les rendre « sensibles »** au risque, conscients de l'enjeu et de leur responsabilité. L'objectif est d'acquérir les bons gestes au quotidien et **les bons réflexes** en cas de crise, en visant l'appropriation générale du sujet pour développer un esprit de résilience.

Distinguons cyber-hygiène individuelle et cyber-hygiène collective.

La cyber-hygiène individuelle relève du comportement individuel de chacun car les hackers, profitant de nos négligences, visent surtout notre messagerie et nos accès aux systèmes d'information.

La cyber-hygiène collective, déclinée selon la taille de l'entreprise, son secteur d'activité et ses risques digitaux, dépend de la Sécurité Informatique, de la DSI mais aussi des propriétaires des processus (séparation des tâches pour les processus Finance, règles de base dans l'utilisation du cloud SaaS...).

En testant l'efficacité, l'auditeur contribue à la sensibilisation à la cyber-hygiène individuelle et à l'adéquation entre la cyber-hygiène collective et l'appétit aux risques de l'entreprise.

En animant l'identification des scénarios critiques, les simulations de crise ou la communication de la veille des évènements externes, les équipes risques et contrôle interne contribuent aussi à la sensibilisation des fonctions métiers en facilitant, par un vocabulaire commun, leur compréhension d'un sujet souvent considéré comme trop technique.

12 Source : Gartner « Measuring and Managing Information Risk »
13 Source : Gartner « 2019 Audit Plan Hot Spots Report Excerpts »

Il faut distinguer cyber-hygiène individuelle et cyber-hygiène collective, déclinée selon la taille de l'entreprise, son secteur d'activité et ses risques digitaux.

Grands Principes

Les grands principes de la sensibilisation et du développement d'une cyber-hygiène sont les suivants :

- S'appuyer sur les travaux et les outils mis à disposition par l'ANSSI pour la sensibilisation des collaborateurs à la cyber-hygiène (cf. bibliographie).
- Vérifier l'existence d'une procédure de sécurité informatique pertinente, incluant les notions de responsabilité de chacun et de protection de la confidentialité, de l'intégrité et de la disponibilité des données, traitements et systèmes, ainsi qu'une classification de l'information selon son degré de confidentialité, avec des règles de sécurité par niveau.
- La sensibilisation à la cyber-hygiène individuelle est **obligatoire pour tous** car la solidité de la chaîne dépend du maillon le plus faible.
- Pour chaque métier ou fonction dans l'entreprise, les responsabilités et les principes à respecter en matière de cyber-hygiène collective sont clairement établis, communiqués et régulièrement audités. Ils sont, le cas échéant, en ligne avec la cartographie et l'évaluation des risques numériques.
- L'entreprise doit **inclure les personnes externes de son écosystème** (sous-traitants, fournisseurs...) dans son périmètre de sensibilisation et les engager à respecter ses règles de cyber-hygiène.
- Un responsable a été désigné pour chacun des sujets de la sensibilisation et un budget a été alloué. Les RH peuvent être impliquées pour supporter le déploiement de solutions de e-learning.
- Des **tests récurrents du degré de sensibilisation** sont réalisés, permettant de mesurer l'évolution de la culture de cyber-hygiène au sein de l'entreprise ainsi que l'efficacité des techniques pédagogiques utilisées. Ces dernières doivent susciter l'envie d'appliquer les règles, par l'utilisation de l'émotionnel, d'exemples, d'images, d'outils interactifs...

Bonnes pratiques

1. Challenger le plan de sensibilisation existant

Avec pour prérequis l'existence de procédures de sécurité informatique liées à la cyber-hygiène et le niveau d'appétit aux risques cyber, l'auditeur peut vérifier l'existence d'un plan de sensibilisation formalisé, sponsorisé par la Direction générale, couvrant toutes les populations et fonctions dans l'entreprise, ainsi que les tierces parties concernées.

Ce plan doit :

- couvrir les sujets mis en avant par l'ANSSI en les priorisant,
- être cohérent avec l'exposition de l'entreprise aux différents risques (selon le secteur d'activité, les technologies numériques utilisées…),
- utiliser les formes les plus appropriées pour marquer les esprits de toutes les sensibilités : théorie et exercices pratiques, utilisant des facteurs émotionnels…,
- prévoir des actions répétitives et évolutives,
- être monitoré par le suivi de la dynamique de la courbe d'apprentissage obtenu, par exemple, grâce aux tests décrits au point 2.

