IFECMAG

LE MAGAZINE DE LA PROFESSION COMPTABLE

1ER TRIMESTRE 2023

DOSSIER

JAMAIS SANS MON EXPERT

LA CYBER SÉCURITÉ

#75

PROTECTION SOCIALE
RETRAITE
ÉPARGNE DE L'ENTREPRENEUR

"Avec le conseil de votre expert-comptable."

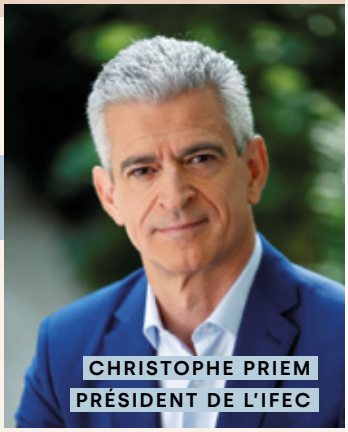
aprei

AGISSONS POUR L'ENTREPRENEURIAT INDIVIDUEL

Créée en 1994 par la Profession Comptable, l'association compte plus de 12 000 adhérents. Elle a pour vocation de promouvoir l'entrepreneuriat individuel et de mettre en oeuvre des solutions de protection sociale et de placements, en faveur du chef d'entreprise, conseillées par les experts-comptables.

Pour toute information : contact@aprei.fr - Tél : 01 42 56 83 07
APREI - 139, rue du Faubourg Saint Honoré - 75008 PARIS

LE MOT DU PRÉSIDENT



CHRISTOPHE PRIEM
PRÉSIDENT DE L'IFEC

L'année 2023 a démarré sur les chapeaux de roues pour toutes nos consœurs et tous nos confrères, dans un contexte dit de « post-crise sanitaire » mais aussi de crise économique avec l'inflation, notamment en matière d'énergie. Cette crise met à rude épreuve les trésoreries de nombreux clients qui ont déjà pour certains leurs PGE à rembourser mais aussi leurs prêts courants.

Nous, professionnels du chiffre, demeurons à leurs côtés pour les accompagner dans leurs démarches. Parmi ces démarches, il y en a bien une dont nous aimerions nous passer, c'est l'utilisation du Guichet unique en lieu et place d'Infogreffe, alors qu'il fonctionnait très bien. Cette démarche est devenue chronophage et souvent stérile. Vous êtes nombreux à avoir signé notre pétition pour le retour d'Infogreffe et expliqué en commentaires tous les dysfonctionnements que vous avez pu subir.

L'IFEC n'a de cesse de dénoncer ces dysfonctionnements et de demander une réhabilitation complète d'Infogreffe au Gouvernement, comme vous pourrez le lire dans l'article dédié à ce sujet.

Un autre fait marquant : la représentation de notre profession au sein du Conseil National de l'Ordre des Experts-Comptables. Nos candidats à l'élection 2024 de la présidence du CNOEC s'expriment dans une tribune pour donner le ton de nos objectifs, nos choix, nos priorités quant aux actions du CNOEC, pour éviter sa mise sous tutelle.

Je vous invite donc à découvrir ce numéro 75 de l'IFEC MAG, avec sa nouvelle maquette. Vous y trouverez les rubriques habituelles, nos actions phares comme le tour de France des régions sur la facture électronique et un dossier dédié à la CYBER SECURITE.

L'IFEC reste plus que jamais à vos côtés pour vous informer, vous former, vous aider dans vos démarches et vous défendre !

Je remercie tous les contributeurs à ce numéro.

Je souhaite à tous une excellente période fiscale et je vous donne rendez-vous à notre prochain Congrès à Lyon les 22 & 23 juin prochains à la Cité Internationale. Ce Congrès aura pour ambition d'aborder « L'Ecosystème du cabinet : vers une révolution ! ».

Une caisse à l'image de la profession

solide

Anticipation et rigueur sont les piliers de la profession et ceux de la gestion d'une caisse qui a su multiplier ses réserves en propriété par 12 en l'espace de 30 ans.

Cavec

IFEC MAG #75

DOSSIER • DOSSIER • DOSSIER • DOSSIER • DOSSIER

DOSSIER • DOSSIER • DOSSIER • DOSSIER • DOSSIER

21

LA CYBER SÉCURITÉ

JAMAIS SANS MON EXPERT

IFEC MAG est édité par l'Institut Français des Experts-Comptables et des Commissaires aux Comptes
139, rue du Faubourg Saint-Honoré 75008 Paris

Tél. 01 42 56 49 67

E-mail ifec@ifec.fr

Site internet www.ifec.fr

Directeur de la publication Christophe Priem

Rédacteur en chef Grégory Blin

Responsable des publications Florence Davoust

Direction artistique Bureau Jany

Conception et réalisation Gaëlle Tissier

Photos IFEC, Freepik, Aurélie Coudière, Jean-Christophe Marmara

Impression Groupe Morault

ISSN N° 2109-196X

Merci à l'ensemble des contributeurs de ce numéro.

Damien CHARRIER
Porte-parole IFEC au Conseil National
de l'Ordre des Experts-Comptables

Florent BURTIN

L'IFEC ne mettra pas le CNOEC sous tutelle

Chères Consœurs, chers Confrères,

Devant les nombreuses interrogations que nous entendons sur le terrain, nous souhaitons vous apporter un éclairage sur nos motivations et nos choix quant à l'élection de Cécile de SAINT MICHEL en tant que nouvelle Présidente du CNOEC et nos priorités pour la mandature des deux ans à venir.

Le 21 décembre 2022, lors de sa 437ème session, le Conseil National de l'Ordre des Experts-Comptables a procédé à l'élection de son Président. Deux candidats ECF se sont alors déclarés, Jean-Luc FLABEAU et Cécile de SAINT MICHEL.

> **" Avec quelques élus ECF, le choix de l'IFEC s'est porté sur la candidate Cécile de SAINT MICHEL car nous avons été sensibles à son discours d'ouverture, de respect et à sa volonté de rompre avec les pratiques de l'ancienne gouvernance, menée par Lionel CANESI.**

Cette session a revêtu un parfum de comédie burlesque avec l'annulation irrespectueuse de dernière minute de Lionel CANESI d'un entretien avec Madame la ministre Olivia GRÉGOIRE, la démission des élus ECF puis le retour de certains pour éviter de perdre leur mandat de Président en région. Notons qu'avec cette démission collective, le risque avéré était la mise sous tutelle du CNOEC.

Ce soutien, donné à Cécile de SAINT MICHEL et à son équipe ECF par les membres de l'IFEC, n'est pas un blanc-seing et ouvre une nouvelle période de 2 ans pour le Conseil national, avec une gouvernance basée sur l'intérêt général de la profession, la transparence, la communication entre élus et l'exigence sur les projets menés. **Il s'est agi de dire non à la continuité d'une politique autocratique.**

Rappelons les manquements et les inepties de l'ancienne gouvernance, à commencer par **l'achat de l'immeuble du 4 place du Palais Bourbon** : une acquisition pour 57 M€, soit plus de 50 000 € du m² ; un financement sur 30 ans à un taux supérieur à celui autorisé lors de la session à 3,6 % (soit un coût de 80 M€); un immeuble de 1 150 m² qui ne pourra accueillir qu'environ un tiers des permanents soit 60 personnes, sans sortie organisée du bail ferme de l'immeuble actuel puisque celui-ci a été acquis avant une éventuelle négociation ; une délibération sans concertation et sans donner un accès à l'information à l'IFEC. L'IFEC n'en restera pas là et instruit ce dossier. D'ores et déjà, Cécile de SAINT MICHEL nous a ouvert l'accès à la documentation sur l'acquisition de l'immeuble.

L'investissement dans la société d'investissement Drakarys, avec un flou orchestré sur la campagne de levée de fonds, la gouvernance, la gestion, les bénéficiaires et l'indépendance numérique promise.

Un exercice vertical et centralisé du pouvoir au CNOEC, avec à la clé une confiscation systématique de tous les débats sur les décisions stratégiques pour la profession hors des sessions du Conseil national ; une attaque frontale menée par le CNOEC envers plusieurs Conseils régionaux compromettant ainsi leur présence de terrain construite sur le long terme avec l'écosystème sur les sujets de formation et d'attractivité ; une augmentation de 100 € par confrère des cotisations du Conseil national proposée à l'ordre du jour reçu la veille de la date du vote. Ce qui revient à lever un impôt de 2,3 M€ en une journée.

Une insuffisance d'anticipation et d'efficience du CNOEC dans des projets stratégiques, tel que celui du Guichet unique, géré par l'INPI, qui désorganise nos cabinets et bloque nos clients. Notons que le CNOEC participe au comité de pilotage du Guichet unique.

Les élus IFEC assument leur participation à cette nouvelle gouvernance. Deux élus IFEC sont actuellement Vice-présidents du CNOEC. Nous participons également à la gouvernance de commissions désignée par la session extraordinaire du 2 février 2023. Nous sommes en position minoritaire au Comex du CNOEC et à la Commission permanente.

L'objectif des élus IFEC est simple : permettre à votre institution d'agir efficacement en rétablissant un fonctionnement efficace et démocratique.

Il nous paraît, à ce stade, important de vous préciser qu'aujourd'hui seul Lionel CANESI par sa prise de parole claire et intelligible, lors de la session du 21 décembre 2022, est considéré comme démissionnaire du Conseil national. Il a toutefois, par les textes qui régissent la profession, le droit de participer à toutes ses sessions en sa qualité d'ancien Président. Lionel CANESI a annoncé en session qu'il mènera une action juridique pour faire reconnaitre l'annulation de sa démission du 21 décembre.

L'objectif de ces différentes manœuvres est clairement affiché : mettre à défaut le Conseil national, avec pour conséquence une mise sous tutelle du Commissaire du Gouvernement, et provoquer des élections anticipées, l'intérêt personnel primant sur l'intérêt collectif.

Cette position irresponsable a confirmé la volonté des élus IFEC de s'impliquer dans le fonctionnement du CNOEC pour les deux années à venir, tout en laissant la majorité de la gouvernance, de l'impulsion des projets à l'équipe ECF de Cécile de SAINT MICHEL.

Cette gouvernance sera marquée de notre part par le sens des responsabilités et le rejet de toute démagogie. Il importe de dédramatiser les évènements du vote interne du CNOEC pour s'atteler de toute urgence à la préparation de l'avenir de notre profession et d'écarter les intérêts personnels qui ne doivent pas prendre le pas sur la défense de nos valeurs.

Dans cette période nouvelle, ouverte lors de la session du 2 février dernier, tournons-nous vers l'avenir et mettons toutes nos forces pour défendre l'intérêt général de la profession et construire son avenir.

Nous en prenons l'engagement !

**Pendant les deux ans à venir,
les priorités des élus IFEC seront de s'assurer :**

- **Que le fonctionnement du CNOEC revienne à la normale avec l'information et le recul nécessaire à la prise de décision, en particulier sur les projets stratégiques ou engageant sur le long terme la profession ;**
- **Que les projets stratégiques soient gérés dès lors qu'ils concernent notre secteur d'activité, pour éviter le fiasco du Guichet unique. Nous pensons en priorité à la facture électronique ;**
- **Que le projet jefacture.com, lancé par la mandature IFEC de Charles-René TANDE, en cours de finalisation au sein d'ECMA, bénéficie d'une mise en place opérationnelle réussie au service de toute la profession ;**
- **Que l'attractivité de la profession et l'adéquation de la formation des futurs experts-comptables et des collaborateurs soient au niveau des attentes du marché ;**
- **Que les relations soient apaisées et constructives entre le Conseil national d'une part et les Conseils régionaux d'autre part, dans un objectif partagé d'efficacité des missions de l'Ordre auprès des consœurs, des confrères et de notre écosystème, avec une volonté affichée de respect des actions des CRO au bénéfice de la proximité, du territoire et de l'image de la profession ;**
- **Que les cotisations du Conseil national n'augmentent pas au-delà de ce qui serait nécessaire à son bon fonctionnement.**

ACTUALITÉS

Le Guichet unique : mise en péril de l'économie ?

Le Guichet électronique des formalités d'entreprises (Guichet unique) est un portail internet sécurisé, auprès duquel toute entreprise est tenue de déclarer sa création, la modification de sa situation ou la cessation de ses activités depuis le 1er janvier 2023. Il remplace notamment le service Infogreffe, jusque-là performant. L'INPI a été désigné par le gouvernement comme opérateur du Guichet unique.

Ce Guichet était en ligne depuis plusieurs mois avant son lancement officiel le 1er janvier. Des bugs sont apparus très vite et les professionnels ont lancé de nombreuses alertes sur les dysfonctionnements. L'IFEC s'est saisi du problème pour défendre les professionnels.

L'IFEC s'engage

Le 15 décembre 2022, l'IFEC adressait un courrier à Bruno Le Maire et à Olivia Grégoire pour alerter sur les dysfonctionnements.

L'IFEC a parallèlement lancé une large consultation par le biais d'une pétition auprès de ses consœurs et confrères mais aussi des professions concernées par l'utilisation du Guichet unique, avec l'objectif de faire prendre conscience au gouvernement de la nécessité d'une réelle simplification administrative pour soutenir la croissance des entreprises et l'économie nationale.

À peine quelques jours après le lancement officiel du Guichet unique, la plateforme subissait une attaque informatique paralysant le système.

Le 10 janvier 2023, l'IFEC adressait un nouveau courrier à Bruno Le Maire et Olivia Grégoire pour dénoncer les dysfonctionnements ; L'IFEC avait alors déjà collecté 3 600 signatures sur la pétition (Experts-comptables, Avocats, Notaires, Greffiers du Tribunal de Commerce, Entrepreneurs, Organisations patronales et autres mandataires) et des centaines de commentaires.

L'IFEC s'est insurgé de la réponse du ministère liant les dysfonctionnements du Guichet unique à l'attaque informatique, pour ensuite admettre que l'attaque n'était pas la seule raison.

Un livre blanc pour alerter

Le 18 janvier, l'IFEC organisait une conférence de presse en présence de Christophe PRIEM, Président national de l'IFEC, Damien CHARRIER, Vice-Président de l'IFEC, Emmanuel RASKIN, Président national d'ACE (Avocats Ensemble), Wahib DAHMANI, Président du CJEC, et Alexandre MESCHBERGER, représentant de l'ANECS. L'IFEC et l'ACE, au nom des professions concernées par le Guichet unique ont confirmé leur souhait du retour d'Infogreffe, dans son ensemble, en attendant que les dysfonctionnements du Guichet unique disparaissent.

L'IFEC a remis son Livre Blanc intégrant les commentaires des professionnels sur les dysfonctionnements à la presse mais aussi à Matignon le jour même.

> **" Fin janvier, l'IFEC avait collecté plus de 4 000 signatures sur la pétition.**

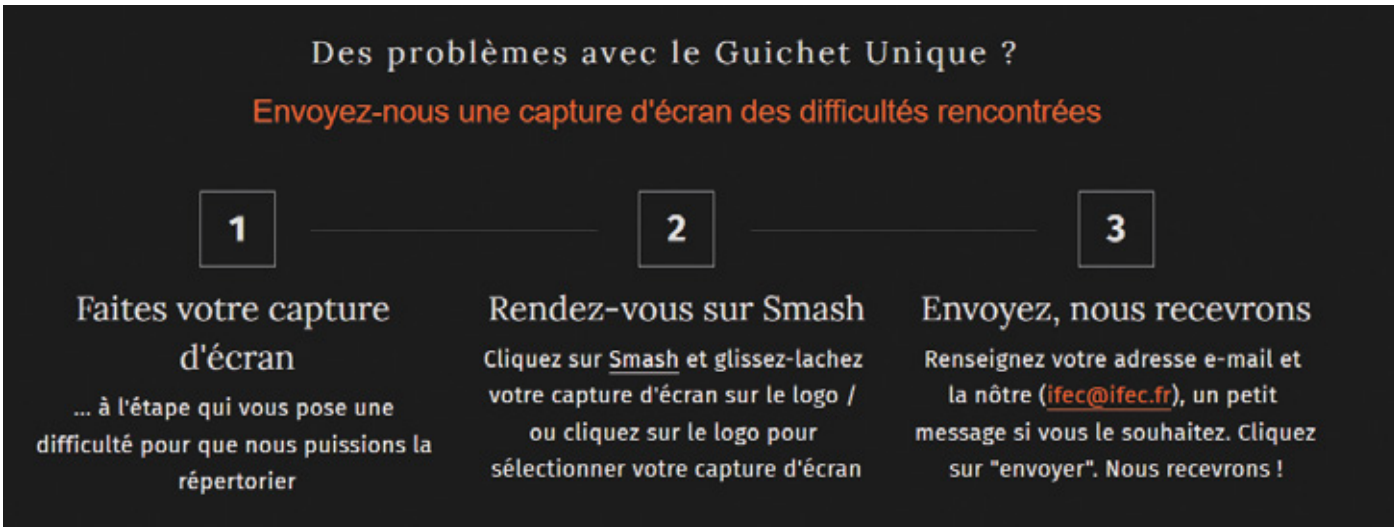
Le 9 février, l'IFEC lançait un site web "sosguichetunique.com" avec un questionnaire permettant aux utilisateurs du Guichet unique de faire part des difficultés rencontrées et d'envoyer une capture d'écran des problèmes rencontrés.

Tirer les enseignements

L'IFEC aurait souhaité que soient tirés les enseignements de la crise sanitaire pendant laquelle les Experts-comptables et les Commissaires aux comptes ont joué leur rôle de tiers de confiance.

À ce titre, la profession a exprimé le besoin d'une pérennisation de la simplification des démarches administratives engagées lors de la crise sanitaire et souhaitait que ces dernières évoluent plus encore pour accélérer la sortie de crise des entreprises.

> Force est de constater que le Guichet unique ne répond pas à cet objectif !



