Commission numérique

1re édition
Septembre 2024

LA SÉCURITÉ NUMÉRIQUE DU CABINET D'AVOCAT

2. La gestion du risque cyber

GUIDE PRATIQUE

CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

SOMMAIRE

INTRODUCTION 4

LA MÉTHODE DE GESTION DES RISQUES CYBER 8

La gestion des risques 8

La méthode proposée 10

FOCUS SUR L'ÉVALUATION DES PRESTATAIRES 24

Pourquoi évaluer les prestataires ? 24

Comment évaluer les prestataires ? 25

Que faire des évaluations ? 28

FICHES PRATIQUES DE SCÉNARIOS REDOUTÉS 32

Scénario 1 : perte ou vol d'un ordinateur du cabinet 34

Scénario 2 : un rançongiciel bloque l'accès à mes données clients ou à mes données métier 41

Scénario 3 : un nouveau dossier fait peser un risque cyber sur le cabinet 48

Scénario 4 : un tiers a accès à ma boite mail et détourne des fonds CARPA (usurpation d'identité et falsification de RIB) 56

Scénario 5 : un membre quitte le cabinet pour monter son propre cabinet (ou pour rejoindre un cabinet existant) et part avec tout ou partie des dossiers clients 63

REFERENCES 72

Cliquez sur cette icône pour **revenir directement au sommaire** et **naviguer facilement** à travers le guide

INTRODUCTION

Après le premier guide cybersécurité des cabinets d'avocats publié en novembre 2023, le Conseil national des barreaux poursuit ses travaux et présente ce nouveau guide à destination des avocats.

À la différence du premier volume du guide du CNB, qui établissait une liste de mesures techniques à mettre en œuvre quel que soit votre exercice professionnel, la perspective est ici inversée : le risque est apprécié au regard de votre cabinet, de son activité, de ses clients, de son organisation et de son écosystème (prestataires, sous-traitance etc.).

L'objet de ce nouveau guide est le risque cyber vu sous l'angle du métier d'avocat c'est-à-dire sous l'angle de votre exercice professionnel.

Tout cabinet d'avocat dispose d'un patrimoine immatériel constitué de toutes les informations qu'il reçoit et qu'il traite dans le cadre de son activité professionnelle. Ces informations doivent être sécurisées.

En effet, différentes menaces pourraient peser sur votre cabinet. Tout d'abord, les informations de votre cabinet peuvent être convoitées par des attaquants opportunistes qui représentent la menace la plus courante pour les cabinets. Ensuite, les pannes ou des incidents matériels peuvent également entrainer une inaccessibilité des données du cabinet ou une atteinte a leur intégrité. En outre, si vous détenez des informations sensibles et stratégiques, des concurrents de vos clients, voire des Etats pourraient être intéresses par ces données. Votre cabinet peut enfin être victime de clients mécontents ou d'un ancien membre tentant de vous nuire.

L'objectif de ce guide est de vous aider à améliorer la sécurité de l'information de votre cabinet, qu'il s'agisse de la sécurité de l'information en elle-même qui peut avoir une valeur économique pour des tiers ou de la sécurité des applications que vous utilisez dans votre cabinet pour traiter ces informations.

La cybersécurité ne se limite pas à des mesures techniques. Elle concerne l'organisation de votre cabinet, les processus métier mis en place pour traiter les informations des clients. Tout au long de ce guide, nous verrons que les mesures à mettre en place pour sécuriser votre cabinet sont tout aussi bien techniques qu'organisationnelles.

Pour vous permettre d'atteindre cet objectif, ce guide se fonde sur une méthode de gestion du risque cyber, la méthode EBIOS RM, développée par l'ANSSI, et qui représente l'état de l'art.

Nous avons adapté cette méthode aux cabinets d'avocats et à leurs spécificités. L'idée n'est pas de faire de vous des experts en cybersécurité, mais de vous donner des clés et vous aider à vous poser les bonnes questions pour faire de votre cabinet un lieu numérique sûr afin que vos clients puissent vous confier en toute confiance leurs données.

Ce guide tient pour acquise la sécurité du système d'information du cabinet au regard d'un référentiel, le socle de sécurité du premier volume de ce guide :

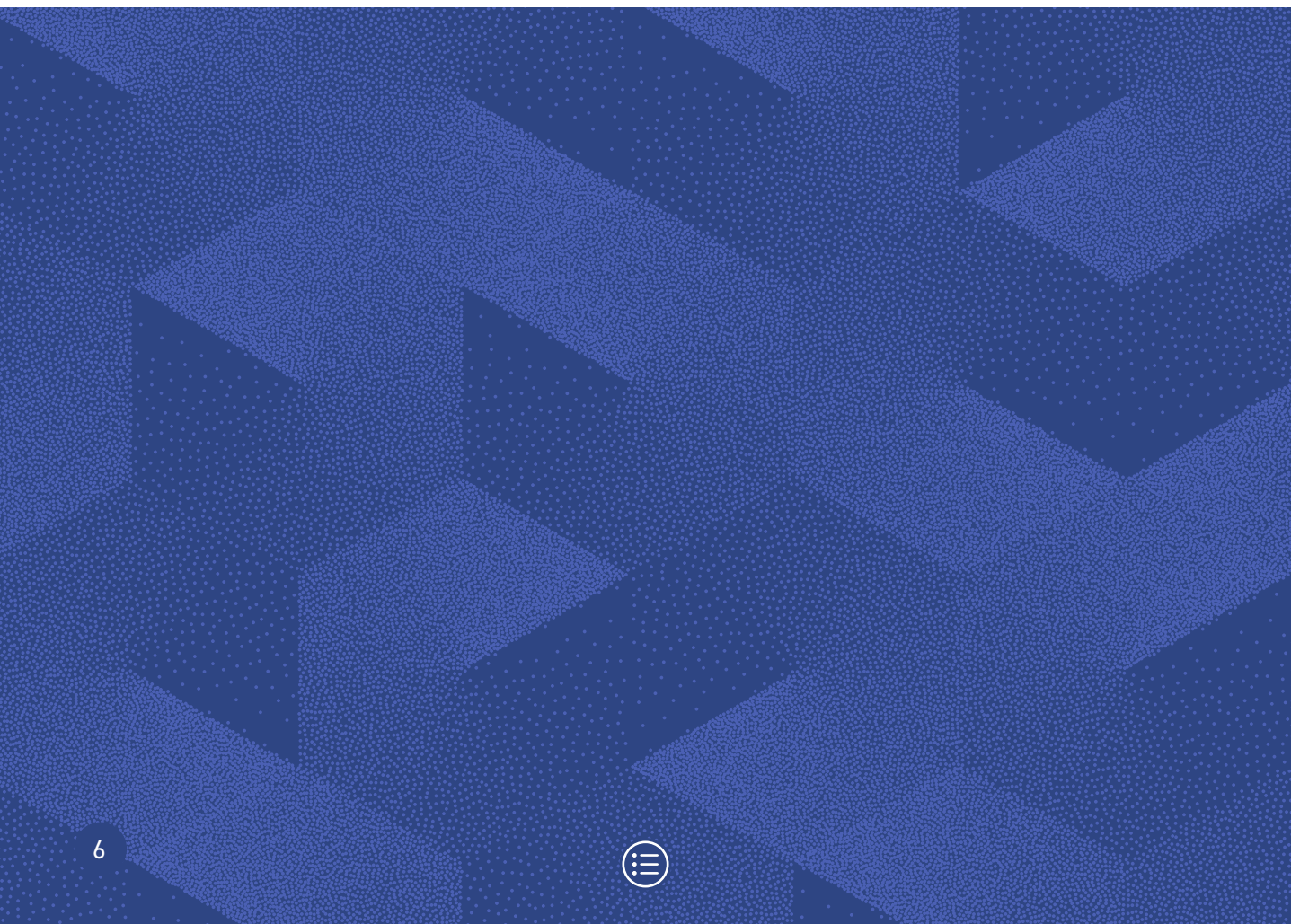
- une évaluation pourra être effectuée périodiquement (ex : une fois par an) pour évaluer la progression de l'évaluation au regard du référentiel retenu ;
- le référentiel retenu peut constituer un socle de base de sécurité, contenant des mesures communes à tous les systèmes d'information (ex : gestion saine des mots de passe, antivirus, ...).

Ce guide développe un processus simple et partagé de gestion des risques de sécurité de l'information dans votre cabinet :

- ce processus doit permettre le partage de la culture du risque du cabinet avec ses membres (nous n'avons pas tous la même appétence au risque) ;
- il doit permettre d'arbitrer sur les risques à intégrer au plan de traitement, et sur les mesures, complémentaires à celles du socle de sécurité, à mettre en œuvre pour diminuer les risques ou encore permettre de prendre conscience et d'assumer / accepter certains risques.

Bien entendu, une politique de sécurité de l'information doit être élaborée, et diffusée pour mise en œuvre dans le cabinet. Cette politique de sécurité de l'information est alimentée des mesures du socle de sécurité auquel s'ajoute celles décidées dans le cadre du plan de traitement des risques.

Après avoir vu la méthode de gestion de risque (1) et la question importante de l'évaluation des prestataires et des sous-traitants (2), nous mettrons en œuvre cette méthode dans cinq scénarios qui sont conçus comme des fiches pratiques (3).



LA MÉTHODE DE GESTION DES RISQUES CYBER

La gestion des risques 8
La méthode proposée 10

LA MÉTHODE DE GESTION DES RISQUES CYBER

LA GESTION DES RISQUES

Définition du risque

Un risque est « *un évènement dommageable dont la survenance est incertaine, quant à sa réalisation ou à la date de cette réalisation* »[1].

Plus techniquement, le risque est « *l'effet de l'incertitude sur les objectifs* » d'une organisation (ex : un cabinet d'avocat) (norme ISO 27000:2018) ou encore la « *Possibilité qu'un événement redouté survienne et que ses effets impactent les missions de l'objet de l'étude [càd de l'organisation visée par l'étude, un cabinet d'avocat]* » (EBIOS RM).

Pour simplifier, nous retiendrons du risque la définition suivante : un risque est la survenance d'un évènement dont les conséquences sont redoutées pour l'activité du cabinet.

Le processus de gestion des risques

Le processus de gestion des risques regroupe, selon la norme ISO 27005:2022, l'ensemble des activités suivantes :

- l'établissement du contexte ;
- l'appréciation des risques comprenant :
  - l'identification des risques,
  - l'analyse des risques,
  - l'évaluation des risques,
- le traitement des risques.

Ces activités se retrouvent dans les différents ateliers de la méthode EBIOS RM, qui est la méthode de référence en matière de risque numérique, publiée par l'ANSSI[2]. Elle constitue l'état de l'art.

1. Vocabulaire juridique Cornu, V° Risque
2. La méthode EBIOS Risk Manager | ANSSI (cyber.gouv.fr)

Cette méthode repose sur 5 ateliers :

- **Atelier n°1,** consacré au cadrage et au socle de sécurité, permet d'établir le contexte ;
- **Atelier n°2,** consacré à la source de risque, permet d'identifier la source du risque et procède à son analyse ;
- **Ateliers n°3 et 4,** consacrés aux scénarios stratégiques et opérationnels, permettent d'évaluer le risque selon sa gravité et sa vraisemblance ;
- **Atelier n° 5** est consacré au traitement des risques.

Le processus de gestion du risque cyber demande un engagement de la part d'une organisation, sur le temps long, ce qui suppose un suivi, des tests réguliers et la mise en place de mesures de sécurité. En effet, le risque cyber évoluant, il est indispensable que les organisations s'adaptent en permanence et ajustent leur niveau de protection à l'état de la menace qui pèse sur elle.

C'est la raison pour laquelle la méthode EBIOS s'adresse, en tout premier lieu, à la direction des organisations :

- → le processus de gestion des risques est un processus qui implique fortement la direction et les métiers, il doit permettre à la direction de s'approprier le traitement des risques qu'elle doit assumer,
- → seuls la direction et les métiers ont connaissance de ce qui est important pour le cabinet : les « valeurs métiers » du cabinet,
- → les techniciens interviennent pour définir les éléments techniques qui viennent supporter les valeurs métiers : les biens supports.

Le processus de gestion des risques peut être répété sur différents périmètres (l'intégralité du cabinet, certains dossiers, certains services ou projets, etc.) et sur différents niveaux de profondeur, en fonction des acteurs et des attendus.

BONNES PRATIQUES :

La direction doit accepter de ne pas traiter tous les risques dès la première itération, pour se concentrer sur les risques les plus importants pour le cabinet.

Une approche qui se veut exhaustive peut conduire à un plan de traitement des risques contenant des centaines de risques, ce qui n'est, en général, pas gérable.

Il est recommandé de se concentrer, à chaque étape du processus, sur les **éléments les plus importants pour l'activité de votre cabinet.**

LA MÉTHODE PROPOSÉE

ÉTAPE 1 : Le cadrage – Mise en contexte

Pour identifier les risques, un cadrage ou mise en contexte est nécessaire. Ce cadrage repose sur une cartographie de trois éléments laquelle détermine les scénarios de risques : activités, données et outils.

Activités

Afin d'identifier et d'évaluer les risques qui pèsent sur le cabinet, il est important d'appréhender les différents éléments de votre organisation qu'il est possible de décomposer en trois grands groupes :

- les activités du cabinet ;
- les données du cabinet ;
- les outils utilisés.

Les activités du cabinet

Pour évaluer les risques qui pèsent sur un cabinet, il est important de bien identifier quelles sont les activités qui y sont pratiquées. Bien que ces activités puissent varier en fonction de la spécialité du cabinet, il est possible d'identifier plusieurs grands groupes d'activités.

L'évaluation des activités du cabinet permet d'identifier les risques cyber qui sont liés.

Les relations clients

Les relations clients constituent une part essentielle du quotidien d'un cabinet d'avocats.

Cela comprend :

- l'organisation de rendez-vous en cabinet ;
  - organisation et tenue de réunions en personne avec les clients
- l'organisation de rendez-vous en visioconférence ;
  - tenue de réunion à distance via des outils de visioconférence
- la communication avec les clients pour maintenir avec eux un contact régulier et répondre à leurs questions :
  - envois et réceptions de courriels
  - appels téléphoniques
  - visioconférences

Tâches administratives

Les tâches administratives forment une autre composante importante des activités d'un cabinet. Elles comprennent notamment :

- la gestion des paiements du personnel ;
- le recrutement de nouveaux collaborateurs ;
- la facturation du cabinet ;
- la comptabilité du cabinet.

Rédaction et révision de documents juridiques

La rédaction et la révision de documents juridiques sont des activités centrales. Cela inclut la création de contrats, d'accords et d'autres documents légaux, ainsi que la révision des documents existants pour s'assurer de leur validité juridique et de leur adéquation aux besoins des clients.

Les outils et les données traitées par un cabinet varient en fonction des activités pratiquées. Les cabinets utilisent couramment des outils de visioconférence, des logiciels de gestion de cabinet, des bases de données juridiques en ligne et des systèmes de gestion de documents.

Les risques cyber auxquels un cabinet est exposé varient eux aussi au regard des activités pratiquées. Par exemple, un cabinet qui utilise intensivement les technologies de visioconférence et de communication en ligne devra se protéger contre les risques liés à la confidentialité des données échangées et à la sécurité des plateformes utilisées.