2. Tester l'assimilation des règles de base de la cyber-hygiène par l'ensemble des utilisateurs et le degré de sensibilisation des fonctions standard de l'entreprise

Ces tests, éventuellement réalisés par l'Audit, doivent couvrir l'ensemble des collaborateurs et des fonctions, par exemple par des campagnes de phishing.

Le premier test peut être un courriel de phishing général non ciblé, par exemple un jeu-concours aux couleurs d'un organisme fictif prétendument mandaté par l'entreprise ou son CSE. Pour télécharger le bulletin d'inscription au jeu, il faut cliquer sur un lien, ce qui déclenche un message incitant à télé-charger un plug-in pour avoir accès au document.

L'objectif est de recenser les utilisateurs qui cliquent sur le lien, premier degré d'imprudence, et ceux, encore plus imprudents, qui tentent de télécharger le plug-in.

Le deuxième test de phishing, **ciblé sur une population homogène** (par exemple les comptables, le marketing…), doit être basé sur les centres d'intérêt de celle-ci.

Le courriel, censé émaner d'un cabinet (fictif), propose de télécharger le résultat d'une enquête sur

un sujet supposé intéresser ladite population. À nouveau, l'email contient un lien ou document à télécharger, qui incite à télécharger un plug-in.

Restitution des résultats des tests

- Une restitution anonymisée évite de stigmatiser les utilisateurs imprudents, notamment vis-à-vis de leur hiérarchie, tandis qu'une restitution nominative permet de les identifier pour leur faire suivre une formation adaptée, dans une **démarche pédagogique et non punitive**. Il conviendra néanmoins au préalable avant tout test et restitution de bien vérifier la conformité des procédures envisagées avec le DPO (« Data Protection Officer »/ « Délégué à la Protection des Données »).
- L'audit doit alors identifier les travaux collectifs à mener selon ces retours d'expérience.

Quelques dangers à éviter

- Ne pas usurper une adresse interne existante pour ne pas décrédibiliser un service ou un collaborateur, ni l'adresse d'un organisme externe existant pour éviter de troquer le risque juridique contre le risque cyber.
- La restitution des tests doit être effectuée avec tact car la campagne ciblée augmente le risque de toucher des personnes (dont certaines de niveau hiérarchique élevé) qui s'estiment suffisamment vigilantes.

3. Tester le degré de **sensibilisation de la DSI** et du RSSI et s'assurer de l'indépendance et de l'influence du RSSI sur la DSI
    - Existe-il une veille (des nouveaux modes d'attaques et moyens de protection…) bien propagée pour la sensibilisation, et un plan de formation pour les équipes DSI et RSSI ?
    - La **RSSI est-elle indépendante de la DSI** et influente sur celle-ci ?
    - L'inventaire des systèmes et logiciels informatiques est-il à jour, ainsi que les règles d'implémentation des patchs (fréquence et priorisation notamment) ?
    - Vérifier la maturité du processus de gestion des habilitations et des droits à privilèges élevés dans les couches applicatives mais aussi techniques.
    - Le niveau d'automatisation des outils de sécurité est-il adapté aux enjeux et risques de l'entreprise : modélisation de la politique de mots de passe, système de chiffrement disponible pour les utilisateurs, authentification multi-facteurs…
    - Réaliser un test de simulation de crise peut aussi révéler le degré de résilience de l'entreprise.

4. Tester le degré de sensibilisation des intervenants externes

Les tests ci-dessus doivent aussi être appliqués au reste de l'écosystème de l'entreprise, notamment les principaux partenaires, fournisseurs ou sous-traitants, pour éviter qu'un maillon faible externe ne

crée, par rebond, un risque majeur pour l'entreprise. Attention cependant à en **informer la direction des organismes testés** pour limiter le risque commercial ou juridique.

Note : des éléments complémentaires sont disponibles sur le dossier Workplace, à l'adresse : https://bit.ly/30vvghf

PRENDRE EN COMPTE LE RISQUE CYBER DANS LES PROJETS INFORMATIQUES

Eric Chemama & Ivan Glandières

Introduction : Enjeux & menace

L'intégration de la cybersécurité dans les projets informatiques suscite l'intérêt du public : elle intéresse 78% des votants selon un sondage de l'IFACI. Cependant, comment s'assurer de la correcte & suffisante prise en compte du risque cyber dans le cycle projet ?

