Fiche Thématique – Cybersécurité

Introduction

Cette fiche thématique est destinée aux commissaires aux comptes souhaitant intégrer la cybersécurité dans leur pratique professionnelle, quel que soit leur niveau de connaissance technique sur le sujet.

La cybersécurité est aujourd'hui l'un des risques majeurs pour les entreprises, y compris les PME. En tant que tiers de confiance, le commissaire aux comptes a un rôle légitime à jouer dans l'identification et la sensibilisation à ce risque, qui peut directement affecter la fiabilité de l'information financière et la continuité d'activité des entités auditées.

Cette fiche se compose de cinq parties complémentaires, conçues pour être utilisées de manière modulaire selon vos besoins :

Partie 1 – Une définition de la cybersécurité et de ses enjeux pour les entreprises.

Partie 2 – Les idées reçues les plus fréquentes chez les dirigeants, avec les arguments pour les déconstruire lors de vos échanges.

Partie 3 – Un panorama des principaux scénarios d'attaque, des signaux d'alerte à repérer et des mesures préventives à connaître.

Partie 4 – Des arguments concrets pour convaincre un chef d'entreprise de l'utilité d'une démarche cyber.

Partie 5 – Une description des travaux que le commissaire aux comptes peut mettre en œuvre, du plus simple au plus approfondi.

1. Qu'est-ce que la cybersécurité ?

La cybersécurité regroupe l'ensemble des pratiques, outils et politiques destinées à protéger les systèmes d'information, les données et les usages numériques. Elle est devenue un enjeu stratégique pour toutes les organisations, quel que soit leur secteur d'activité ou leur taille. La cybersécurité est un des piliers structurants de « l'hygiène informationnelle ».

+ 10% chaque année

Ces dernières années, les autorités observent une hausse continue des incidents de sécurité déclarés, qu'il s'agisse de violations de données, d'intrusions ou de tentatives d'extorsion. Les attaques sont également de plus en plus massives, certaines touchant désormais plusieurs centaines de milliers voire plusieurs millions de personnes.

PME – Des cibles privilégiées

Compte tenu de l'industrialisation et de l'automatisation des cyberattaques, toutes les entités peuvent être des cibles. La majorité des cyberattaques concerne les PME, qui représentent une part prépondérante des compromissions traitées par les autorités et les acteurs de la cybersécurité. Elles sont aujourd'hui perçues comme les cibles les plus vulnérables, en raison de moyens informatiques limités, d'une sensibilisation inégale et de pratiques de sécurité encore insuffisamment déployées.

1 entreprise sur 2

A déjà subi une cyberattaque

Les attaques par rançongiciel (ransomware en anglais) connaissent une progression spectaculaire d'une année sur l'autre. Un rançongiciel est un logiciel malveillant qui bloque l'accès aux fichiers ou aux ordinateurs en les chiffrant.

Au-delà de l'augmentation du nombre d'incidents, leur gravité progresse également : les analyses montrent qu'une cyberattaque peut entraîner une interruption durable d'activité, qui constitue la part la plus importante du préjudice total. Les organisations victimes peuvent perdre une part significative de leurs revenus, subir une atteinte à leur réputation et, dans un nombre alarmant de cas, ne jamais s'en relever.

Une cyberattaque peut également entraîner des impacts juridiques et réputationnels majeurs pour l'entité. Lorsqu'une violation de données personnelles survient, l'organisation a l'obligation de notifier l'incident à la CNIL sous 72 heures. Cette déclaration peut déclencher un contrôle approfondi susceptible de révéler d'éventuels manquements au RGPD. Les sanctions administratives peuvent atteindre jusqu'à 4 % du chiffre d'affaires mondial, ce qui constitue un risque financier significatif, en particulier pour les structures déjà fragilisées par l'attaque. Par ailleurs, la divulgation ou la perte de données – qu'elles concernent des clients, des salariés ou des partenaires – peut altérer durablement la confiance accordée à l'entreprise. L'impact sur l'image, la réputation et la crédibilité commerciale est souvent profond et difficilement réversible, faisant du risque cyber un enjeu stratégique bien au-delà du seul périmètre informatique.

2. Les idées reçues et leurs réponses

"Je suis une petite entreprise, donc je ne risque rien."

Un mythe dangereux.

Les cybercriminels ciblent également les structures les plus petites, car elles disposent souvent de moins de protections.

