Les enjeux du numérique et la mission du commissaire aux comptes

Olivier Arthaud, Président de la Compagnie Régionale des Commissaires aux Comptes de Lyon

Nicolas Touchet, Commissaire aux Comptes et Expert Comptable associé

Sommaire

1. LA TRANSFORMATION NUMÉRIQUE

Périmètre et enjeux

- Depuis l'an 2000, plus d'une entreprise sur deux du classement Fortune 500 a disparu ou a fait faillite,
- Toutes les entreprises sont concernées quelque soit leur taille,
- Toutes les offres de produits et services sont concernées,
- Tous les processus de l'entreprise sont concernés,
- Toute l'expérience client est transformée,
- Toute la notation de l'entreprise devient permanente et publique,
- Toute la distribution est réinventée,
- Toute la communication est devenue numérique,
- Toute la concurrence se transforme,
- Tout l'écosystème se construit et s'anime.

- Les positions de leader depuis le 19ème siècle sont remises en question par des entreprises qui ont de 3 et 10 ans !

Que de risques et d'opportunités !

Les facteurs clés de succès de la transformation numérique

- L'engagement du dirigeant,
- La culture de l'entreprise ouverte au changement et à l'innovation,
- La veille technologique et concurrentielle,
- L'implication et la formation de tous,
- Un responsable nommé et des relais désignés,
- Des milléniaux embauchés et écoutés,
- L'écoute de l'écosystème,
- L'excellence opérationnelle et le LEAN Management,
- La flexibilité et l'agilité, …

Tous les acteurs sont concernés, la transformation est encore plus sur l'homme et la culture que sur les technologies.

2. L'IMPORTANCE DU SYSTÈME D'INFORMATION (SI)

Définition

Jusqu'au début des années 2000, l'informatique était un moyen dont il fallait gérer les coûts et effectuer un suivi d'activité annuel.

Désormais, le SI est devenu omniprésent. Plus qu'un moyen ou une composante de l'organisation, le SI est devenu la colonne vertébrale de l'entreprise et de son activité.

En 2017, la gouvernance des SI consiste à …

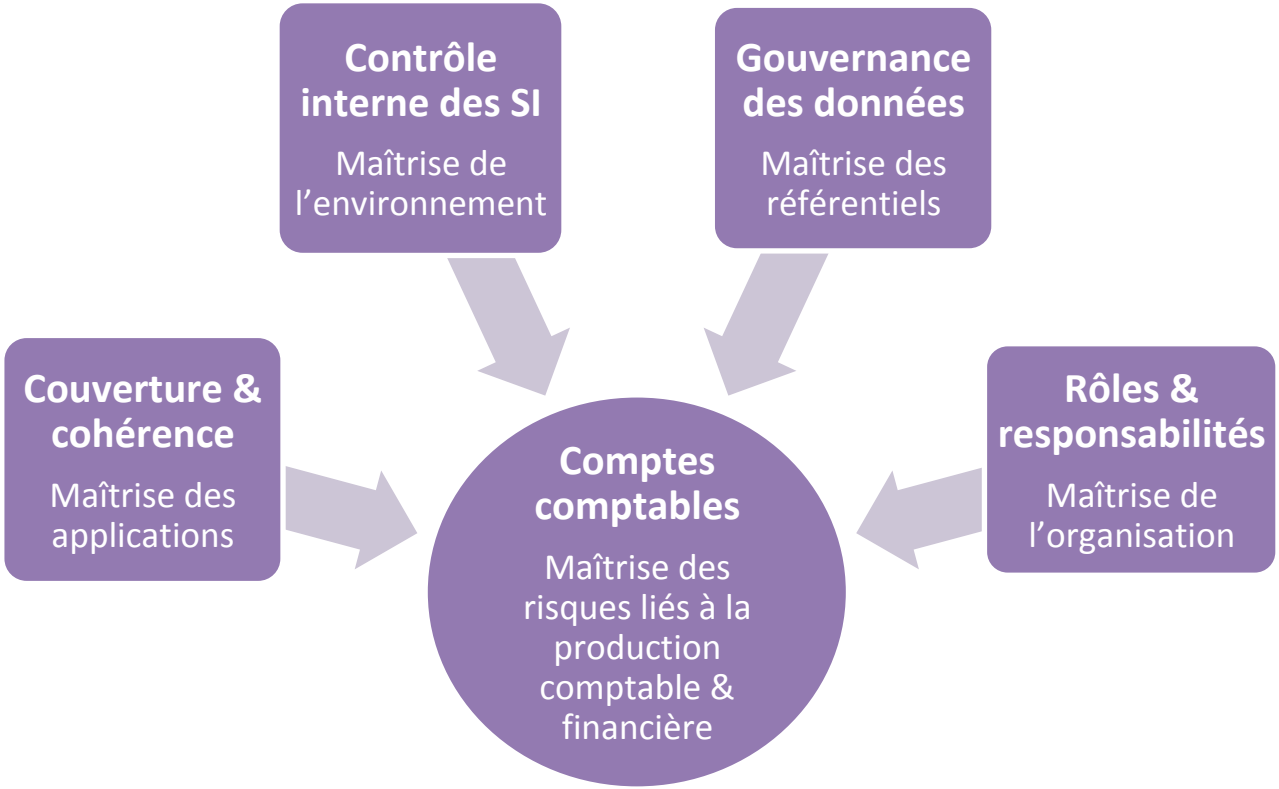
- **Piloter,**
- **Aligner,**
- **Organiser,**
- **Sécuriser.**