L'auditeur ou contrôleur interne observe les projets informatiques pour qu'ils répondent aux objectifs de délais, de maîtrise des coûts, de qualité et de périmètre fonctionnel. Ces projets sont exposés en même temps aux risques Cyber avec un risque d'inadaptation des dispositifs de maîtrise et notamment :

- L'absence de méthodologie de projet ;
- L'inexpérience des métiers dans la formulation des exigences de sécurité ;
- La programmation non maîtrisée ;
- La perte de contrôle du développement ;
- L'inadaptation du périmètre des tests et de la recette ;
- Les environnements de test inadapté (outils, environnement spécifique, etc.) ;
- La méthodologie d'élaboration des scénarios d'attaque et de réponse ;
- Le profil des testeurs et l'expérience.

[...] Il est crucial d'identifier dès l'étape de lancement « définition du projet » avec la Direction générale, les risques cyber qui menaceront la solution.

Grands principes

Il est tout d'abord **absolument primordial de maitriser en amont l'identification et la catégorisation par type de projet**. Cela doit permettre la mise en place d'une réponse appropriée (ex : identification des risques cyber liés à un développement mineur sur une application interne VS ; les risques liés à une refonte de site-web marchant disponible au grand public & incluant du paiement en ligne).

Ensuite, il est crucial d'identifier dès **l'étape de lancement & « définition du projet » avec la Direction générale**, les risques cyber qui menaceront la solution afin de pouvoir identifier dès la conception les mesures de sécurité à intégrer pour s'en prémunir. En amont, l'identification exhaustive des projets et maintenance ainsi que leur catégorisation sont également des points d'attention.

Dans le prolongement, il est important que les objectifs de la stratégie de tests soient adéquats à la solution logicielle et aux enjeux et risques identifiés sur le projet (fiche projet). La stratégie doit fournir une démarche sur laquelle les chefs de projet pourront s'appuyer pour définir et organiser leurs différents tests. Les caractéristiques d'un produit « logiciel » leur permettront d'apprécier les attentes et le niveau de préoccupation en matière de stratégie de tests.

La revue de code et les tests automatisés apportent un niveau de maitrise des vulnérabilités identifiées au sein de programmes et de projets de tests comme celui de l'OWASP, en développement depuis de nombreuses années. L'objectif du projet est d'aider les développeurs à comprendre « quoi », « pourquoi », « quand », « où » et « comment » tester des applications Web.

Bonnes pratiques

1. Identification & catégorisation des projets

Un projet informatique peut prendre plusieurs formes : projet de refonte ERP, projet de développement interne, évolution mineure d'un système, etc., l'entreprise devra renforcer les processus d'identification des projets afin d'assurer une couverture totale.

L'entreprise dispose de processus robustes permettant d'identifier tout nouveau projet (ex : via la validation de l'engagement de dépense (Finance), via la validation des évolutions (IT), etc.). Ainsi, tous les types de projet sont identifiés sans exception, et soumis aux personnes compétentes pour identifier d'éventuels risques cyber.

Il convient alors ensuite de mesurer le risque - **une méthode telle que EBIOS Risk Manager pourra**

être employée - et de contextualiser ce risque en fonction du secteur d'activité et de l'exposition du projet.

L'entreprise dispose d'une matrice de catégorisation des projets : en fonction du type, du périmètre, du montant, etc. chaque projet est catégorisé. Pour chaque catégorie, une méthode d'analyse et d'identification du risque cyber est déroulée. Cette démarche aura pour résultat :

- Une couverture exhaustive des projets de l'entreprise ;
- Une méthode d'analyse adaptée à chaque catégorie de projet et/ou évolution ;
- Une réponse au risque cyber appropriée.

2. Stratégie de tests

Les caractéristiques d'un produit doivent évoluer pour apprécier les attentes et le niveau de préoccupation en matière de stratégie de tests. Le niveau de criticité (rapport entre les enjeux / risques) est à apprécier afin d'y pourvoir et répondre aux critères qualité selon la norme ISO 25010 [14].

Les exigences de sécurité doivent être **définies et analysées pour chaque étape du cycle de vie d'une application**, traitées et gérées de manière adéquate et continue. Elles doivent être traitées de la **même manière que les exigences de fonctionnalité, de qualité et de facilité d'utilisation**.