De plus, l'industrialisation des cyberattaques a donné naissance à une nouvelle forme de menace : les attaques opportunistes à large spectre. Loin d'être le fruit du hasard, ces attaques automatisées scannent méthodiquement l'ensemble du tissu économique à la recherche de cibles vulnérables. Les entreprises insuffisamment protégées ne sont pas des victimes collatérales : elles sont précisément celles que les attaquants cherchent à atteindre. Les petites structures et celles dont la maturité en cybersécurité est faible sont ainsi délibérément dans le viseur, non pas malgré leur taille, mais souvent à cause d'elle.

Message clé pour le client : aujourd'hui, la taille n'est plus un facteur protecteur. Les attaques sont automatisées, massives et indiscriminées : toute organisation peut être impactée.

"Les attaques, c'est pour les grands groupes ou les institutions."

Plus vrai depuis longtemps.

Les autorités nationales enregistrent depuis plusieurs années une forte croissance du nombre de déclarations d'incidents, toutes tailles et tous secteurs confondus. Les petites structures sont même surreprésentées parmi les victimes (les grandes structures ont réalisé de réels efforts pour améliorer leur maturité).

Message clé pour le client : si des acteurs d'envergure sont médiatisés, les petites structures représentent la majorité silencieuse des victimes.

"J'ai un prestataire informatique / mes logiciels sont en SaaS : je suis protégé."

Une sécurité surestimée.

Faire appel à un prestataire informatique (infogérant) permet de déléguer la gestion de certains paramètres de sécurité à un acteur mieux formé et outillé pour cela, mais cela ne garantit en aucun cas une protection totale. Les contrats de services (CGV - conditions générales de vente, SLA - Service Level Agreement) prévoient souvent des responsabilités limitées, notamment en cas d'attaque, de perte de données ou d'indisponibilité : la sécurisation du système d'information reste partagée, et certaines obligations essentielles (gestion des accès, sauvegardes, configuration, surveillance…) demeurent à la charge de l'entreprise. Il peut exister un écart de perception (expectation gap) entre ce que l'entité croit confier à son prestataire et ce que celui-ci s'engage contractuellement à couvrir. Cet écart peut laisser des pans entiers du système d'information sans protection effective, sans que l'entité en soit consciente.

Le recours à des solutions en mode SaaS appelle une vigilance supplémentaire. Au-delà de la question de la délégation du niveau de sécurité à un fournisseur externe, ces solutions impliquent que vos données soient accessibles depuis Internet, ce qui constitue une exposition supplémentaire aux risques cyber. Ce choix doit donc faire l'objet d'une évaluation attentive, notamment en fonction du niveau de sensibilité des données concernées et de la maturité de l'entreprise en matière de cybersécurité.

Par ailleurs, plusieurs incidents récents démontrent que même un prestataire bien établi peut être compromis : dans certains cas, l'attaque vise le fournisseur, et ses clients subissent l'impact en cascade. Le risque ne disparaît donc jamais complètement.

Message clé pour le client : avoir un prestataire ou utiliser des solutions SaaS ne permet pas de se couvrir en totalité du risque cyber. La cybersécurité reste une responsabilité partagée qui exige des contrôles internes, une vigilance continue et une compréhension claire des limites contractuelles.

"On a un antivirus, donc on est protégé."

Une vision trop limitée.

Les attaques actuelles passent majoritairement par l'humain : le phishing[1] est à l'origine d'une part très importante des incidents recensés en France. Pour comprendre pourquoi ces attaques sont si efficaces, il faut comprendre les limites des outils de protection classiques.

Un antivirus, même intégré à la messagerie pour analyser les pièces jointes, est conçu pour détecter des contenus malveillants connus (virus, fichiers infectés, liens suspects répertoriés). Or, le phishing[1] ne repose pas nécessairement sur un fichier malveillant : il s'appuie sur la manipulation psychologique. Un email de phishing[1] bien conçu peut ne contenir aucun élément techniquement dangereux, et pourtant conduire un collaborateur à saisir ses identifiants sur un faux site, à virer des fonds ou à divulguer des informations sensibles. L'antivirus ne voit rien, parce qu'il n'y a rien à voir sur le plan technique.