La relance de l'économie nécessite une mobilisation totale de l'ensemble de l'écosystème des entreprises. Les Experts-comptables et les Commissaires aux comptes sont aux côtés de leurs clients, chacun dans leur rôle, pour accompagner au mieux les entreprises dans cette période compliquée (post-covid, inflation, ...).

L'histoire a démontré qu'il était nécessaire d'effectuer des tests importants afin d'avoir la certitude que les objectifs d'efficience pourront être atteints, or les premières informations qui nous sont parvenues concernant la mise en œuvre du Guichet unique ne rentrent pas dans une logique simplificatrice des formalités des entreprises.

La décision prise par le gouvernement en 2017 de reporter l'entrée en vigueur du prélèvement à la source avait permis aux différents acteurs concernés, dont les Experts-comptables, de se préparer au mieux, et de faire ainsi de ce grand projet un succès unanimement salué.

L'accompagnement pour la relance de l'économie

Le décalage d'un an de l'échéance fixée au 1er janvier 2023 aurait été de nature à faciliter la bonne mise en œuvre de ce projet mais aussi et surtout, de permettre aux entreprises et à ceux qui les accompagnent de se concentrer sur l'essentiel : la relance de notre économie.

C'est pourquoi l'IFEC a demandé au Gouvernement de remettre en service Infogreffe tant que le Guichet unique ne fonctionnerait pas de façon optimale. Réponse négative du Gouvernement qui a remis en fonction une petite partie d'Infogreffe, en affirmant que le Guichet unique serait optimal début mars 2023.

Le 16 février, la profession apprenait qu'une partie d'Infogreffe allait rouvrir à compter de lundi 20 février ; le Gouvernement avoue ainsi que les dysfonctionnements du Guichet unique sont de nature à plomber l'activité des entreprises et donc de l'économie. Les formalités concernées sont les modifications et cessations comportant une inscription au registre du commerce et des sociétés (notamment les modifications/cessations de sociétés commerciales, artisanales et agricoles). Pour l'instant, cette réouverture est effective jusqu'au 30 juin 2023.

> Cela suppose que le Guichet unique ne sera pas opérationnel avant l'été !

Les mesures conservatoires du gouvernement ?

Un arrêté du 28 décembre 2022 relatif à la mise en œuvre d'une procédure dérogatoire destinée à assurer la continuité du service en cas de difficulté grave de fonctionnement du service informatique du Guichet unique a été publié au Journal Officiel.
Cet arrêté a pour objet de fixer les modalités de mise en œuvre de la solution technique de secours en cas de difficulté grave de réalisation des formalités d'entreprise.

Le déclenchement de la procédure technique de secours est conditionné au respect de 3 critères cumulatifs :

- Indisponibilité générale du service informatique ou blocage d'un type de formalité en particulier et ayant un caractère répétitif empêchant le dépôt des dossiers uniques (création, modification ou cessation d'activité) sur la plateforme « Guichet unique » ;
- Impossibilité de déterminer une solution alternative permettant le dépôt du dossier unique sur la plateforme « Guichet unique » ;
- Impossibilité pour l'INPI de résoudre le blocage du dépôt du dossier unique dans un délai de quinze jours à compter de la réception du signalement ou de la transmission par un membre du collège stratégique chargé d'évaluer la nécessité de déclencher la procédure de secours.

Le 16 février, le Gouvernement déclarait par communiqué de presse :
... Pour certaines formalités, la voie papier, qui constituait la majorité des formalités avant l'entrée en vigueur du Guichet unique, a été temporairement autorisée en complément de la voie dématérialisée de manière à offrir à l'usager la voie la plus adaptée à ses besoins...
... A compter du lundi 20 février 2023, avec le concours des greffiers des tribunaux de commerce, les formalités de modification et de cessation comportant une inscription au registre du commerce et des sociétés (notamment les modifications/cessations de sociétés commerciales, artisanales, agricoles) pourront être réalisées en ligne sur la plateforme www.infogreffe.fr, jusqu'au 30 juin prochain. Cette nouvelle voie d'accès pourrait concerner jusqu'à 15 % du flux total de formalités.

Les commentaires sur la pétition

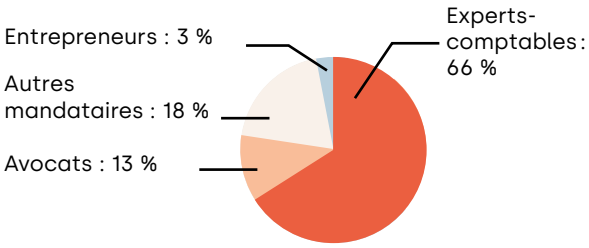
La lenteur, les erreurs, les anomalies, les bugs de saisie, les SIRET entreprises non reconnus, les adresses et les noms de communes inexistants, l'impossibilité de signer, d'obtenir un extrait Kbis, la demande de pièces inutiles, la délégation de paiement impossible, l'obligation de remplir des informations déjà transmises, des formalités non validées sans explication, une hotline indisponible, etc. : la plateforme est jugée « usine à gaz », chronophage, non adaptée, défaillante et surtout « dangereuse » en l'état pour le bon déroulement de l'activité économique.

Quelques titres de presse :

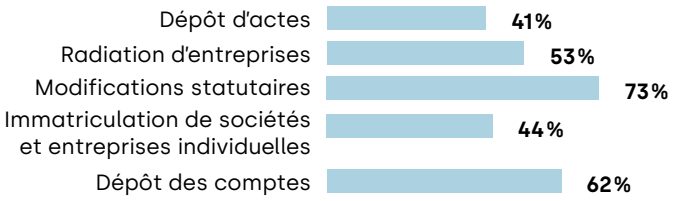
Option finance : Guichet unique : chronique d'un désastre annoncé.
Editions législatives : dysfonctionnement du Guichet unique : experts-comptables et avocats réclament la réouverture à 100 % d'infogreffe.
L'opinion : les entreprises excédées par le Guichet unique voulu par bercy.
Les nouvelles publications : Guichet unique INPI : un imbroglio prévisible aux retombées en cascade.
Le monde du chiffre : experts-comptables et avocats vent debout contre le Guichet unique.
L'usine digitale : les débuts laborieux du Guichet unique des entreprises.
Le Figaro : Guichet unique des entreprises : le gouvernement reconnaît des difficultés.
Les Affiches Parisiennes : Guichet unique : "Nous demandons de rouvrir les services d'Infogreffe".

Le site web **sosguichetunique.com** de l'IFEC a collecté entre le 9 et le 24 février 2023 : 262 réponses !

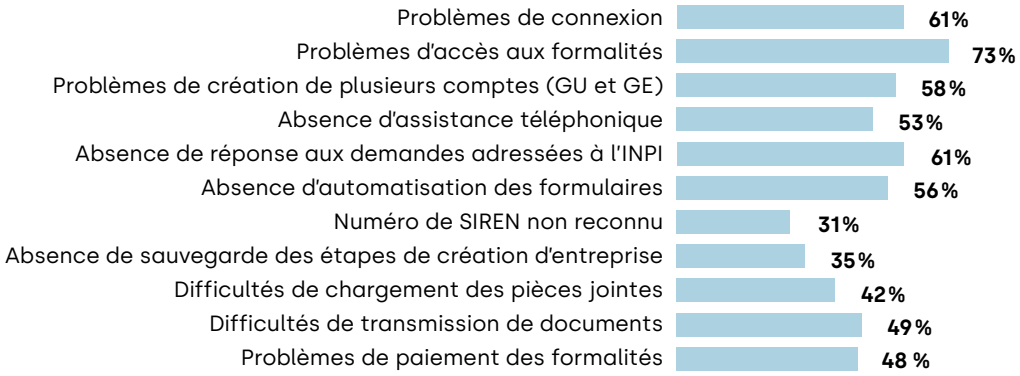
Audience



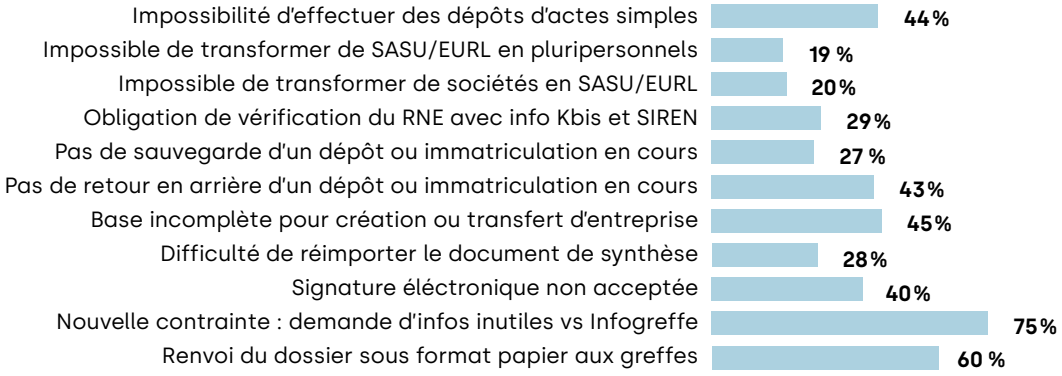
Difficulté d'achèvement des formalités



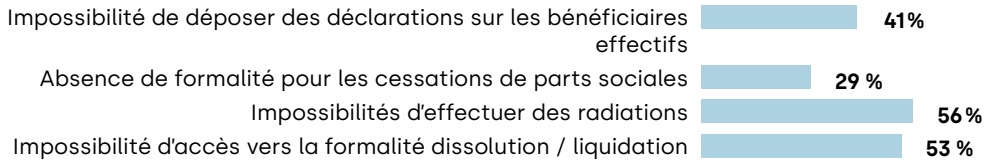
Les dysfonctionnements techniques de la plateforme



Les dysfonctionnements liés à la création / transformation de société / dépôt



Les dysfonctionnements liquidation et radiation de société / absence de formalité



L'IFEC a organisé le **8 mars 2023** un **webinaire** à destination des utilisateurs du **Guichet unique** pour faire un nouvel état des lieux des dysfonctionnements et échanger sur les pratiques.

jefacture.com

6 conseils pour réussir le déploiement de la facturation électronique

PUBLIREPORTAGE • Par Jessica POUSSART, chef de produit jefacture.com

La généralisation de la facturation électronique marquera un véritable tournant pour la profession comptable. Elle révolutionnera votre quotidien, celui de vos collaborateurs mais aussi de vos clients. Dès le 01 juillet 2024, toutes les entreprises devront être en capacité de recevoir l'ensemble des factures émises au format électronique par les grandes entreprises pour ensuite en émettre progressivement, en fonction de leur taille. Mais comment se lancer dans le projet et déployer sans embûches la facturation électronique au sein de votre cabinet et chez vos clients ? Jessica POUSSART, chef de produit jefacture.com vous livre ses 6 conseils.

1 • Anticiper pour mieux se préparer

Le passage à la facture électronique obligatoire va modifier les habitudes de travail : certains process vont évoluer et certaines tâches vont disparaitre. En fonction de votre équipement actuel, des investissements dans de nouveaux logiciels sont potentiellement à prévoir ainsi qu'une réorganisation pour accompagner vos collaborateurs vers de nouvelles missions. Votre cabinet et vos clients vont devoir s'adapter pour se mettre en conformité au 01 juillet 2024. Avec deux périodes fiscales avant l'entrée en vigueur de la réforme, le mot d'ordre est d'anticiper pour éviter le goulot d'étranglement lors des derniers mois précédant l'échéance. Prenez un temps d'avance pour mener ce projet sereinement et faites le nécessaire pour rester au cœur des flux de facturation de vos clients.

2 • Transformer les contraintes en opportunités

Nombreux sont les experts-comptables et leurs collaborateurs à être inquiets quant à l'arrivée de l'obligation et des changements qu'elle va induire. Cependant, bien loin d'être une contrainte, la généralisation de la facturation électronique est une excellente opportunité pour les entreprises françaises et d'autant plus pour les cabinets. Tout d'abord, pour repenser et optimiser les processus existants dans votre cabinet mais également chez vos clients. Ensuite, pour développer toute une panoplie de nouvelles missions telles que la facturation, la relance et le recouvrement des factures pour compte de tiers… En développant de nouvelles expertises, vous pourrez ainsi renforcer votre position de premiers conseillers des entreprises et être toujours au plus près des dirigeants.

3 • Rassurer et impliquer vos collaborateurs

La facturation électronique va apporter de réels avantages pour vos collaborateurs qui vont voir diminuer considérablement leurs tâches administratives quotidiennes : moins de saisie, moins de relances pour les pièces comptables manquantes… Malgré ces avantages évidents, vous pourrez rencontrer des réticences au changement de la part de vos collaborateurs. Rassurez-les et faites preuve de pédagogie pour leur expliquer les évolutions à venir et pour les convaincre des impacts positifs pour leur métier : l'abandon des tâches chronophages et leur montée en compétence sur des tâches à plus forte valeur ajoutée. Vos collaborateurs étant vos meilleurs alliés, impliquez-les au maximum dans ce projet d'envergure pour votre cabinet et vos clients.

4 • Dresser un état des lieux de l'existant

Avant de se lancer pleinement dans la stratégie d'accompagnement de vos clients, procédez à un état des lieux exhaustif. Qui sont les clients concernés par la réforme ? Dans quelle mesure : e-invoicing et/ou e-reporting ? Quels outils sont utilisés au sein de leur entreprise ? Quelles adaptations seront nécessaires pour se conformer aux exigences de cette nouvelle règlementation ? Si certaines entreprises se sont saisies rapidement du sujet de la facture électronique, d'autres, en revanche, ne sont pas encore suffisamment informées, ni au sujet de la réforme, ni sur l'impact que cette dernière aura sur leur quotidien. Ne tardez pas à faire ce bilan pour pouvoir définir un plan d'action et d'accompagnement adapté à chacun de vos clients.

5 • Communiquer pour faire adhérer vos clients

L'adhésion de vos clients assurera la réussite du projet. En communiquant en amont sur la réforme, ses dates clés, ses impacts mais aussi les opportunités qu'elle offrira en contrepartie, vous pourrez ainsi lever les potentiels freins et inquiétudes. Tous les moyens sont bons pour glisser ces informations : restitution de bilans, newsletters, invitations à des webinaires d'information… Usez de votre imagination, simplifiez le discours, on ne vous rapprochera jamais d'avoir trop communiqué sur le sujet ! Un autre conseil : désignez et formez un référent facture électronique au sein de votre cabinet qui sera la porte d'entrée unique pour répondre à toutes les questions des clients mais également de vos collaborateurs.

6 • S'équiper et équiper vos clients

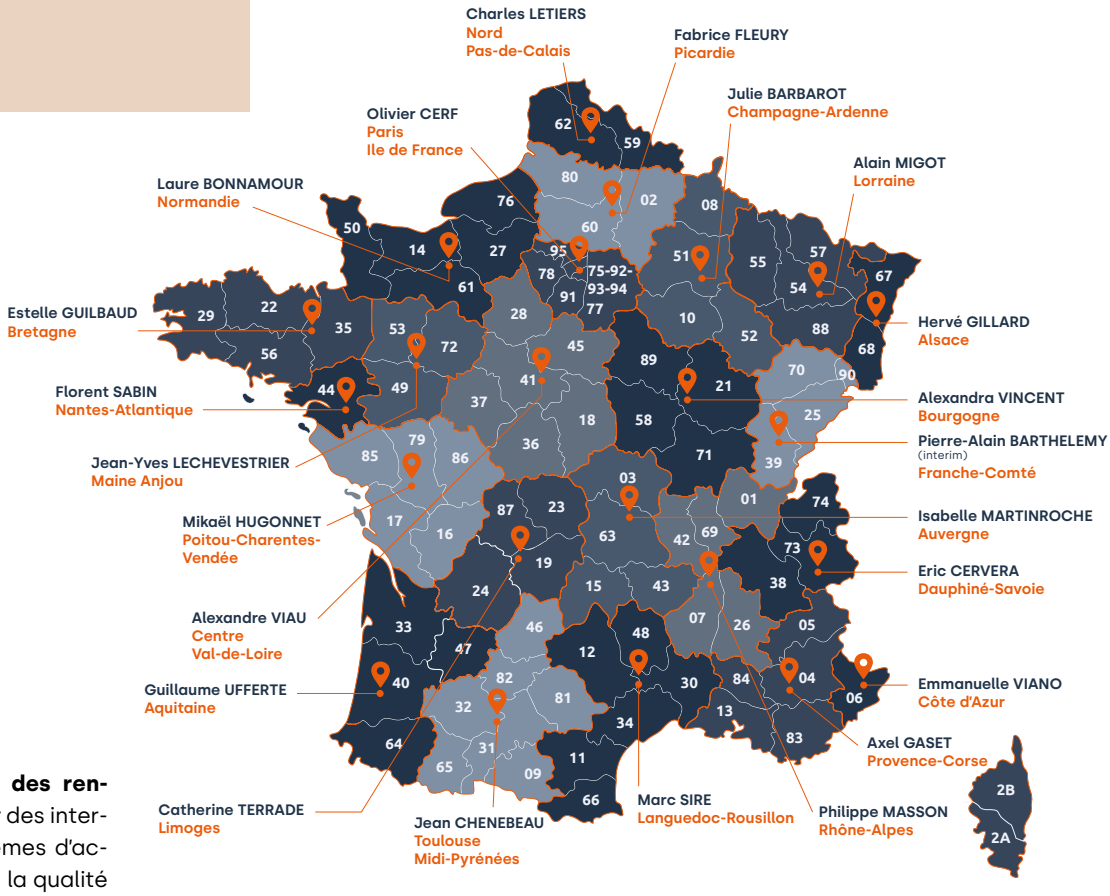
Le marché de la facture électronique fait face à l'émergence de nombreuses plateformes ayant ambition de devenir PDP. En effet, vos clients risquent de se faire démarcher par ces multiples acteurs, dont les banques. Le choix de la plateforme est donc crucial tant pour vos clients que pour votre cabinet.