Les auditeurs doivent en outre dresser une liste des mesures de vérification permettant de prouver qu'une application a atteint le niveau de confiance souhaité.

Les Normes internationales de l'ISO/IEC « Quality Evaluaton Division 2504n » fournissent des exigences, des recommandations et des lignes directrices pour l'évaluation de logiciels, qu'elles soient effectuées par des évaluateurs, des éditeurs ou des développeurs.

Le champ d'application des modèles de qualité se concentre sur les spécifications et l'évaluation des logiciels et systèmes informatiques. Les objectifs des tests du logiciel et du système concernent les objectifs de contrôle suivants : s'assurer de l'identification de critères de contrôle de la qualité dans le cadre de l'assurance de la qualité; s'assurer de l'identification des critères d'acceptation d'un produit; vérifier l'établissement de mesures de caractéristiques de qualité à l'appui de ces activités.

14 ISO/IEC 25010:2011 - Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models

3. Revue de code et testing

La sécurité dans les développements est désormais intégrée en natif dans les cycles de développement de projets.

L'OWASP [15] recommande aux organisations d'établir un programme de sécurité des applications afin d'obtenir des informations et d'améliorer la sécurité sur Internet de leurs applications et API.

Le projet de l'OWASPP ASVS (Application Security Verification Standard) permet de prévenir les principales menaces avec l'application de guides et de métriques pour le développement de solutions.

Le « Guide de tests OWASP » est un cadre de tests pour leur prise en compte dans chacune des phases du développement :

Cependant **les outils de test de sécurité seuls ne suffisent pas. Certaines études [16] ont démontré qu'au mieux, les outils ne peuvent détecter que 45% des vulnérabilités globales**. Des ressources humaines qualifiées et la formation aux tests permettront d'améliorer la prise en compte des résultats des outils de tests automatisés.

Sur la base de ces résultats, la pratique recommande d'inclure des informations de catégorisation des vulnérabilités, de la menace, de la cause fondamentale des problèmes de sécurité (p. Ex. Bogues de sécurité, faille de sécurité), de la technique de test, de la correction de la vulnérabilité et de l'indice de gravité de la vulnérabilité. OWASP Top 10 - 2017 apporte une vision complète sur les « Ten Most Critical Web Application Security Risks ».

Note : des éléments complémentaires sont disponibles sur le dossier Workplace, à l'adresse : https://bit.ly/30vvghf

15 L'Open Web Application Security Project (OWASP) est une communauté ouverte qui permet aux organisations de développer, d'acquérir et de maintenir des applications.
16 Marco Morana, Intégration de la sécurité dans le cycle de vie des logiciels - Analyse de rentabilité - http://www.blackhat.com/presentations/bh-usa-06/bh-us-06-Morana-R3.0.pdf

PARTIE III ALLER PLUS LOIN

CONCLUSION INTERMÉDIAIRE : LE CHEMIN DEVANT NOUS

Guy-Philippe Goldstein

Cela a été rappelé par les différents experts dans la première partie de ce document : la cybersécurité n'est pas un sujet technique. C'est un sport collectif qui nécessite la mise sous tension de l'ensemble de l'organisation. Dans cette action commune qui doit faire de l'organisation, et de son écosystème, une équipe unie face à une menace de plus en plus importante, les auditeurs et les contrôleurs internes jouent un rôle déterminant. Les premières réponses aux neuf questions ici définies permettront à ces acteurs fondamentaux de commencer à trouver leurs marques.

Mais la partie ne fait que commencer.

D'une part, cela a été souligné dans l'introduction, le choix a été fait d'une réflexion introductive sur chacune des questions clés définies. De nombreuses raisons ont milité à cela. D'une part, les sous-questions, très nombreuses, ont été priorisées en fonction de leur importance et de la facilité à pouvoir obtenir rapidement (ou non) des débuts de réponse [17].

D'autre part, il apparait clairement que l'environnement cyber évolue rapidement – on parle souvent de « générations technologiques » durant entre 18 et 24 mois. Mais on pourrait également évoquer, de manière concomitante à ces transformations technologiques, l'évolution rapide des thématiques : on parle aujourd'hui beaucoup de résilience et de coopération, quand hier on évoquait essentiellement la protection des réseaux. Et on peut penser que de nouveaux thèmes, dans deux ou trois ans, deviendront tout aussi essentiels.