Données

Qu'ils soient de grande ou de petite taille, les cabinets d'avocats détiennent un nombre important de données nécessaires à l'exercice de leur activité. Ces données, très intéressantes pour les cyberattaquants, constituent le patrimoine immatériel du cabinet d'avocat.

Dans ces conditions, les professionnels doivent faire preuve d'une vigilance accrue et d'exigences strictes en matière de sécurité lors du traitement de ces informations. La divulgation ou l'accès non autorisé à ces données pose des problèmes majeurs en termes de confidentialité et de sécurité.

Une atteinte à la disponibilité, à l'intégrité ou à la confidentialité de ces données pourrait nuire aux intérêts des personnes concernées (droits et libertés, secret des affaires, propriété intellectuelle, etc.) ainsi qu'à la continuité des activités du cabinet.

La variété des données détenues par les cabinets d'avocats et la diversité des supports sur lesquels elles sont stockées/traitées, rendent pratiquement impossible l'identification d'une liste exhaustive. Cependant, pour affiner la cartographie de votre patrimoine immatériel, il est essentiel d'établir une hiérarchie entre les différents « groupes » de données traitées :

- les données de vos clients couvertes par le secret professionnel ;
- les données sensibles au sens du RGPD et hautement personnelles au sens de la CNIL (ex : données médicales sur l'état de santé, la vie personnelle, la situation économique, les rapports professionnels et la situation au travail, la religion, les opinions politiques, les opinions syndicales, etc.) ;
- les données couvertes par le secret des affaires (ex : des informations sur une fusion-acquisition) ;

- les données protégées par un droit de propriété industrielle (ex : données de R&D, etc.) ;
- les données stratégiques (ex : fichiers clients, dossiers, pièces constitutives comme la pièce d'identité, les relevés, la déclaration d'impôt qui contient le numéro fiscal, le numéro de sécurité sociale, etc.) ;
- les données relatives aux membres du cabinet ;
- des données fournisseurs (ex : contrats de maintenance, contrats d'entretien, contrat de bail, contrat de location ou d'achat de photocopieur, de matériel informatique, etc.).

Bien que certaines catégories de données aient un degré d'importance identique pour tous, cette importance peut varier en fonction de l'activité spécifique de chaque cabinet.

Ces données et informations n'exigent pas le même besoin de protection. L'état des lieux du patrimoine immatériel du cabinet permet d'identifier les données qu'il faut protéger en priorité. Plus la donnée est sensible, plus la politique de sécurisation pesant sur le cabinet doit être rigoureuse.

Il est essentiel que la politique de sécurité et de confidentialité du cabinet garantisse la sécurité des données qu'il traite. Pour plusieurs raisons, le cabinet doit être un coffre-fort numérique afin de :

- garantir la continuité de l'activité du cabinet ;
- garantir le respect du secret professionnel ;
- pouvoir mettre en avant des arguments relatifs à la sécurité du cabinet pour se différencier des cabinets concurrents.

Les outils

Au-delà des « données » en elles-mêmes (ex : un numéro de téléphone, un bulletin de salaire, un diagnostic médical, etc.), il est important d'identifier les outils du cabinet via lesquels ces données sont traitées :

- outils de traitement de texte (ex : LibreOffice, Word, Adobe, Pages, etc.) ;
- outils de communication électronique (ex : Thunderbird, Gmail, e-Mail, Outlook, etc.) ;
- outils de stockage (ex : NextCloud, Google Drive, e-Drive, iCloud, etc.) ;
- outil d'exploitation du cabinet (logiciel cabinet, CRM, GED, etc.) ;
- matériel physique (ex : ordinateur, téléphone mobile, tablette, etc.).

La cartographie des données et des outils utilisés permet à l'avocat d'avoir une meilleure vision et de prendre conscience des conséquences engendrées par l'indisponibilité de l'un de ces outils.

Une fois ces éléments identifiés, il est possible d'étudier différents scénarios de risques afin de déterminer quelles sont les activités essentielles pour le cabinet, les mesures à prendre pour les sécuriser et les outils à utiliser.

En établissant des scénarios de risques (ex : perte de l'ordinateur professionnel), le cabinet pourra prendre conscience des données impactées à la suite de cet évènement, des outils qui ne pourront plus être utilisés et des activités susceptibles d'être paralysées pendant un certain laps de temps.

En établissant des scénarios de risques (ex : la perte de l'ordinateur professionnel), le cabinet prendra conscience des impacts de l'évènement sur la vie du cabinet.

EXEMPLE

Anonymisation des documents et enrichissement de la base documentaire du cabinet. Constituer une base de connaissances solide permet au cabinet de capitaliser sur son expérience passée, d'améliorer son efficacité opérationnelle et de mieux servir ses clients.

- **Biens supports associés :**
  - logiciel de gestion électronique des données (GED) ;
  - logiciels d'anonymisation des données ;
  - les compétences du collaborateur chargé de l'enrichissement de la base documentaire.
- **Besoin de sécurité :**
  - disponibilité : 2/4 (il est acceptable de ne pas disposer de ce processus pendant un « certain » temps) ;
  - intégrité : 4/4 (des données fiables et intègres sont primordiales) ;
  - confidentialité : 4/4 (les documents non anonymisés sont en entrée du processus).
- **Les évènements que je redoute :**
  - la modification frauduleuse de documents stockés dans la base de données documentaires ;
  - l'absence prolongée du responsable de la documentation ;
  - la divulgation de contrats clients.

ÉTAPE 2 : L'appréciation des risques

L'appréciation des risques repose sur trois étapes : l'identification des risques (1), leur analyse suivie de leur évaluation (2).

Cette appréciation est fondée sur l'étude des **conséquences** en cas de concrétisation du risque et de la **vraisemblance** d'apparition de ce risque.

Le résultat de cette appréciation est le niveau de risque qui correspond à la mesure de l'importance du risque, exprimée par la combinaison du niveau d'impact et de la vraisemblance :

- la gravité varie selon le nombre d'impacts et leur niveau mais aussi selon la valeur accordée au risque étudié par le cabinet (EBIOS RM)
- la vraisemblance varie selon l'exposition aux menaces, le niveau de vulnérabilité et les mesures de sécurité mises en place (EBIOS RM)

Identification du risque

Pour identifier un risque, il est nécessaire d'apprécier les conséquences de la survenance de l'évènement redouté sur :

- la disponibilité des données du cabinet ;
- l'intégrité des données du cabinet ;
- la confidentialité des données du cabinet.

Au préalable, il est nécessaire d'être conscient de ses besoins de sécurité qui sont synthétisés dans le tableau (cf. page suivante) :

BESOINS DE SÉCURITÉ			
Niveau	**Disponibilité**	**Intégrité**	**Confidentialité**
1	• Besoin de disponibilité de **niveau faible.** • La durée d'interruption maximale acceptable ne doit **pas excéder une semaine ouvrée.**	• **Aucun besoin d'intégrité.**	• **Information publique.** • Les informations **peuvent être diffusées à toute personne.**
2	• Besoin de disponibilité de **niveau moyen.** • La durée d'interruption maximale acceptable ne doit **pas excéder 24 heures ouvrées.**	• Besoin d'intégrité de **niveau moyen.** • Une perte momentanée d'intégrité est acceptée, si elle est corrigée dans **un délai inférieur à 24h et ne remet pas en cause le service fourni.**	• **Information interne.** • Les informations ne doivent **pas être diffusées à des personnes extérieures au cabinet.**
3	• Besoin de disponibilité de **niveau fort.** • La durée d'interruption maximale acceptable ne doit **pas excéder 4 heures ouvrées.**	• Besoin d'intégrité de **niveau fort.** • **Une perte momentanée d'intégrité n'est pas acceptée.** Toute perte d'intégrité entraîne l'arrêt du service jusqu'au rétablissement de l'intégrité.	• **Information confidentielle.** • Les informations ne doivent pas être diffusées à des personnes autres que celles figurant dans la liste des destinataires, une perte de confidentialité pourrait avoir un impact financier, juridique ou d'image pour le cabinet. **Impact existant mais modéré.**
4	• Besoin de disponibilité de **niveau maximum.** • La durée d'interruption maximale acceptable doit être **inférieure à 1 heure ouvrée.**	• Besoin d'intégrité de **niveau maximum.** • Aucune perte d'intégrité n'est acceptée. **Toute perte d'intégrité est corrigée immédiatement sans impact sur le service.**	• **Information sensible.** • Les informations ne doivent pas être diffusées à des personnes autres que celles figurant dans la liste des destinataires, une perte de confidentialité **pourrait avoir des impacts financiers et juridiques très importants pour le cabinet.**

Ce risque ne se limite pas à votre cabinet, son organisation (équipe du cabinet), ses outils, ses process métier, mais dépend également de son écosystème c'est-à-dire de vos prestataires informatiques et de vos sous-traitants.

Il dépend aussi des clients du cabinet et de la sensibilité des données (ex : client célèbre, grande entreprise, secrets d'affaires ou de fabrication, affaires pénales sensibles, etc.). Dans ces conditions, le cabinet peut faire l'objet d'une attaque ciblée pour mettre la main sur ces informations.

Plusieurs évènements peuvent être identifiés comme une source de risque pour les cabinets d'avocat.

EXEMPLE

- indisponibilité des données :
  - perte ou vol d'ordinateur, téléphone portable, tablette ;
  - crypto-lockage des données client du cabinet ou des données métiers du cabinet (modèles, base de connaissances, etc.) ;
  - perte de données d'un prestataire (ex : défaut de maturité cyber du prestataire informatique qui stockerait les codes d'accès au compte administrateur du cabinet en clair dans un fichier Word sur l'un de ses serveurs insuffisamment sécurisé) ;
  - dysfonctionnement d'un prestataire (ex : arrêt du fonctionnement du mail) ;
  - malveillant pathologique (ex : client mécontent)
- compromission de l'intégrité des données : le membre quittant le cabinet souhaite nuire au cabinet en modifiant frauduleusement des documents dans la base documentaire en vue d'en altérer le contenu pour entrainer, dans le futur, la génération de documents dont les bases juridiques ne seraient pas exactes (hypothèse du vengeur) ;
- compromission de la confidentialité des données :
  - mon smartphone permet à des personnes malveillantes d'écouter des conversations confidentielles avec mes clients ;
  - un tiers (un Etat, un concurrent de l'un de mes clients ou une organisation criminelle) accède à la boite mail de mon cabinet, aux dossiers de mes clients.

Cet évènement est redouté en raison du dommage qu'il cause au cabinet puisqu'il peut entraîner une cessation totale ou partielle d'activité, pendant une durée de quelques heures, ou dans le pire des cas, de plusieurs jours à plusieurs semaines ce qui peut occasionner :

- perte de clients ;
- mise en cause de la responsabilité civile professionnelle de l'avocat ;
- sanction de la CNIL pour non-conformité au RGPD ;
- poursuite déontologique ;
- atteinte réputationnelle.

Analyse et évaluation du risque

Pour évaluer les risques, la méthode proposée consiste à se mettre en situation c'est-à-dire à établir des scénarios : dans la situation de mon cabinet, quelles seraient les conséquences de la réalisation du risque pour l'activité de mon cabinet ?

Calcul du niveau de risque

Le niveau de risque s'apprécie dans son contexte (celui de votre cabinet) au moyen de la formule suivante :

G x **V** = **R**

Gravité x **V**raisemblance = **Niveau de Risque**

Évaluation des risques

Afin de partager la culture du risque dans le cabinet, pour évaluer le niveau des risques identifiés, de manière reproductible, il est nécessaire de définir des échelles de Gravité, et de Vraisemblance.

→ Une fois les acteurs d'accord sur ces échelles, l'évaluation du niveau de risque de chaque risque identifié sera facilitée.

Exemple d'échelle d'évaluation de la Gravité du risque

Niveau de l'échelle	Définition
G4 Critique	**Conséquences désastreuses pour le cabinet avec d'éventuels impacts sur l'écosystème.** Incapacité pour le cabinet d'assurer la totalité ou une partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. Le cabinet ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 Grave	**Conséquences importantes pour le cabinet.** Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. Le cabinet surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G2 Significative	**Conséquences significatives mais limitées pour le cabinet.** Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. Le cabinet surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 Mineure	**Conséquences négligeables pour le cabinet.** Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. Le cabinet surmontera la situation sans trop de difficultés (consommation des marges).

Exemple d'échelle d'évaluation de la Vraisemblance du risque

Niveau	Description de la Vraisemblance
V4 Très vraisemblable	La source de risque **va probablement** atteindre son objectif en empruntant l'un des modes opératoires envisagés ou un tel scénario s'est déjà produit au sein du cabinet (historique d'incidents) La vraisemblance du scénario de risque est **élevée.**
V3 Vraisemblable	La source de risque **peut atteindre** son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est **significative.**
V2 Peu vraisemblable	La source de risque **a relativement peu de chances** d'atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est **faible.**
V1 Invraisemblable	La source de risque **a très peu de chances** d'atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est **très faible.**

L'attaquant, dans le vocable de la méthode EBIOS RM, est une source de risque qui possède un niveau de motivation et un objectif (objectif visé).

Dans ce guide, et dans le but d'adapter la méthode EBIOS RM, nous entendrons la source de risques au sens général :

- un attaquant opportuniste qui profite d'une faille de votre socle de sécurité pour mener une attaque cyber (ex : mot de passe faible, système d'exploitation ou de logiciels non mis à jour, etc.). Rappelons que le socle de sécurité n'est pas uniquement constitué de mesures techniques mais également de process métier ;
- un attaquant qui mène une attaque ciblée contre votre cabinet en raison des données qu'il possède. Dans ce cas, il convient de s'interroger sur les attaquants possibles et sur leurs motivations.

EXEMPLE

- un concurrent de l'un des clients du cabinet souhaiterait connaitre les clauses contractuelles entre mon client et une partie prenante avec laquelle le concurrent de mon client souhaite travailler ;
- un vengeur (ex : ancien membre du cabinet) souhaite nuire au cabinet ;
- le crime organisé souhaiterait modifier le RIB du cabinet utilisé par les clients pour le paiement des factures pour détourner les fonds du cabinet.

- lorsque les sources de risques et les motivations associées (couple source de risques / objectifs visés par la source de risques) sont identifiées, et les prestataires évalués, il est nécessaire d'élaborer les différents scénarios stratégiques (qui peuvent impliquer l'ensemble des parties prenantes, dont les prestataires et les sous-traitants). Ces scénarios stratégiques sont les chemins d'attaque que pourrait emprunter, plus ou moins vraisemblablement, une source de risque identifiée pour atteindre ses objectifs.

Dans tous les cas, la vraisemblance du risque dépend de différents éléments (non exhaustif) :

- historique d'incident (le cabinet a-t-il déjà fait l'objet de la même attaque ? ou d'une autre ?) ;
- socle de sécurité mis en place au sein du cabinet (mesures techniques et process métier mis en place, notamment après un incident) ;
- état de la menace cyber ;
- écosystème du cabinet (prestataires et sous-traitants).

Exemple d'échelle d'évaluation du niveau de risque

L'étape de l'appréciation du risque se termine par le calcul du niveau des risques qui rend possible leur traitement.

	Vraisemblance			
Gravité	V1 Invraisemblable	V2 Peu vraisemblable	V3 Vraisemblable	V4 Très vraisemblable
G1 Mineur	1	2	3	4
G2 Significative	2	4	6	8
G3 Grave	3	6	9	12
G4 Critique	4	8	12	16

ÉTAPE 3 : Le traitement des risques

Lorsque tous ces éléments sont collectés, il est possible d'évaluer le niveau de risque associé à chaque scénario en prenant en compte la vraisemblance estimée associée aux scénarios et la gravité des événements redoutés par le cabinet.