Lors du choix de plateforme pour votre cabinet, vous devrez prendre en compte : sa conformité aux exigences réglementaires, sa compatibilité avec vos outils existants, sa richesse fonctionnelle et les services additionnels proposés.
Pour vos clients, assurez-vous que la plateforme que vous allez recommander vous garantira de rester au cœur de leurs flux de facturation et vous permettra une récupération fluide et simple de leurs factures. A vous d'être prescripteur du meilleur choix de plateforme pour l'ensemble de vos clients, le tout dans l'intérêt de votre cabinet.

Créée par des experts-comptables pour les experts-comptables et leurs clients, jefacture.com est la plateforme de facturation électronique, future PDP de la profession.

ACTUALITÉS

La vie des sections IFEC



Les sections IFEC organisent des rencontres régionales animées par des intervenants de qualité sur des thèmes d'actualité tels que la digitalisation, la qualité de vie au travail, le télétravail, la facture électronique, la gestion de patrimoine… Autant de **sujets riches à partager entre gens du métier, à Paris comme en régions.** Mais aussi leur Assemblée Générale annuelle, des afterworks, des apéros Pacioli, des challenges karting ou voile, des week-ends de ski, pour des échanges conviviaux.

Quelques exemples

Ainsi, **la section Paris Ile-de-France** a organisé ces derniers mois des rencontres sur les actualités de la profession et des conférences sur les thèmes de la lutte anti-blanchiment, la cyber sécurité, l'investissement en immobilier ancien et les avantages fiscaux liés, les Holdings… mais aussi des apéros Pacioli à l'occasion de l'Epiphanie et de la Chandeleur.

En Normandie, la section IFEC organise des animations, des Mardis de l'IFEC sur la société holding comme outil de structuration du patrimoine privé, la protection des risques du dirigeant ou encore sur la gestion de la garde à vue.

A Toulouse, l'événement sportif annuel qui fédère la section est sans aucun doute le challenge karting du mois de septembre. Et, en coordination avec la section IFEC Aquitaine, la section IFEC Toulouse Midi-Pyrénées organise chaque année en janvier un week-end de ski à Baqueira-Béret en Espagne. Cette année, l'événement a conquis plus de 70 participants !

La section Languedoc-Roussillon a également organisé son moment de ski, à l'occasion de son séminaire Fiscalité fin janvier.

La section IFEC Champagne-Ardenne a organisé en novembre une soirée dédiée à la RSE. Au programme : comprendre les évolutions réglementaires du reporting extra-financier, l'interconnectivité entre ce dernier et le reporting financier, l'outil DIAG RSE, l'organisation de la CNCC pour accompagner les CAC dans leur transformation et le plan de formation.

Deux événements majeurs pour la section **IFEC Nantes-Atlantique**, avec les rendez-vous Experts sur les régimes matrimoniaux et le PACS en septembre et la Conviviale de Nantes en décembre.

La section IFEC Auvergne a choisi deux thèmes importants : Protéger et valoriser le capital humain par l'attractivité de sa marque employeur et comment jedataviz.com peut aider les cabinets à accompagner leurs clients.

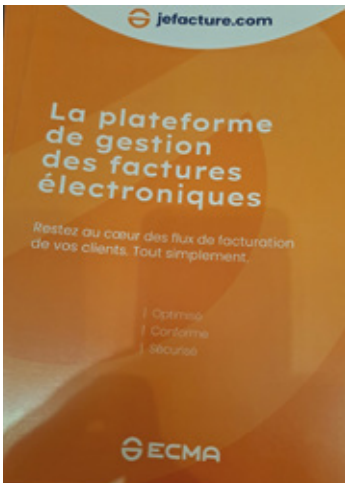
La section IFEC Nord Pas-de-Calais a, quant à elle, organisé en novembre une Matinale chez BPI Lille avec une présentation de BPI France, sa stratégie, les outils mis à dispositions des entreprises, ses interactions avec les experts-comptables... En décembre, elle organisait un Mardi de l'IFEC sur le Plan Epargne Retraite Obligatoire. Et en mars, sur l'URSSAF.

La section IFEC Provence-Corse a organisé en janvier une soirée sur le PER – Plan Epargne Retraite- qui regroupe 7 enveloppes fiscales et sociales : comment être sûr que certains de vos clients ne sont pas en excédents fiscaux ou sociaux ?

La facture électronique fait son tour de France

La facturation électronique entre les entreprises françaises assujetties à la TVA interviendra progressivement entre 2024 et 2026. Celles-ci devront se conformer à des procédures encadrées. Après le succès des webinaires sur la facture électronique pour permettre aux experts-comptables et commissaires aux comptes de tout savoir sur l'obligation de cette dernière, ECMA a décidé de poursuivre l'aventure en allant dans les sections IFEC souhaitant étoffer leurs connaissances et s'approprier l'outil JEFACTURE.COM pour aborder la période fiscale avec sérénité. Quatorze sections IFEC ont répondu présentes pour ce tour de France sur la facture électronique, du 5 janvier au 9 mars 2023. À travers une formation de 4 heures, elles ont pu aborder la méthodologie, le décryptage et un atelier de mise en pratique. La formation en présentiel était gratuite et ouverte à tous, experts-comptables et collaborateurs, adhérents IFEC ou non. Une attestation de formation est délivrée à la fin de chaque session. Rien de tel pour avoir des moments d'échanges conviviaux entre consœurs et confrères. Des centaines de professionnels du chiffre ont participé à ce tour de France !

> **"En janvier, la formation Facture Electronique a été dispensée dans les sections IFEC Picardie, Toulouse, Lorraine, Languedoc-Roussillon, Centre Val-de-Loire, Nantes-Atlantique, Paris Ile-de-France, Limoges. En février dans les sections Nord-Pas-de-Calais, Côte d'Azur, Normandie, Champagne-Ardenne et Aquitaine. Et en mars, la section IFEC Provence-Corse."**



Association loi 1901 créée à l'initiative du Conseil national de l'ordre des experts-comptables, ECMA est une structure dédiée à la production et la commercialisation des services numériques facilitant l'exercice de la profession d'expert-comptable. La plateforme de factures électroniques jefacture.com bénéficie de l'identification forte proposée par Comptexpert, le système d'authentification de l'Ordre.

IR ou IS : quelle fiscalité choisir pour la structure détenant l'immobilier locatif ?

PAR MELANIE COLLU

Directrice Ingénierie Patrimoniale
Expert & Finance

L'option à l'IS des sociétés de personnes qui ont une activité de gestion de leur propre patrimoine, telles que les SCI, est une question toujours délicate, et l'arbitrage entre IS et IR nécessite de soupeser les avantages et les inconvénients des deux régimes.

L'analyse avant le choix

Il convient de rappeler qu'une SCI ayant une activité purement civile, telle que la location d'immeubles nus, et qui n'a pas fait l'objet d'une option fiscale particulière, est dite fiscalement translucide (ou semi-transparente). Selon ce régime, le résultat fiscal de la société est calculé au niveau de celle-ci et est imposable entre les mains de chacun des associés, à hauteur de la quote-part détenue dans le capital social. Lorsque les associés sont des personnes physiques, les règles de détermination du résultat dépendent de la nature de l'activité de la société. Ainsi, en cas de location d'immeubles nus, il s'agira des règles des revenus fonciers.

L'option à l'impôt sur les sociétés peut s'avérer intéressante, ne serait-ce que par la comparaison des taux d'imposition sur les flux : 15 % en cas de bénéfice du taux réduit sur les 42 500 premiers euros de résultats (38 120 € auparavant) et 25 %, au-delà, pour le taux de droit commun vs barème de l'impôt sur le revenu, dont la tranche marginale peut atteindre 45 % en tenant compte de l'ensemble des autres revenus du foyer auxquels s'ajoutent les prélèvements sociaux au taux actuel de 17,2 % et dont on peut encore attendre une hausse de quelques points dans les années à venir. Il ne faut, par ailleurs, pas négliger la possibilité, à l'IS, de déduire du résultat fiscal les annuités d'amortissement de l'immeuble permettant d'aboutir, à terme, à des économies significatives (économies moindres en cas de cession ultérieure de l'immeuble compte tenu des modalités de calcul des plus-values IS).

> **En ne comparant que les frottements fiscaux liés à l'imposition sur le résultat, l'option pour l'IS semble évidente. Toutefois, il y a lieu de prendre en considération la fiscalité liée à la distribution des résultats de la SCI.**

En effet, dans le cas d'une SCI fiscalement translucide (IR), dès lors que l'intégralité du résultat fiscal de la société est imposée entre les mains des associés, la distribution ultérieure de ce résultat, sous quelle forme que ce soit, n'est pas imposable. Au contraire, dans le cas d'une société à l'IS, les distributions de résultats répondent à la définition fiscale des revenus distribués, quand bien même, elles n'auraient pas été effectivement payées à l'associé et seraient venues créditer un compte courant d'associé. En considérant que ces revenus sont soumis à une fiscalité de 30 % (PFU – incluant les prélèvements sociaux), le match IR /IS n'est finalement pas si simple.

Exemple chiffré

Comparatif du net en poche sur la base d'un résultat IR ou IS - 1 000 €

	IR			IS	
TAUX	30 %	41 %	45 %	15 %	25 %
IMPÔT	300	410	450	150	250
PRÉLÈVEMENTS SOCIAUX	172	172	172	0	0
NET APRÈS IMPÔT	528	418	378	850	750
DISTRIBUTION	528	418	378	850	750
PFU	0	0	0	255	255
NET PERÇU	528	418	378	595	525
NET PERÇU APRÈS CSG DÉDUCTIBLE EN N+1	548,4	445,88	408,6	595	525

Le choix de l'IS se confirme également par la recherche de la capacité d'investissement des contribuables. Ainsi, en réalisant une projection financière de l'investissement sur 30 ans, nous pouvons constater qu'à fonds propres équivalents, le montant de l'investissement en société IS peut être jusqu'à deux fois supérieur à celui d'un investissement en structure IR.

Données de l'exemple

- Fonds propres : Hypothèse de 600 000 €,
- Emprunt : Varie en fonction de la capacité de remboursement permise par le loyer net de fiscalité – Emprunt amortissable sur 20 ans au taux de 2 %,
- TMI : 41 %,
- Loyer : 5 % du prix d'acquisition avec une revalorisation de 1 % par an,
- Amortissements : Amortissement sur 30 ans de 80 % de la valeur du bien correspondant aux structures amortissables.

	IS	IR
INVESTISSEMENT	2 000 K€	920 K€
VALEUR N+30	3 622 K€	1 666 K€
LIQUIDITÉS CUMULÉES	1 242 K€	392 K€
VALORISATION GLOBALE	4 864 K€	2 058 K€
REVENU LOCATIF NET AVANT DISTRIBUTION	1 095 K€	392 K€
IMPÔT SUR LA DISTRIBUTION	30 %	-
REVENU LOCATIF NET APRÈS DISTRIBUTION	767 K€	392 K€
PRIX DE CESSION NET + LIQUIDITÉES	4 072 K€	2 058 K€
MONTANT DISPONIBLE APRÈS DISTRIBUTION	2 850 K€	2 058 K€

Une telle différence s'explique principalement par les économies liées à la méthode de détermination du résultat fiscal et à la différence de taux d'imposition, qui, combinés, permettent de bénéficier d'une capacité d'emprunt supérieure.

Par la suite, compte tenu de sa valeur de départ, le bien acquis à l'IS offre des revenus proportionnellement supérieurs à ceux qui auraient été appréhendés via structure IR.

En outre, en cas de cession suivie de la distribution du résultat de cession, les investisseurs IS pourront disposer d'un net en poche largement supérieur à celui calculé en fiscalité IR.

Si ces arguments militent en faveur d'une option IS à la création de la structure, quelle est l'opportunité d'une option IS en cours de vie sociale ?

L'intérêt d'une option IS en cours de vie est également avéré en matière d'optimisation de la fiscalité des flux. Ainsi, quelle que soit la date de création de la structure et la durée de détention des biens, dès lors que le contribuable connaît une tranche marginale d'imposition supérieure à 30 %, l'option IS permet de réaliser des économies.

À cela, vient s'ajouter une opportunité de création de valeur non négligeable dans les cas où le bien est détenu par la SCI depuis plus de 20 ans et présente une plus-value latente significative.

Dans ce contexte, les conseillers auront intérêts à étudier l'opportunité d'une option à l'IS doublée d'une revalorisation des valeurs de l'actif de la société.

Ce mécanisme, offert par le législateur à l'article 202 ter du CGI, permet d'appliquer à la plus-value de réévaluation, constatée à l'occasion du passage à l'IS, le régime des plus-values immobilières des particuliers assorties, bien entendu, des abattements pour une durée de détention.

> **En contrepartie de cette fiscalité immédiate, la SCI pourra amortir le bien sur sa valeur actuelle et sur une durée (généralement 30 à 40 ans) dont le point de départ est le premier exercice à l'IS.**

L'option à l'IS en cours de vie permettra dès lors de matérialiser la plus-value et de profiter du régime des abattements. Régime dont l'existence pourrait être remise en cause dans les années à venir, compte tenu des récents débats parlementaires et de la dernière loi de finances (débats n'ayant pas échappé aux investisseurs avertis).

Enfin, il convient de préciser que cet « écart de revalorisation », déjà fiscalisé entre les mains des associés, pourra habilement faire l'objet d'une distribution, afin de constituer des revenus complémentaires défiscalisés sur les années qui suivent celles de l'option.

Contact :
Email : mchiche@expertetfinance.fr
Tél. 06 14 22 76 39

Le service aux confrères avant tout !

PAR PHILIPPE VINCENT

Président de la CRCC de Versailles et du Centre

> **La CRCC de Versailles et du Centre est forte de la richesse économique de son territoire, des vignobles des Pays de Loire aux tours de la Défense, en passant par les plaines de la Beauce. La diversité de ce territoire offre à nos professionnels une variété de secteurs et de missions qui permet à chacun d'exprimer ses talents selon les modalités d'exercice qui l'épanouissent.**

Cette singularité pose un enjeu de cohésion, de cohérence de nos actions depuis la réforme territoriale : près de 2 400 inscrits, représentant 43 % de la base nationale d'honoraires déclarés, 56 000 mandats dont les 2/3 sont détenus par des cabinets de moins de 10 salariés (avec une forte représentation du secteur associatif), répartis sur 10 départements. Garantir un service aux confrères homogène et de proximité demeure la priorité de notre conseil pour 2023 !

Cela passe d'abord par la pérennisation d'une gouvernance représentative de toutes les sensibilités de la profession - avec notamment la pratique d'un binôme Président / Vice-Président composé d'un représentant de petits et de grands cabinets, en alternance - et de tout le territoire, avec la présence de délégués territoriaux sur Orléans et Bourges.

Notre CRCC est plus globalement engagée dans des actions de proximité, en relais des actions stratégiques fixées par la CNCC sur trois axes :

→ **1. Promouvoir** sans relâche la profession, auprès des élus de notre territoire, des acteurs économiques, des étudiants, des jeunes diplômés ; par exemple, la CRCC de Versailles et du Centre a lancé un cycle de conférences, en partenariat avec le CJEC, « Diriger une association, les bons réflexes » qui rencontre un vif succès auprès des responsables d'association et permet de mettre en avant un professionnel de la commune. Un succès qu'il convient de transformer en les déployant sur l'ensemble de notre territoire. Pour ce faire, la CRCC contacte les mairies, fournit le support, organise la manifestation avec les consœurs et les confrères qui souhaitent s'emparer du sujet. Nous continuons également à soutenir financièrement et à promouvoir les publications de l'Institut Messine, dont les travaux contribuent à nous placer, lors de nos échanges avec les élus, au cœur de la réflexion économique.

→ **2. Accompagner** nos consœurs et nos confrères dans leur montée en compétence, notamment sur les enjeux de durabilité, et le respect de leurs obligations de formation : développement et gratuité d'une formation de 7 heures sur les outils de la CNCC, prise en charge d'une journée du programme d'accréditation à venir sur la durabilité, avec tenue de sessions sur Tours, Orléans, Bourges…

→ **3. Renforcer** l'attractivité de la profession, un sujet que nous avons pris à bras le corps. La 22e édition de notre Journée pédagogique, organisée avec l'académie de Versailles, a cette année encore rassemblé près de 500 jeunes. Il est fondamental de faire découvrir nos métiers aux jeunes et de proposer à ceux qui embrassent cette filière des formations de haut niveau. D'où le partenariat avec Sup'Expertise que nous vous avons annoncé récemment. C'est un outil d'excellence au service de la formation initiale et de la formation continue des professionnels, soutenue par l'alliance des trois institutions franciliennes.

> Ce sont les clés de l'attractivité de notre profession et de la confiance apportée aux acteurs économiques.

Jamais sans mon expert

LA CYBER SÉCURITÉ

DOSSIER • DOSSIER • DOSSIER

DOSSIER • DOSSIER • DOSSIER

Christophe PRIEM
Centre Val de Loire
Président de l'IFEC

Marie-Christine LAMPERT
Paris Ile-de-France
Dirigeante Associée
Expert-comptable, L3 Conseils

Stéphane JULLIEN
Rhône-Alpes
Directeur du Système d'Information Groupe IN EXTENSO

Eric AGUILAR
Occitanie
CEO ACSF
Cyber sécurité financière numérique/fintech
Officier de réserve Gendarmerie nationale

Christophe FORET
Nord
Président C-Risk
Co-chair FAIR Institute Paris

CHRISTOPHE PRIEM
PRÉSIDENT DE L'IFEC

LE MOT DU PRÉSIDENT

Depuis l'invasion de Poutine en Ukraine, le nombre de cyberattaques a fortement décuplé. Aujourd'hui, nous sommes dans un monde fortement digitalisé et les cybermenaces sont par conséquent omniprésentes.