Enfin, beaucoup des membres de l'IFACI appartiennent à des organisations aux dimensions européennes, sinon mondiales. Cet aspect a été en partie abordé dans ces premières réponses, avec le choix de référentiels à la fois nationaux et internationaux.

17 L'ensemble de ces réflexions de priorisation sont disponibles sur le site Workplace

Néanmoins, cette compréhension d'enjeux à minima européens pourrait nécessiter là encore certains compléments. Pour toutes ces raisons, une philosophie itérative, une pierre après l'autre, a été privilégiée plutôt que de vouloir faire un document exhaustif et définitif, ce qui paraissait comme illusoire. Plutôt donc, essayer de jeter les bases d'un village qui s'étend années après années – que de vouloir construire une cathédrale qui prendrait plusieurs décennies.

Et agrandir ce village, qui puisse par la suite se transformer en une cité plus vaste, couvrant plus de thèmes et de territoires, est un effort finalement assez simple. Il suffira au lecteur qui souhaite apporter sa pierre aux premières fondations posées par les vingt-quatre premiers « éclaireurs » de simplement répondre aux questions suivantes :

- Suis-je d'accord ou pas avec les réflexions et suggestions proposées ici ?
- Quand je ne suis pas d'accord sur le fond– pour quelles raisons ? Les propositions exposées ici sont-elles inopérantes dans certains cas/sous certaines conditions ? Et alors, que proposer à la place ?
- Quand je suis d'accord sur le fond, y a-t-il cependant des éclaircissements et nuances qui manquent ? Pourrais-je illustrer avec des exemples concrets, y compris dans mon environnement de travail ?

On l'aura compris : c'est par la confrontation des points de vue, et de là, l'identification des cas où certaines propositions fonctionnent, mais peuvent être enrichies ; et des cas où elles trouvent leurs limites, et peuvent être modifiées, que, pierre après pierre, la réflexion générale et pratique pour les auditeurs et les contrôleurs internes pourra s'enrichir et se renforcer.

Cet apport pourra avoir lieu soit en déposant les commentaires sur **le dossier Workplace** également à l'adresse **https://bit.ly/30vvghf** en précisant la question dont il est fait référence.

Les organisateurs de cet effort remercient d'avance tous les membres de l'IFACI qui souhaiteront s'exprimer et contribuer à ce développement, tout en saluant à nouveau les vingt-quatre premiers « explorateurs », qui ont jeté ici les fondations de cette réflexion.

MINI BIOGRAPHIE DES PARTICIPANTS

Les 24 premiers « explorateurs »

Arnaud Burin des Roziers

Diplomé de l'Université DePaul à Chicago ainsi que de son MBA, ancien auditeur interne pour différentes unités de PSA Peugeot Citroën, Arnaud est responsable pour l'audit interne de Poclain Hydraulics, après avoir été le Directeur administratif et financier de la filiale en Inde.

Bruno Lechaptois

Bruno est Directeur Adjoint du Contrôle Interne pour Orange. Après un parcours d'ingénieur, puis de contrôleur de gestion et de directeur financier, dans différentes sociétés en Europe, Bruno a élaboré et mis en place le programme Sarbanes-Oxley pour le groupe Orange, et poursuivi le développement du contrôle interne au-delà du domaine financier.

Christian Giangreco

Diplômé de l'université de Technologie de Compiègne et de Southampton University, Christian est auditeur interne au siège de Naval Group. Son parcours professionnel s'est principalement articulé autour de la conception de systèmes de combat et du management d'affaire en France et à l'international (Singapour, Brésil, Italie) pour la DCNS et Naval Group.

Eric Chemama

Auditeur en systèmes d'information, concepteur-formateur certifié pour IFACI, Eric Chemama, ingénieur en informatique, a été Manager de projets au sein de grandes banques françaises. Il dirige depuis 2012 le Cabinet EMC Conseil et Formation, spécialisé en audit et contrôle internes.

François Michaud

Diplômé de HEC et expert-comptable, François est Directeur de l'Audit interne du groupe Le Conservateur, groupe mutualiste indépendant d'assurance vie et de gestion patrimoniale. Il a également été Directeur Administratif et Financier des filiales françaises du groupe financier britannique Legal & General puis de JP Colonna-GPS, groupe de courtage.