Cette vulnérabilité est aujourd'hui amplifiée par l'utilisation d'outils avancés : l'intelligence artificielle permet de rédiger des messages parfaitement rédigés et personnalisés, tandis que les techniques de deepfake[2] permettent de simuler la voix ou l'image d'un dirigeant pour ordonner un virement ou obtenir des accès. Ces attaques ciblent précisément ce que les outils automatisés ne peuvent pas protéger : le jugement humain.

Message clé pour le client *:* la cybersécurité est un ensemble de pratiques, pas un logiciel.

[1] L'hameçonnage (ou phishing) est un SMS ou courriel frauduleux destiné à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour une personne de confiance.

[2] *Deepfake :* Technique basée sur l'intelligence artificielle, qui permet de créer des trucages ultraréalistes (ou hypertrucages) d'images, de vidéos et de sons, à des fins de fraude, de désinformation et de cyberharcèlement.

> “ Je suis assuré cyber, donc je suis couvert.”

Une protection nécessaire mais pas totale.

Contrairement à une idée répandue, détenir une assurance cyber ne garantit pas une prise en charge complète en cas d’attaque. Les contrats d’assurance comportent très souvent de nombreuses exclusions (les sinistres liés à des failles connues, à une négligence manifeste ou à un défaut de prévention, les amendes administratives et les sanctions réglementaires sont généralement exclues ...) qui peuvent limiter fortement l’indemnisation. Les garanties offertes sont par ailleurs très variables selon les contrats, et certaines clauses peuvent restreindre l’étendue du remboursement, en particulier lorsque l’origine de l’incident ou la négligence de tiers n’est pas clairement établie.

Dans la majorité des cas, la perte d’exploitation — pourtant souvent le poste de coût le plus élevé après une cyberattaque — est peu ou pas indemnisée, ou soumise à des conditions strictes (délais de carence, plafonds bas, justificatifs difficiles à produire). De nombreux retours d’expérience montrent que des entreprises attaquées ont découvert trop tard que leur contrat ne couvrait qu’une fraction de leur préjudice réel.

Message clé pour le client : une assurance cyber peut être utile, mais elle est loin d’offrir une protection totale. Elle ne dispense ni d’un niveau de sécurité suffisant, ni d’une gestion rigoureuse du risque cyber : c'est un levier de résilience (capacité à se relever après un incident), un filet de sécurité financier qui n'intervient qu'après la survenance du sinistre. Elle ne prévient pas l'attaque, ne protège pas les données et ne garantit pas la continuité d'activité. Une couverture assurantielle ne saurait donc se substituer aux mesures de prévention et de protection qui restent indispensables.

> “ J’ai des sauvegardes, donc je pourrai redémarrer facilement.”

Une confiance trompeuse.

Disposer de sauvegardes est indispensable, mais cela ne garantit en rien une reprise rapide ou effective de l’activité en cas de cyberattaque. Dans de nombreuses situations, les sauvegardes n’ont jamais été testées, ou les tests datent de plusieurs années : au moment critique, elles s’avèrent incomplètes, inutilisables ou impossibles à restaurer dans les délais nécessaires. Par ailleurs, certaines attaques infiltrent silencieusement le

système pendant des semaines : les sauvegardes peuvent alors être infectées depuis longtemps, rendant impossible un redémarrage propre.

Même lorsque les sauvegardes sont saines, la restauration peut être extrêmement longue. Dans certains environnements, la récupération intégrale des données stockées hors site peut nécessiter plusieurs semaines : par exemple, une restauration complète depuis un cloud peut représenter plus de deux mois de téléchargement avant de pouvoir relancer l'activité.

Enfin, il est essentiel de rappeler que des sauvegardes ne constituent pas à elles seules un plan de continuité d'activité (PCA) ou un plan de reprise d'activité (PRA) :

- Les sauvegardes protègent les données,
- Le PCA (Plan de Continuité d'Activité) organise le maintien des activités les plus critiques en mode dégradé pendant l'incident, afin que l'entreprise puisse continuer à fonctionner a minima malgré la crise,
- Le PRA (Plan de Reprise d'Activité) structure le redémarrage rapide de l'activité après une interruption, avec une perte de données maîtrisée.

Ces deux plans sont complémentaires et tous deux indispensables à la survie de l'entreprise. Sans PCA/PRA, les sauvegardes seules ne permettent ni de maintenir une activité minimale pendant la crise, ni d'assurer un redémarrage organisé après l'incident.