Pour y faire face, malheureusement, tout le monde n'est pas logé à la même enseigne. Alors que les ETI et les grands groupes sont relativement bien armés contre les cyber-risques, les TPE et PME peinent à se protéger, faute de moyens et de temps.

Les hackers l'ont bien compris et les ciblent en priorité afin de tenter d'accéder à leur système d'information ; aucune organisation n'est totalement à l'abri d'une attaque aujourd'hui.

On peut donc dire que, si la transformation numérique est source de développement et d'opportunités pour les entreprises, elle se double d'une menace grandissante pour celles-ci.

Tous les secteurs d'activité sont visés par les cyberattaques.

Le contexte du télétravail a accentué ces risques. Le télétravail a en effet mis au jour les failles de sécurité des entreprises. Les collaborateurs ont été amenés à travailler avec du matériel personnel et mal protégés, non sécurisés par VPN. Ils ont pu travailler, échanger, télécharger sans une sécurité optimale.

C'est pourquoi, l'entreprise doit repenser la mise en place des systèmes de défense pour se protéger, sachant que le premier risque à réduire est l'erreur humaine. Il faut donc savoir se préparer aux cyber risques ; c'est une étape fondamentale dans la gestion de crise.

I Des chiffres et des définitions

Eric AGUILAR
Occitanie
CEO ACSF
Cyber sécurité financière numérique/fintech
Officier de réserve Gendarmerie nationale

Plus de 4 000 cyberattaques par jour dans le monde !

Les cyberattaques constituent le nerf de la guerre numérique. On estime qu'une entreprise française sur deux est visée chaque année par une cyberattaque. **En 2022, 45 % des entreprises ont subi une attaque réussie** (dommages matériels et réputationnels) contre 54 % en 2021. Ces derniers mois, l'actualité nous a montré que tout le monde peut être touché : hôpitaux, institutions, collectivités locales, les pompiers, les groupes du CAC40 tout comme les PME et TPE.

Le paysage du « cyber espace » est en constante évolution. **La cybercriminalité,** qui comprend le vol, le détournement de fonds, le piratage et la destruction de données, **a augmenté de 600 % depuis la pandémie de COVID-19**. Avec la démocratisation du cloud et du télétravail, tous les secteurs doivent adopter de nouvelles solutions de cyber sécurité, obligeant les entreprises, les États et les institutions à adapter leurs techniques de travail pour mieux protéger leurs données.

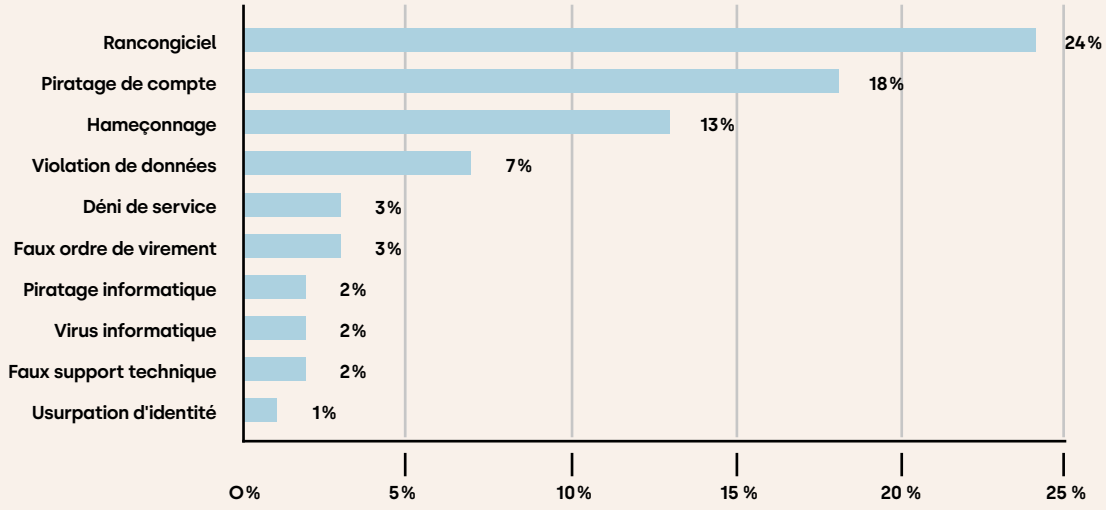
Dans son rapport annuel d'activité, le GIP ACYMA (Groupement d'Intérêt Public Action contre la Cyber malveillance) révèle une hausse importante des demandes d'assistance en ligne : **173 000 demandes en 2021** pour la plateforme cybermalveillance.gouv.fr, soit 65 % de plus que l'année 2020 (voir graphique*).

Même constat dans le rapport d'activité 2021 de la Commission nationale de l'informatique et des libertés (CNIL), **où les PME et les micro-entreprises représentaient 69 % des notifications de violations de données personnelles** liées au piratage informatique.

De son côté, l'ANSSI aura enregistré **1 082 intrusions au sein de systèmes d'informations en 2021**, soit 37 % de plus qu'en 2020.

On estime que la cybercriminalité coûtera aux entreprises du monde entier environ 10 500 milliards de dollars par an d'ici à 2025, contre 3 000 milliards de dollars en 2015, selon le rapport de Cybersecurity Ventures. La cybercriminalité représente même à ce jour le plus grand transfert de richesse économique de l'histoire, comme le précise le rapport d'AT&T.

Principales recherches d'assistance pour les entreprises et associations



Quelques définitions

- ANSSI : l'Agence Nationale de la Sécurité des Systèmes d'Information, instance officielle, accompagne les entreprises en fonction de leur profil par des actions de conseil, de politique industrielle et de réglementation afin de rendre disponibles des produits de sécurité et des services de confiance.
- Cyberattaque : Une cyberattaque désigne tout acte malveillant portant atteinte à un système IT pour des raisons d'ordre politico-économique. Vol de données, phishing, ransomware, spoofing...
- Cryptovirus : Cryptovirus ou Crytolocker est un ransomware ou rançongiciel, un logiciel pirate imaginé et conçu par des cybercriminels. Depuis 2013, ce logiciel malveillant se promène sur le Net en infiltrant les ordinateurs des utilisateurs de Microsoft ou Windows.
- DDOS : Une attaque par déni de service distribué (DDoS) est une arme de cyber sécurité visant à perturber le fonctionnement des services ou à extorquer de l'argent aux organisations ciblées.
- Hacker : Est un spécialiste informatique qui recherche les moyens de contourner les protections logicielles et matérielles.
- Malware : logiciel malveillant.
- Phishing : L'hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance.
- Rançongiciel ou Ransomware : Est un cheval de Troie qui chiffre les fichiers de l'utilisateur et prend en otage ses données personnelles afin qu'il puisse demander à leur propriétaires une somme d'argent.

II Cyber mois 2022 : faire face aux cyberattaques

Eric AGUILAR
Occitanie
CEO ACSF
Cyber sécurité financière numérique/fintech
Officier de réserve Gendarmerie nationale

« Si vous pensez que les produits de sécurité offrent à eux seuls une véritable sécurité, vous vous contentez de l'illusion de sécurité. »
Kevin MITNICK

Cybermalveillance.gouv.fr, autorité gouvernementale, a piloté avec l'ANSSI en octobre 2022 une campagne de sensibilisation aux cyberattaques.

Place au Cyber Mois 2022 !
Octobre, c'est le mois pour prendre conscience ou approfondir ses connaissances des enjeux de sécurité numérique et, ainsi, adopter les bons réflexes pour sécuriser ses usages. Nous sommes tous de plus en plus actifs dans nos vies numériques, et par conséquent, de plus en plus exposés aux cyber-risques qui ne cessent d'augmenter.

C'est l'occasion de faire un point sur les cyberattaques : **Sous quelle forme peut se manifester une cyberattaque ? Comment les éviter ?**

Qu'est-ce qu'une cyberattaque ?

> **" Une cyberattaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant.**

Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les « smartphones » ou les tablettes[1].

Les cyberattaques peuvent prendre différentes formes, parmi les plus fréquentes :

- **Le phishing**

Le phishing ou l'hameçonnage est une forme d'escroquerie. Le fraudeur se fait passer pour un organisme connu (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il envoie un mail demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment les coordonnées bancaires (numéro de compte, codes personnels, etc.)[2].

Plus récemment apparaissent les escroqueries au faux RIB, où le pirate intercepte (middle attaque) le formulaire bancaire d'un fournisseur afin de le substituer par un RIB mentionnant ses coordonnées bancaires et de tromper son client[3]. Les boites email des « deux côtés », client ou fournisseur peuvent avoir été piratées !

Si des identifiants peuvent être récupérés grâce au phishing, certains hackers utilisent des méthodes nettement plus simples : ils testent les mots de passe les plus logiques par rapport au compte. Prénoms, dates de naissance, de mariage, adresse... Ils essayent des dizaines de combinaisons jusqu'à tomber sur la bonne. Pour éviter cela, il faut choisir des mots de passe compliqués, et ne pas hésiter à jeter un œil sur le site qui indique si le mot de passe a été piraté.

- **Le Faux Ordre de Virement (FOVI)**

L'escroquerie aux faux ordres de virement (FOVI) est un type d'arnaque qui, par persuasion, menaces ou pressions diverses, vise à amener la victime à réaliser un virement de fonds non planifié. Parfois présenté comme émanant d'un dirigeant et ayant un caractère « urgent et confidentiel », on parle alors « d'arnaque au Président », communément.

1. https://www.gouvernement.fr/risques/risques-cyber
2. https://www.cnil.fr/fr/cnil-direct/question/le-phishing-cest-quoi
3.https://www.cybermalveillance.gouv.fr/medias/2021/01/Faux-Ordres-De-Virement.pdf

Une variante consiste à usurper l'identité d'un fournisseur pour communiquer de nouvelles coordonnées bancaires (changement de RIB) sur lesquelles il faut effectuer un règlement.

Une autre variante consiste à usurper l'identité d'un chargé de clientèle bancaire pour valider une opération en attente de paiement, (divulgation mot de passe et login), ou bien d'un salarié pour demander le changement des coordonnées bancaires où virer son salaire. Le compte bancaire appartenant à l'escroc est souvent situé à l'étranger, en Europe où par la suite les sommes détournées rebondiront aussitôt sur des comptes Asiatiques.

Cette catégorie d'escroquerie est généralement réalisée par téléphone et systématiquement confirmées par email. Elle concerne tous les types d'organisation[4].

- **Le piratage informatique**

Le piratage informatique ou atteinte au STAD, (système de traitement automatisé des données), consiste à s'introduire, sans autorisation, dans une ressource comme un ordinateur, un serveur, un réseau, un service en ligne ou un téléphone mobile, ou tout autre objet connecté. L'objectif du pirate informatique est de prendre le contrôle de la ressource et/ou de dérober des informations dans le but d'en faire un usage malveillant.

En pratique, le piratage informatique peut prendre deux formes principales : le piratage d'un compte ou le piratage d'un équipement[5].

Pour les hackers, il est facile de créer un réseau wifi public, gratuit et sans mot de passe, en usurpant le nom d'un réseau connu (café, galerie commerçante...). Les utilisateurs qui vont vouloir s'y connecter sont cependant en danger, car les pirates pourront se servir de ce lien informatique pour voler leurs données numériques. Afin de se protéger contre les faux réseaux wifi, il faut s'assurer de la fiabilité du réseau... Il ne faut jamais installer de mise à jour en utilisant un réseau wifi inconnu, et encore moins d'acheter des produits.

- **Les attaques par logiciel malveillant**

Un logiciel malveillant, malware en anglais, est un programme ou un code créé dans le but de causer des dommages à un serveur, à un réseau ou à un ordinateur. Il s'introduit en douce dans un système informatique, de sorte que lorsque l'utilisateur s'aperçoit que son système est infecté, des données ont généralement déjà été compromises[6].

Par exemple, un cheval de Troie informatique ou Trojan est un programme d'apparence inoffensive, mais qui contient un logiciel malveillant installé par l'utilisateur lui-même, ignorant qu'il fait pénétrer un intrus malveillant sur son ordinateur.

- **Les rançongiciels**

L'attaque par rançongiciel, ransomware en anglais, désigne une cyberattaque qui bloque l'accès à l'appareil ou à des fichiers en les chiffrant et réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

Les chiffres démontrent en effet un intérêt décroissant des cybercriminels pour les particuliers, jugés sans doute moins solvables, tandis que les rançongiciels constituent la première cybermenace chez les professionnels, avec une hausse de plus de 95 % en 2021[7].

Deux types de ransomwares co-existent : ceux qui relèvent de l'espionnage et de la vente de données sur le dark, (origine criminalité organisée, étatique) à forte rançon et ceux qui relèvent d'opportunisme, de robots, ou d'organisations criminelles, uniquement destinés à récupérer une rançon « résiduelle » pour déchiffrer les fichiers compromis.

> **L'usage de la cryptomonnaie est exclusivement dédié à ces fins.**

4.https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/escroquerie-faux-ordres-virement-fovi

5.https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/quels-sont-les-differents-types-de-piratage-informatique

6.https://www.crowdstrike.fr/cybersecurity-101/malware/

7.https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybersecurite-les-cybermalveillances-les-plus-frequentes

Comment éviter les cyberattaques ?

Dans un contexte d'industrialisation et de professionnalisation de la cybercriminalité, le droit est une arme essentielle pour renforcer la stratégie de sécurisation de ses actifs. Il est nécessaire d'être précautionneux et de rester vigilant en ligne. Il existe de nombreuses choses à faire, en amont, ou ne pas faire, pour se protéger de ces attaques.

A FAIRE POUR LES ENTREPRISES

- **Protéger et valoriser votre actif informationnel**
  - Audit et diagnostic (identifier les données stratégiques et sensibles ; identifier les partenaires clés et les sources de risques commerciaux et juridiques…),
  - Compliance RGPD (sécuriser la licéité et la disponibilité de vos bases de données…),
  - Secret des affaires (cartographie et protection défensive de votre patrimoine immatériel…).

- **Sécuriser vos contrats du numérique**
  - Sous-traitance (rédiger, négocier, et mettre en place vos accords de sous-traitance…),
  - Conditions générales (maintenance dynamique de vos conditions générales…),
  - Accords d'échanges de données (encadrer et valoriser vos échanges de données…),
  - Responsabilité des partenaires (négocier, rédiger des clauses de responsabilité des prestataire…).

- **Définir une PSSI (Politique de Sécurité du Système d'Information)**

- **Souscrire une assurance cyber-risques**

A FAIRE POUR LES PARTICULIERS

- **Activer votre filtre anti-spam**
- **Télécharger un logiciel anti-virus**
- **Installer l'authentification à deux facteurs**
- **Survoler l'URL avant de cliquer**
- **Chercher les fautes d'orthographe et de grammaire**

A NE PAS FAIRE

- **Cliquer sur des téléchargements inconnus**
- **Répondre à des appels ou des emails d'expéditeurs inconnus**
- **Dévoiler vos informations personnelles à des sources inconnues**
- **Utiliser le même mot de passe pour se connecter à plusieurs comptes différents**
- **Se servir d'un ordinateur professionnel à des fins personnelles, confusion des boites emails, aller sur les réseaux sociaux, télécharger des fichiers ou applications diverses…**

Que faire en cas de cyberattaque ?

Si vous pensez être victime d'une cyberattaque, quel qu'en soit le type, voici quelques conseils à adopter :

Premiers réflexes :

- **Déconnectez immédiatement les équipements suspects du réseau et les éteindre**, en retirant le câble réseau ou en déconnectant le Wi-Fi, afin d'éviter la propagation de l'attaque.
- **Laissez les équipements suspects allumés, uniquement en cas de ransomware et sur le poste récepteur du message de compromission demandant la rançon, n'essayez pas de les modifier** afin de préserver les éléments techniques nécessaires à la compréhension de l'incident puis éventuellement à l'enquête.
- **Ne connectez aucun autre appareil** sur le réseau.
- **Gardez les preuves de l'attaque** (messages reçus, machines touchées, journaux de connexions…).
- **Contactez immédiatement le service informatique ou le prestaire informatique,** pour qu'il puisse déclencher la mise en place d'un dispositif adéquat de gestion de l'incident.

Piloter la crise (si vous êtes responsable) :

- **Déposez plainte** avant toute action de remédiation en fournissant toutes les preuves en votre possession.
- **Mettez en place une cellule de crise** pour gérer les conséquences de la cyberattaque et coordonner les actions.
- **Tenez un registre** des évènements et des actions réalisées pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.
- **Avertissez la CNIL dans les 72h**, si des données à caractère personnel ont été consultées, modifiées ou détruites. En cas de risque élevé pour les données, vous devez également notifier les personnes concernées.
- Si vous êtes un opérateur d'importance vitale, **prévenez l'ANSSI dans les meilleurs délais.**
- **Mettez en place des solutions de secours** pour pouvoir continuer d'assurer les services indispensables : activez vos plans de continuité et de reprise d'activité (PRA/PCA) si vous en disposez.
- **Préparez une stratégie de communication** adaptée au sujet afin d'informer avec le juste niveau de transparence vos administrés, agents, partenaires, fournisseurs…

Sortir de la crise :

- **Faites une remise en service progressive et contrôlée** après vous être assuré que le système attaqué a été corrigé de ses vulnérabilités et en surveillant son fonctionnement pour pouvoir détecter toute nouvelle attaque.
- **Tirez les conclusions, les enseignements pour améliorer la sécurité** après une intrusion et définissez les plans d'action et d'investissements techniques, organisationnels, contractuels, financiers, humains à réaliser pour pouvoir éviter, ou a minima, pouvoir mieux gérer l'éventuelle prochaine crise.