Le niveau des risques

Nous considérons trois niveaux de risques calculés en fonction de la vraisemblance et de la gravité :

- **FAIBLE ;**
- **MODÉRÉ ;**
- **MAJEUR.**

L'évaluation du niveau de risque permet de proposer une option de traitement des risques, dans le cadre d'une procédure qui a pour objet de prioriser les risques à traiter.

Les options de traitement des risques

Il existe 4 options de traitement des risques :

- **Évitement :** consiste à arrêter et éviter toute activité qui présente un risque
- **Réduction :** implique des actions (mise en œuvre de mesures de sécurité techniques ou organisationnelles) qui permettent de réduire la vraisemblance d'un risque ou sa gravité
- **Partage :** consiste à partager le risque avec des parties externes, en souscrivant une assurance qui couvre les conséquences ou en sous-traitant à un partenaire dont le rôle consiste à surveiller le système d'information et à entreprendre des actions immédiates destinées à arrêter une attaque avant qu'un niveau de dommage défini ne soit atteint
- **Maintien :** consiste à prendre la décision de maintenir le risque sans mise en œuvre de mesure particulière. Le maintien du risque implique la mise en surveillance de ce risque pour détecter une variation de sa vraisemblance ou de ses impacts

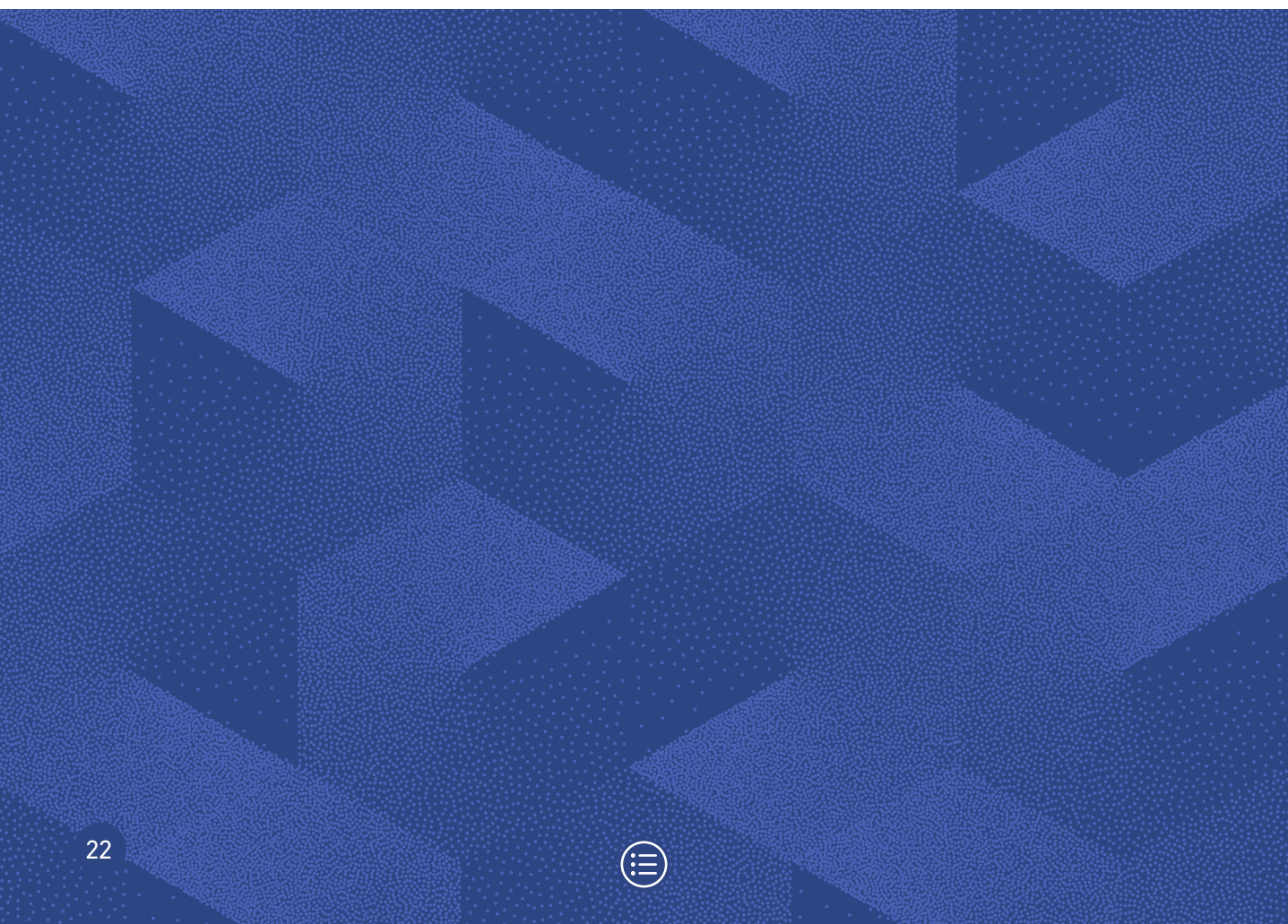
La stratégie de traitement des risques

En fonction du niveau des risques et des différentes options de traitement, une stratégie de traitement des risques du cabinet peut voir le jour :

- les risques **FAIBLES** (1 - 6) sont acceptés et constitueront ainsi des risques résiduels. Le cabinet peut toutefois décider de réduire ces risques ;
- l'opportunité de mettre en œuvre des mesures de sécurité permettant de réduire les risques **MODÉRÉS** (8 - 9) doit être envisagée. Le cabinet peut choisir de maintenir le risque ;
- les risques **MAJEURS** (12 - 16) doivent être couverts par des mesures de sécurité afin de les réduire à un niveau acceptable. Si le cabinet fait le choix de maintenir un risque MAJEUR, la justification de ce maintien doit être approuvée par la direction du cabinet.

Les risques résiduels

Une fois le risque évalué, les options de traitement des risques retenues, il est nécessaire, pour chaque risque, de préciser les mesures de sécurité à mettre en œuvre (élaboration du plan de traitement des risques), et évaluer l'impact des mesures sur la vraisemblance et la gravité qui demeureront pour les risques ainsi traités. Il s'agit d'évaluer la vraisemblance résiduelle et la gravité résiduelle permettant d'évaluer le risque résiduel (risque qui demeurera après mise en œuvre des mesures).



FOCUS SUR L'ÉVALUATION DES PRESTATAIRES

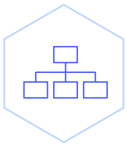
Pourquoi évaluer les prestataires ? 24
Comment évaluer les prestataires ? 25
Que faire des évaluations ? 28

FOCUS SUR L'ÉVALUATION DES PRESTATAIRES

POURQUOI ÉVALUER LES PRESTATAIRES ?

Évaluer les prestataires dans le domaine de la cybersécurité est crucial pour plusieurs raisons importantes :

Identification des risques : l'évaluation des prestataires par un cabinet d'avocats permet de déterminer les risques liés aux activités de ces derniers en matière de cybersécurité. Par exemple, cette évaluation pourrait révéler la manipulation non autorisée de données des clients du cabinet par des prestataires de services informatiques tiers, exposant ainsi des informations confidentielles à des tiers non autorisés.



Analyse de l'impact : cette évaluation permet également d'évaluer l'impact que les activités des prestataires peuvent avoir sur la sécurité de l'information du cabinet. Par exemple, une violation de la sécurité des données chez un fournisseur de services de stockage cloud pourrait compromettre l'intégrité ou la confidentialité des dossiers clients sensibles stockés dans le cloud.

Appréciation des vulnérabilités : elle permet d'évaluer les vulnérabilités des prestataires susceptibles d'être exploitées par des attaquants. Par exemple, une évaluation pourrait révéler des vulnérabilités dans les systèmes de messagerie utilisés par un prestataire pour communiquer avec le cabinet d'avocats, exposant ainsi les communications à des interceptions non autorisées.

Évaluation des menaces : on évalue les menaces susceptibles de peser sur les prestataires ainsi que leurs conséquences pour le cabinet. Par exemple, cela pourrait être des menaces telles que les attaques de phishing ciblant les employés du prestataire, qui pourraient être exploitées pour obtenir un accès non autorisé aux systèmes du cabinet via des comptes compromis.

Détermination des risques résiduels : après une évaluation, on détermine les risques résiduels associés à l'externalisation de certaines fonctions. Par exemple, même si des mesures de sécurité strictes sont mises en place pour encadrer la gestion des données client par un prestataire, il y a toujours un risque résiduel lié à la possibilité de failles de sécurité internes au prestataire, comme des erreurs humaines ou des vulnérabilités non découvertes dans ses systèmes. Ces risques résiduels doivent être pris en compte dans la stratégie globale de gestion des risques du cabinet d'avocats.

Planification des mesures de sécurité : cette évaluation sert à guider la planification des mesures de sécurité à adopter pour atténuer les risques identifiés. Par exemple, l'évaluation pourrait mener à l'instauration d'une procédure de vérification régulière des pratiques de sécurité des prestataires, à la mise en place de mécanismes de contrôle d'accès renforcés pour limiter l'accès aux données sensibles et à l'élaboration de contrats de prestation de services comprenant des clauses spécifiques sur la sécurité des informations.

COMMENT ÉVALUER LES PRESTATAIRES ?

L'évaluation d'un prestataire en matière de cybersécurité repose souvent sur quatre critères clés pour déterminer le niveau de risque associé à la relation.

Ces critères sont :

- **Dépendance :** pour un cabinet d'avocats, la dépendance à un prestataire peut se manifester, par exemple, par la nécessité de confier des tâches critiques telles que la gestion des bases de données clients, des outils de gestions de dossiers ou encore la gestion des outils de communication électronique avec les clients et les juridictions. Cette dépendance peut résulter de besoins spécifiques en matière de technologies spécialisées ou de compétences techniques que le cabinet ne possède pas en interne.
- **Pénétration :** la pénétration dans le cadre d'un cabinet d'avocats pourrait se référer à l'accès étendu d'un prestataire à des informations confidentielles sur les clients, aux documents juridiques sensibles ou aux données à caractère personnel. Par exemple, un prestataire fournissant des services de stockage cloud ou gérant les serveurs ou encore les postes de travail du cabinet pourrait avoir un accès direct aux dossiers électroniques des clients, ce qui constituerait une pénétration significative.
- **Maturité cyber :** pour un cabinet d'avocats, la maturité du sous-traitant en matière de cybersécurité est essentielle pour assurer la confidentialité, l'intégrité et la disponibilité des informations du cabinet et de ses clients. Cela pourrait comprendre la mise en place de mesures de sécurité comme le chiffrement des données, l'authentification à deux facteurs, des politiques de gestion des accès strictes, ou encore des procédures de sauvegarde robustes.
- **Confiance :** dans le contexte d'un cabinet d'avocats, la confiance envers un prestataire est primordiale en raison de la nature hautement confidentielle des informations qui sont manipulées. La réputation du prestataire, ses références dans le domaine de la sécurité de l'information, ainsi que ses certifications pertinentes (ex : ISO 27001) jouent un rôle crucial dans l'établissement d'une relation de confiance. Un historique de performances fiable et des garanties quant à la protection des données des clients contribuent également à renforcer cette confiance.

Ces quatre critères peuvent être évalués selon une échelle (cf. exemples ci-dessous), ce qui permettra de calculer le niveau de menace du prestataire.

Niveau de Menace = (Pénétration x Dépendance) / (Maturité cyber x Confiance)				
Niveau	Dépendance	Pénétration	Maturité SSI	Confiance
1	● **Relation non nécessaire** aux fonctions stratégiques.	● **Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs** (poste de travail, ordiphone, etc.).	● Des règles d'hygiène sont appliquées ponctuellement et non formalisées. **La capacité de réaction sur incident est incertaine.**	● Les intentions de la partie prenante **ne peuvent être évaluées**.
2	● **Relation utile** aux fonctions stratégiques.	● **Accès avec privilèges de type administrateur à des terminaux utilisateurs** (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux sites de l'organisation.	● Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. **La sécurité numérique est conduite selon un mode réactif.**	● Les intentions de la partie prenante **sont considérées comme neutres.**
3	● Relation **indispensable mais non exclusive.**	● **Accès avec privilèges de type administrateur à des serveurs « métier »** (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	● **Une politique globale est appliquée en matière de sécurité numérique**. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	● Les intentions de la partie prenante sont **connues et probablement positives.**
4	● **Relation indispensable et unique** (pas de substitution possible à court terme).	● **Accès avec privilèges de type administrateur à des équipements d'infrastructure** (annuaires, DNS, DHCP, commutateurs, pare-feu, hyperviseurs, baies de stockage, etc.) ou accès physique aux salles serveurs du cabinet.	● **La partie prenante met en œuvre une politique de management du risque.** La politique est intégrée et prend pleinement en compte une dimension proactive.	● Les intentions de la partie prenante **sont parfaitement connues et pleinement compatibles avec celles du cabinet.**

EXEMPLE

Votre cabinet, ne disposant pas de technicien informatique, envisage de faire appel à un prestataire ayant bonne réputation pour la gestion des postes de travail et l'assistance aux utilisateurs.

- **Dépendance : 4**
  - **Évaluation :** Le cabinet dépend fortement du prestataire pour la gestion des postes de travail, car il ne dispose pas de technicien en interne pour assurer cette fonction critique.
  - **Risque associé :** Une forte dépendance expose le cabinet au risque de perturbation majeure en cas de dysfonctionnement du prestataire, pouvant entraîner une interruption des activités et des retards dans les procédures.
- **Pénétration : 4**
  - **Évaluation :** Le prestataire a un accès complet aux postes de travail des avocats, y compris aux données et aux applications sensibles stockées sur ces postes.
  - **Risque associé :** Une pénétration élevée accroît le risque de fuite de données confidentielles en cas de violation de la sécurité chez le prestataire, ce qui pourrait compromettre la confidentialité des informations clients et porter atteinte à la réputation du cabinet.
- **Maturité cyber : 3**
  - **Évaluation :** Le prestataire est bien établi et possède une bonne réputation dans le domaine de la cybersécurité. Il met en œuvre des pratiques de sécurité avancées telles que le chiffrement des données, la surveillance continue et la formation régulière du personnel.
  - **Risque associé :** Bien que le prestataire ait une maturité cyber élevée, aucun système n'est à l'abri des failles de sécurité. Un incident de sécurité chez le prestataire pourrait toujours compromettre la sécurité des données du cabinet.
- **Confiance : 3**
  - **Évaluation :** Le prestataire bénéficie d'une bonne réputation sur le marché et est reconnu pour son professionnalisme et son engagement envers la sécurité des données.
  - **Risque associé :** Bien que le prestataire inspire confiance, il ne dispose pas de certification. Il est important de reconnaître que toute organisation peut être victime d'une violation de sécurité. Une confiance excessive pourrait augmenter les risques pour le cabinet.

Dans cet exemple, le niveau de menace est de (4x4) / (3x3) = 1,8

QUE FAIRE DES ÉVALUATIONS ?

Lorsque les prestataires sont identifiés et évalués, il est possible de les classer par niveau de menace. Cette approche permet de traiter dans un premier temps les prestataires dont le niveau de menace est le plus élevé. L'approche est itérative, ce qui permet, sur la durée, d'améliorer le niveau de sécurité de l'information, en ordonnant, de manière objective, les itérations.