Message clé pour le client : avoir des sauvegardes est indispensable, mais loin d'être suffisant. Seules des sauvegardes testées, combinées à un PCA/PRA formalisé, permettent une véritable résilience en cas d'attaque.

" Une fuite de données vient forcément de l'extérieur."

Une vision incomplète du risque.

Beaucoup d'organisations imaginent que les fuites de données résultent exclusivement d'attaques menées par des acteurs externes. En réalité, une part significative des incidents provient de l'intérieur : erreurs humaines (mauvaises manipulations, envoi de documents au mauvais destinataire, configuration incorrecte), négligences (partage non contrôlé, absence de mot de passe, stockage non sécurisé) ou actes malveillants commis par un salarié, un prestataire ou un ex-collaborateur disposant encore d'accès actifs. Ces situations sont d'autant plus fréquentes qu'elles ne déclenchent pas toujours d'alertes techniques immédiates.

Dans certains cas, la fuite est même accidentellement facilitée par l'organisation elle-même, faute de procédures, de contrôle des droits d'accès ou de sensibilisation. L'idée que la menace provient uniquement "d'Internet" ou "des hackers" occulte une réalité majeure : les personnes ayant déjà accès au système d'information représentent un vecteur de risque tout aussi important.

Message clé pour le client : les fuites de données ne viennent pas seulement de l'extérieur. Elles proviennent très souvent de l'intérieur, volontairement ou non. La maîtrise des accès, la sensibilisation et la gestion du facteur humain sont donc essentielles pour réduire le risque.

" La cybersécurité, ce n'est pas le rôle du commissaire aux comptes / il n'a pas la compétence."

Une perception réductrice du rôle du commissaire aux comptes.

Il est fréquent que les dirigeants considèrent que la cybersécurité relève exclusivement de l'informatique ou du prestataire technique, et que le commissaire aux comptes n'a pas vocation à intervenir sur ces sujets. Pourtant, la cybersécurité constitue aujourd'hui un facteur de risque majeur pouvant impacter la fiabilité de l'information financière, la continuité d'activité, les flux comptables ou encore l'intégrité des données. À ce titre, l'analyse du risque cyber entre pleinement dans la prise de connaissance du système d'information.

Le commissaire aux comptes a toute légitimité pour :

- Identifier les facteurs de risque susceptibles d'affecter l'information financière,
- Apprécier le niveau de maîtrise internalisé par l'entité,
- Sensibiliser le dirigeant sur les enjeux et les conséquences possibles,
- Faire appel, si nécessaire, à des spécialistes.

Message clé pour le client : la cybersécurité fait partie intégrante de la compréhension du système d'information de l'entreprise. Le commissaire aux comptes a toute compétence et toute légitimité pour évaluer le risque, alerter et contribuer à la maîtrise globale du dispositif.

“ La cybersécurité coûte forcément très cher.”

Une fausse croyance qui freine l’action.

Beaucoup d’organisations hésitent à renforcer leur cybersécurité, convaincues que seules des solutions coûteuses — infrastructures sophistiquées, prestations spécialisées, outils avancés — permettent de se protéger efficacement. En réalité, la majorité des incidents pourraient être évités ou fortement limités grâce à des mesures simples, peu coûteuses et immédiatement actionnables : authentification multi-facteurs (MFA), gestion rigoureuse des accès, mises à jour régulières, procédures internes claires, sensibilisation des collaborateurs, vérification systématique des RIB, sauvegardes isolées et testées, etc.

De nombreuses attaques exploitent avant tout des failles humaines ou organisationnelles plutôt que des failles techniques complexes. Une politique de mots de passe robuste, un processus de validation renforcé, ou encore une sensibilisation minimale au phishing[1] constituent des protections à très faible coût mais à très fort impact. Pour la plupart des PME, ces mesures représentent un investissement modéré comparé au coût moyen d’une interruption d’activité, d’une fuite de données ou d’une remise en état complète du système.

Message clé pour le client : la cybersécurité n’est pas qu’une affaire de budget. Une grande partie de la protection repose sur des bonnes pratiques accessibles, une organisation claire et quelques mesures techniques simples. Se protéger efficacement commence souvent par des actions simples, économiques et largement à portée des PME.

“ Le vrai danger, c’est la rançon.”