III Des exemples d'attaques

Eric AGUILAR
Occitanie
CEO ACSF
Cyber sécurité financière numérique/fintech
Officier de réserve Gendarmerie nationale

Des exemples d'attaques relayés par la presse...

Une attaque de grande ampleur

SEPTEO, un groupe de 2 400 personnes, spécialisé dans le logiciel pour les notaires, les avocats, les SIRH et l'immobilier (12 millions d'utilisateurs) a été victime d'une cyberattaque en janvier 2023. Des experts techniques et d'investigation indépendants ont été mobilisés. « Nos investigations continuent et Notamail reste perturbé mais les indicateurs de ce matin sont positifs » déclarait le dirigeant début février.

Des hackers pro-russes

Les attaques par déni de service distribué (DDoS) reprennent du poil de l'ours, en ce début d'année 2023. Les groupes de hackers pro-russes inquiètent de nombreux pays à la suite de cyberattaques à l'encontre de ministères, hôpitaux et banques.

> **Depuis le 1er janvier 2023, plus d'une centaine de cyberattaques de type DDoS ont été détectées, lancées par des groupes de pirates pro-russes plus ou moins organisés. Parmi les « team » les plus virulentes, hors le groupe nationaliste Killnet, présenté par ZATAZ* au lancement du conflit entre la Russie, l'ours NoName057.**

Depuis le 1er janvier, ZATAZ a repéré des dizaines d'attaques contre la Lituanie, l'Italie, la Pologne, l'Estonie, le Danemark, la République Tchèque, l'Ukraine, l'Allemagne.

Des élections ciblées

Des cyberattaques qui se veulent politiques. Par exemple, plusieurs sites internet tchèques ont été visés le premier jour du scrutin du second tour des élections présidentielles. Les sites Internet du candidat à la présidence Petr Pavel et du ministère tchèque des Affaires étrangères se sont retrouvés bloqués sous les coups de NoName057.

Hôpitaux compris

Pour rappel, un DDoS a pour mission de rendre inutilisable un service informatique en le noyant de fausses connexions. Imaginez un camion de poubelle venir déverser ses détritus devant vos portes et fenêtres. Plus personne ne peut sortir, ni entrer, dans le logement. Killnet a utilisé cette méthode à l'encontre de sites web appartenant à des hôpitaux américains, forçant le ministère américain de la Santé et des Services sociaux à publier une alerte avertissant les établissements de santé des tactiques du groupe pirate.

> **" Il est probable que des groupes ou des opérateurs de rançongiciels pro-russes, tels que ceux du défunt groupe Conti, répondront à l'appel de Killnet et apporteront leur soutien. Cela entraînera probablement que les entités ciblées par Killnet seront également touchées par des ransomwares ou des attaques DDoS comme moyen d'extorsion, une tactique que plusieurs groupes de ransomwares ont utilisée ».**

Acheter des DDoS

Les autorités agissent, mais les malveillants trouvent toujours, pour le moment, les ressources pour leurs actions. En décembre 2022, le ministère de la Justice saisissait, avec l'aide d'autorités judiciaires de par le monde, 48 sites (6 noms de domaine principaux) utilisés par des vendeurs de services DDoS. Des sites web qui permettent aux utilisateurs d'acheter des minutes de DDoS afin d'inonder de fausses connections leurs cibles.

> **Les américains avouaient que « cette mesure d'application de la loi » pouvait n'avoir que très peu d'impact sur des groupes tels que Killnet « qui a transformé son service DDoS à louer en une opération hacktiviste ».**

Le Danemark victime des DDoS

Il y a quelques semaines, le Danemark a annoncé relever son niveau d'alerte cyber à la suite de cyberattaques contre des banques et le ministère de la Défense du pays.

> **" Nous élevons à nouveau le niveau de menace contre le Danemark, entre autres sur la base du niveau élevé d'activité des groupes de pirates informatiques pro-russes contre les pays de l'OTAN, y compris le Danemark » annonce le Centre danois pour la recherche cyber sécurité sur Twitter.**

Un pays précurseur dans le 100 % numérique. La digitalisation par défaut : santé, impôts, Etc. Ce qui n'empêche pas les DDoS ou encore les infiltrations de type ransomware comme après l'attaque à l'encontre de DSB, équivalent de la SNCF, le 29 octobre 2022. Une cyberattaque ayant paralysé le trafic ferroviaire.

Les DDoS utilisées comme couverture

Bien que les attaques DDoS ne causent généralement pas de dommages majeurs ou durables, elles peuvent provoquer des interruptions de service qui s'étendent sur plusieurs heures, voire plusieurs jours. Akamai a publié un rapport révélant que les incidents DDoS en Europe avaient augmenté de 73 % en 2022, avec davantage de campagnes impliquant désormais des tactiques d'extorsion. Ils ont averti que les attaques DDoS sont désormais de plus en plus utilisées comme couverture pour de véritables intrusions impliquant des ransomwares et des vols de données.

La santé touchée

Le groupe Ramsay invite le personnel administratif de ses cliniques à ne plus toucher l'informatique jusqu'à nouvel ordre à la suite de la découverte d'une anomalie ! Plusieurs établissements de santé du groupe Ramsay (Toulouse, Bourg-en-Bresse) tournent au ralenti, le temps de contrôler des anomalies informatiques découvertes. « Des anomalies ont été détectées sur certains serveurs informatiques et nous soupçonnons une tentative d'intrusion extérieure confirme le service presse à ZATAZ. Par mesure de sécurité pour protéger les patients, employés et partenaires, la procédure de sécurité a été immédiatement déclenchée, à savoir la fermeture des accès extérieurs. Nous avons immédiatement informé nos partenaires et les autorités sanitaires et mobilisé des experts techniques et d'investigation indépendants, et l'enquête que nous avons menée avec eux n'a révélé aucun vol de données ni aucun cas de propagation de l'incident à nos patients. » Voilà qui est rassurant. Action, réaction.

Arnaque à la Sécu

En juin 2022, ce fut un envoi massif de SMS demandant « la mise à jour de la carte vitale », par un pirate informatique inconnu, à destination de centaines de milliers de français. Derrière ce phishing qui pourrait sembler classique, il s'agissait d'une cyberattaque massive à l'encontre des hexagonaux.

> **Ce pirate informatique a lancé sa malveillance informatique de Russie. Son SMS est propre, efficace, rapide : « Assurance Maladie : Renouvellement obligatoire de votre Carte Vitale à effectuer avant le 10/06/2022. Rendez-vous immédiatement sur : assurance-maladie[.]com ».**

Jusqu'ici, rien de particulier. Quand vous sélectionnez, sans cliquer, sur l'url proposé, une page d'erreur. Seulement, le format et le support exploité, les smartphones, permettent bien des manipulations. Quand vous cliquez sur l'adresse web présente dans le message, redirection vers la page usurpatrice. Sur téléphone portable cela passe en douceur, sans faire apparaitre la moindre trace de malversation. Autant dire que 99 % des gens pourront tomber dans le piège. D'autant plus que l'internaute arrivera sur une page sans faute, aux couleurs, logo et url ressemblant comme deux gouttes d'eau à l'assurance maladie : [ameli]carte-vitale.com.

De la suite dans les idées

Le black hat a des moyens, du temps et de la suite dans les idées. Il ne s'est pas contenté d'AMELI. Il s'est organisé pour viser une dizaine d'entreprises officiant sur le territoire hexagonal. Le pirate a lancé des cyberattaques aux couleurs de la Banque Populaire, Caisse d'Epargne, Netflix, FNAC, ...

> **Une motivation qui peut s'expliquer par la recherche massive de données et d'un besoin important de liquidité pour des pirates qui souffrent, aussi, du conflit entre la Russie et l'Ukraine.**

Les collectivités locales pas épargnées

Une cyberattaque contre la région Normandie s'ajoute à une longue liste de collectivités territoriales touchées par les pirates en 2022. **L'impact de cette opération est conséquent puisque 600 serveurs et 1 500 ordinateurs ont été arrêtés.** Compte tenu de leur impact, les attaques contre les régions et les départements sont plus médiatisés, les données de millions d'habitants peuvent être prises en otage et divulguées sur les forums de hackers. De plus en plus d'organismes publics sont touchés par des cyberattaques.

Un ransomware déjoué aux USA

Après une opération secrète de plusieurs mois, le ministère américain de la Justice (DOJ) et ses partenaires internationaux (en Allemagne, aux Pays-Bas et en France) ont mis hors d'état de nuire un réseau international de ransomware connu sous le nom de Hive. Depuis 2021, le groupe de ransomware Hive a ciblé plus de 1 500 victimes à travers le monde, obtenant plus de 100 millions de dollars en paiements de rançon de la part d'hôpitaux, d'écoles, ou encore de sociétés financières. Les autorités ont désorganisé le groupe de ransomware Hive en infiltrant ses réseaux informatiques et en saisissant ses clés de déchiffrement.

*ZATAZ : est un site web français d'information traitant principalement de la délinquance informatique.

Témoignage d'une cyberattaque au cabinet L3 Conseils

Marie-Christine LAMPERT
Paris Ile-de-France
Dirigeante Associée
Expert-comptable, L3 Conseils

Le cabinet L3 Conseils est une petite structure de 8 personnes qui intervient dans le conseil et l'accompagnement de petites et moyennes entreprises de tous secteurs avec une bonne connaissance du milieu audiovisuel. L3 Conseils compte environ 300 clients ; elle a subi une cyberattaque par cryptovirus dans la nuit du 23 au 24 mai 2019.

« L'attaque est survenue heureusement juste après nos bilans et le traitement de la TVA du mois d'avril. C'était miraculeux si on peut dire...

Pour rappeler le contexte, on avait classiquement un serveur de production qui hébergeait également la messagerie, un seul site, une sauvegarde sur un NAS avec une réplication au domicile via une liaison internet. Le prestataire informatique est un ami et le contour de la mission n'était pas vraiment formalisé.

Le 24 mai au matin, nous avons constaté en arrivant au bureau que nous n'avions plus accès à rien (la connexion à distance était également inactive depuis 7h du matin). Les fichiers étaient cryptés ; un visuel de tête de mort apparaissait à l'ouverture des fichiers sur tous les postes. Nous avons vite compris ce qui arrivait et avons rapidement constaté l'ampleur du désastre ; presque toutes les sauvegardes avaient été chiffrées. Le premier réflexe a été de tout débrancher d'internet.

Un message nous invitait à contacter le pirate dans le « darkweb » mais cela ne nous tentait pas... !

Nous n'avons jamais su si les données avaient été aspirées. Nous étions en tous cas paralysés. La seule partie non cryptée était la base bureautique contenant les dossiers annuels et les dossiers permanents. La messagerie était bloquée mais heureusement, nous avions les contacts dans les téléphones.

Nous avons très rapidement mis en place un mail de secours et envoyé un message d'attente à nos clients.

L'assurance groupe, contactée, nous a mis en contact très vite avec une cellule spécialisée d'experts en cyberattaque. Nous avons déposé plainte (sans grand espoir) et averti la CNIL. Les experts ont alors fait un état des lieux précis afin de savoir notamment combien de clés de chiffrement avaient été utilisées et si le ransomware était connu.

Au bout de deux jours, nous savions qu'il n'y avait rien à faire si ce n'est de payer la rançon. Il fallait donc discuter avec le pirate, il n'a pas répondu pendant une semaine. Une semaine difficile car nous étions dans l'incertitude et à l'arrêt complet. Les paies de mai n'ont pas pu être faites, nous avons demandé aux clients de verser des acomptes à leurs salariés.

Le pirate a enfin répondu en demandant 15 000 € en bitcoins pour nous débloquer. Il faut 2 semaines pour ouvrir un wallet permettant de payer en bitcoins mais le cabinet spécialisé en possédait un et a donc payé le pirate à notre place (rançon payée par virement par nous en attendant de connaitre la position de l'assurance).

Une fois la somme visible sur son portefeuille virtuel, le pirate a envoyé des clés de déchiffrement. Elles ont d'abord été testées par les experts puis déployées sur notre serveur et tout a été décrypté en quelques heures au bout de 15 jours !

Sur le plan humain, cette expérience a été un bon test de cohésion d'équipe et nos clients ont tous été compréhensifs.

Sur le plan technique, ce fut une leçon : nous ne pouvons pas espérer éviter les attaques mais nous savons que le meilleur moyen est de réfléchir en amont à comment réagir quand cela se produit.

L'expérience nous a tous rendus méfiants et conscients de la vulnérabilité des systèmes. Nous sensibilisons maintenant nos clients régulièrement. Aujourd'hui, nous n'avons plus de serveur, nous utilisons le cloud et systématiquement la double authentification, tout en veillant bien à la qualité de nos sauvegardes ».

Fallait-il vraiment payer ?

Le cabinet n'avait pas vraiment le choix. Mais il peut arriver qu'il y ait une sur-attaque. Un virus peut rester sourd plusieurs mois. Il est important de faire une sauvegarde de la sauvegarde. La mise en place de la double authentification est un bon réflexe.

www.l3conseils.fr

Témoignage d'une cyberattaque au cabinet In Extenso

Stéphane JULLIEN
Rhône-Alpes
Directeur du Système d'Information
Groupe IN EXTENSO

Ignorer le risque n'est pas une option

Sur le plan IT, In Extenso est sur une architecture complexe gérée de manière centralisée et orientée volumétrie et flux de données avec environ 1 500 serveurs à l'échelle du groupe, 700 lignes réseaux et 6 000 unités de bureautique. En tant que profession réglementée, la protection de la donnée est un sujet fondamental au niveau de notre activité.
Avant la cyberattaque, il est bon de préciser que In Extenso est certifié ISO27001, que nous sommes équipés d'un outil contre la fuite de données et que nous avons un management de la sécurité avec un ensemble d'outils de protection et de supervision.

Tout commence par un coup de fil...

En avril 2021, je reçois un appel, un dimanche à 1 h du matin, c'est la supervision de notre infrastructure qui m'informe que toute notre activité est à l'arrêt du fait d'une attaque ; nous sommes entièrement cryptolockés. Une fois la stupeur passée, il est temps de dérouler le process de gestion de crise que nous avons anticipé. Une réunion est organisée le dimanche matin avec la direction générale et les parties prenantes pour constater et prendre les premières décisions fondamentales lors d'un incident de ce type.

Un premier constat

Nous avons été attaqués par un groupe russe de cybercriminalité qui demande une rançon. Il est important de savoir que dans ce cadre nous avons affaire à une organisation internationale qui fonctionne comme une entreprise avec un ROI sur les attaques et par conséquent des moyens considérables et une sophistication des techniques d'attaques.

> **"La première question qui ressort est « devons-nous payer ? ».**

Cette question se traduit en fait par un constat simple : avons-nous des sauvegardes, sont-elles cryptées et avons-nous une stratégie de restauration qui permette de rétablir les services essentiels ? Les pirates, lorsqu'ils lancent une attaque comme celle-ci sont dans votre système depuis plusieurs mois ; la stratégie qui consiste à restaurer votre système au jour précédent l'attaque est inefficace car votre sauvegarde embarque les outils des pirates. Nous avions délocalisé nos sauvegardes en dehors de notre SI. Par conséquent, il est décidé lors de cette première réunion de ne pas payer et de nous relever de cette attaque par nous-mêmes.

> **"La deuxième question qui ressort est « Combien de temps cela va durer ? ».**

Cette question est très délicate et varie d'une entreprise à l'autre. Il faut savoir qu'en moyenne la remédiation d'un tel évènement prend plusieurs mois ; il est nécessaire de se concentrer sur les services essentiels de l'entreprise afin de ne pas pénaliser le business, la feuille de route est rapidement tracée.

La remédiation

La stratégie est simple : nous couper du monde, considérer que tout élément du SI est corrompu, même ce qui ne le semble pas à première analyse, remettre à blanc l'intégralité du système d'information, en reconstruire un plus sécurisé et réinjecter uniquement les données métier des sauvegardes et enfin rétablir progressivement le service.
Derrière cette simple phrase se cache une complexité importante, **les points fondamentaux à retenir sont :**
La communication doit être gérée finement ; une organisation est mise en place ; la communication est gérée par la direction générale avec des points journaliers avec le DSI ; personne d'autre ne communique à l'extérieur ni ne communique avec les équipes.
C'est un projet, par conséquent et au vu des enjeux, l'approximation n'a pas sa place, celui-ci doit être géré dans les règles de l'art. Tout doit être tracé. Tout doit être vérifié. Tout doit être maîtrisé.
Une trentaine de partenaires, des équipes opérationnelles 24/24, une gestion de projet avec plus de 3 000 lignes d'opérations tracées, un process cadré, mécanique et organisé nous ont permis de revenir à une situation business opérationnelle en moins d'un mois. Aucune fuite de données n'a été constatée et nous avons drastiquement élevé nos exigences en termes de sécurité, que ce soit en interne comme pour nos partenaires externes.

De la menace à l'opportunité

Cet événement nous a permis de prendre conscience qu'il existe différents niveaux dans les cybermenaces. Bien évidement nous avons révisé notre système de management de la sécurité, nos process internes ainsi que nos outils. La sensibilisation de l'ensemble des collaborateurs aux problématiques de sécurité a été renforcée et nous pouvons dire à la suite de cet événement que la protection cyber des actifs de l'entreprise ainsi que ceux de nos clients fait vraiment partie de l'ADN du groupe. Toutes les mesures de sécurité peuvent être vues comme un dogme de la DSI à l'échelle du groupe par certains mais elles sont nécessaires et intransigeantes, on a toujours le niveau de sécurité du maillon le plus faible.

Nous avons subi une nouvelle attaque du même groupe en août 2021, cette fois-ci sans succès, malgré la violence de l'attaque (20 000 tentatives de connexions étrangères à l'heure pendant 3 jours), les pirates ont été détectés instantanément et notre système a tenu le choc.