Il s' agit donc de mettre en phase la production de valeur reconnue du SI avec la stratégie de l'entreprise.

Tout ceci requiert un paradigme différent : le SI comme actif pour créer de la valeur.

Lien entre SI et états financiers

Pour évaluer la gouvernance du système d'information de nos clients, nous recommandons de concentrer les travaux sur les axes suivants :



3. LES ENJEUX DU CONTRÔLE INTERNE

Le contrôle des accès

Le contrôle des accès vise :

- **A disposer de droits proportionnels aux besoins des utilisateurs,**
- **A garantir la sécurité des actifs de l'entreprise,**
- **A offrir un niveau de sécurité approprié pour les transactions au sein d'un système d'information,**
- **A assurer la maîtrise des opérations par une entité.**

Le contrôle des accès

L'analyse des tâches incompatibles au sein de l'entité

Appréciation par le commissaire aux comptes de l'environnement de contrôle interne :

- Cartographie des risques,
- Diagramme de flux,
- Cartographie des systèmes d'information.

Appréciation par le commissaire aux comptes du fonctionnement du dispositif de contrôle interne :

- Qualité des procédures et des contrôles (« Design »),
- Fiabilité des procédures et des contrôles.

L'analyse de la séparation des tâches (« SOD »)

Adéquation entre les droits d'accès aux applications et les tâches incompatibles.

Restreindre ou supprimer les droits en fonction des tâches identifiées comme incompatibles entre elles.

Le contrôle des accès

L'adéquation entre le niveau de droit d'accès et le niveau hiérarchique

Exemples de droits d'accès avec des responsabilités élevées :

- Changer un taux de TVA ,
- Création / modification / suppression RIB,
- Paiements / décaissements.

Exemples de droits d'accès avec des responsabilités faibles :

- Saisie,
- Lettrage.

Avant tout, c'est l'exercice du jugement professionnel adapté à la taille de l'entité et à l'analyse des risques qui prévaut.

Le contrôle des accès

Exemple de matrice de tâches incompatibles – cycle des ventes :

Le risque de fraude

1. Cas de fraude pouvant avoir comme origine un dysfonctionnement dans le contrôle des accès :

- Paiement non fondé déclenché dans ERP ayant entraîné une sortie de trésorerie significative,
- Fraude au Président,
- Création d'un fournisseur / salarié fictif dans un système informatique.