Une vision trop limitée du risque

Les analyses montrent que la majorité du coût d’une cyberattaque provient de l’interruption d’activité : même sans paiement de rançon, les pertes d’exploitation (arrêt de la production, commandes bloquées, impossibilité de facturer, pertes de clients) constituent le premier poste de préjudice pour les entreprises.

Mais l'impact financier ne se limite pas à l'opérationnel. Une cyberattaque peut également entraîner :

- Un risque réputationnel majeur : perte de confiance des clients, dégradation de l'image, exposition médiatique négative ;
- Un risque juridique, notamment en cas de violation de données personnelles, avec des contrôles potentiels de la CNIL et des amendes pouvant atteindre 4 % du chiffre d'affaires mondial en cas de non-conformité.

Message clé pour le client : le risque cyber, ce n'est pas seulement la rançon. C'est d'abord la perte d'exploitation, mais aussi des conséquences réputationnelles et des enjeux juridiques potentiellement très lourds. Se protéger, c'est préserver à la fois son activité, son image et sa conformité.

3. Panorama des scénarios d'attaque

Cet ensemble de scénarios permet d'illustrer les vecteurs d'attaque existants et de sensibiliser les chefs d'entreprise aux principaux signaux d'alerte et aux dispositifs de contrôle à mettre en place.

Type de menace	Vecteurs d'entrée (comment l'attaque se produit)	Conséquences	Signaux d'alerte	Mesures préventives
Fraudes financières (arnaque au président, faux RIB, FOVI[3])	Ingénierie sociale (phishing[1], vishing[4], deepfake[2] voix/vidéo) ; compromission de messagerie (client, fournisseur, cabinet) ; usurpation d'identité (dirigeant, DAF, DGFiP, prestataire)	Ordres de virement frauduleux ; détournement de règlements ; modification de coordonnées bancaires ; litiges fournisseurs/clients	Demandes urgentes et confidentielles ; contournement des circuits habituels ; pression temporelle ; changement de RIB ; légères anomalies dans l'adresse de l'expéditeur ; alertes des autorités sur des vagues d'usurpation - typosquatting[5] (remboursements ou arriérés d'impôts)	Vérification systématique par téléphone sur numéro connu pour tout changement de RIB ; séparation des tâches et validation multi-canal ; procédure "sans exception" pour tout virement hors routine ; DMARC[6] (DKIM/SPF) ; authentification multifactorielle ; sensibilisation anti-phishing/vishing
Rançongiciel & extorsion	Phishing[1] ; identifiants compromis ; exploitation de	Arrêt d'activité ; pertes d'exploitation	Alertes EDR/antivirus désactivées ; augmentation	Sauvegardes 3-2-1-1-0[7] ; authentification multifactorielle partout ; patching[8] priorisé

[3] FOVI (Faux Ordre de Virement International) : fraude consistant à usurper l'identité d'un dirigeant, d'un partenaire ou d'une autorité pour obtenir un virement bancaire exceptionnel et urgent, souvent sous couvert de confidentialité.
[4] Le vishing ou hameçonnage par téléphone est une forme d'arnaque qui consiste à utiliser un appel téléphonique pour tromper les gens en leur faisant croire qu'ils parlent à un conseiller bancaire ou à un autre professionnel de confiance.
[5] Le typosquatting est une technique de cyberattaque qui consiste à enregistrer un nom de domaine très proche d'un site légitime, en exploitant les erreurs de frappe courantes des utilisateurs.
[6] Domain-based Message Authentication, Reporting and Conformance : le DMARC basé sur le domaine est un protocole de sécurité des e-mails. Le DMARC vérifie les expéditeurs d'e-mails en s'appuyant sur les protocoles DNS (Domain Name System), DKIM (DomainKeys Identified Mail) et SPF (Sender Policy Framework)
[7] La règle de sauvegarde 3-2-1 est une bonne pratique de sauvegarde consistant à disposer d'au moins 3 copies des données (la donnée de production et deux sauvegardes), stockées sur 2 supports différents, dont 1 copie externalisée (hors site). Le principe est complété par 1 sauvegarde immuable ou hors ligne (protégée contre toute modification ou suppression, notamment en cas de rançongiciel) et par 0 erreur, ce qui implique des tests réguliers de restauration afin de vérifier l'intégrité et l'exploitabilité des sauvegardes.
[8] Un patching est une mise à jour ciblée conçue pour résoudre des problèmes spécifiques liés au logiciel, en se concentrant généralement sur la correction de vulnérabilités, de bugs ou d'autres failles susceptibles de compromettre la sécurité ou les fonctionnalités d'un système.