En conclusion, il faut se poser les bonnes questions

Ayez les bonnes questions. La question n'est pas de savoir si ça va arriver, mais quand. **Il faut se demander « que vais-je faire une fois que mon système sera corrompu ? ». C'est la seule question qui compte vraiment.**

Prévoyez la crise, rejouez le scénario avant. Ayez une démarche proactive. Qui communique ? Ai-je les bons partenaires ? Qui appeler en cas de besoin et surtout comment ? Quelles sont les stratégies de retour à la normale ? Lors d'une attaque, le stress, les enjeux, vous n'aurez pas les idées claires et ça ne sera plus le moment de vous demander ce qu'il faut faire. Surtout choisissez avant le bon partenaire opérationnel qui saura vous conseiller et vous accompagner. Si vous n'avez pas les ressources internes pour gérer les problématiques de sécurité, externalisez l'activité et prenez un SOC (Security Operation Center).

Investir dans une stratégie Cyber peut être très couteux ; mettez vos investissements dans un système de sauvegarde fiable et sécurisé en premier lieu ; faites un audit de vos sauvegardes et de la protection de celles-ci.

Prenez une assurance Cyber spécialisée. De la même manière, une remédiation peut être couteuse, choisissez un contrat d'assurance pour vous faire accompagner sur ce type de sinistre.

En ce qui concerne notre stratégie actuelle, elle est sur deux volets : d'une part la protection et d'autre part la capacité au travers de l'automatisation de réduire le temps de reconstitution et remédiation d'une attaque à une semaine. La sensibilisation et formation est aussi un élément central et notre système d'information est testé plusieurs fois par an au travers de tests techniques (pentest) mais aussi de tests de phishing pour l'ensemble des collaborateurs.

L'uniformisation de votre système d'information, de vos actifs IT, la gestion perpétuelle de vos mises à jour sont un élément clé. La gestion des droits d'accès et de « qui a accès à quoi » doivent être maîtrisés, l'idéal étant de limiter au maximum les privilèges.

Ne soyez pas naïfs, les cyberattaques sont un risque et comme tout risque il se gère, sa probabilité, son impact sont très élevés. Par conséquent, ignorer ce risque n'est pas une option et fonder la protection des actifs et des services essentiels d'une entreprise sur la chance n'en n'est pas une non plus.

In Extenso réalise des services à destination des TPE-PME, tant dans les domaines de l'expertise comptable que dans les domaines liés à la gestion et à l'accompagnement du chef d'entreprise.

Notre groupe propose un service professionnel complet, à tous les stades de la vie de l'entreprise et sur l'ensemble des domaines liés à la gestion de l'activité de nos clients : comptabilité, fiscalité, gestion, juridique, conseil social et paies, gestion du patrimoine du dirigeant, conseil en innovation-croissance, transmission d'entreprise.

In Extenso est l'interlocuteur privilégié de plus de 120 000 clients appartenant à tous les secteurs d'activité et a réalisé en 2022 un chiffre d'affaires de 500 millions d'euros.

In Extenso est un groupe avec plus de 5 500 collaborateurs répartis sur 250 agences.

I Cyber risques, cyber sécurité et gouvernance

Christophe FORET
Nord
Président C-Risk
Co-chair FAIR Institute Paris

La cyber sécurité et les cyber risques sont devenus des thèmes récurrents et centraux de nos conversations, et nous pensons tous parler des mêmes choses. Mais est-ce vraiment toujours le cas ?

La Cyber Sécurité

La cyber sécurité fait référence à l'ensemble des activités, des méthodes et des solutions permettant d'assurer la sécurité des systèmes informatiques – et des informations qu'ils contiennent. Elle est ainsi un ensemble de réponses aux risques cyber.

> **Le plus grand problème avec la communication c'est l'illusion qu'elle ait eu lieu.**
> George Bernard Shaw

Au fur et à mesure de la digitalisation de nos économies et nos sociétés au cours de la dernière décennie (>60 % du PIB mondial digitalisé fin 2025[1]), la cyber sécurité est devenue un des tous premiers postes budgétaires de la direction informatique puisqu'elle représente jusque plus de 10 % du budget informatique.

Apparemment à juste titre lorsqu'on rapproche ces investissements de la place qu'occupent les risques cyber dans les classements des risques opérationnels. Ainsi, le baromètre des risques de Allianz[2], celui du World Economic Forum[3] et beaucoup d'autres, classent, depuis plusieurs années, le risque cyber parmi les trois ou quatre risques opérationnels les plus importants.

Les Risques Cyber

Puisque ce sont les risques cyber qui légitiment les investissements en sécurité informatique, définissons de quoi on parle. Le Larousse définit le risque comme étant « la possibilité, la probabilité d'un fait, d'un évènement considéré comme un mal ou un dommage ». Singulièrement, le monde de l'entreprise a élargi cette définition et ISO 31000 définit le risque comme étant : "l'effet de l'incertitude sur les objectifs" et laisse ainsi la possibilité de conséquences préjudiciables… ou bénéfiques.

Dans le secteur informatique, la norme ISO/IEC Guide 73 précise que c'est « la possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et cause ainsi un préjudice à l'organisation. Il est mesuré en termes de combinaison de la probabilité d'occurrence d'un événement et de ses conséquences. »

Ces imprécisions sémantiques sont loin d'être anodines car on parle de risque en pensant alternativement aux vulnérabilités, aux menaces, aux vecteurs d'attaques ou encore aux impacts redoutés sur la disponibilité, la confidentialité ou l'intégrité des systèmes d'informations et les données.

Cyber risque : Toute **atteinte**, volontaire ou non à la **confidentialité, l'intégrité ou la disponibilité** des **données** numériques ou du **système** d'information.

MENACE	impacte →	**ACTIF**	résultant en →	**SINISTRE**
Cybercriminels, Acteurs des Etats-nations, Script Kiddies, Nature, Personnel, Clientèle, Tierces parties, etc…		Données, Site web, Applications, Réseau, Serveur etc…		Atteinte à la **C**onfidentialité Perte d'**I**ntégrité des données Pannes/in**D**isponibilité

1. WEF 2019 & International Monetary Fund 2020, 2. Allianz Risk Barometer 2022, 3. WEF Global Risks report 2023

La Gouvernance des risques cyber et de la sécurité de l'information

On voit bien que le risque cyber mérite une définition plus précise. Initialement technologique, il ne peut plus être considéré seulement comme une problématique technique mais bien comme un véritable risque métier. Après avoir été géré principalement par les experts sécurité du département informatique, c'est un sujet dont les fonctions métiers et régaliennes de l'entreprises doivent s'emparer avec l'aide des experts informatiques et de la cyber sécurité pour comprendre quels sont ces risques en les liants aux actifs métiers (données, applications, processus industriels, propriété intellectuelle, ...) les plus essentiels au bon fonctionnement de l'entreprise.

Il existe de nombreux frameworks et méthodes pour conduire un programme de sécurité des SI et/ou gérer les risques – NIST, ISO31000 et 27005, EBIOS RM, ... Mais la plupart sont destinées à des populations d'experts et ne s'adressent donc pas aux responsables métiers. Ils restent génériques et pas prescriptifs quant à la mise en œuvre de ce qu'ils préconisent. Or la gestion des risques pour répondre correctement à l'exigence de la gouvernance de la sécurité informatique doit justement éclairer, assister la prise de décision.

Les entreprises ont donc jusqu'à présent utilisé des approches essentiellement qualitatives qui reposent sur l'expérience et le savoir-faire des experts et des cartographies haut/moyen/bas ou rouge/orange/vert pour classifier les risques. Les démarches pour prioriser les investissements en cyber sécurité sont guidées par la conformité et les bonnes pratiques qui sont certes nécessaires mais pas suffisantes – des études du Gartner montrent ainsi que de lourds investissements n'apportent pas forcément un gain important en termes d'amélioration de la sécurité, faute d'avoir investi là où cela était réellement nécessaire[4].

Pour efficacement décider des priorités sur lesquelles l'entreprise doit porter ses efforts, toutes les fonctions métiers, IT et infosec doivent parler le même langage afin de se comprendre et comparer puis choisir ensemble les solutions de sécurité les plus adaptées. L'approche qualitative et les avis divergents des experts ne suffisent pas. Il faut un modèle détaillé et robuste qui permette de mesurer et classifier les scenarios de risques entre eux, dans le contexte de l'entreprise (activités, géographie, business model, nature des données collectées et traitées, ...). Sur cette base objective et quantifiable, l'entreprise pourra sélectionner les contrôles et solutions de sécurité qui réduiront le plus l'exposition aux cyber risques.

Le rôle des professions du chiffre dans la gestion des risques cyber

Dans toutes les entreprises mais en particulier celles de taille intermédiaire et les PME, les experts-comptables ont un rôle à jouer dans cette identification des actifs critiques et des risques associés. En effet, ils ont une bonne connaissance des chaines de valeur, c'est-à-dire de la manière dont l'entreprise produit sa proposition de valeur. Ils ont la connaissance, d'un point de vue financier, des actifs, y compris ceux intangibles dont une partie croissante est sous une forme digitale et donc exposée en premier chef aux risques cyber.

> Enfin, c'est précisément un des rôles des experts-comptables et des commissaires aux comptes que de rendre compte des résultats économiques et financiers de l'entreprise et d'identifier, puis évidement de quantifier, les risques et incertitudes qui pèsent sur l'atteinte de ces résultats.

4. https://www.gartner.com/en/newsroom/press-releases/2016-12-09-gartner-says-many-organizations-falsely-equate-it-security-spending-with-maturity

La quantification des risques cyber

Christophe FORET
Nord
Président C-Risk
Co-chair FAIR Institute Paris

Le standard FAIR™ (Factor Analysis for Information Risk) explique comment analyser et exprimer les risques en termes métiers et, lorsque c'est nécessaire, quantifier financièrement les scénarios de risques cyber et opérationnels.

Analyser et exprimer les scénarios de risques

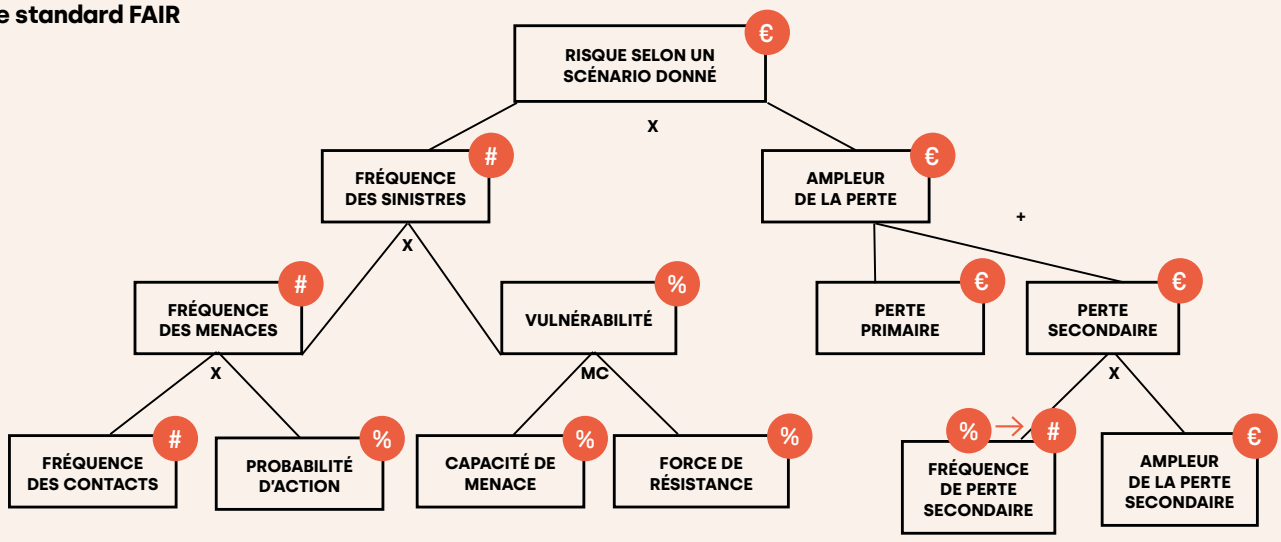
Pour analyser et exprimer les scénarios de risques, le standard FAIR propose une ontologie qui est une série de définitions de termes décrivant également les liens entre ces termes et les concepts sous-jacents. Elle est plus complète et détaillée que celles qu'on trouve dans les standards déjà mentionnés.

L'ontologie permet d'articuler les scénarios de risques de manière précise, en les liant aux enjeux métiers. La précision du modèle FAIR permet d'éviter de confondre, comme dans beaucoup de registres de risques, des menaces, des actifs, des conclusions d'audit, des inquiétudes, des contrôles, ... qui sont souvent des composantes du risque mais pas un risque en eux-mêmes. Par ailleurs, en les reliant aux enjeux et processus métiers, on évite de poser des questions qui n'ont pas de réponse ou qui sont trop génériques pour être pertinentes pour l'organisation.

Quantification financière des scénarios de risques

Le standard FAIR se base sur l'utilisation des statistiques et des probabilités pour quantifier certains scenarios. C'est la robustesse de la modélisation de l'ontologie qui permet ainsi d'utiliser ces deux branches des mathématiques que sont les statistiques et les probabilités, qui constituent les sciences de l'aléatoire.

Le standard FAIR



Lorsque cela est nécessaire pour une prise de décision entre plusieurs solutions de sécurité, la quantification se fait grâce à la décomposition en variables de la probabilité d'occurrence d'une part et de l'importance de l'impact, d'autre part.

A chacune de ces variables sont associées des plages de valeurs. Ces plages de valeurs sont obtenues auprès des fonctions IT, infosec et métiers de l'entreprise, ou, lorsqu'elles ne sont pas disponibles (par exemple lors de l'analyse de scenarios de risque pas encore rencontrés), elles peuvent être estimées grâce à des techniques de décomposition et de calibration .

Ces plages de valeurs servent ensuite d'échantillonnage aux simulations Monte-Carlo qui produisent des montants de pertes potentielles et les probabilités associées

FAIR aide ainsi le management à prendre des décisions éclairées en matière de réponse aux cyber risques en leur apportant une meilleure visibilité et compréhension que les autres méthodes. Il permet de répondre aux deux questions que se posent tous les dirigeants, lorsqu'ils doivent prendre une décision :

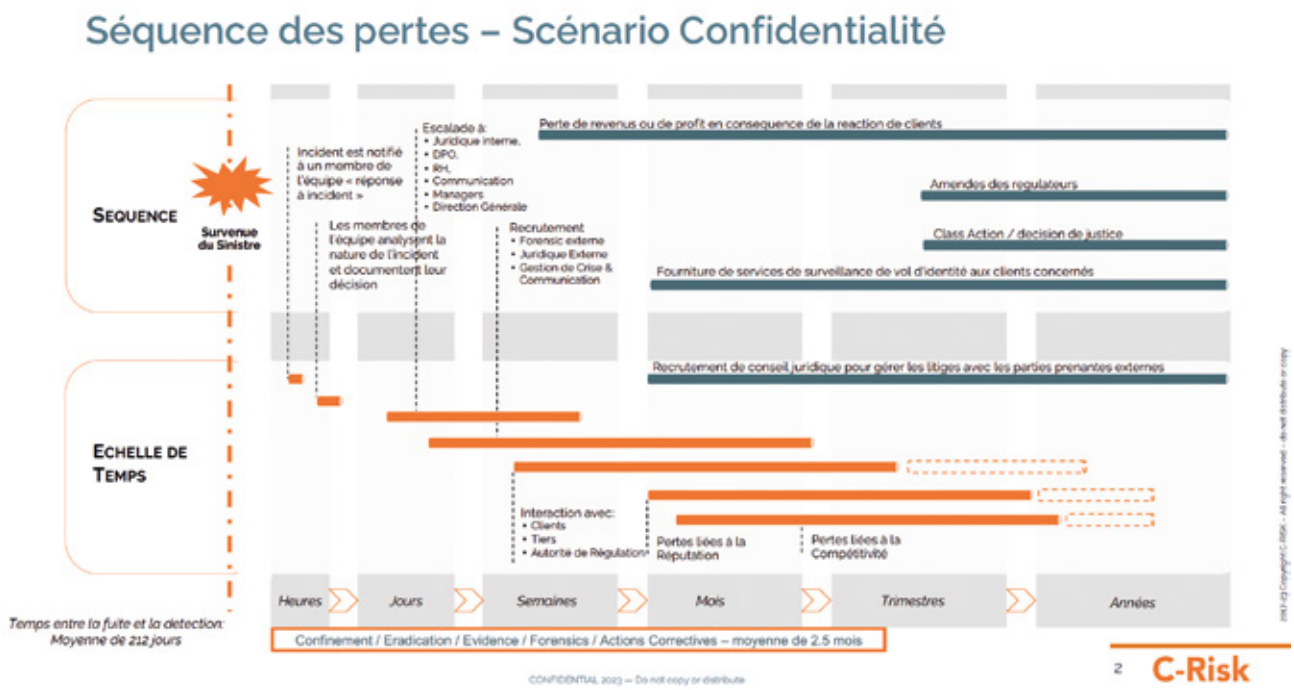
- Combien de fois un sinistre pourrait se produire dans les X prochains mois ?
- S'il se produit, combien coûtera ce sinistre ?

FAIR permet d'obtenir une vision plus globale de la sécurité de l'organisation et de répondre, pratiquement, à des questions de la direction sur des scenarios de risques précis tel que celui de la conformité au RGPD :

- Quel est mon risque global ?
- Quels sont mes risques les plus importants ? sur lesquels de mes actifs ?
- Quels investissements ont permis de réduire mes risques et de combien ?
- Entre deux solutions de mise en œuvre d'un contrôle, laquelle est la plus efficace pour réduire mon risque ?
- Quels sont les risques que l'organisation ne peut assumer et qu'il faut transférer pour être couvert par une assurance cyber ?
- Dans le contrat de cyber assurance qui nous est proposé, quelles sont les clauses d'exclusion qui sont ou non acceptables ?