2. Des axes de travail pour le commissaire aux comptes :

- La cartographie des systèmes d'information,
- L'organisation de la DSI,
- Un questionnaire d'évaluation.

Questions à poser

1. L'organisation auditée a-t-elle documenté sa politique de contrôle d'accès et tient-elle à jour une matrice des autorisations ?

2. Concernant la gestion des droits d'accès :

- Qui décide de l'attribution / retrait des droits d'accès ?
- Qui saisit la création / suppression des droits d'accès ?

3. Les utilisateurs ont-ils l'interdiction de divulguer, communiquer, partager leur mot de passe ?

4. Les mots de passe ont-ils une obligation de complexité (longueur mini, 3 types de caractères différents…) ?

5. Les postes de travail se verrouillent-ils automatiquement après quelques minutes d'inutilisation ?

Conclusion

1. Des diligences sur le contrôle des accès rentrent dans les diligences du commissaire aux comptes et sont partie intégrante de la démarche d'audit,

2. Une limitation du risque de fraude,

3. Un apport de valeur ajoutée au client en faisant des recommandations sur ce thème.

➢ **Le contrôle des accès, un incontournable dans l'appréciation du dispositif de contrôle interne de l'entité auditée.**

4. LA CONDUITE DES PROJETS INFORMATIQUES

Les facteurs à considérer

Pourquoi parler de conduite de projet ?

Parce qu'en moyenne, 30 % du budget d'une entreprise est consacré à des projets. Cela participe de l'évolution, de l'adaptation et de la transformation de toute entreprise en croissance ou non. Les projets SI ont très souvent un impact direct ou indirect sur les états financiers. Le pilotage des projets et leur réussite ou leur échec peuvent avoir des conséquences graves sur l'activité de l'entreprise.

Vis-à-vis des projets, le commissaire aux comptes doit donc s'assurer d'au moins deux choses :

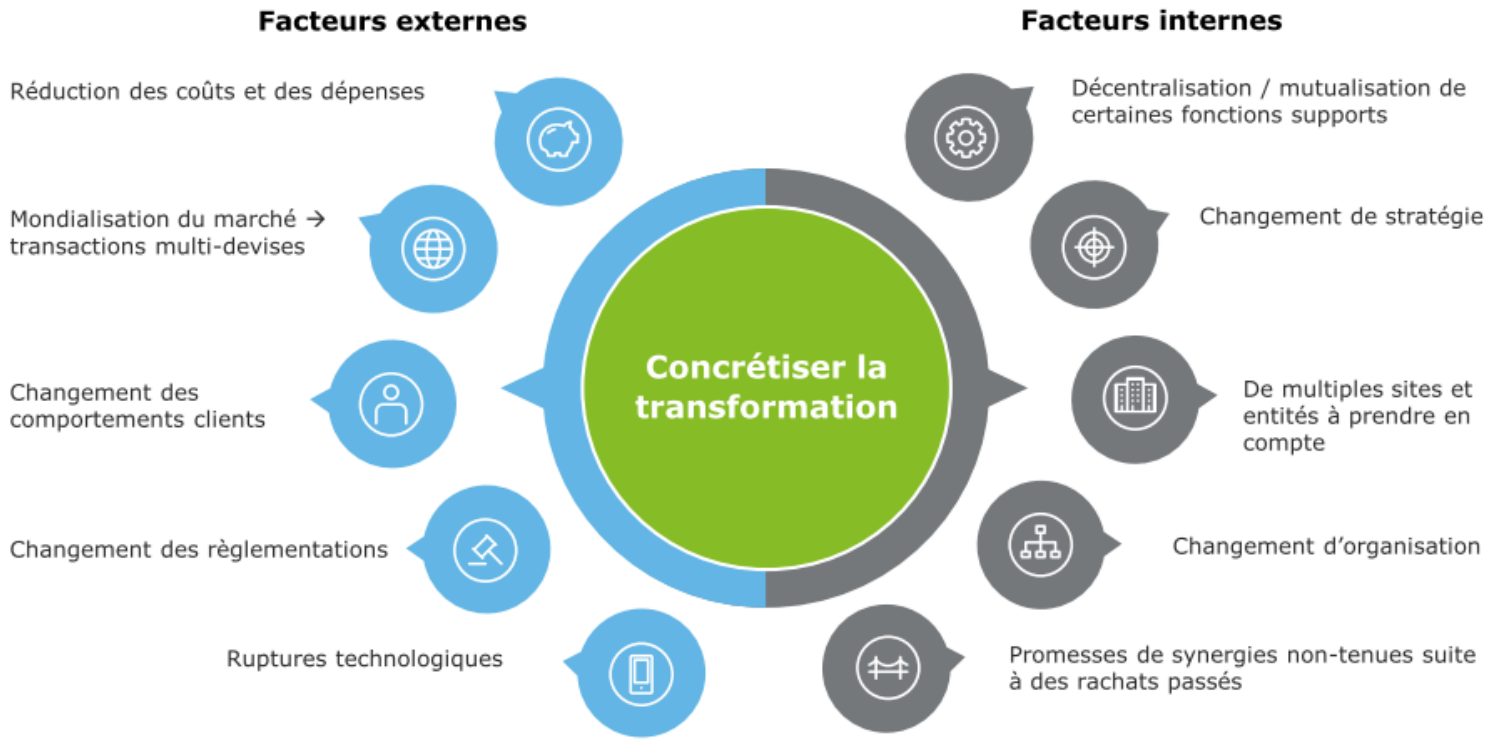
- **En termes d'approche :** le(s) projet(s) a (ont) été mené(s) selon les règles de l'art et respecte(nt) un cadre de contrôle interne suffisant,