Ainsi, dans un premier temps, le cabinet peut traiter les prestataires représentant une menace élevée pour le cabinet, puis par la suite, ceux qui représentent un niveau de menace moindre, et aussi accepter les risques associés à ceux qui ont un niveau de menace faible.

Le cabinet peut définir une procédure de gestion (simple et efficace) de ses prestataires en considérant le niveau de menace évalué.

Dans notre exemple, le niveau de menace varie entre 1 et 16.

Nous pourrions considérer, pour adresser le risque, 3 **types de prestataires et des mesures associées à chaque type :**

Type 1

LES PRESTATAIRES DONT LE NIVEAU DE MENACE EST INFÉRIEUR À 2

(niveau faible)

Un contrat avec un prestataire de Type 1 doit avoir, au minimum, les caractéristiques suivantes :

- **pas de SLA exigé,** éventuellement un indicateur interne de taux de satisfaction ;
- **un accord de confidentialité ;**
- **engagement sur les clauses du RGPD** en cas de traitement de données à caractère personnel.

Type 2

LES PRESTATAIRES DONT LE NIVEAU DE MENACE EST COMPRIS ENTRE 2 ET 5

(niveau considéré comme moyen dans l'exemple)

Un contrat avec un prestataire de Type 2 doit avoir, au minimum, les caractéristiques suivantes :

- **engagement sur des SLA** (si la nature de la prestation le justifie), calcul et transmission des indicateurs ;
- **un accord de confidentialité ;**
- **engagement sur les clauses du RGPD,** en cas de traitement des données à caractère personnel ;
- **principales mesures de sécurité décrites dans le contrat.**

Type 3

LES PRESTATAIRES DONT LE NIVEAU DE MENACE EST SUPÉRIEUR À 5

(niveau considéré comme élevé dans l'exemple)

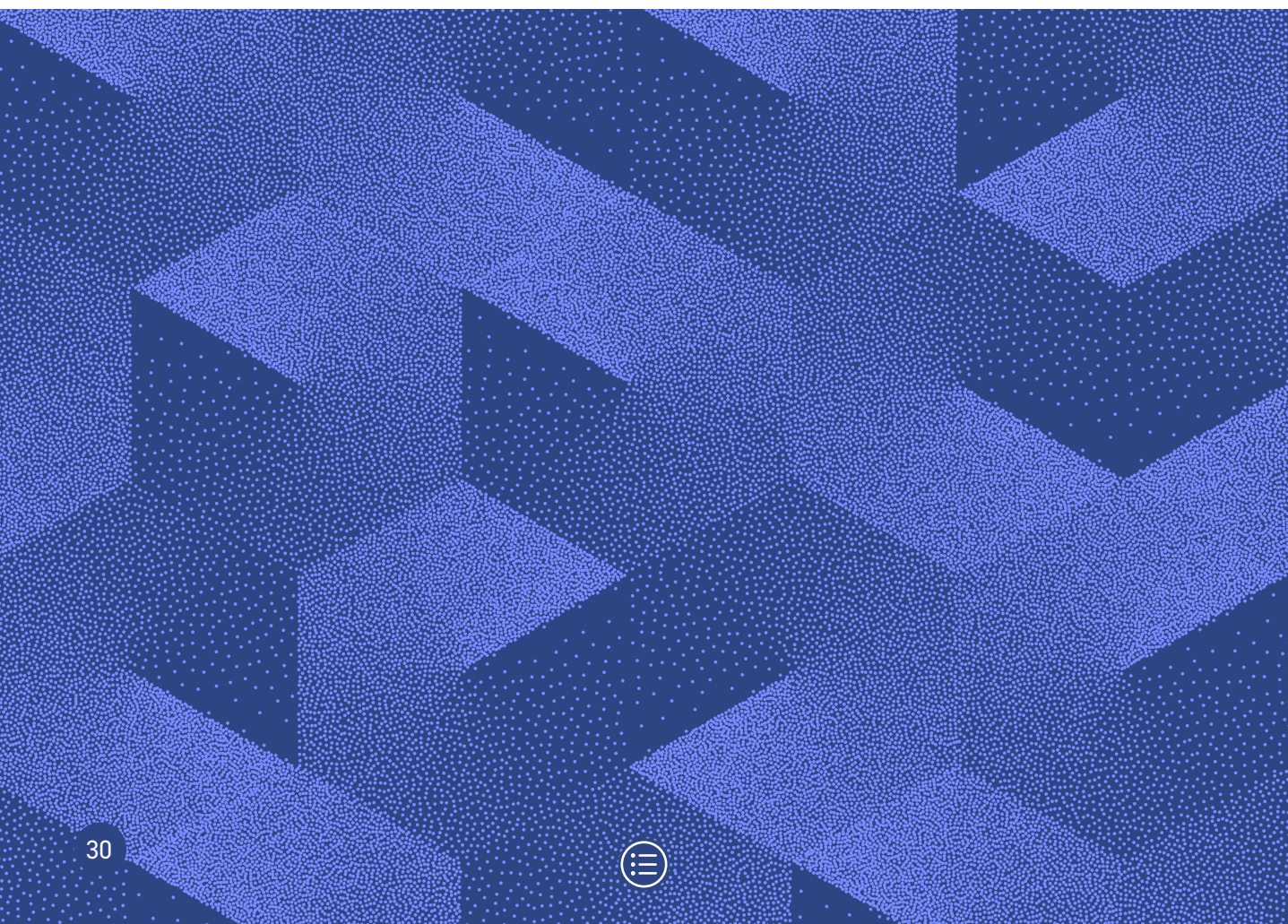
Un contrat avec un prestataire de Type 3 doit avoir les caractéristiques suivantes :

- **engagement sur des SLA** (si la nature de la prestation le justifie), calcul et transmission des indicateurs ;
- **un accord de confidentialité ;**
- **engagement sur les clauses du RGPD,** en cas de traitement des données à caractère personnel ;
- **liste détaillée des mesures de sécurité** ou mise en œuvre d'un **plan d'assurance sécurité** (PAS) ;
- **réalisation d'un audit** au minimum toutes les x années.

FOCUS SUR LES PRESTATAIRES AVOCATS

Il est fréquent que les avocats sous-traitent certaines parties de leurs dossiers à d'autres cabinets. Cette collaboration élargit le réseau des entités impliquées. Par conséquent, il devient impératif d'évaluer les cabinets avec lesquels vous collaborez. La méthode d'évaluation est la même que celle appliquée aux prestataires « techniques » afin de s'assurer qu'ils adhèrent aux mêmes exigences en matière de cybersécurité. Cette évaluation doit garantir que chaque partie est impliquée dans la gestion des informations et est équipée pour protéger son écosystème informatique contre les cybermenaces.

Découvrons maintenant cinq scénarios de risques majeurs auxquels un cabinet peut être confronté, et comment y faire face efficacement



FICHES PRATIQUES DE SCÉNARIOS REDOUTÉS

Scénario 1 : perte ou vol d'un ordinateur du cabinet 34

Scénario 2 : un rançongiciel bloque l'accès à mes données clients ou à mes données métier 41

Scénario 3 : un nouveau dossier fait peser un risque cyber sur le cabinet 48

Scénario 4 : un tiers a accès à ma boite mail et détourne des fonds CARPA (usurpation d'identité et falsification de RIB) 56

Scénario 5 : un membre quitte le cabinet pour monter son propre cabinet (ou pour rejoindre un cabinet existant) et part avec tout ou partie des dossiers clients 63

FICHES PRATIQUES DE SCÉNARIOS REDOUTÉS

Dans cette dernière partie, il s'agit de mettre en œuvre la méthode développée précédemment.

Mise en oeuvre de la méthode

L'objectif que nous poursuivons est de vous mettre en situation en élaborant différents scénarios. Il existe plusieurs scénarios redoutés par un cabinet, sans prétendre à l'exhaustivité on peut penser à :

- la presse à scandale qui souhaite connaitre des éléments de la vie privée d'un client très célèbre du cabinet et tente de corrompre un collaborateur pour obtenir des informations confidentielles ;
- un membre quittant le cabinet souhaite lui nuire en modifiant frauduleusement des documents dans la base documentaire en vue d'en altérer le contenu pour entrainer, dans le futur, la génération de documents dont les bases juridiques ne seraient pas exactes ;
- le crime organisé souhaiterait détourner les fonds destinés au cabinet en modifiant des factures générées avant communication aux clients afin de modifier les coordonnées bancaires présentes sur chaque facture ;
- l'incendie ou l'inondation qui détruit une partie ou l'entièreté du cabinet ;
- un membre du cabinet qui clique sur un lien malveillant.

Nous vous proposons cinq scénarios, élaborés dans le but de vous aider à comprendre comment mettre en œuvre la méthode d'évaluation des risques au sein de votre propre cabinet :

- **Scénario 1 :** perte ou vol d'un ordinateur du cabinet
- **Scénario 2 :** un rançongiciel bloque l'accès aux données clients ou aux données métier du cabinet
- **Scénario 3 :** un nouveau dossier fait peser un risque cyber sur le cabinet
- **Scénario 4 :** un tiers a accès à la boite mail du cabinet et détourne des fonds CARPA (usurpation d'identité et falsification de RIB)
- **Scénario 5 :** un membre quitte le cabinet pour monter son propre cabinet (ou pour rejoindre un cabinet existant) et part avec tout ou partie des dossiers clients

Il est important de noter que ces scénarios s'inspirent des menaces cyber parmi les plus fréquentes rencontrées par les cabinets d'avocats, mais qu'ils ne couvrent pas l'ensemble des risques auxquels votre cabinet pourrait faire face.

Comment avons-nous conçu ces scénarios ?

Chaque scénario repose sur une mise en situation, sur un risque que nous avons pré-identifié comme un risque courant pour votre cabinet d'avocat.

Le risque étant déjà identifié, la méthode que nous exposerons sera simplifiée. Nous serons alors amener à développer deux points particuliers :

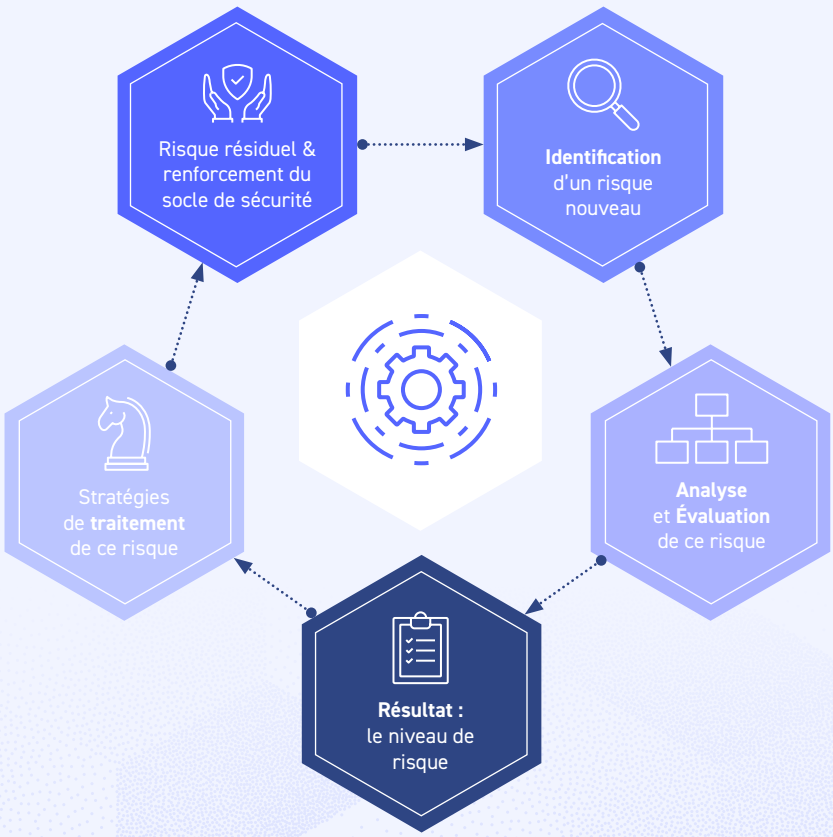
- l'analyse et l'évaluation du risque ;
- le traitement du risque.

L'objectif est de vous montrer comment la méthode se met en œuvre en vous donnant :

- des exemples d'échelles d'évaluation dont vous puissiez vous inspirer pour évaluer les risques que vous aurez identifiés dans votre cabinet,
- des exemples de stratégies de traitement des risques à déployer pour consolider le socle de sécurité de votre cabinet.

Ainsi, nous vous invitons à adapter chaque scénario aux spécificités de votre cabinet et de votre activité.

LA MÉTHODE ITÉRATIVE



Calcul du niveau de risque

G x **V** = **R**

Gravité x **V**raisemblance = niveau de **R**isque

SCÉNARIO 1 :
PERTE OU VOL D'UN ORDINATEUR DU CABINET

IDENTIFICATION DU RISQUE

Dans ce scénario, vous perdez votre ordinateur dans un train, lorsque vous revenez à votre place, après être parti téléphoner, il n'est plus là ; ou le scénario ou vous vous faites voler votre ordinateur à la suite du cambriolage de vos locaux professionnels ou dans votre voiture stationnée sur la voie publique.

ANALYSE ET ÉVALUATION DU RISQUE

Pour apprécier ce risque, il est nécessaire d'adopter une approche contextuelle en simulant la situation de votre cabinet si le risque se réalisait en termes de disponibilité, d'intégrité et de confidentialité des données du cabinet.

En pratique, il s'agit de se poser la question suivante : si ce scénario se réalisait au sein de mon cabinet, quelles en seraient les conséquences ?

L'appréciation du risque dépend ainsi d'une double évaluation :

- L'évaluation de la **gravité (G)** des conséquences pour le cabinet si le risque se réalisait :
  - perte de client
  - mise en cause de la responsabilité civile professionnelle de l'avocat
  - sanction de la CNIL pour non-conformité au RGPD
  - poursuites déontologiques
  - atteinte réputationnelle
- L'évaluation de la probabilité de survenance du risque appelée vraisemblance du **risque (V).**

G

Évaluation de la GRAVITÉ du risque

Dans ce scénario, l'évaluation de la gravité de la situation de votre cabinet si le risque se réalisait dépend des éléments suivants :

- **lieu de stockage de vos données** (en local sur votre ordinateur, sur un serveur, dans le cloud) ;
- existence de **sauvegarde** ;
- **chiffrement des données** de votre ordinateur perdu ou volé.

NOTRE OBJECTIF :

Il est possible d'envisager différentes hypothèses dont la gravité varie en fonction des éléments d'évaluation mentionnés ci-dessus. Cette évaluation a pour objectif de répondre à la question suivante :

Quel est le niveau de sécurisation de l'ordinateur perdu ou volé ?