Frédéric Vilanova

Frederic est expert en audit et gouvernance cybersécurité & systèmes d'information. Ingénieur, ESCP, MIT, passé par EY, PWC et CAP GEMINI, il dirige Effective Yelllow, éditeur de logiciels spécialisés en management : Audit Interne, Systèmes d'Information, Cybersécurité, Intelligence Economique. Il veille à la qualité du design des logiciels et services associés.

Gilles Brunet

Ingénieur INSA Lyon, ancien consultant, Gilles est Directeur de missions au sein de la Direction de l'Audit Interne du Groupe Orange en charge des domaines sécurité de l'information et IT. Il assure également la présidence de l'antenne régionale Auvergne-Rhône-Alpes de l'IFACI et est certifié CISA (Certified Information System Auditor) et CRMA (Certified in Risk Management Assurance).

Gustavo Bohlen

Diplomé de l'Université de Liège et de la London School of Economics, Gustavo a tenu les fonctions de conseil juridique et d'auditeur interne pour Keytrade Bank. Gustavo est désormais en charge de la conformité pour Transferwise.

Isabelle Boisbouvier

Diplômée de l'EPF, Isabelle est responsable de la Gestion des Risques au sein du Groupe Thalès, après avoir occupé de nombreuses fonctions chez Gemalto, entre -autre comme responsable contrôle Interne Groupe ainsi qu'en charge de la gouvernance des systèmes d'information au niveau corporate.

Ivan Glandières

Ivan est Auditeur Interne IT au sein du Groupe Rexel. Diplômé de l'E.I.S.T.I en 2015, Ivan a passé 3 ans chez en tant qu'Auditeur IT en cabinet d'audit (Mazars) avant de rejoindre l'Audit Interne du Groupe Rexel en 2018.

Jean-François Charbonnier

Après différentes fonctions à la direction générale de l'armement, Jean-François prend la responsabilité de l'audit interne, activité qu'il créera au secrétariat général pour l'administration. Promoteur de l'audit interne dans le secteur public, il intervient en formation initiale et continue. Il est Lauréat du prix Hintze décerné collégialement au Groupe professionnel administrations de l'Etat qu'il préside actuellement.

Jean-Paul Parisot

Diplômé de l'Institut d'Etudes Politiques de Toulouse et de l'IAE France, Jean-Paul est responsable maitrise des risques à l'AGEFIPH après avoir dirigé plusieurs régions et territoires. Au sein de l'AGEFIPH, Jean-Paul dirige une équipe en charge de la gestion des risques, de l'audit interne, du contrôle interne et de la prévention des fraudes.

Marie-Hélène Laimay

Marie-Hélène est administrateur et membre de comité d'audit d'organisations publiques et privées, après une large experience internationale en audit et gestion des risques.

Marie-Line Tipret

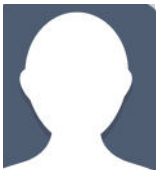
Mare-Line est Directeur Audit et Contrôle Groupe Primonial, en charge de l'audit, du contrôle permanent et de la conformité et des risques pour le Groupe. Après un début de carrière dans un cabinet d'audit, elle a été Responsable Conformation des Services d'Investissement (RCSI) de W Finance, filiale d'Allianz puis a intégré Primonial en 2012 comme Directeur des Services Support.

Marjolaine Alquier-de l'Epine

Diplômée de l'Unversité Panthéon Assas (Paris II), Marjolaine est directrice Audit & Contrôle Interne pour Covivio. Elle y dirige les fonctions d'audit interne, de contrôle interne de la conformité et de gestion du risque pour le Groupe.

Mathias Lorilleux

Diplômé de l'Université Pierre et Marie Curie ainsi que de l'IAE Paris – Sorbonne Business School, Mathias dirige l'audit des systèmes d'information pour un groupe confidentiel du secteur financier. Auparavant, il a occupé plusieurs fonctions d'audit des systèmes d'information pour la BPCE et pour le groupe PNB Paribas.



Michel Archaud

Diplômé de Sup de Co Marseille, Michel est responsable de l'audit interne à la Société du Canal de Provence, en charge de l'audit interne et légal, de la gestion de projet ERP, de la consolidation légale et du contrôle de gestion et du reporting corporate.