Type de menace	Vecteurs d'entrée (comment l'attaque se produit)	Conséquences	Signaux d'alerte	Mesures préventives
	vulnérabilités d'équipements de bordure (VPN, pare-feu) ; rebond via prestataire ou supply chain	; fuite de données et double extorsion (menace de publication)	anormale du flux sortant ; défaillance des sauvegardes ; connexions VPN atypiques	des équipements d'accès ; EDR/XDR ; plan de continuité (PCA) et de reprise (PRA) ; exercices de crise
Vol & fuite de données / compromission du système d'information	Exploitation de vulnérabilités (VPN, pare-feu, IoT[9] non durcis) ; compromission d'un prestataire informatique, éditeur ou compte administrateur SaaS ; mise à jour contaminée ; accès techniques réutilisés	Intrusions persistantes ; mouvements latéraux[10] ; exfiltration massive de données ; atteinte à la réputation	Actions d'administration hors créneaux habituels ; connexions depuis plusieurs adresses IP inhabituelles ; tickets "urgents" anormaux	Inventaire des surfaces exposées ; patching accéléré ; bastion d'administration[11] ; cloisonnement réseau ; journaux impossibles à effacer (WORM[12]) ; contrats prestataires avec exigences SSI ; audits réguliers ; authentification multifactorielle pour les administrateurs

[9] Internet of Things (IoT) décrit le réseau de terminaux physiques, les « objets », qui intègrent des capteurs, des logiciels et d'autres technologies en vue de se connecter à d'autres terminaux et systèmes sur Internet et d'échanger des données avec eux.
[10] Le mouvement latéral est une tactique que les cybercriminels utilisent pour pénétrer plus profondément dans le réseau d'une organisation après avoir obtenu un accès non autorisé.
[11] Le bastion d'administration crée un accès unique pour l'ensemble de vos connexions qu'elles soient internes (DSI, RSSI, Administrateurs systèmes et réseaux ...) ou externes (consultants, auditeurs, télémainteneurs...).
[12] WORM (Write Once Read Many) : Le stockage WORM impose un modèle de sécurité zéro confiance en dépouillant même les administrateurs les plus privilégiés de la capacité à modifier ou supprimer des données.

4. Arguments pour éclairer la prise de décision du chef d'entreprise

"Une mission qui protège votre activité, pas seulement vos données."

« Aujourd'hui, les cyberattaques ne sont plus un problème informatique : ce sont des événements qui paralysent l'activité, coupent la facturation, bloquent la production et impactent la trésorerie. Un diagnostic cybersécurité vous permet d'identifier les vulnérabilités qui pourraient provoquer un arrêt d'activité, souvent plus coûteux que la rançon elle-même. En d'autres termes : c'est un outil de préservation de votre continuité d'exploitation. »

"Vous gagnez en sérénité décisionnelle :
nous transformons un risque flou en un risque maîtrisé."

« Beaucoup d'entreprises savent qu'elles sont exposées, mais ne savent pas où, comment, ni dans quelle proportion.
Une analyse de votre risque Cyber vous apporte une photographie claire et objective de votre exposition cyber : points faibles, priorités, scénarios réalistes. Vous pouvez alors prendre des décisions éclairées, hiérarchisées et proportionnées à votre réalité opérationnelle. C'est un gain concret : moins d'incertitudes, plus de maîtrise. »

"Vous protégez aussi vos équipes :
l'humain est la première cible des attaques."

« La majorité des attaques passent par une erreur humaine ou par de l'ingénierie sociale. En renforçant vos procédures internes et vos réflexes métier, vous protégez aussi vos collaborateurs :

- Moins de stress en cas d'appel suspect,
- Moins de risques de faute involontaire,
- Plus de confiance dans leurs décisions.

Vous gagnez une organisation plus robuste sans être plus lourde. »

« Vous bénéficiez d'un regard indépendant et d'un interlocuteur de confiance »

« La cybersécurité est un sujet sensible : technique, anxiogène et souvent mal compris. Notre mission vous apporte à la fois un regard neutre, sans conflit d'intérêts, et un accompagnement pédagogique pour aborder ces enjeux avec clarté.