G1	G2	G3	G4
☐ Les données de l'ordinateur perdu ou volé sont **dans le cloud,** les données sont chiffrées et vous avez la **possibilité d'effacer les données à distance** ☐ L'ordinateur perdu ou volé contient toutes les données du cabinet mais **les données sont chiffrées et vous disposez d'une sauvegarde datant de la veille**	☐ L'ordinateur perdu ou volé **contient toutes les données du cabinet** ☐ Vos données sont chiffrées, mais vous n'avez **pas de sauvegarde récente** seulement de quelques semaines.	☐ L'ordinateur perdu ou volé **contient toutes les données du cabinet** ☐ Vos données ne sont pas chiffrées, et **vous n'avez qu'une vieille sauvegarde datant de 6 à 12 mois.**	☐ L'ordinateur perdu ou volé contient **toutes les données du cabinet,** ☐ **vos données** ne sont pas chiffrées, et vous n'avez pas de sauvegarde.
Dans ces deux cas, la situation est d'une **gravité mineure**	La situation est significative **(G2)**, car cette perte de données **vous contraint à reconstituer votre base de données et à récupérer les données perdues,** ce qui a nécessairement un impact sur l'activité du cabinet Les données étant chiffrées, il n'existe **pas de risque d'atteinte à la confidentialité**	La situation est grave, **l'activité du cabinet est très fortement perturbée** le temps de reconstituer les dossiers en cours (recherche de mail, nécessité de contacter vos clients, vos contradicteurs, la juridiction, etc.) Si votre ordinateur tombait entre de mauvaises mains, vos données n'étant pas chiffrées, cela ferait planer **un risque de fuite de données et d'atteinte à la confidentialité**	La situation est critique, **l'activité du cabinet est très fortement perturbée voire interrompue** le temps de reconstituer vos dossiers (recherche de mail, nécessité de contacter vos clients, vos contradicteurs, la juridiction, etc.) Si votre ordinateur tombait entre de mauvaises mains, vos données n'étant pas chiffrées, cela ferait planer **un fort risque de fuite de données et d'atteinte à la confidentialité**
Mineure (Conséquences négligeables pour le cabinet)	**Significative** (Conséquences significatives mais limitées pour le cabinet)	**Grave** (Conséquences importantes pour le cabinet)	**Critique** (Conséquences désastreuses pour le cabinet avec d'éventuels impacts sur l'écosystème)

Évaluation de la VRAISEMBLANCE du risque

Lorsqu'on évalue la vraisemblance d'un risque, il s'agit de répondre à la question suivante : quelles sont les probabilités que le cyber-attaquant atteigne son objectif ?

Dans ce scénario, la vraisemblance de perte ou de vol ne dépend pas de l'utilisation d'outils informatiques, mais de votre comportement avec votre ordinateur.

Par exemple, laissez-vous votre ordinateur sans surveillance (dans un train par ex.) ? Visible dans votre voiture lorsqu'elle est en stationnement dans la rue ?

En suivant cet exemple, l'échelle de l'évaluation de la vraisemblance pourrait être :

ÉVALUATION DE LA VRAISEMBLANCE DU RISQUE	
V1 Invraisemblable	• Je sors du wagon téléphoner **avec mon ordinateur.**
V2 Peu vraisemblable	• Je laisse mon ordinateur **dans ma chambre d'hôtel** lorsque je suis en déplacement mais je le place **dans un coffre-fort.**
V3 Vraisemblable	• Je laisse **mon ordinateur sans surveillance** sur le siège passager de ma voiture stationnée **sur la voie publique.**
V4 Très vraisemblable	• Je laisse **mon ordinateur sans surveillance dans le train** lorsque je sors du wagon pour téléphoner.

RÉSULTAT : le niveau de risque

Selon la méthode, l'issue de cette appréciation est un résultat, le niveau de risque.

Ce niveau de risque se calcule dans son contexte (celui de votre cabinet) au moyen de la formule suivante :

Niveau de risque = Gravité x Vraisemblance.

En croisant les niveaux de gravité et de vraisemblance, vous obtiendrez le niveau de risque de votre cabinet qu'il est possible d'illustrer de la façon suivante :

	V VRAISEMBLANCE			
G GRAVITÉ	Invraisemblable	Peu vraisemblable	Vraisemblable	Très vraisemblable
Mineure	1	2	3	4
Significative	2	4	6	8
Grave	3	6	9	12
Critique	4	8	12	16

Le niveau de risque est déterminé par la multiplication de deux facteurs : la gravité du risque et sa vraisemblance.

Illustrons les résultats de ce tableau en raisonnant sur trois hypothèses correspondant à trois niveaux de risque différents.

NIVEAU DE RISQUE FAIBLE (1-6)

En effet, **un risque dont la gravité est critique** (G4) pour le cabinet **n'implique pas nécessairement un niveau de risque élevé** dès lors qu'il est invraisemblable (V1).

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V1 = 4

À l'inverse, il est possible qu'**un risque soit très vraisemblable** (V4), mais d'une **gravité mineure** (G1) : le risque est alors d'un niveau faible.

Ex : Niveau de risque = Gravité x Vraisemblance = G1 x V4 = 4

Un niveau de risque faible est encore possible lorsque la **gravité est significative** (G2) et que la probabilité de réalisation du **risque est peu vraisemblable** (V2).

Ex : Niveau de risque = Gravité x Vraisemblance = G2 x V2 = 4

NIVEAU DE RISQUE MODÉRÉ (8-9)

En effet, un risque dont la **gravité est critique** (G4) pour le cabinet peut exposer le cabinet à un niveau de risque modéré dès lors qu'il est **peu vraisemblable** (V2).

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V2 = 8

À l'inverse, un risque **très vraisemblable** (V4) peut exposer le cabinet à un niveau de risque modéré dès lors que sa **gravité est seulement significative** (G2).

Ex : Niveau de risque = Gravité x Vraisemblance = G2 x V4 = 8

Il est encore possible que le cabinet soit exposé à un niveau de risque modéré si les deux facteurs sont équilibrés car **le risque serait grave** (G3) et **sa réalisation vraisemblable** (V3)**.**

Ex : Niveau de risque = Gravité x Vraisemblance = G3 x V3 = 9

NIVEAU DE RISQUE ÉLEVÉ (12-16)

Dans ce cas, les deux facteurs de risque sont au niveau le plus élevé : la **gravité est critique** (G4) et sa réalisation **très vraisemblable** (V4)

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V4 = 16

En conclusion, pour réduire le niveau global du risque, il est possible de jouer sur l'un des deux facteurs, la gravité ou la vraisemblance du risque, en appliquant les mesures de traitement du risque.

TRAITEMENT DU RISQUE

Rappelons que dans le traitement du risque, quatre options sont possibles :

- l'acceptation du risque et de ses conséquences ;
- le refus du risque, ce qui suppose, par exemple, que vous ne vous déplaciez plus avec votre ordinateur de peur de leur perdre ;
- le partage du risque, difficile à mettre en œuvre dans cette hypothèse ;
- la réduction consiste à mettre en œuvre des mesures de sécurité. Ce sera l'objet des développements suivants.

Nous nous concentrerons sur les hypothèses 2 (risque **MODÉRÉ**) et 3 (risque **MAJEUR**) dans le but que le **risque résiduel,** c'est-à-dire le niveau de risque subsistant après la mise en place des mesures de sécurité, soit acceptable pour vous.

Hypothèse n° 2
STRATÉGIES DE TRAITEMENT DU RISQUE MODÉRÉ

Lorsque le niveau de risque est modéré, il convient de déterminer la stratégie de traitement du risque opportune : le risque peut être maintenu, car il est acceptable pour vous, ou au contraire réduit, car il est d'un niveau trop élevé

- dans cette hypothèse, nous vous recommandons **la mise en place de mesures de sécurité,** car elles sont simples à mettre en œuvre et d'un coût limité (analyse coût / bénéfice) :
  - la diminution de la gravité du risque réside dans la mise en place d'un **politique de sauvegarde plus fréquente dans le cabinet**
  - la diminution de la vraisemblance consiste, comme précédemment, **à ne pas laisser votre ordinateur sans surveillance et, si vous le laissez, il est nécessaire qu'il soit dans un endroit sûr** (ex. attaché au cadenas de votre bureau dans les locaux de votre cabinet)

CALCUL DE VOTRE **RISQUE RÉSIDUEL**

→ Une fois ces mesures mises en place, votre niveau de risque résiduel serait faible : la gravité du risque serait mineure et sa réalisation deviendrait peu vraisemblable.

→ On constate donc, à nouveau, la grande efficacité de mise en place de ces mesures de sécurité qui ne sont pas d'une grande complexité (technique ou organisationnelle)

Hypothèse n° 3
STRATÉGIES DE TRAITEMENT DU RISQUE MAJEUR

Si le niveau de risque est majeur (16), il est fortement recommandé de mettre en place deux types de mesures de sécurité pour réduire le risque :

MESURES POUR DIMINUER SA GRAVITÉ :

- **Mise en place de sauvegardes** en respectant les principes suivants :
  - identification des données à sauvegarder
  - diversification des solutions de sauvegarde (cf. fiche 4 du t. 1 du guide cyber)
  - détermination d'une fréquence de sauvegarde
  - Mise en place du **chiffrement des données de votre ordinateur** (cf. fiche 3 du t.1 du guide cyber)

MESURES POUR DIMINUER SA VRAISEMBLANCE :

- **ne jamais laisser votre ordinateur sans surveillance**
- si vous le laissez, **il est impératif qu'il soit dans un endroit sûr** (ex : attaché au cadenas de votre bureau lorsque vous quittez les locaux de votre cabinet ou dans un coffre-fort de votre chambre d'hôtel)

CALCUL DE VOTRE **RISQUE RÉSIDUEL**

→ Une fois ces mesures mises en place, votre niveau de risque résiduel serait :

- après la mise en place des mesures d'atténuation de la gravité du risque (sauvegarde et chiffrement) : gravité du risque mineur (G1)
- après la mise en place des mesures d'atténuation de la vraisemblance du risque : risque peu vraisemblable (2)
- soit un niveau de risque résiduel qui deviendrait faible (niveau 2 : 1x2)

→ On constate donc la grande efficacité de mise en place de ces mesures de sécurité qui ne sont pas d'une grande complexité (technique ou organisationnelle)

SCÉNARIO 2 : UN RANÇONGICIEL BLOQUE L'ACCÈS À MES DONNÉES CLIENTS OU À MES DONNÉES MÉTIER

IDENTIFICATION DU RISQUE

Le scénario est celui où vous arrivez un matin à votre cabinet et lorsque vous démarrez votre ordinateur, ce dernier est bloqué. Votre système d'information est victime d'un rançongiciel qui demande, le cas échéant, le paiement d'une rançon pour retrouver l'accès à vos données ou empêcher leur divulgation.

ANALYSE ET ÉVALUATION DU RISQUE

Pour apprécier ce risque, il est nécessaire d'adopter une approche contextuelle en simulant la situation de votre cabinet si le risque se réalisait en termes de disponibilité, d'intégrité et de confidentialité des données du cabinet.

En pratique, il s'agit de se poser la question suivante : si ce scénario se réalisait au sein de mon cabinet, quelles en seraient les conséquences ?

L'appréciation du risque dépend ainsi d'une double évaluation :

- L'évaluation de la **gravité (G)** des conséquences pour le cabinet si le risque se réalisait :
  - perte de client
  - mise en cause de la responsabilité civile professionnelle de l'avocat
  - sanction de la CNIL pour non-conformité au RGPD
  - poursuites déontologiques
  - atteinte réputationnelle
- L'évaluation de la probabilité de survenance du risque appelée vraisemblance du **risque (V).**

G

Évaluation de la GRAVITÉ du risque

Dans ce scénario, l'évaluation dépend de la gravité de la situation de votre cabinet si le risque se réalisait dépend des éléments suivants :

- **de l'ampleur de l'attaque :**
  - touche-t-elle le seul accès aux données client et métier du cabinet ? Toute activité est alors bloquée ?
  - touche-t-elle également l'accès aux moyens de communication du cabinet, les mails sont-ils aussi bloqués ?
  - L'attaquant menace-t-il de divulguer les données en cas de non-paiement d'une rançon ?
- **existence de sauvegarde qui détermine le délai de retour à la normale :**
  - quelques heures pour restaurer la sauvegarde de la veille
  - plusieurs jours ou plusieurs semaines pour récupérer vos données dans vos mails (si vous y avez toujours accès) et auprès de vos clients

NOTRE OBJECTIF :

Il est possible d'envisager différentes hypothèses dont la gravité varie en fonction des éléments d'évaluation mentionnés ci-dessus. Cette évaluation a pour objectif de répondre à la question suivante :

Quel est le niveau de sécurisation de votre système d'information ?

G1	G2	G3	G4
Ce type de situation n'est, en principe, pas d'une gravité mineure	L'attaque : ☐ **rend indisponible les données du cabinet** (client et base de connaissances) ☐ les moyens de communication du cabinet (mail) **demeurent disponibles** ☐ **l'attaquant ne menace pas de divulguer les données** en cas de non-paiement d'une rançon. ☐ il existe une sauvegarde récente, **plusieurs heures seront nécessaires pour un retour à la normale**	L'attaque : ☐ **rend indisponible les données du cabinet** (client et base de connaissances) ☐ les moyens de communication du cabinet (mail) **demeurent disponibles** ☐ **l'attaquant ne menace pas de divulguer les données** en cas de non-paiement d'une rançon ☐ en l'absence de sauvegarde récente, **plusieurs semaines seront nécessaires pour un retour à la normale**	L'attaque : ☐ **rend indisponible les données du cabinet** (client et base de connaissances) ☐ **rend indisponible les moyens de communication** du cabinet (mail) **L'attaquant menace de divulguer les données** en cas de non-paiement d'une rançon En l'absence de sauvegarde récente, **plusieurs semaines seront nécessaires pour un retour à la normale**
Mineure (Conséquences négligeables pour le cabinet)	**Significative** (Conséquences significatives mais limitées pour le cabinet)	**Grave** (Conséquences importantes pour le cabinet)	**Critique** (Conséquences désastreuses pour le cabinet avec d'éventuels impacts sur l'écosystème)

V

Évaluation de la VRAISEMBLANCE du risque

La vraisemblance de l'attaque dépend de l'organisation de votre cabinet :

- vos processus métier, en particulier votre vigilance et celle des membres de votre cabinet dans l'appréciation de la fiabilité des mails et pièces jointes ;
- et de la mise en place, dans votre cabinet (à la suite d'une attaque ou non), du socle de sécurité comme la sensibilisation des collaborateurs, l'installation d'un antivirus, de logiciel anti-hameçonnage ou de sauvegarde, ou encore la mise à jour de vos systèmes d'exploitation et logiciels.

ÉVALUATION DE LA VRAISEMBLANCE DU RISQUE	
V1 Invraisemblable	• Dans la situation actuelle, de recrudescence des attaques contre les cabinets d'avocat (cf. rapport déc. 2022), ce risque n'est pas invraisemblable
V2 Peu vraisemblable	• **Membres du cabinet sensibilisés** aux risques des mails (rançongiciels) et **logiciels antivirus et anti-hameçonnage** sont installés. • Les **mises à jour des systèmes d'exploitation et logiciels** sont effectuées.
V3 Vraisemblable	• **Absence de sensibilisation du cabinet** aux risques liés aux mails (rançongiciels) même si des logiciels antivirus et anti-hameçonnage sont installés
V4 Très vraisemblable	• **Absence de logiciel adapté** (antivirus et anti-hameçonnage). • **Absence de sensibilisation du cabinet** au risque des mails (rançongiciels). • **Mise à jour** des systèmes d'exploitation et des logiciels de votre cabinet **non faite.** • **Pas de politique de mots de passe forts** ni d'usage de mécanisme d'authentification multi facteurs.

RÉSULTAT : le niveau de risque

Selon la méthode, l'issue de cette appréciation est un résultat, le niveau de risque.