- **En termes de données :** les données et états financiers impactés ou produits à l'issue du projet sont exhaustifs, fiables, et correctement comptabilisés.

S'agissant d'audit, les projets les plus directement impactant sont ceux touchant le SI financier, que cela soit dans le cadre d'un changement de logiciel, d'une migration de version, d'une intégration ou d'une cession d'activité. Ce sont là les exemples les plus évidents, mais cela ne signifie pas que les autres projets ne concernent pas le commissaire aux comptes !

Les facteurs à considérer

Piloter un projet, c'est anticiper et contrôler l'ensemble des facteurs qui peuvent influer sur son bon déroulement



→ Un impact évident sur la traduction comptable de l'activité économique de l'entreprise !

La matrice RACI

La gestion de projet repose en grande partie sur la définition et l'exécution des rôles et responsabilités des parties prenantes.

Ceux-ci sont matérialisés dans un document appelé le RACI.

Cet outil est indispensable pour établir les attendus vis-à-vis de chaque partie prenante et ainsi lever toute ambiguïté dans les processus de décision.

R : Responsable, ou Réalisateur

A : Approbateur (« Accountable » en anglais)

C : Consulté

I : Informé

Il ne peut y avoir qu'un seul A par tâche

Exemple :

Description de l'activité	DAF	Directeur Comptable	DSI	Intégrateur
Tâche 1	A	R	C	I
Tâche 2	R	A	C	I
Tâche 3	C	R	A	I
Tâche 4	I	R	C	A

Les phases d'un projet

Quelle que soit la méthodologie adoptée, les phases logiques d'un projet sont les suivantes :

Expression du besoin > modélisation détaillée > paramétrage > tests > cycle de validation de conformité > fonctionnement en double > mise en production

L'enchainement, la durée et l'ordonnancement de ces phases varie en fonction de la méthodologie utilisée (cycle en V, agile, hybride,…). Mais leur nature demeure identique afin de respecter un ordre logique de conception.

A chaque phase correspondent des risques spécifiques. Exemples :

- Quel doit être le contenu des spécifications (expression du besoin et modélisation) ?
- Quels sont les facteurs clés d'une recette fiable ?
- Pourquoi la reprise de données est-elle sensible ?
- Le pilotage est-il assuré de manière proactive et fait-il l'objet d'une communication régulière ?