La sécurisation des systèmes d'information et des actifs digitaux requièrent toujours les gestes d'hygiène cyber de base comme ceux de l'ANSSI ou les 20 contrôles du CIS. Mais prioriser les investissements ne peut plus être du seul ressort des experts de la sécurité. Toutes les fonctions de l'entreprises doivent communiquer entre elles pour articuler les risques cyber en termes métiers quantifiables et ainsi prendre les décisions stratégiques pour se protéger le plus efficacement possible.

Exemple de livrable



Projection vers le futur

Eric AGUILAR
Occitanie
CEO ACSF
Cyber sécurité financière numérique/fintech
Officier de réserve Gendarmerie nationale

L'anticipation des cybermenaces pour les prochaines années constitue l'un des plus gros chantiers menés par nos autorités gouvernementales sous l'égide de l'ANSSI.

Les cyberattaques ont été classées au cinquième rang des risques les plus importants, selon un rapport du World Economic Forum. Cette nouvelle industrie criminelle protéiforme affecte les particuliers, les institutions, les États et surtout notre tissu économique. Elle continue inlassablement de croître en 2023.

Pour les années à venir, selon un ouvrage collectif élaboré et mis en ligne par le Campus Cyber, les défis à relever dans ce domaine à horizon 2030, seront principalement axés :

- sous l'angle de l'ultra-connectivité,
- de l'ultra-cloisonnement,
- de l'ultra-green,
- ou encore de l'ultra-réglementation.

Opportunités et types d'attaques informatiques et défis à relever varient selon les tendances futures auxquelles le monde se confrontera dans les années à venir.

Dans le cas **d'un monde ultra-connecté**, par exemple, les cyberattaquants seront en mesure de cibler un éventail de cibles et d'accès sans précédent et pourront s'appuyer sur la généralisation de plateformes numériques et de réseaux sociaux pour réaliser leurs opérations malveillantes. Il faudra dans ce cas s'attendre à un recours plus large à des réseaux de bots pour lancer des attaques, une instantanéité de propagation de malwares ou encore à la multiplication de services numériques piégés et la diffusion en masse de fausses informations tous secteurs confondus.

Si la tendance **d'un monde hyper-cloisonné** prédomine, l'avenir de la cybercriminalité devrait alors passer par la recrudescence de cyber gangs spécialisés sur des cibles bien déterminées, simplifiant d'autant leur détection. « La proximité entre Etats et cybercriminels permet aux groupes d'être dotés de meilleures capacités offensives tout en bénéficiant d'impunité et de protection dans leur propre espace souverain », prévient le rapport. Dans ce contexte, on devrait alors voir monter en puissance les actions de déstabilisation sur des services critiques nationaux avec la multiplication « d'attentats numériques », le renforcement d'attaques par rançongiciels et complexes de niveau étatique, du cyber-espionnage, voire aussi de la destruction physique de certains câbles sous-marins ou de satellite et sur des chaines d'approvisionnement critiques.

Dans le cas **d'un monde dominé par les enjeux écologiques**, les cyberattaquants s'adaptent aussi bien en monétisant par exemple leurs services à des fins d'hacktivisme visant des systèmes trop énergivores mais aussi en privilégiant les actions de manipulations, d'arnaques nécessitant peu d'exploitation de ressources informatiques élevées rendues à ce stade beaucoup plus compliquées. Dans ce scénario, il faudra alors s'attendre à la prolifération d'attaques contre la réputation des personnes (morales ou physiques), la destruction de systèmes numériques trop énergivores, des attaques contre des chaines d'approvisionnement non locales ou encore l'instrumentalisation des idéologies environnementales à des fins de cyberattaques par rançongiciel, extorsion...

Enfin, dans le cadre d'un f**utur de société hyper-réglementée** « les cyberattaquants profitent de la multiplicité des régulations pour entreprendre du cyber chantage. Ils menacent de dénoncer leurs victimes aux régulateurs pour non-conformité, ou proposent de faux services de régularisation », indique le guide.

« Les investissements humains et financiers portant sur la sécurité sont délaissés au profit de ceux œuvrant uniquement à la mise en conformité réglementaire aux nouvelles exigences, dans une logique parfois idéologique et sans prise en compte des risques réels ». Avec à la clé une explosion de cyber-extorsions, la recrudescence d'attaques usurpant des autorités régulatrices, la montée en puissance de fausses amendes…

Sur cette base de scénarios évolutifs dans notre monde, les défis cyber sécurité à relever peuvent ainsi être adaptés en se focalisant sur **5 priorités communes :**

- sécuriser par défaut tous les systèmes numériques,
- redonner aux individus le contrôle de leur vie numérique et de leurs données,
- s'orienter vers une résilience à grande échelle à base d'automatisation et d'IA,
- combattre l'impunité des cybercriminels,
- développer l'attractivité de la filière cyber sécurité.

Enjeu de souveraineté nationale, la sécurité numérique commence à s'imposer parmi les administrations, entreprises et particuliers. Cependant, l'évolution des cyberattaques et le renforcement induit du contrôle de l'Etat risquent d'atteindre systématiquement nos libertés individuelles à l'horizon 2030.

Audit conseil sécurité financière et patrimoine

Avec la participation d'Eric AGUILAR, CEO ACSFP, expert en sécurité financière, proche collaborateur ayant dirigé comme Officier au sein de plusieurs Sections des recherches en Gendarmerie nationale, des enquêteurs financiers « Fintech », cyber et analystes criminels. Expert en gestion et communication de crise, sa connaissance fine de la cyber et son expérience de terrain seront des atouts précieux pour épauler vos différents services.

- Intervention dans des entreprises victimes de cyber attaque/conseil/gestion de crise,
- Formation et entraînement de dirigeants, DAF, juridiques, équipes opérationnelles, experts-comptables et CAC, avocats, officiers publics, lutte contre les cyber-risques, gestion de crise,
- Expertise croisée, fruit d'une riche expérience de terrain permettant de prévenir les risques, la fraude, le blanchiment et de pérenniser la poursuite d'activité,
- Expert en cryptoactifs, NFT, blanchiment, droit pénal des affaires.
- Expert dans le montage PCA/PRA entreprise pour crise CYBER.

E-mail : aguilar.eric@neuf.fr
Tél : + 33 (0) 6 40 37 51 67

LE RGPD
Bien plus qu'une réglementation, Un véritable atout et un levier de développement

PAR JÉRÔME BICHET

Président de LOB-Line of Business

Le Règlement général sur la protection des données personnelles (**RGPD**) est entré en vigueur **le 25 mai 2018.** Il a pour vocation d'assurer de manière concrète et absolue le respect du principe supérieur de protection de la vie privée.

Ce règlement est basé sur le principe « d'auto-responsabilité » de toutes les entreprises en vertu duquel ces dernières doivent notamment :

→ Créer et maintenir à jour un registre de leurs traitements de données personnelles ;

→ Déployer des mesures concrètes afin de garantir la protection, la maîtrise de ces données ;

→ Désigner, en fonction de leurs enjeux propres, un délégué à la protection des données personnelles (plus communément appelé « DPO » pour *Data Protection Officer*).

Le respect de ces obligations est souvent perçu comme **complexe** et parfois même comme **un obstacle** au business. C'est ce qui explique que la conformité au **RGPD** est vécue exclusivement comme une contrainte et souvent reportée car **non prioritaire.**

Or, nous constatons que cet enjeu est fortement **créateur de valeur** pour toutes les sociétés qui l'intègrent à leur quotidien mais aussi au sein de leurs valeurs essentielles d'entreprise. La conformité RGPD devient alors un réel **atout de confiance** et de **fidélité** pour :

→ les clients,
→ les partenaires commerciaux,
→ les salariés.

En faire l'impasse, c'est ne pas intégrer le « train » des nouvelles exigences sur lesquelles le monde d'aujourd'hui et de demain se construit.

Une création de valeur ajoutée importante

Le **RGPD** est un outil de modernité en ce qu'il permet de s'interroger sur des enjeux transverses au cœur du développement de chaque structure. Ces derniers dépassent le « simple » sujet de la protection des données personnelles et s'étend aussi bien aux opportunités liées aux technologies ou solutions émergentes, qu'à la définition des offres ou services.

Il faut retenir que tout est -presque- possible à condition d'assurer la mise en œuvre effective des principes de responsabilité et de transparence.

Le **RGPD** encourage les entreprises à placer au centre de leurs préoccupations la parfaite connaissance de leurs flux de données. Ce qui finalement protège et valorise d'autant plus ce patrimoine ô combien important que constituent aujourd'hui les données clients, prospects, salariés, etc.

Le **RGPD** offre aux entreprises et à leurs dirigeants une occasion formidable de s'interroger sur leurs valeurs et leurs objectifs concernant la gestion des données afin de disposer d'une vision globale sur cet enjeu clé. Il doit aussi permettre de renforcer les actions ou les mesures nécessaires pour se préserver des menaces cyber.

La bonne prise en compte du **RGPD** est donc :

→ Un gage de confiance numérique vis à vis de l'ensemble des personnes ou entreprises avec lesquelles vous interférez et qui sont de plus en plus sensibles à ce sujet.

→ Une garantie de confiance numérique vis-à-vis des cocontractants avec qui le non-respect de la réglementation peut être un motif de non reconduction, voire de résiliation du contrat.

Le **RGPD** est par conséquent un outil puissant de modernité et d'opportunité et ce quelle que soit la taille de l'entreprise. C'est un des plus grands « agitateurs communs » pour encadrer et protéger la collecte de données personnelles et ce, au bénéfice de tous (clients, salariés, ...) mais aussi de toutes les sociétés quelle que soit leur activité.

FOR-
MA-
TION

Le **RGPD** est le garant d'un nouveau principe fondamental, la **dignité digitale**, dont chacun de nous a besoin.

La prise en main de cet enjeu de protection des données n'est donc pas qu'une simple question de respect de la réglementation ou d'image.
Cette conformité est devenue un puissant attrait économique, capable de profiter aux entreprises de toute taille et de tous secteurs, y compris les PME.

Par conséquent, prendre des mesures adéquates axées sur la durabilité et l'éthique concernant les données est un élément déterminant pour les entreprises qui souhaitent se démarquer de la concurrence. Elles peuvent également, selon les critères d'analyse « ESG », développer une influence positive sur de nombreux aspects de la sphère économique de chacune d'entre elles, en particulier concernant leurs investissements et/ou leur développement.

Le risque de contrôle et de sanction

Parmi les possibilités de contrôles que peut exercer la CNIL, vient s'ajouter la procédure simplifiée. Il s'agit d'une procédure très rapide permettant de démultiplier la capacité de contrôle.

Bien que les sanctions prononcées via cette procédure ne soient pas rendues publiques, force est de constater que la typologie de sociétés ciblées par les contrôles a bien changé. En décembre 2022, ce sont aussi des médecins ou des universités qui ont été dans le viseur de la CNIL, bien loin des univers de Google ou Microsoft.

La CNIL élargit désormais ses contrôles aux structures de tailles très réduites.

Cette tendance se fait également ressentir dans les contrôles menés sur les sites internet.

Si vous n'avez pas forcément un site internet, vous avez assurément une base de données clients. Il est absolument essentiel d'appréhender les risques qui gravitent autour de ces bases de données car elles constituent le cœur de votre métier.

La conformité est un levier fort dans la prise en compte du risque Cyber

Si demain votre base de données client est inaccessible ou piratée, comment assurer la continuité d'activité ?

L'immense atout du **RGPD** réside dans sa corrélation avec les enjeux de sécurité.

La protection des données implique de respecter un certain nombre de bonnes pratiques et de mettre en place des mesures de sécurité qui améliorent le niveau de protection face aux ransomwares, aux attaques au président et autres attaques pirates et d'organiser la continuité d'activité en préparant un plan de reprise d'activité.

Il est désormais absolument incontournable de prendre à bras le corps cet enjeu aux multiples facettes et de capitaliser sur la mise en œuvre de la conformité **RGPD**.

LOB-Line of Business peut vous accompagner dans votre démarche et prendre en charge de bout en bout votre mise en conformité au **RGPD** notamment au regard de nos expertises **RGPD** et cyber et de notre solution de conformité **HotlineDPO**.

Si vous souhaitez aller plus loin dans la bonne appréhension de ces enjeux pour vos salariés ou vos clients.
Nous proposons des formations dédiées au sein de l'**IFOR**.
N'hésitez pas à vous inscrire.

CAS PRATIQUE JURIDIQUE

Les limites de la sous-traitance des activités d'expertise comptable

PAR LANDRY DUMAS

Landry Dumas est Responsable Juridique et des Affaires sociales IFEC

« La sous-traitance est une opération par laquelle une personne (le donneur d'ordre) confie à une autre (le sous-traitant), sous sa responsabilité, l'exécution de tout ou partie d'un contrat d'entreprise ».

Le délit d'exercice illégal de la profession

Dans un contexte de fortes mutations et d'intensification du paysage concurrentiel, le recours à la sous-traitance dans la profession ne relève plus de cas isolés ; et cette pratique n'est pas sans risque.

Il convient de rappeler, s'il en était besoin, que l'expertise comptable est une profession réglementée par l'Ordonnance de 1945.

Comme le prévoit l'article 2 de cette Ordonnance, certaines activités ou missions relèvent de la compétence exclusive des experts-comptables inscrits à l'Ordre.

Elles ne peuvent donc être exercées par une personne non inscrite, sous peine de délit d'exercice illégal de la profession comptable.

Le délit d'exercice illégal de la profession comptable est prévue par l'article 20 de l'Ordonnance susmentionnée, et il est caractérisé par l'interdiction faite à toute personne non inscrite à l'Ordre, d'effectuer de manière habituelle, en son nom propre et sous sa responsabilité, des travaux comptables.

L'extension du délit à la sous-traitance

Alors même que les termes de l'article 20 visent expressément les travaux comptables exécutés au nom propre et sous la responsabilité du contrevenant, la chambre criminelle de la Cour de cassation[1] a considéré que cet article devait également s'appliquer aux travaux comptables exécutés pour le compte d'un expert-comptable inscrit, sous le contrôle et la responsabilité de celui-ci.

Autrement dit, l'article 20 doit être interprété comme interdisant aussi à tout cabinet d'expertise comptable inscrit à l'Ordre de sous-traiter, à un non-expert-comptable, des activités relevant de son monopole.

> **« L'exigence prévue à l'article 20 s'attache essentiellement à la qualité de l'auteur direct des travaux exécutés ».**

Au cas particulier de la décision précitée, la Cour de cassation a retenu la condamnation d'un cabinet d'expertise comptable pour complicité d'exercice illégal.

Ce cabinet avait en effet confié à un prestataire sous-traitant, non expert-comptable, la réalisation des travaux de **saisie de comptabilité** et **d'établissement des déclarations fiscales.**

Considérant que ces activités relevaient du monopole des experts-comptables, les Hauts magistrats ont jugé qu'elles ne pouvaient être sous-traitées à une personne extérieure à la profession.

> **« La sous-traitance est possible entre experts-comptables, membres de l'Ordre, dans les conditions visées par l'article 18 du code des devoirs professionnels ».**

Les Hauts magistrats ont également relevé que le cabinet d'expertise comptable, donneur d'ordre, n'avait délégué aucun expert-comptable auprès de la société sous-traitante, et ce même occasionnellement, afin de s'assurer du respect des dispositions légales encadrant l'exercice de la profession d'expert-comptable.

Un monopole justifié par l'intérêt général

En février 2022, la chambre criminelle de la Cour de cassation[2] s'était déjà prononcée par l'intermédiaire d'une QPC (question prioritaire de constitutionna-

lité), pour atteinte à la liberté d'entreprendre, protégée par l'article 4 de la Déclaration des droits de l'homme et du citoyen de 1789.

Concrètement, il s'agissait de savoir si l'interdiction du recours par les experts-comptables à des sous-traitants non-inscrits au tableau de l'Ordre des experts-comptables, pour l'exécution de travaux comptables, porte une atteinte disproportionnée à la liberté d'entreprendre ?

> Retenant que le monopole des experts-comptables est justifié par l'intérêt général, les Hauts magistrats – après avoir relevé que l'interdiction faite aux experts-comptables, « dont l'exercice de la profession est protégé », de sous-traiter des opérations comptables à des tiers non-inscrits au tableau de l'Ordre, est « une conséquence nécessaire de la réglementation de leur activité » – jugent l'atteinte proportionnée à la liberté d'entreprendre.

Le périmètre des activités réservées

On notera la fluctuation des décisions de la Cour de cassation quant à la définition des activités relevant du monopole des experts-comptables.

Dans sa décision du 4 octobre dernier, la Cour de cassation y intègre notamment la saisie comptable. Cela ne va pas de soi dans la mesure où cette tâche, et plus généralement celle de la tenue comptable, n'est pas toujours considérée comme une activité réservée à l'expert-comptable ; comme l'illustre une décision de la chambre commerciale de la Cour de cassation[3] rendue en juin 2014.

1. Cass. Crim. n° 21-85.594 ; 4 octobre 2022
2. Cass. Crim. n° 22 février 2022 ; 21-85.594, Inédit
3. Cass. Com. n° 619 F-P+B

La CAVEC ce qui change en ce début 2023

Revalorisation de la retraite complémentaire, des indemnités journalières mais aussi augmentation des cotisations… Plusieurs valeurs ont été revues en 2023, tenant à la fois compte du contexte inflationniste et de la volonté de toujours garantir la meilleure protection aux experts-comptables et commissaires aux comptes.

L'année 2022 ayant été marquée par une inflation record, à des niveaux que nous n'avions pas connus depuis les années 1980, le Conseil d'administration a pris la décision qui lui semblait la plus juste et solidaire.