Ce niveau de risque se calcule dans son contexte (celui de votre cabinet) au moyen de la formule suivante :

Niveau de risque = Gravité x Vraisemblance.

En croisant les niveaux de gravité et de vraisemblance, vous obtiendrez le niveau de risque de votre cabinet qu'il est possible d'illustrer de la façon suivante :

	V VRAISEMBLANCE			
G GRAVITÉ	Invraisemblable	Peu vraisemblable	Vraisemblable	Très vraisemblable
Mineure	1	2	3	4
Significative	2	4	6	8
Grave	3	6	9	12
Critique	4	8	12	16

Le niveau de risque est déterminé par la multiplication de deux facteurs : la gravité du risque et sa vraisemblance.

Illustrons les résultats de ce tableau en raisonnant sur trois hypothèses correspondant à trois niveaux de risque différents.

NIVEAU DE RISQUE FAIBLE (1-6)

En effet, **un risque dont la gravité est critique** (G4) pour le cabinet **n'implique pas nécessairement un niveau de risque élevé** dès lors qu'il est invraisemblable (V1).

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V1 = 4

À l'inverse, il est possible qu'**un risque soit très vraisemblable** (V4), mais d'une **gravité mineure** (G1) : le risque est alors d'un niveau faible.

Ex : Niveau de risque = Gravité x Vraisemblance = G1 x V4 = 4

Un niveau de risque faible est encore possible lorsque la **gravité est significative** (G2) et que la probabilité de réalisation du **risque est peu vraisemblable** (V2).

Ex : Niveau de risque = Gravité x Vraisemblance = G2 x V2 = 4

NIVEAU DE RISQUE MODÉRÉ (8-9)

En effet, un risque dont la **gravité est critique** (G4) pour le cabinet peut exposer le cabinet à un niveau de risque modéré dès lors qu'il est **peu vraisemblable** (V2).

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V2 = 8

À l'inverse, un risque **très vraisemblable** (V4) peut exposer le cabinet à un niveau de risque modéré dès lors que sa **gravité est seulement significative** (G2).

Ex : Niveau de risque = Gravité x Vraisemblance = G2 x V4 = 8

Il est encore possible que le cabinet soit exposé à un niveau de risque modéré si les deux facteurs sont équilibrés car **le risque serait grave** (G3) et **sa réalisation vraisemblable** (V3)**.**

Ex : Niveau de risque = Gravité x Vraisemblance = G3 x V3 = 9

NIVEAU DE RISQUE ÉLEVÉ (12-16)

Dans ce cas, les deux facteurs de risque sont au niveau le plus élevé : la **gravité est critique** (G4) et sa réalisation **très vraisemblable** (V4)

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V4 = 16

En conclusion, pour réduire le niveau global du risque, il est possible de jouer sur l'un des deux facteurs, la gravité ou la vraisemblance du risque, en appliquant les mesures de traitement du risque.

TRAITEMENT DU RISQUE

Rappelons que dans le traitement du risque, différentes options sont possibles :

- l'acceptation et le refus du risque et ses conséquences qui n'appellent pas de commentaire particulier ;
- le partage et la réduction du risque qui seront l'objet des développements suivants.

Nous nous concentrerons sur les hypothèses 3 (risque **MAJEUR**) et 2 (risque **MODÉRÉ**) et dans le but que le **risque résiduel**, c'est-à-dire le niveau de risque subsistant après la mise en place des mesures de sécurité, soit acceptable pour vous.

Hypothèse n° 3
STRATÉGIES DE TRAITEMENT DU RISQUE MAJEUR

Si le niveau de risque est majeur (16), il est fortement recommandé de mettre en place une stratégie de partage et de réduction du risque :

MESURES JOUANT SUR LA GRAVITÉ DU RISQUE :

- **la mise en place d'un plan de sauvegarde** pour s'assurer d'un redémarrage rapide de l'activité. Ce plan doit respecter les principes suivants (cf. fiche 4 du t. 1 du guide cyber) :
  - identification des données à sauvegarder
  - la diversification des solutions de sauvegarde
  - selon une fréquence de sauvegarde définie
- une solution est aussi de partager le risque en souscrivant **une police d'assurance cyber qui vous accompagnera en cas de cyberattaque de votre cabinet**

MESURES JOUANT SUR LA VRAISEMBLANCE DU RISQUE :

il est possible de mettre en place plusieurs mesures qui diminuent la vraisemblance de la survenance de ce risque :

- installation d'un **logiciel d'antivirus et d'anti-hameçonnage** (fiche 3 du t. 1 du guide cyber)
- **le maintien à jour de vos logiciels** qui corrige les failles de sécurité (fiche 3 du t.1 du guide cyber)
- **sensibilisation des membres du cabinet aux risques cyber** dans l'utilisation des mails en mettant en place des formations, une charte informatique (fiche 9 du t.1 du guide cyber).

CALCUL DE VOTRE **RISQUE RÉSIDUEL**

→ Une fois ces mesures mises en place, votre niveau de risque résiduel serait faible :

- la gravité du risque passerait de critique (qui met en jeu la survie du cabinet) à significatif (votre assurance cyber, si vous en avez une, pouvant prendre en charge la négociation avec l'attaquant et la question de la rançon) ;
- après la mise en place des mesures d'atténuation de la vraisem blance du risque, le risque pourrait devenir peu vraisemblable (2)
- soit un niveau de risque qui deviendrait faible (niveau 4 : 2x2)

→ À nouveau, ces mesures (techniques et organisationnelles), qui ne sont pas d'une grande complexité, ont une grande efficacité en matière de sécurité cyber

POUR ALLER PLUS LOIN

Pour réduire encore votre risque, vous pouvez étudier la possibilité de mettre en place un SOC (*Security Operation Center*) dont l'un des objectifs est d'opérer, au moyen de logs, une surveillance continue d'un système d'information en détectant les activités anormales dont certaines sont des attaques cyber. La mise en place d'un SOC suppose de recourir à un expert en cybersécurité, ce qui nécessitera des investissements financiers pour votre cabinet et un certain temps de déploiement. Tout dépendra alors d'une analyse coût / bénéfice.

Hypothèse n° 2
STRATÉGIES DE TRAITEMENT DU RISQUE MODÉRÉ

Lorsque le niveau de risque est modéré, il convient de déterminer la stratégie de traitement du risque opportune : le risque peut être maintenu, car il est acceptable pour vous, ou au contraire réduit ou partagé, car il est d'un niveau trop élevé :

- dans cette hypothèse, nous vous recommandons **la mise en place de mesures de sécurité,** car elles sont simples a mettre en œuvre et d'un cout limité après une analyse cout / bénéfice (cf. hypothèse 2 pour les mesures à mettre en œuvre)
- Comme dans l'hypothèse 3, la gravité du risque est maitrisable par la mise en place d'**un plan de sauvegarde** et par **la souscription d'une police d'assurance,** ou **la mise en place d'un SOC**

CALCUL DE VOTRE **RISQUE RÉSIDUEL**

→ Une fois ces mesures mises en place, votre niveau de risque résiduel serait faible **(niveau 2 : 1x2)** : la gravité du risque serait mineure et il deviendrait peu vraisemblable

SCÉNARIO 3 : UN NOUVEAU DOSSIER FAIT PESER UN RISQUE CYBER SUR LE CABINET

IDENTIFICATION DU RISQUE

Votre cabinet représente une entreprise spécialisée dans les technologies innovantes. Cette entreprise est sur le point de déposer un brevet pour un procédé révolutionnaire dans son domaine et vous l'accompagnez dans ce processus. Conscient de la valeur stratégique et économique de ces informations, un concurrent de votre client ou un Etat cherche à s'en emparer pour gagner un avantage concurrentiel.

Afin d'obtenir des informations confidentielles sur le procédé ou le produit, le concurrent ou un Etat décide, dans un premier temps, de pirater le système d'information de votre cabinet en usurpant l'identité ou en corrompant l'un de vos collaborateurs. S'il ne parvient pas à ses fins, il pourra mettre en œuvre des attaques plus sophistiquées avec un effet d'escalade.

Les informations dérobées sont ensuite publiées dans la presse, les conséquences sur la réputation de votre cabinet sont importantes.

Cet exemple est intéressant, car il montre que l'analyse de risques du cabinet peut être amenée à évoluer au cours de la vie du cabinet, notamment au moment de l'acquisition de nouveaux clients.

ANALYSE ET ÉVALUATION DU RISQUE

Pour apprécier ce risque, il est nécessaire d'adopter une approche contextuelle en simulant la situation de votre cabinet si le risque se réalisait en termes de disponibilité, d'intégrité et de confidentialité des données du cabinet.

En pratique, il s'agit de se poser la question suivante : si ce scénario se réalisait au sein de mon cabinet, quelles en seraient les conséquences ?

L'appréciation du risque dépend ainsi d'une double évaluation :

- L'évaluation de la **gravité (G)** des conséquences pour le cabinet si le risque se réalisait :
  - perte de client
  - mise en cause de la responsabilité civile professionnelle de l'avocat
  - sanction de la CNIL pour non-conformité au RGPD
  - poursuites déontologiques
  - atteinte réputationnelle
- L'évaluation de la probabilité de survenance du risque appelée vraisemblance du **risque (V).**

G

Évaluation de la GRAVITÉ du risque

Dans ce scénario, l'évaluation de la gravité de la situation de votre cabinet si le risque se réalisait dépend, dans ce scénario, de plusieurs éléments :

- l'accessibilité des données clients visées : les données particulièrement stratégiques et/ou sensibles sont-elles protégées par un mécanisme de chiffrement dans votre cabinet ?
- le niveau de risque réputationnel pour votre cabinet : quelle(s) serai(en)t les conséquences pour votre cabinet, et pour votre client, si les informations relatives à un procédé révolutionnaire sont divulguées avant le dépôt du brevet ?

NOTRE OBJECTIF :

Il est possible d'envisager différentes hypothèses dont la gravité varie en fonction des éléments d'évaluation mentionnés ci-dessus. Cette évaluation a pour objectif de répondre à la question suivante :

Quel est le niveau de sécurisation de votre système d'information ?

Ce type de situation n'est pas d'une gravité mineure	☐ Les **données stratégiques** et économiques dérobées sont **chiffrées** Ni la source de l'attaque, ni le concurrent ou l'Etat ayant ciblé le cabinet **ne peut lire le contenu des données dérobées**	☐ **Les données stratégiques et économiques dérobées sont en clairs,** toutefois seules les personnes concernées sont informées de l'attaque Dans cette situation, les conséquences réputationnelles (perte de confiance, perte potentielle de clients futurs) **sont présentes mais moindres**	☐ **Les données stratégiques et économiques dérobées sont en claires** et la presse communique sur cette attaque Dans cette situation, les conséquences réputationnelles pour le cabinet sont telles que **le cabinet n'est pas certain de pouvoir s'en remettre**
G1 **Mineure** (Conséquences négligeables pour le cabinet)	**G2** **Significative** (Conséquences significatives mais limitées pour le cabinet)	**G3** **Grave** (Conséquences importantes pour le cabinet)	**G4** **Critique** (Conséquences désastreuses pour le cabinet avec d'éventuels impacts sur l'écosystème)

V

Évaluation de la VRAISEMBLANCE du risque

Pour évaluer cette vraisemblance, il est important de prendre en compte plusieurs facteurs qui influencent la probabilité de survenance de cet évènement :

- avez-vous déjà subi une attaque (ou une tentative d'attaque) similaire par le passé ?
- les données visées sont-elles précieuses pour des attaquants potentiels ?
- les informations sensibles comme les secrets de fabrication ou les brevets attirent-elles des menaces spécifiques ?

Quel est le niveau de motivation (en fonction de l'objectif visé) de la source du risque et les moyens dont elle dispose pour mener à bien son attaque ? Une fois la source de l'attaque et son objectif visé identifié (un concurrent de votre client, un Etat voulant mettre la main sur le brevet de votre client), la vraisemblance du risque dépendra de la motivation et des moyens de la source de risques. Une personne motivée avec des moyens rend le risque plus vraisemblable.

Le chemin d'attaque dépend grandement de l'organisation de votre cabinet et de la mise en place d'un SOC (Security Operation Center) dont l'un des objectifs est d'opérer, au moyen de logs, une surveillance continue d'un système d'information en détectant les activités anormales dont certaines sont des attaques cyber. Cette surveillance continue permet une réaction rapide en cas d'attaque. La mise en place d'un SOC suppose de recourir à un expert en cybersécurité, ce qui nécessitera des investissements financiers, qui peuvent être importants, pour votre cabinet.

D'autres questions peuvent également permettre d'évaluer la vraisemblance de ce risque dans l'organisation de votre cabinet :

- quelle(s) information(s) sur mes collaborateurs sont disponibles publiquement ? Comment pourraient-elles être utilisées par une personne malveillante ?
- les membres du cabinet sont-ils en mesure d'identifier un e-mail de phishing ?
- utilise-t-on des méthodes d'authentification robustes pour l'accès aux dossiers les plus sensibles (ex. l'authentification multi facteurs) ?
- ai-je la possibilité de surveiller les connexions et activités menées sur le système d'information du cabinet et de détecter rapidement des comportements suspects (mise en place d'un SOC) ?

ÉVALUATION DE LA VRAISEMBLANCE DU RISQUE

V1 **Invraisemblable**	• **Accès très limité aux informations** sur le cabinet et ses membres • **Sensibilisation importante des membres** du cabinet aux risques cyber • **Mesures d'authentifications multi facteurs** et contrôle stricts • **Mesures organisationnelles et techniques de sécurité robuste** et surveillance constante des accès et activités menées sur le SI du cabinet **(mis en place d'un SOC)** • **La source du risque est peu motivée** et elle dispose de **moyens très limités**
V2 **Peu vraisemblable**	• **Accès limité aux informations** sur le cabinet et ses membres • **Sensibilisation régulière des membres** du cabinet aux risques cyber • **Mesures d'authentification forte** • **Protocoles de sécurité importants** et surveillance régulière des accès et activités menées sur le SI du cabinet **(SOC mis en place)** • **La source du risque est peu motivée** et elle dispose de **moyens limités**
V3 **Vraisemblable**	• **Accès à des informations susceptibles d'être utilisées par des personnes mal intentionnées** sur le cabinet et/ou ses membres • **Rare sensibilisation des membres** du cabinet aux risques cyber • **Mesures d'authentification simple** • **Protocoles de sécurité faibles** et surveillance rare des accès et activités menées sur le SI du cabinet **(pas de mise en place d'un SOC)** • **La source du risque est motivée** et elle dispose de **moyens importants**
V4 **Très vraisemblable**	• **Diffuser des informations de nature de professionnelle** sur les réseaux sociaux • **Pas ou peu de sensibilisation des membres** du cabinet aux risques cyber • **Pas ou peu de mesure d'authentification supplémentaire** • **Pas de protocole de sécurité** ni surveillance des accès et activités menées sur le SI du cabinet • **Un incident de ce type s'est déjà produit** • **Vous n'avez pas mis en place de SOC** • **La source du risque est très motivée** et elle dispose de **moyens considérables**

RÉSULTAT : le niveau de risque

Selon la méthode, l'issue de cette appréciation est un résultat, le niveau de risque.

Ce niveau de risque se calcule dans son contexte (celui de votre cabinet) au moyen de la formule suivante :

Niveau de risque = Gravité x Vraisemblance.