5. LES MISSIONS D'AUDIT

Périmètre et enjeux

- **La prise en compte de la digitalisation des données devient un facteur clé de réussite des missions d'audit :**

- Recours +/- extensif aux applications informatiques,
- Volumétrie de transactions de plus en plus importante.

  - **L'approche par sondage devient moins pertinente**
  - **L'utilisation d'outils d'analyse des données est plus pertinente**

- **Les outils informatiques d'audit de données :**

- Facilitent le travail du commissaire aux comptes,
- Permettent une atteinte plus aisée de l'assurance raisonnable,
- Documentent l'approche d'audit par les risques.

Analyse des risques

- **Les principaux outils du marché (Caseware Idea et ACL) sont une réponse appropriée à la mise en œuvre par l'auditeur de l'analyse des données :**

  - Outils adaptés à un professionnel sans formation informatique spécifique.

- **Fichiers sources possibles :**

  - Le fichier des Ecritures Comptables (FEC),

  - Fichier de données opérationnelles (stocks, factures, expéditions, référentiels, Paie, entrées-sorties du personnel…).

Analyse des risques

- **Principales fonctionnalités nécessaires des outils d'analyse de données**

Fonctionnalités communes aux outils type tableur et outils d'analyse de données	Fonctionnalités propres aux outils d'analyse de données
• Tris et index • Sélection / filtre d'enregistrements • Calcul de données (dates, chiffres, textes) • Contrôles de conformité • Représentation graphique des données	• Piste d'audit • Jointures entre fichiers • Recherche/Exclusion de doublon • Ruptures de séquences numériques, de dates • Stratification • Analyse loi de Benford • Sélection aléatoire d'un échantillon de données • Automatisation des contrôles • Nombre illimités de données

Mise en œuvre de la mission

1. **Adopter une démarche de mise en œuvre appropriée,**
2. **Identifier les applications et interfaces gérant les données auditées (Cartographie du SI),**
3. **Déterminer :**
   - Les fichiers et champs à obtenir,
   - La nature des contrôles à réaliser,
   - Les formats de fichiers à vous transmettre,
   - Les paramètres d'extraction (bornes des périodes , SI source, champs, etc…).
4. **Vérifier les fichiers transmis et exploiter l'analyse statistique des données,**
5. **Préparer – harmoniser les données,**
6. **Mettre en œuvre dans l'outil les contrôles prévus,**
7. **Analyser les anomalies identifiées.**

Questions / Réponses

1. Faut-il être informaticien pour utiliser ce type d'outils ?
2. Au bout de combien de temps vais-je devenir opérationnel avec ces outils ?
3. Mon client va-t-il accepter de me transmettre des fichiers dans le cadre de ma mission ?
4. Faut-il déclarer à la CNIL les fichiers que je vais récupérer / traiter / créer depuis ceux du client ?
5. Peut-on me reprocher de ne pas utiliser ce type d'outil dans mes missions de commissaire aux comptes ?
6. Si j'ai bien compris, je ne peux plus utiliser Excel ?

Conclusion

1. Le mouvement de transformation digitale des entreprises entraine une inflation du volume de données rendant obsolète les approches par sondages (tests) et le recours aux outils bureautiques traditionnels,

2. Les outils informatiques d'audit de données facilitent le travail de l'auditeur et renforcent son assurance raisonnable,

3. Ils sont un élément de renforcement de la valeur ajoutée du commissaire aux comptes pour ses clients.

- **L'utilisation de l'informatique par l'auditeur : un outil incontournable du professionnel 2.0.**

6. L'EXPLOITATION DES SYSTEMES

Contexte

- La fonction « exploitation des systèmes » est essentielle pour la pérennité des entreprises,

- Elle entre dans le périmètre de la mission du commissaire aux comptes.