Nelly Thieriot

Diplômée de l'IAE Grenoble (DESS Audit), Nelly a été Manager chez Grant Thornton Lyon. Elle a également été Auditrice interne chez Delfingen Industry (équipementier automobile, Franche Comté) puis chez Condat SA (lubrifiants industriels, Rhônes Alpes), deux sociétés internationales et, pour Delfingen, cotée en partie sur le second marché.

Olivier Meyer

Diplômé de l'Institut National des Télécommunications, Olivier est le directeur pour l'audit interne des systèmes d'information au niveau groupe pour le Groupe Adecco. Auparavant, il a été Senior Manager IT pour la cabinet d'audit conseil KPMG.

Olivier Sznitkies

Titulaire du CISA, du CISM, et du CFE, Olivier a dirigé l'audit interne Europe, Moyen Orient Afrique du Groupe LafargeHolcim après une expérience d'une quinzaine d'années comme Auditeur SI chez KPMG et Arthur Andersen. Il a contribué à la rédaction de nombreuses publications comme le Guide d'Audit de la Gouvernance des Systèmes d'Information.

Tatiana Postil

Diplômée du MBA de Solvay Business School et de l'Université Libre de Bruxelles, Tatiana dirige l'audit interne de Keytrade Bank. Elle a été auparavant Senior Internal Auditor pour le groupe d'assurance Generali en Belgique, et a occupé plusieurs fonctions de contrôle et de gestion du risque pour Axa Banque Europe.

Vétéa Lucas

Certiifié CISA (Isaca) et ISO/IEC 27001 Lead Auditor, Vétéa dirige les fonctions de sécurité et de conformité IT pour le Royaume-Uni, l'Irlande et les pays Nordiques et d'Europe Centrale pour le groupe Sodexo. Auparavant, il occupait des fonctions de consultant sur la sécurité des systèmes d'information pour les sociétés Provadys et Lexsi.

Vincent Maret

Vincent Maret est Associé chez KPMG, responsable des activités Cybersécurité et Protection des données personnelles

Xavier Guiffard

Xavier est Directeur de l'Audit Informatique du Groupe Vivendi (dont Universal Music Group, Groupe Canal+, Havas, Dailymotion...), en charge entre autre de la maîtrise des risques IT. Diplômé de l'EDHEC, consultant chez Deloitte et Atos consulting, il a ensuite rejoint le Groupe Vivendi où il a occupé des fonctions de responsable SI, directeurs audit internet ou directeur logistique.

RESSOURCES ET BIOGRAPHIES

Compléments & Outils sur chacun des chapitres

Voir le Dossier Workplace également disponible à l'adresse : https://bit.ly/30vvghf

ANSSI

Guide d'Hygiène Informatique, «renforcer la sécurité de son système d'information en 42 mesures», Version 2.0, Septembre 2017
(Note : contient également une large bibliographie d'autres ressources ANSSI – disponible à https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf)

Guide pour l'élaboration d'une politique de sécurité de système d'information, Section 3 : Principes de sécurité, Direction centrale de la sécurité des systèmes d'information, Mars 2004, disponible à https://www.ssi.gouv.fr/uploads/IMG/pdf/pssi-section3-principes-2004-03-03.pdf

ANSSI & AMRAE

Maîtrise du risque numérique: l'atout confiance, novembre 2019
https://www.ssi.gouv.fr/uploads/2019/11/anssi_amrae-guide-maitrise_risque_numerique-atout_confiance.pdf

IFACI

Cyber-risques : Enjeux, Approches & Gouvernance, Juin 2018 –
Disponible à https://www.ifaci.com/actualites/comment-aborder-le-cyber-risque/

CIS / Center for Internet Security
Principales ressources disponibles à https://www.cisecurity.org/, inclut CIS Controls® V7.1 (liste des 20 contrôles clés)

GARTNER

2020 Audit Plan: Hot Spots, Risk Areas to Watch, 2019 –
Disponible à https://www.gartner.com/en/audit-risk/insights/trending-topics/audit-hot-spots

GUIDE DES RISQUES CYBER IFACI 2.0

LES QUESTIONS DE L'AUDITEUR ET DU CONTRÔLEUR INTERNE

2020

Institut Français de l'Audit et du Contrôle Internes - 98bis, Boulevard Haussmann
75008 Paris - Tél. : 00 48 08 40 331+ Fax : 20 48 08 40 331+ - institut@ifaci.com