En croisant les niveaux de gravité et de vraisemblance, vous obtiendrez le niveau de risque de votre cabinet qu'il est possible d'illustrer de la façon suivante :

	V VRAISEMBLANCE			
G GRAVITÉ	Invraisemblable	Peu vraisemblable	Vraisemblable	Très vraisemblable
Mineure	1	2	3	4
Significative	2	4	6	8
Grave	3	6	9	12
Critique	4	8	12	16

Le niveau de risque est déterminé par la multiplication de deux facteurs : la gravité du risque et sa vraisemblance.

Illustrons les résultats de ce tableau en raisonnant sur trois hypothèses correspondant à trois niveaux de risque différents.

NIVEAU DE RISQUE FAIBLE (1-6)

En effet, **un risque dont la gravité est critique** (G4) pour le cabinet **n'implique pas nécessairement un niveau de risque élevé** dès lors qu'il est invraisemblable (V1).

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V1 = 4

À l'inverse, il est possible qu'**un risque soit très vraisemblable** (V4), mais d'une **gravité mineure** (G1) : le risque est alors d'un niveau faible.

Ex : Niveau de risque = Gravité x Vraisemblance = G1 x V4 = 4

Un niveau de risque faible est encore possible lorsque la **gravité est significative** (G2) et que la probabilité de réalisation du **risque est peu vraisemblable** (V2).

Ex : Niveau de risque = Gravité x Vraisemblance = G2 x V2 = 4

NIVEAU DE RISQUE MODÉRÉ (8-9)

En effet, un risque dont la **gravité est critique** (G4) pour le cabinet peut exposer le cabinet à un niveau de risque modéré dès lors qu'il est **peu vraisemblable** (V2).

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V2 = 8

À l'inverse, un risque **très vraisemblable** (V4) peut exposer le cabinet à un niveau de risque modéré dès lors que sa **gravité est seulement significative** (G2).

Ex : Niveau de risque = Gravité x Vraisemblance = G2 x V4 = 8

Il est encore possible que le cabinet soit exposé à un niveau de risque modéré si les deux facteurs sont équilibrés car **le risque serait grave** (G3) et **sa réalisation vraisemblable** (V3)**.**

Ex : Niveau de risque = Gravité x Vraisemblance = G3 x V3 = 9

NIVEAU DE RISQUE ÉLEVÉ (12-16)

Dans ce cas, les deux facteurs de risque sont au niveau le plus élevé : la **gravité est critique** (G4) et sa réalisation **très vraisemblable** (V4)

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V4 = 16

En conclusion, pour réduire le niveau global du risque, il est possible de jouer sur l'un des deux facteurs, la gravité ou la vraisemblance du risque, en appliquant les mesures de traitement du risque.

TRAITEMENT DU RISQUE

COMME ÉVOQUÉ PRÉCÉDEMMENT, QUATRE OPTIONS DE TRAITEMENT DU RISQUE S'OFFRENT À VOUS :

- l'acceptation du risque et de ses conséquences : en effet, il est tout à fait possible pour vous de choisir d'accepter le risque, si vous estimez que les coûts pour prévenir ce risque sont disproportionnés pour votre cabinet et que le survenance du risque vous paraît peu vraisemblable ;
- le refus du risque : dans une situation aussi sensible, votre cabinet peut prendre la décision de refuser ce risque et prendre la décision de ne pas accepter de prendre ce dossier impliquant des informations extrêmement sensibles et/ou stratégiques, afin de ne pas exposer votre cabinet aux conséquences de la réalisation de ce risque ;
- le partage du risque avec un tiers (ex. souscrire à une assurance cyber, faire appel à sous-traitant en raison de la technicité du dossier) ;
- la réduction du risque, qui consiste dans cette situation à mettre en œuvre de mesures de sécurité afin de réduire la probabilité ou l'impact de ce risque.

Nous nous concentrerons sur les hypothèses 2 (risque **MODÉRÉ**) et 3 (risque **MAJEUR**) et sur les mesures de réduction ou de partage du risque dans le but que le risque résiduel, c'est-à-dire le niveau de risque subsistant après la mise en place des mesures de sécurité, soit acceptable pour vous.

Hypothèse n° 2
STRATÉGIES DE TRAITEMENT DU RISQUE MODÉRÉ

Lorsque le niveau de risque est modéré, il convient de déterminer la stratégie de traitement du risque opportune : le risque peut être maintenu, car il est acceptable pour vous, ou au contraire réduit ou partagé, car il est d'un niveau trop élevé :

Pour cela, il est possible de contribuer à réduire la gravité et la vraisemblance de ce risque :

- la gravité d'une part, **en mettant en place des mesures de chiffrement des dossiers les plus sensibles**
- la vraisemblance d'autre part, **en intégrant dans votre cabinet des mesures d'authentification multi facteurs ou en mettant en place un SOC** par exemple

CALCUL DE VOTRE **RISQUE RÉSIDUEL**

→ Une fois ces mesures mises en place, votre niveau de risque résiduel serait faible **(niveau 2 : 1x2)** : la gravité du risque serait mineure (G1) et il deviendrait peu vraisemblable (V2)

Hypothèse n° 3
STRATÉGIES DE TRAITEMENT DU RISQUE MAJEUR

Si le niveau de risque est majeur (16), il est fortement recommandé de mettre en place une stratégie de partage et de réduction du risque :

MESURE POUR DIMINUER SA GRAVITÉ :

- **Mesures de chiffrement des dossiers les plus sensibles**

MESURES POUR DIMINUER SA VRAISEMBLANCE :

- **il est possible de mettre en place plusieurs mesures qui diminuent la vraisemblance de la survenance de ce risque :**
  - la sensibilisation des membres du cabinet sur les risques cyber et notamment ceux liés à la communication d'informations sur les réseaux sociaux
  - la mise en place de systèmes d'authentification robustes
  - la surveillance régulière des accès et activités menées sur le SI du cabinet en mettant en place un SOC (qui est un process complexe qui demande des investissements financiers)
  - si la motivation et les moyens de l'attaquant sont importants, il sera nécessaire de mettre en place des mesures de sécurité avec un expert cyber

CALCUL DE VOTRE **RISQUE RÉSIDUEL**

→ Une fois ces mesures mises en place, votre niveau de risque résiduel serait faible :

- la gravité du risque passerait de critique (qui met en jeu la survie du cabinet) à **mineure (G1) ;**
- après la mise en place des mesures d'atténuation de la vraisemblance du risque, le risque pourrait devenir **peu vraisemblable (V2)**
- **soit un niveau de risque qui deviendrait faible (niveau 4 : 2x2)**

SCÉNARIO 4 : UN TIERS A ACCÈS À MA BOITE MAIL ET DÉTOURNE DES FONDS CARPA (USURPATION D'IDENTITÉ ET FALSIFICATION DE RIB)

IDENTIFICATION DU RISQUE

L'arnaque au faux RIB a pour objectif de tromper la victime, en usurpant l'identité d'un créancier avec lequel elle est en relation, afin de lui faire réaliser un virement vers un compte bancaire détenu par un escroc.

Ce type d'escroquerie résulte souvent du piratage d'un compte de messagerie électronique. Cela peut concerner le compte mail du créancier avec lequel la victime est en contact, ou bien celui de la victime elle-même, que l'escroc aura pris en main.

Dans ce scénario, un cyberattaquant pirate votre messagerie électronique et intercepte vos mails. Il intercepte dans ces messages votre RIB original et le remplace par un RIB frauduleux, sur lequel figurent ses données bancaires, et le transmet au client débiteur (flux entrant CARPA) ou à la CARPA (flux sortant) le tout au préjudice du bénéficiaire légitime.

ANALYSE ET ÉVALUATION DU RISQUE

Pour apprécier ce risque, il est nécessaire d'adopter une approche contextuelle en simulant la situation de votre cabinet si le risque se réalisait en termes de disponibilité, d'intégrité et de confidentialité des données du cabinet.

En pratique, il s'agit de se poser la question suivante : si ce scénario se réalisait au sein de mon cabinet, quelles en seraient les conséquences ?

L'appréciation du risque dépend ainsi d'une double évaluation :

- L'évaluation de la **gravité (G)** des conséquences pour le cabinet si le risque se réalisait :
  - perte de client
  - mise en cause de la responsabilité civile professionnelle de l'avocat
  - sanction de la CNIL pour non-conformité au RGPD
  - poursuites déontologiques
  - atteinte réputationnelle
- L'évaluation de la probabilité de survenance du risque appelée vraisemblance du **risque (V).**

G

Évaluation de la GRAVITÉ du risque

Dans ce scénario l'évaluation de la gravité de la situation de votre cabinet si le risque se réalisait dépend de plusieurs éléments :

- **la souscription du cabinet à un contrat d'assurance cyber risque qui couvre les dommages liés aux incidents cyber ;**
- l'article L.12-10-1 du Code des assurances prévoit que pour pouvoir être indemnisé des pertes et dommages causés par une atteinte à un système de traitement automatisé de données, l'assuré doit déposer plainte auprès des autorités compétentes au plus tard 72h00 après la connaissance de l'atteinte.

NOTRE OBJECTIF :

Il est possible d'envisager différentes hypothèses dont la gravité varie en fonction des éléments d'évaluation mentionnés ci-dessus. Cette évaluation a pour objectif de répondre à la question suivante :

Quel est votre niveau de sécurité numérique ?

G1	G2	G3	G4
☐ **Un contrat d'assurance cyber a été souscrit** par le cabinet ☐ **Pas de risque réputationnel**	☐ **Un contrat d'assurance** cyber a été souscrit par le cabinet ☐ **Risque réputationnel**	☐ **Aucun contrat d'assurance cyber n'a été souscrit** par le cabinet Le détournement de fonds est important mais **la survie du cabinet n'est pas menacée et sans risque réputationnel**	☐ **Aucun contrat d'assurance cyber n'a été souscrit** par le cabinet Le détournement de fonds est si important qu'il **met en péril la survie du cabinet et la réputation du cabinet est entachée**
Mineure (Conséquences négligeables pour le cabinet)	**Significative** (Conséquences significatives mais limitées pour le cabinet)	**Grave** (Conséquences importantes pour le cabinet)	**Critique** (Conséquences désastreuses pour le cabinet avec d'éventuels impacts sur l'écosystème)

Évaluation de la VRAISEMBLANCE du risque

Cette évaluation dépend des éléments suivants :

- le niveau de sécurité de la messagerie électronique utilisée par le cabinet ;
- les mesures d'organisation interne au cabinet et la procédure de communication et de vérification des RIB ;
- solution de messagerie électronique utilisée par le cabinet ;
- robustesse des mots de passe définis sur ces solutions ;
- chiffrement des données échangées

La vraisemblance de perte ou de vol ne dépend pas que de l'utilisation d'outils informatiques, mais aussi de mesures organisationnelles mises en place au sein du cabinet.

ÉVALUATION DE LA VRAISEMBLANCE DU RISQUE	
V1 Invraisemblable	• Utilisation d'**une solution de messagerie sécurisée** • **Communication des RIB via des outils de partage sécurisés** différents de ma messagerie professionnelle • **Sensibilisation aux risques cyber** • **Une procédure de vérification des coordonnées bancaires** communiquées est mise en place
V2 Peu vraisemblable	• Utilisation d'une **solution de messagerie sécurisée** pour communiquer mon RIB à mes créanciers • **Sensibilisation aux risques cyber** • **Une procédure de vérification des coordonnées bancaires** communiquées est mise en place
V3 Vraisemblable	• Utilisation d'une solution de **messagerie électronique grand public non sécurisée** pour communiquer mon RIB à mes créanciers • **Faible sensibilisation aux risques cyber mais les outils sont mis à jour et les mots de passe sont robustes** • **Aucune procédure de vérification des coordonnées bancaires** communiquées n'est mise en place
V4 Très vraisemblable	• Utilisation d'une solution de **messagerie électronique grand public non sécurisée** pour communiquer mon RIB à mes créanciers • **Les mots de passe utilisés sont basiques** • Les outils informatiques du cabinet ne sont **pas toujours mis à jour** • **Aucune procédure de vérification des coordonnées bancaires** communiquées n'est mise en place • **Non-sensibilisation aux risques cyber**

RÉSULTAT : le niveau de risque

Selon la méthode, l'issue de cette appréciation est un résultat, le niveau de risque.

Ce niveau de risque se calcule dans son contexte (celui de votre cabinet) au moyen de la formule suivante :

Niveau de risque = Gravité x Vraisemblance.

En croisant les niveaux de gravité et de vraisemblance, vous obtiendrez le niveau de risque de votre cabinet qu'il est possible d'illustrer de la façon suivante :

	V VRAISEMBLANCE			
G GRAVITÉ	Invraisemblable	Peu vraisemblable	Vraisemblable	Très vraisemblable
Mineure	1	2	3	4
Significative	2	4	6	8
Grave	3	6	9	12
Critique	4	8	12	16

Le niveau de risque est déterminé par la multiplication de deux facteurs : la gravité du risque et sa vraisemblance.

Illustrons les résultats de ce tableau en raisonnant sur trois hypothèses correspondant à trois niveaux de risque différents.

NIVEAU DE RISQUE FAIBLE (1-6)

En effet, **un risque dont la gravité est critique** (G4) pour le cabinet **n'implique pas nécessairement un niveau de risque élevé** dès lors qu'il est invraisemblable (V1).

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V1 = 4

À l'inverse, il est possible qu'**un risque soit très vraisemblable** (V4), mais d'une **gravité mineure** (G1) : le risque est alors d'un niveau faible.

Ex : Niveau de risque = Gravité x Vraisemblance = G1 x V4 = 4

Un niveau de risque faible est encore possible lorsque la **gravité est significative** (G2) et que la probabilité de réalisation du **risque est peu vraisemblable** (V2).

Ex : Niveau de risque = Gravité x Vraisemblance = G2 x V2 = 4

NIVEAU DE RISQUE MODÉRÉ (8-9)

En effet, un risque dont la **gravité est critique** (G4) pour le cabinet peut exposer le cabinet à un niveau de risque modéré dès lors qu'il est **peu vraisemblable** (V2).

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V2 = 8

À l'inverse, un risque **très vraisemblable** (V4) peut exposer le cabinet à un niveau de risque modéré dès lors que sa **gravité est seulement significative** (G2).

Ex : Niveau de risque = Gravité x Vraisemblance = G2 x V4 = 8

Il est encore possible que le cabinet soit exposé à un niveau de risque modéré si les deux facteurs sont équilibrés car **le risque serait grave** (G3) et **sa réalisation vraisemblable** (V3)**.**

Ex : Niveau de risque = Gravité x Vraisemblance = G3 x V3 = 9

NIVEAU DE RISQUE ÉLEVÉ (12-16)

Dans ce cas, les deux facteurs de risque sont au niveau le plus élevé : la **gravité est critique** (G4) et sa réalisation **très vraisemblable** (V4)

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V4 = 16

En conclusion, pour réduire le niveau global du risque, il est possible de jouer sur l'un des deux facteurs, la gravité ou la vraisemblance du risque, en appliquant les mesures de traitement du risque.