Référentiels

NEP 240 pour la prise en compte de la possibilité de fraude, NEP 330 pour l'évaluation du contrôle interne, NEP 620 pour les experts tiers.

Conséquences d'une perte de services informatiques

Les conséquences d'une perte de services informatiques et/ou d'une perte de données :

- **Arrêt de la production,**
- **Clients perdus,**
- **Procès,**
- **Dépôt de bilan,**
- **…**

Mieux vaut anticiper !

Quelques exemples

Pas de suivi des sauvegardes et pas de tests de restauration :

Cas fréquent d'une sauvegarde mal paramétrée : le compte rendu affiché indique : « 0 erreur de sauvegarde ». La personne en charge du suivi est satisfaite. Mais juste au-dessus de « 0 erreur de sauvegarde », il est noté « 0 fichier sauvegardé – 0 octet sauvegardé » !!! En cas de panne ou de vol du serveur, la perte de données est certaine.

- **Importance de la fonction exploitation des systèmes.**

Quelques exemples

Pas de surveillance des « logs » ou des alertes :

Si un des deux disques en miroir sur un serveur est en panne, le serveur fonctionne quand même ! Si la panne du premier disque n'est pas détectée et remédiée, la panne du deuxième disque entrainera une interruption de services.

Autre exemple : le journal de sécurité du serveur indique un échec de connexion, avec erreur de mot de passe, plusieurs fois par seconde : cela signifie un piratage en cours, avec recherche automatique du mot de passe par tests de toutes les combinaisons de caractères possibles. Si ce piratage n'est pas détecté, au bout de quelques jours ou de plusieurs mois, le mot de passe pourra être trouvé par le pirate.

- **Importance de la fonction exploitation des systèmes.**

Quelques exemples

Pas de séparation des tâches développement / exploitation :

Création de fonctions secrètes par le développeur dans les logiciels. Ces fonctions secrètes peuvent être utilisées par lui pour commettre des fraudes qui échapperont aux procédures de contrôle interne.

- **Importance des procédures de contrôle interne.**

Questions à poser

L'audit de la fonction « exploitation des systèmes informatiques » peut être réalisé en phase d'intérim.

Il faut commencer par identifier la ou les personnes en charge de l'exploitation des systèmes.

Exemples de questions à poser :

- **Les procédures d'exploitation sont-elles documentées ?**
- **Les fonctions de développement, de tests et d'exploitation sont-elles séparées ?**
- **Existe-il un antivirus sur tous les équipements de l'organisation auditée ?**
- **Existe-il une gestion centralisée et une remontée automatique d'alertes pour les antivirus ?**

Questions à poser

- L'existence d'un antivirus est-elle exigée sur les équipements personnels des utilisateurs, avant l'autorisation de se connecter au système d'information ?
- La prestation de services par des tiers est-elle encadrée et gérée ?
- Externalisation, sous-traitance, Cloud… : Les risques associés sont-ils évalués et des clauses de réversibilité sont-elles prévues ?
- Les données sont-elles sauvegardées automatiquement au moins une fois par jour ?
- Le bon fonctionnement des sauvegardes est-il suivi selon une procédure formelle ?
- Des tests de restauration sont-ils menés régulièrement ?

Le PCA (Plan de Continuité d'Activité)

Le PCA doit permettre à une entité de :

- **Préserver la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal,**
- **Répondre à ses obligations externes : réglementaires, contractuelles etc,**
- **Répondre à ses obligations internes : suivie de l'entreprise, risque d'image, risque de perte de marché etc.**

➢ **L'audit du PCA s'inscrit dans le cadre de la NEP 315 et la NEP 570.**

Le PCA (Plan de Continuité d'Activité)

Le référentiel documentaire attendu :

1. **Politique Sécurité des Systèmes d'Information (PSSI) :**

- Règles pour maintenir le SI à un certain niveau de sécurité.

2. **Plan de Continuité d'Activité qui s'inscrit dans le PSSI :**

- Inclut le Plan de Reprise d'Activité,
- Inclut le Plan de Reprise Informatique.