En tant que tiers de confiance, nous évaluons de manière indépendante vos risques, vos procédures et vos points de vigilance. Parce que nous connaissons déjà votre organisation, nous pouvons vous vulgariser les sujets techniques, répondre à vos questions et vous éclairer dans vos décisions, sans dramatiser ni minimiser.

Vous gagnez un interlocuteur fiable, neutre et indépendant, capable de vous aider à comprendre votre exposition cyber et à agir avec sérénité. »

5. Travaux du commissaire aux comptes : une démarche progressive en trois niveaux

Pour accompagner les entités dans la compréhension et la maîtrise de leur risque cyber, le commissaire aux comptes peut s'appuyer sur une démarche graduée allant d'une prise de connaissance minimale (niveau 0) à un audit approfondi du risque cyber (niveau 2).

Cette approche permet d'adapter le niveau d'intervention aux besoins de l'entité, à son niveau d'exposition et à la maturité de son système d'information.

Niveau 0 – Intégration d'un volet cybersécurité dans la prise de connaissance (mission de certification des comptes)

Objectif : prendre connaissance du risque cyber à l'aide du questionnaire suivant.

Cette prise de connaissance du risque cyber peut être incluse dans la mission de certification des comptes et ne constitue pas une prestation complémentaire.

Enjeux :

- Documenter la compréhension du risque cyber.
- Identifier les risques pouvant impacter le contrôle interne et la production d'informations financières.
- Informer l'entité sur les facteurs de risques cyber existants dans son entité.

Comment faire ?

La CNCC met à disposition un questionnaire de prise de connaissance du risque cyber.

Niveau 1 – Diagnostic de maturité cyber (basé sur des entretiens uniquement) réalisé par un auditeur financier

En fonction des risques relevés lors de la prise de connaissance et portés à la connaissance du chef d'entreprise, le commissaire aux comptes peut proposer à ce dernier la réalisation d'une prestation de diagnostic permettant ainsi d'obtenir un état des lieux sur l'exposition de l'entité face au risque de cybersécurité (identification des forces et des faiblesses et proposition de recommandations).

Objectif : apprécier le degré de maturité de l'entité face à son risque cyber.

Enjeux :

- Identifier les forces et les faiblesses de l'entité
- Proposer des recommandations adaptées aux faiblesses identifiées

Comment faire ?

La CNCC met à disposition un outil de diagnostic afin d'accompagner les commissaires aux comptes dans l'évaluation du degré de maturité de l'entité face aux risques de cybersécurité.

A noter qu'aucun test technique (pas de vérification, pas d'intrusion, pas d'analyse forensique) n'est prévu dans le cadre de ce diagnostic.

Il convient également de préciser que toutes les questions sont pondérées de manière égale. Il appartient au commissaire aux comptes d'apprécier, selon son jugement professionnel, la criticité de chaque réponse négative, certaines d'entre elles (par exemple l'absence de sauvegardes isolées ou d'authentification multifacteur) peuvent être considérées comme des signaux d'alerte majeurs quel que soit le score global obtenu.

Niveau 2 – Evaluation du risque cyber réalisée par un expert en cybersécurité couplée à des tests d'intrusion – prestation

Objectif : **Identifier et évaluer les vulnérabilités exploitables** du système d'information en simulant des attaques réelles

Enjeux

- Tester la robustesse du SI face à des scénarios crédibles d'attaque.
- Proposer des recommandations.

Exemples de travaux possibles (liste non exhaustive) :

- Tests d'intrusion (interne, externe, phishing[1] ciblé).
- Analyse des sauvegardes (intégrité, isolation, fréquence, restauration).
- Évaluation du PCA / PRA (existence, qualité, capacité de reprise).
- Examen des configurations critiques (VPN, pare-feu, MFA, accès administrateurs).
- Tests de résilience (simulation d'incident, exercice de crise).
- Analyse des risques avec méthodologie cyber structurée (ex. EBIOS Risk Manager[13]).

Le commissaire aux comptes peut faire appel à un expert pour la réalisation de cette évaluation du risque cyber.

[13] EBIOS Risk Manager (EBIOS RM) : méthode de référence française d'analyse et de gestion des risques numériques, développée par l'ANSSI. Elle permet d'évaluer les risques cyber en tenant compte du contexte de l'organisation, des menaces réelles qui la ciblent et de ses enjeux métiers, afin de définir des mesures de sécurité adaptées et proportionnées.