Pour soutenir les affiliés retraités, la Cavec a ainsi choisi le versement, mi-octobre, d'une aide forfaitaire de 300 euros.

> **" Nous avons décidé de ne pas attendre la réévaluation annuelle de nos retraites complémentaires, et d'enclencher un mécanisme de solidarité, en ayant recours à nos réserves, rappelle Frédéric Rogier, Président de la Cavec. Nous avons opté pour un montant fixe de 300 euros, plutôt que proportionnel, pour des raisons de solidarité avec les pensionnés aux revenus plus modestes, les plus affectés par l'inflation ».**

Valeur du point versé réévaluée à + 5,6 %

La réévaluation annuelle, entrée en vigueur en 2023, a quant à elle été calculée « sur l'inflation constatée en septembre 2022, date à laquelle nous procédons aux arbitrages de pilotage de la caisse, explique Frédéric Deknuydt, directeur de la caisse. La valeur du point de versement de retraite complémentaire a ainsi été augmentée du montant de l'inflation constaté à cette date, à savoir 5,6 %. Elle est fixée à 1,2672 euro en 2023 – contre 1,20 euro en 2022 ».

« C'est grâce à notre autonomie de gestion et à l'équilibre de notre régime que nous avons la possibilité de procéder à ces arbitrages », poursuit Frédéric Rogier.

Augmentation des cotisations de + 6,5 %

En lien immédiat, le point de cotisation est revu à la hausse et passe à 14,815 euros en 2023 – contre 13,95 euros en 2022 – soit une hausse de 6,5 %. « L'enjeu pour notre caisse est de poursuivre la baisse progressive du taux de rendement de notre régime, afin d'assurer son équilibre de long terme, et alors que nous entrons dans une période de déficit dit technique », explique Frédéric Deknuydt.

En effet, comme nous le savons tous, la génération du baby-boom part massivement à la retraite et le nombre de cotisants ne suffit pas à couvrir ces sorties. « Nous savons que nous devons baisser le taux de rendement mais nous avons décidé de le faire d'une manière douce pour nos affiliés cotisants, afin d'avoir une répartition de l'effort la plus juste possible », commente Frédéric Rogier. «Cette année, notre taux de rendement est de 8,55 % et d'ici 2030, nous visons un taux de rendement à l'équilibre, à 7,93 %, poursuit Frédéric Deknuydt. Ce taux reste très bon ! Et c'est grâce à nos réserves que nous avons la capacité d'adoucir les chocs démographiques et de maintenir notre solidarité professionnelle intergénérationnelle. »

Indemnités journalières augmentées de 20 € à 110 €/jour

Quant aux indemnités journalières en cas de maladie, elles ont elle aussi été revues à la hausse pour garantir un meilleur soutien des affiliés lorsqu'ils en ont besoin.

> « Notre régime invalidité-décès se porte très bien, détaille Frédéric Rogier, ce qui nous autorise à toujours mieux couvrir nos experts-comptables et commissaires aux comptes exposés au risque d'un accident de la vie ».

Pour rappel, les indemnités journalières de notre couverture prévoyance sont versées à partir du 91e jour d'arrêt maladie. En amont de cette période, c'est la CNAVPL qui assure la couverture prévoyance, devenue obligatoire depuis le 1er juillet 2021. Cette couverture a pris le relais du secours mis en place par la Cavec au printemps 2020, lors de la crise Covid. Les indemnités journalières du régime de base sont comprises entre 23 €/jour et 170 €/jour.

Visez l'excellence

SUP EXPERTISE

L'ÉCOLE SUPÉRIEURE
DE L'EXPERTISE COMPTABLE,
DE L'AUDIT ET DU CONSEIL

TAXE D'APPRENTISSAGE 2023

Ce qui change

Déclarez et payez
à l'URSSAF via la DSN
Date limite 2023
5 mai + de 50 salariés
15 mai – de 50 salariés

Fléchez
via la plateforme SOLTEA
Du 25 mai au 7 septembre
et choisir Sup'Expertise
Code UAI 0753461E

Investissez dans la formation de vos futurs collaborateurs

Rendez-vous sur
la page taxe
d'apprentissage
de Sup'Expertise

Un choix qui a du sens

En soutenant **Sup'Expertise** et son **projet éducatif d'excellence**, vous apportez aussi votre contribution à la lutte contre la pénurie de jeunes apprentis souhaitant embrasser nos métiers et facilitez ainsi leur insertion professionnelle.

Laissez-nous vous guider

Christelle Gautier accompagne les entreprises et cabinets d'expertise comptable ou d'audit dans leur versement de la taxe d'apprentissage : Collecte et aide au fléchage vers Sup'Expertise.

Christelle GAUTIER - c.gautier@supexpertise.fr
Tél : 01 44 69 91 51 - 06 28 10 83 49

Code établissement UAI
0753461E

En choisissant Sup'Expertise

Vous investissez
dans un campus moderne à la pointe de la technologie.

Vous soutenez
les collaborateurs et futurs diplômés face aux mutations importantes de nos professions.

Vous encouragez
notre développement et nos offres de formations en alternance, en initiale et en continue.

Vous contribuez
également au développement de modules de formations uniques.

Visez l'excellence
SUP EXPERTISE
L'ÉCOLE SUPÉRIEURE DE L'EXPERTISE COMPTABLE, DE L'AUDIT ET DU CONSEIL

L'école de

ORDRE DES EXPERTS-COMPTABLES Région Paris Ile-de-France · CRCC · CRCC DE VERSAILLES ET DU CENTRE

Filières :
- Comptabilité - Gestion - Management - RH

FORMATION INITIALE
FORMATION CONTINUE
CENTRE DE BILANS ET DE GESTION DES COMPÉTENCES

www.supexpertise.fr

50 rue de Londres - 75008 Paris
Campus : 9 rue du Moulin des Bruyères - 92400 Courbevoie
Association Loi 1901 - NAF 8559A - Siren 784 414 054

cjec

Pragmatiques et engagés !

PAR WAHIB DAHMANI

Elue en octobre dernier, notre équipe respectant la parité et représentative de ses 26 sections, s'est rapidement mise au travail pour aider, informer et représenter ses 1 600 adhérents qu'ils soient créateurs ex nihilo (68 %), diplômés salariés en phase d'association (20 %) ou encore mémorialistes (10 %).

Nous sommes pragmatiques et engagés ! Pragmatiques car nos adhérents ont besoin d'une aide concrète adaptée à leurs problématiques d'installation et de développement. Engagés dans la profession car dans un environnement qui évolue en permanence, nous devons être au cœur du réacteur afin d'appréhender pleinement les évolutions législatives et technologiques et en informer nos adhérents.

C'est ce qui guide notre action depuis notre élection et qui est au centre de nos grand-rendez-vous comme notre Séminaire d'Accueil et de Formation des Élus de section, notre Conseil national de mars dans notre très active section du Nord Pas-de-Calais ou encore nos Estivales qui fêteront les 40 ans du Club !

Pragmatiques

En attendant cet anniversaire, revenons sur notre Séminaire d'Accueil et de Formation des Élus de section ANECS & CJEC, qui a réuni les 10 et 11 février 75 participants dont 32 CJECiens nouvellement élus en région.

Quatre objectifs sont visés au cours du SAFE pour permettre à nos élus d'être opérationnels et performants dès leur retour en section. Tout d'abord, ces deux jours permettent de rencontrer toutes les sections CJEC mais aussi ANECS et ainsi d'élargir son réseau, d'échanger les bonnes pratiques et les trucs et astuces de chacun en toute convivialité. Le second objectif est un objectif de formation, c'est-à-dire présenter concrètement les outils et les process pour faire fonctionner de manière optimale sa section. Dans un troisième temps, nous voyons comment être un relais efficace de la stratégie du Club en région. Et enfin, nous apportons les conseils pour optimiser les relations avec notre écosystème institutionnel et partenarial.

Chacun est reparti équipé et boosté pour répondre au mieux aux besoins des adhérents.

> **" Je profite de l'espace qui m'est donné pour remercier très sincèrement nos fidèles partenaires fondateurs, GAN, LCL et CEGID, qui, cette année encore, nous ont apporté leur soutien sans faille et présenté les thèmes qu'ils proposent d'animer tout au long de l'année en section. Sans eux, nous ne pourrions pas faire aussi bien !**

Engagés

Dans le respect de notre ADN, de nos instances et de nos syndicats, nous souhaitons donner une voix au CJEC sur les sujets d'actualité qui impactent tout autant nos jeunes cabinets que l'ensemble de la profession. Qu'il s'agisse du Guichet unique - "L'enfer est souvent pavé de bonnes intentions"... -, de l'attractivité - "La formation au cœur de la stratégie des cabinets" - nous avons déjà eu l'occasion de nous exprimer. Bien d'autres domaines sont à la réflexion de notre bureau exécutif et de nos adhérents comme les SACC ou encore les cybermenaces et, bien évidemment, la transformation des cabinets au regard de la facture X mais aussi des changements sociétaux qu'engendrent la Covid, la RSE et la crise économique. Nous sommes impatients d'échanger avec nos pairs sur tous ces sujets lors des nombreuses réunions en section afin d'enrichir notre réflexion.

Wahib DAHMANI
Président du CJEC

L'ANECS, toujours au cœur de la profession !

PAR JEAN-PASCAL CHARPENTIER

Alors que nous venons d'entamer une nouvelle année, je souhaitais prendre quelques instants pour revenir sur le dernier quadrimestre 2022 et évoquer les temps forts qui ont émaillé la vie de l'ANECS depuis la reconduction du bureau exécutif, que j'ai la chance de présider.

Démarrons avec le **grandiose 77e Congrès des experts-comptables**, qui s'est tenu à Paris fin septembre sur le thème « Les experts-comptables au cœur de la société ». Ce temps fondamental pour l'ANECS et le CJEC nous permet de rencontrer nos partenaires, d'informer les mémorialistes et jeunes diplômés, et, nouveauté de cette édition, de parler du métier aux étudiants présents sur l'espace attractivité. J'ai aussi eu l'honneur de représenter notre cible lors de la cérémonie de remise du DEC, durant laquelle j'ai pu intervenir devant les quelques 1 500 diplômés sur les enjeux d'attractivité, thème central de notre profession.

Dans le prolongement direct du congrès, notre conseil national ANECS et CJEC, pilier de nos associations, nous a donné l'opportunité d'échanger et de débattre et je remercie ses membres pour la confiance renouvelée au bureau exécutif national. **Côté CJEC, il a également été l'occasion de remercier François MERLET, Président sortant, pour son engagement avec le bureau national et d'accueillir Wahib DAHMANI, nouveau Président avec qui j'ai désormais le plaisir de construire la trajectoire commune de nos associations.**

Puis le focus a été mis sur la préparation aux épreuves du DEC de la session de novembre. Je salue ici le remarquable travail des sections régionales qui ont proposé des sessions intensives de préparation et de révision ainsi que les opérations de prêts de mémentos en partenariat avec Lefebvre Dalloz et les Conseils régionaux de l'ordre. Nous avons aussi organisé le premier webinaire national visant à donner conseils et méthodologie pour utiliser au mieux les mémentos le jour de l'épreuve.

Puis nous avons participer aux **33e Assises de la CNCC** en décembre à Rennes qui ont clôturé 2022 autour des enjeux de durabilité et environnementaux. Cet événement, à la fréquentation record, nous a permis de prendre la pleine mesure de la nécessité pour les auditeurs légaux d'accompagner les structures quelles qu'elles soient dans l'application des nouvelles régulations européennes dites Sustainable Finance Disclosure (SFDR) sur la publication d'informations en matière de durabilité dans le secteur des services financiers.

> **Avec l'arrivée de 2023, l'ANECS est entrée dans son cycle de vie de l'association. Celui-ci va permettre, entre janvier et mars et au travers de divers grands rendez-vous, d'élire, de former et de fédérer les élus régionaux qui, au quotidien, vont informer, aider et représenter les jeunes professionnels sur le terrain. J'ai hâte de rencontrer le cru 2023 et de partager l'énergie qui les a fait s'investir et va concourir à placer l'ANECS toujours au cœur de la profession.**

Jean-Pascal CHARPENTIER
Président de l'ANECS

RSE / Durabilité : L'économie de demain sera durable, ou ne le sera pas !

PAR CAROLE CHERRIER

Vice-Présidente de l'IFEC

La responsabilité sociale et environnementale de l'entreprise connaît aujourd'hui des développements considérables, en lien avec une prise de conscience partagée par tous les acteurs économiques : la performance ne se mesure plus à la seule aune des résultats financiers.

La CSRD, une directive qui concerne toutes les tailles d'entreprises

Le 10 novembre 2022, le Parlement Européen a approuvé une nouvelle directive sur le reporting de la durabilité des entreprises (Corporate Sustainability Reporting Directive ou CSRD). Une fois transposée dans le droit français, cette dernière sera applicable dès l'exercice 2024.

Son périmètre d'application concernera toutes les entreprises de plus de 250 salariés, soit environ 50 000 en Europe, **mais également toutes les entreprises qui s'inscriront dans la chaine de valeur amont et aval de ces entités.**

Un nombre significatif d'entreprises sera donc confronté à la nécessité de produire des informations sur leur impact et sur leur démarche RSE. Les professionnels du chiffre joueront un rôle clé pour établir ces informations extra-financières ou donner l'assurance correspondante.

Ces derniers mois, la CNCC a accéléré ses travaux pour former les auditeurs et leur permettre d'accéder au VISA DURABILITÉ.

Pour les commissaires aux comptes : un VISA pour signer les rapports de Durabilité

L'objectif de ce VISA est de former le maximum de professionnels et de leur donner les moyens de réaliser ces missions d'assurance du reporting de durabilité.

Le VISA DURABILITÉ a pour objectif final de permettre aux professionnels :

- **d'identifier les risques en matière de reporting de durabilité et de mettre en œuvre la démarche d'assurance spécifique au reporting de durabilité,**
- **d'identifier quand avoir recours aux experts, être capable d'échanger avec eux, de comprendre leurs conclusions et les impacts potentiels sur le rapport du commissaire aux comptes.**

Ce parcours allie formation théorique et mise en pratique et s'organise autour de **4 piliers** :

1. **Enjeux ESG pour les entreprises** (connaissances générales)
2. **Normes européennes de reporting** de durabilité (ESRS)
3. **Reporting sur la Taxonomie environnementale**
4. **Assurance du reporting de durabilité** (y.c. taxonomie environnementale) **et digitalisation**

Il concernera les commissaires aux comptes, personnes physiques, inscrits avant le 01/01/2024 ainsi que les personnes qui au 01/01/2024 font l'objet d'une procédure d'agrément qui s'achèvera au plus tard le 01/01/2026 (mémorialistes ...).

> **Le programme complet du VISA DURABILITÉ, les conditions de validation ainsi que le calendrier de mise en place seront dévoilés lors du prochain Congrès de l'IFEC à Lyon, les 22 et 23 juin prochains.**

L'ambitieuse stratégie de finance durable européenne

→ 1. Rediriger les flux de capitaux vers des investissements durables
→ 2. Intégrer systématiquement la durabilité dans la gestion des risques
→ 3. Promouvoir la transparence et une perspective long-terme

Pour les experts-comptables et les cabinets : le programme Atout RSE de l'IFEC

Pour accompagner les experts-comptables et permettre aux cabinets de construire et valoriser facilement une démarche RSE adaptée à leurs activité, mais également de développer de nouvelles offres dans leur cabinet, l'IFEC propose un dispositif complet, développé par Croissance bleue, avec le soutien financier de Bpifrance.

L'objectif est d'identifier les atouts RSE gagnants de chaque cabinet comptable et d'activer concrètement des solutions opérationnelles et valorisantes, en proposant :

- Le diagnostic RSE du cabinet,
- La définition des objectifs RSE stratégiques,
- La construction du plan d'actions RSE à court et moyen termes en fonction des objectifs,
- La définition de l'organisation à mettre en œuvre : déploiement, communication…
- La préparation de l'offre RSE du cabinet.

Pour réserver votre place pour la deuxième promotion Atout RSE de l'IFEC, intégrer un programme motivant, encadré par des professionnels et mettre en place la stratégie de votre cabinet, envoyez vos coordonnées **avant le 30/06/2023 à : atoutrse@croissancebleue.com**

Les places sont limitées aux 30 premiers cabinets inscrits.

ATOUT RSE© Expert Comptable

Un dispositif complet pour permettre aux TPE/PME et aux cabinets comptables de construire et valoriser facilement une démarche RSE adaptée à leur activité.

1. Formation collective
2. Diagnostic et structuration de la démarche RSE personnalisée pour chaque entreprise
3. Editorialisation des premiers contenus et recommandations pour communiquer

Un financement et des outils pour chaque entreprise par les partenaires

bpifrance IFEC Croissance bleue

Envoyez vos coordonnées de contact à : **atoutrse@croissancebleue.com**

HISTOIRE & PATRIMOINE

NOS DEMEURES SONT RARES...
PAS LES AMOUREUX DU PATRIMOINE

Histoire & Patrimoine vous invite à découvrir
son offre exclusive de programmes inscrits et classés,
situés **au cœur des plus belles villes et des plus grandes métropoles de France**,
pour un **investissement et une stratégie fiscale sur-mesure.**

MONUMENT HISTORIQUE • LOI MALRAUX • DÉFICIT FONCIER

Château de Grandchamp,
Le Pecq (78)

Pour toute demande d'information :
Céline SIMONIN : contact@hpre.fr · 06 85 54 42 53

Pour en savoir plus sur nos Demeures :
histoire-patrimoine.fr

Histoire & Patrimoine, 87 rue de Richelieu 75002 Paris SAS au capital de 769 800 €
RCS Paris B 480 309 731 – SIRET 48030973100044

UNE MARQUE ALTAREA