3. **Charte informatique :**

- Règles d'usage pour préciser les responsabilités des utilisateurs.

4. **En cas d'externalisation, rapport ISAE 3402 du prestataire externe.**

Le PCA (Plan de Continuité d'Activité)

La démarche d'élaboration d'un PCA :

1. Définir les objectifs et les activités essentielles,
2. Déterminer les attentes de sécurité pour tenir les objectifs,
3. Identifier, analyser, évaluer et traiter les risques,
4. Définir la stratégie de continuité d'activité,
5. Mettre en œuvre et assurer l'appropriation.

Conclusion

La fonction « exploitation des systèmes » est essentielle pour la pérennité des entreprises auditées.

L'audit de la fonction exploitation : une véritable valeur ajoutée pour la mission du commissaire aux comptes.

Des recommandations utiles pour la survie des entreprises auditées.

7. LES CYBER-ATTAQUES

Caractéristiques

La cybercriminalité en France :

- **Le coût moyen d'une fraude est de 2,7 M$. Le cout médian est de 150 K$,**
- **La cybercriminalité est quasiment la fraude la plus reportée en France (53 %) à seulement trois points du détournement d'actifs (56 %) alors qu'elle ne représente que 32 % dans le monde,**
- **Les entreprises françaises subissent en moyenne 21 incidents de cyber-sécurité par jour !**
- **Les pertes liées aux incidents de cyber-sécurité sont estimées à 3,7 milliards de dollars en France pour 2015.**

Sources :

- ACFE, Report to the Nations on Occupational Fraud and Abuse 2016
- PwC, Global Economic Crime Survey 2016

Caractéristiques

2 types d'infractions :

- **Les formes traditionnelles de criminalité liées aux infractions informatiques : escroqueries, usurpations d'identité, fausses cartes de paiement etc,**

- **L'atteinte à la confidentialité, l'intégrité et la disponibilité des données et des systèmes : accès illégal, interception illégale de messages, atteinte à la propriété intellectuelle etc.**

2 vecteurs de cyber-attaque :

- **L'attaque technique par le canal Internet,**
- **L'ingénierie sociale.**

➢ **La cybercriminalité a toutes les caractéristiques de la fraude telle que définie dans la NEP 240.**

4 familles de cyber-attaques

4 grandes familles d'attaques techniques :

- La diffusion via Internet de programmes malveillants,
- Les attaques techniques par messagerie,
- Les attaques sur le réseau,
- Les attaques sur les mots de passe.

Principales failles exploitées par les attaques techniques :

- La gestion incorrecte de l'authentification et du contrôle d'accès,
- L'injection de données,
- Le manque de cloisonnement des applications informatiques.

L'ingénierie sociale

Failles exploitées par l'ingénierie sociale :

- Facilité d'accès aux informations décrivant l'organisation de l'entreprise,
- Facilité d'accès aux informations personnelles via les réseaux sociaux,
- Utilisation par les collaborateurs de technologies non sécurisées,
- Complexité des organisations,
- Nomadisme professionnel et télétravail,
- Manque d'exemplarité des dirigeants,
- Manque de contrôle interne et de formations associées.

Les bonnes pratiques

1. Sauvegardes régulières,
2. Mise à jour des logiciels, notamment des systèmes et des anti-virus,
3. Choix de mots de passe robustes : j@im€_i@€ly0n!,
4. Identification de tous les utilisateurs,
5. Formation des utilisateurs : confidentialité, mails inconnus, clés USB, etc,
6. Contrôle interne notamment pour l'accès aux moyens de paiement,
7. Protection des données lors des déplacements,
8. Sécurité de l'accès wifi au système de production.

Conclusion

La cyber sécurité concerne toutes les entreprises quelque soit leur taille.

Du bon sens et quelques questions permettent de se faire une première opinion…

… et de renforcer la valeur ajoutée perçue du commissaire aux comptes.

- **La cyber sécurité constitue une opportunité pour la profession.**