TRAITEMENT DU RISQUE

Comme évoqué précédemment, quatre options de traitement du risque s'offrent à vous :

- l'acceptation du risque et de ses conséquences : en effet, il est tout à fait possible pour vous de choisir d'accepter le risque, si vous estimez que les coûts pour prévenir ce risque sont disproportionnés pour votre cabinet et que la survenance du risque vous paraît peu vraisemblable ;
- le refus du risque : dans une situation aussi sensible, votre cabinet peut prendre la décision de refuser ce risque et prendre la décision de ne pas accepter de prendre ce dossier impliquant des informations extrêmement sensibles et/ou stratégiques, afin de ne pas exposer votre cabinet aux conséquences de la réalisation de ce risque ;
- le partage du risque avec un tiers (ex. souscrire à une assurance cyber) ;
- la réduction du risque, qui consiste dans cette situation à mettre en œuvre de mesures de sécurité afin de réduire la probabilité ou l'impact de ce risque.

Nous nous concentrerons sur les hypothèses 2 (risque modéré) et 3 (risque majeur) et sur les mesures de réduction ou de partage du risque dans le but que le risque résiduel, c'est-à-dire le niveau de risque subsistant après la mise en place des mesures de sécurité, soit acceptable pour vous.

Hypothèse n° 2
STRATÉGIES DE TRAITEMENT DU RISQUE MODÉRÉ

Lorsque le niveau de risque est modéré, il convient de déterminer la stratégie de traitement du risque opportune : le risque peut être maintenu, car il est acceptable pour vous, ou au contraire réduit ou partagé, car il est d'un niveau trop élevé :

MESURE JOUANT SUR LA GRAVITÉ DU RISQUE :

- souscription d'une police d'assurance cyber

MESURES JOUANT SUR LA VRAISEMBLANCE DU RISQUE :

- en utilisant une solution de partage de fichier sécurisée
- en mettant en place une procédure de vérification des coordonnées du RIB auprès du créancier/débiteur

CALCUL DE VOTRE **RISQUE RÉSIDUEL**

→ Une fois ces mesures mises en place, votre niveau de risque résiduel serait faible **(niveau 2 : 1x2) :** la gravité du risque serait mineure et il deviendrait peu vraisemblable

→ Ce niveau de risque résiduel serait atteint par la mise en place de mesures techniques et organisationnelles relativement simples

→ la réduction de la gravité du risque, par la souscription d'une assurance cyber, nécessite un investissement financier qu'il sera nécessaire d'arbitrer selon une méthode coût / bénéfice

Hypothèse n° 3
STRATÉGIES DE TRAITEMENT DU RISQUE MAJEUR

Si le niveau de risque est majeur (16), il est fortement recommandé de mettre en place deux types de mesures de sécurité pour réduire le risque :

MESURE POUR DIMINUER SA GRAVITÉ :

- **souscription d'une police d'assurance cyber**

MESURES POUR DIMINUER SA VRAISEMBLANCE :

- **la sensibilisation des membres du cabinet** sur les risques cyber,
- l'utilisation d'**outil numérique sécurisé,**
- la mise en place d'**un socle de sécurité numérique de base,**
- la mise en place d'**une procédure de vérification et de validation de la modification des RIB.**

CALCUL DE VOTRE **RISQUE RÉSIDUEL**

→ Une fois ces mesures mises en place, votre niveau de risque résiduel serait faible : la gravité serait atténuée par **la souscription d'une police d'assurance (G1)** et la probabilité de survenance du risque serait **peu vraisemblable (V2) voire invraisemblable (V1)**

→ Ce niveau de risque résiduel serait atteint par la mise en place de mesures techniques et organisationnelles relativement simples

→ la réduction de la gravité du risque, par la souscription d'une assurance cyber, nécessite un investissement financier qu'il sera nécessaire d'arbitrer selon une méthode coût / bénéfice

SCÉNARIO 5 : UN MEMBRE QUITTE LE CABINET POUR MONTER SON PROPRE CABINET (OU POUR REJOINDRE UN CABINET EXISTANT) ET PART AVEC TOUT OU PARTIE DES DOSSIERS CLIENTS

IDENTIFICATION DU RISQUE

Dans ce scénario, un membre quitte le cabinet et emporte avec lui tout ou partie des dossiers clients du cabinet, conscient de l'importance de ces informations.

Par membre nous entendons au sens large : un associé, un collaborateur libéral ou salarié ou un salarié du cabinet (ex. un juriste devenu avocat)

Ce type de situation peut présenter un risque majeur pour la confidentialité des informations, la réputation du cabinet et la clientèle du cabinet.

ANALYSE ET ÉVALUATION DU RISQUE

Pour apprécier ce risque, il est nécessaire d'adopter une approche contextuelle en simulant la situation de votre cabinet si le risque se réalisait en termes de disponibilité, d'intégrité et de confidentialité des données du cabinet.

En pratique, il s'agit de se poser la question suivante : si ce scénario se réalisait au sein de mon cabinet, quelles en seraient les conséquences ?

L'appréciation du risque dépend ainsi d'une double évaluation :

- L'évaluation de la **gravité (G)** des conséquences pour le cabinet si le risque se réalisait :
  - perte de client
  - mise en cause de la responsabilité civile professionnelle de l'avocat
  - sanction de la CNIL pour non-conformité au RGPD
  - poursuites déontologiques
  - atteinte réputationnelle
- L'évaluation de la probabilité de survenance du risque appelée vraisemblance du **risque (V).**

G

Évaluation de la GRAVITÉ du risque

Dans ce scénario, l'évaluation de la gravité du risque consiste à déterminer l'impact potentiel sur votre cabinet si ce risque se réalise. Celle-ci dépend des éléments suivants :

- **l'ampleur de la fuite, à la fois en termes de perte de client, conséquences juridiques et réputationnelles :**
  - quels types d'informations sensibles sont contenues dans les dossiers clients ?
  - quel est le nombre de dossiers clients concernés ?
  - quelle est la valeur financière de ces clients pour votre cabinet ?
  - quelles seraient les conséquences juridiques (légales, déontologiques) d'une telle fuite d'informations ?
- **le niveau de risque réputationnel pour votre cabinet**

NOTRE OBJECTIF :

Il est possible d'envisager différentes hypothèses dont la gravite varie en fonction des éléments d'evaluation mentionnes ci-dessus. Cette évaluation a pour objectif de répondre a la question suivante :

Quel est le niveau de sécurisation de votre système d'information ?

G1 — Mineure (Conséquences négligeables pour le cabinet)	G2 — Significative (Conséquences significatives mais limitées pour le cabinet)	G3 — Grave (Conséquences importantes pour le cabinet)	G4 — Critique (Conséquences désastreuses pour le cabinet avec d'éventuels impacts sur l'écosystème)
L'attaque : ☐ concerne **un nombre mineur de dossiers** ☐ concerne **des informations générales et non sensibles** ☐ **présente un faible impact financier** ☐ ne présente pas ou peu d'impact sur votre activité	L'attaque : ☐ concerne un **nombre modéré de dossiers** ☐ concerne des **informations internes et/ou non sensibles** ☐ **présente un impact financier modéré** ☐ **présente un impact modéré** (quelques clients sont affectés)	L'attaque : ☐ concerne **un nombre important de dossiers** ☐ concerne **des informations confidentielles et** des données clients sensibles ☐ présente un impact financier élevé ☐ **présente un impact important** sur votre activité (perte de nombreux clients	L'attaque : ☐ **concerne un nombre de dossiers significatif,** au regard du portefeuille de client dans votre cabinet ☐ **concerne des dossiers particulièrement sensibles** (informations stratégiques et économiques, secrets commerciaux, brevets, etc.) ☐ **présente un impact financier** très élevé pour votre cabinet ☐ **présente un impact catastrophique** sur votre activité (perte de client considérable, conséquences réputationnelles)

V

Évaluation de la VRAISEMBLANCE du risque

L'évaluation de la vraisemblance du risque consiste quant à elle à estimer la probabilité que ce risque se réalise au sein de votre cabinet.

Pour évaluer cette vraisemblance il est important de prendre en compte plusieurs facteurs qui influencent la probabilité d'occurrence de cet évènement :

- **de la source du risque et du chemin de l'attaque :**
  - dans cette situation, il s'agira d'une attaque ciblée commise par un ancien membre du cabinet, qui aura transféré sans autorisation tout ou partie des dossiers clients pour lui avant son départ ;
- **de l'organisation de votre cabinet :**
  - le membre a-t-il un accès régulier et direct aux dossiers clients ?
  - quels sont les protocoles de sécurité mis en place au sein de votre cabinet pour contrôler l'accès aux informations sensibles (ex. contrôle des accès, authentification multi facteurs, surveillance des activités avec la mise en place d'un SOC, etc.) ?
  - des accords de confidentialité et de non-concurrence ont-ils été signés ?
  - ce membre a-t-il déjà eu un comportement suspect ?
  - avez-vous mis en place des mesures de protection et de surveillance pour détecter et empêcher le transfert non autorisé de données ?

ÉVALUATION DE LA VRAISEMBLANCE DU RISQUE	
V1 **Invraisemblable**	• **Accès très limité** aux dossiers du cabinet • **Protocoles de sécurité robustes et surveillance continue** • **Clauses de non-concurrence et accords de confidentialité stricte et appliquée** • Aucun antécédent et **comportement irréprochable**
V2 **Peu vraisemblable**	• **Accès partiel et contrôlé aux dossiers** du cabinet • **Protocoles de sécurité importants et surveillance régulière** • **Clauses de non-concurrence et accords de confidentialité partiellement appliqués** • Nombre d'**incidents mineurs**
V3 **Vraisemblable**	• **Accès régulier et non surveillé** à l'ensemble des dossiers du cabinet • **Faibles protocoles de sécurité mis en place** • **Clauses de non-concurrence et accords de confidentialité rarement appliqués** • **Plusieurs incidents** rencontrés
V4 **Très vraisemblable**	• **Accès complet à l'ensemble des dossiers du cabinet** (gestion des accès inexistante) • **Absence de protocoles de sécurité** particulier mis en place au sein de votre cabinet • **Absence de clauses de non-concurrence et d'accords de confidentialité** • **Incidents fréquents et comportement suspect** déjà observés

RÉSULTAT : le niveau de risque

Selon la méthode, l'issue de cette appréciation est un résultat, le niveau de risque.

Ce niveau de risque se calcule dans son contexte (celui de votre cabinet) au moyen de la formule suivante :

Niveau de risque = Gravité x Vraisemblance.

En croisant les niveaux de gravité et de vraisemblance, vous obtiendrez le niveau de risque de votre cabinet qu'il est possible d'illustrer de la façon suivante :

	V VRAISEMBLANCE			
G GRAVITÉ	Invraisemblable	Peu vraisemblable	Vraisemblable	Très vraisemblable
Mineure	1	2	3	4
Significative	2	4	6	8
Grave	3	6	9	12
Critique	4	8	12	16

Le niveau de risque est déterminé par la multiplication de deux facteurs : la gravité du risque et sa vraisemblance.

Illustrons les résultats de ce tableau en raisonnant sur trois hypothèses correspondant à trois niveaux de risque différents.

NIVEAU DE RISQUE FAIBLE (1-6)

En effet, **un risque dont la gravité est critique** (G4) pour le cabinet **n'implique pas nécessairement un niveau de risque élevé** dès lors qu'il est invraisemblable (V1).

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V1 = 4

À l'inverse, il est possible qu'**un risque soit très vraisemblable** (V4), mais d'une **gravité mineure** (G1) : le risque est alors d'un niveau faible.

Ex : Niveau de risque = Gravité x Vraisemblance = G1 x V4 = 4

Un niveau de risque faible est encore possible lorsque la **gravité est significative** (G2) et que la probabilité de réalisation du **risque est peu vraisemblable** (V2).

Ex : Niveau de risque = Gravité x Vraisemblance = G2 x V2 = 4

NIVEAU DE RISQUE MODÉRÉ (8-9)

En effet, un risque dont la **gravité est critique** (G4) pour le cabinet peut exposer le cabinet à un niveau de risque modéré dès lors qu'il est **peu vraisemblable** (V2).

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V2 = 8

À l'inverse, un risque **très vraisemblable** (V4) peut exposer le cabinet à un niveau de risque modéré dès lors que sa **gravité est seulement significative** (G2).

Ex : Niveau de risque = Gravité x Vraisemblance = G2 x V4 = 8

Il est encore possible que le cabinet soit exposé à un niveau de risque modéré si les deux facteurs sont équilibrés car **le risque serait grave** (G3) et **sa réalisation vraisemblable** (V3)**.**

Ex : Niveau de risque = Gravité x Vraisemblance = G3 x V3 = 9

NIVEAU DE RISQUE ÉLEVÉ (12-16)

Dans ce cas, les deux facteurs de risque sont au niveau le plus élevé : la **gravité est critique** (G4) et sa réalisation **très vraisemblable** (V4)

Ex : Niveau de risque = Gravité x Vraisemblance = G4 x V4 = 16

En conclusion, pour réduire le niveau global du risque, il est possible de jouer sur l'un des deux facteurs, la gravité ou la vraisemblance du risque, en appliquant les mesures de traitement du risque.

TRAITEMENT DU RISQUE

Lorsqu'un associé ou un collaborateur quitte le cabinet, le risque de départ avec des dossiers clients est en enjeu crucial pour la sécurité et la pérennité de votre activité. La perte de ces informations peut entrainer des conséquences graves, et la mise en place d'un plan de traitement des risques adapté permet de prévenir ces incidents.

Lors de la phase de traitement du risque, vous avez la possibilité de choisir parmi les options suivantes :

- l'acceptation du risque et de ses conséquences,
- le partage du risque,
- le refus du risque,
- la réduction du risque, qui consiste dans cette situation à mettre en œuvre de mesures de sécurité afin de réduire la probabilité ou l'impact de ce risque.

L'acceptation du risque pour votre cabinet : une fois l'évaluation du niveau de risque effectué, vous pouvez accepter la possibilité qu'un membre puisse partir avec des dossiers clients, en en assumant les conséquences potentielles (perte de clients, pertes financières, etc.).

La mise en place de mesures de sécurité pour réduire le niveau de risque : Nous nous concentrerons sur les hypothèses 2 (risque modéré) et 3 (risque majeur) et dans le but que le risque résiduel, c'est-à-dire le niveau de risque subsistant après la mise en place des mesures de sécurité, soit acceptable pour vous.

Hypothèse n° 2
STRATÉGIES DE TRAITEMENT DU RISQUE MODÉRÉ

Lorsque le niveau de risque est modéré, il convient de déterminer la stratégie de traitement du risque opportune : le risque peut être maintenu, car il est acceptable pour vous, ou au contraire réduit ou partagé, car il est d'un niveau trop élevé :

- Dans cette hypothèse, il est possible pour vous de réduire le niveau de vraisemblance de ce risque, par exemple en :
  - **limitant davantage les accès des membres du cabinet aux dossiers du cabinet,**
  - mettant en place, si ce n'est pas déjà le cas, des **systèmes de surveillance permettant de détecter et signaler toute activité suspecte ou non autorisée** sur les systèmes d'information, tels que des transferts de données (SOC)

CALCUL DE VOTRE **RISQUE RÉSIDUEL**

→ Une fois ces mesures mises en place, votre niveau de risque résiduel serait **faible (niveau 2 : 1x2)** : la gravité du risque resterait significative, mais sa probabilité de réalisation deviendrait peu vraisemblable (V2)

→ Ces mesures de réduction du risque peuvent nécessiter des investissements dont l'opportunité peut être appréciée au moyen d'un raisonnement coût / bénéfice

Hypothèse n° 3
STRATÉGIES DE TRAITEMENT DU RISQUE MAJEUR

Si le niveau de risque est majeur (16), il est fortement recommandé de mettre en place une stratégie de partage et de réduction du risque :

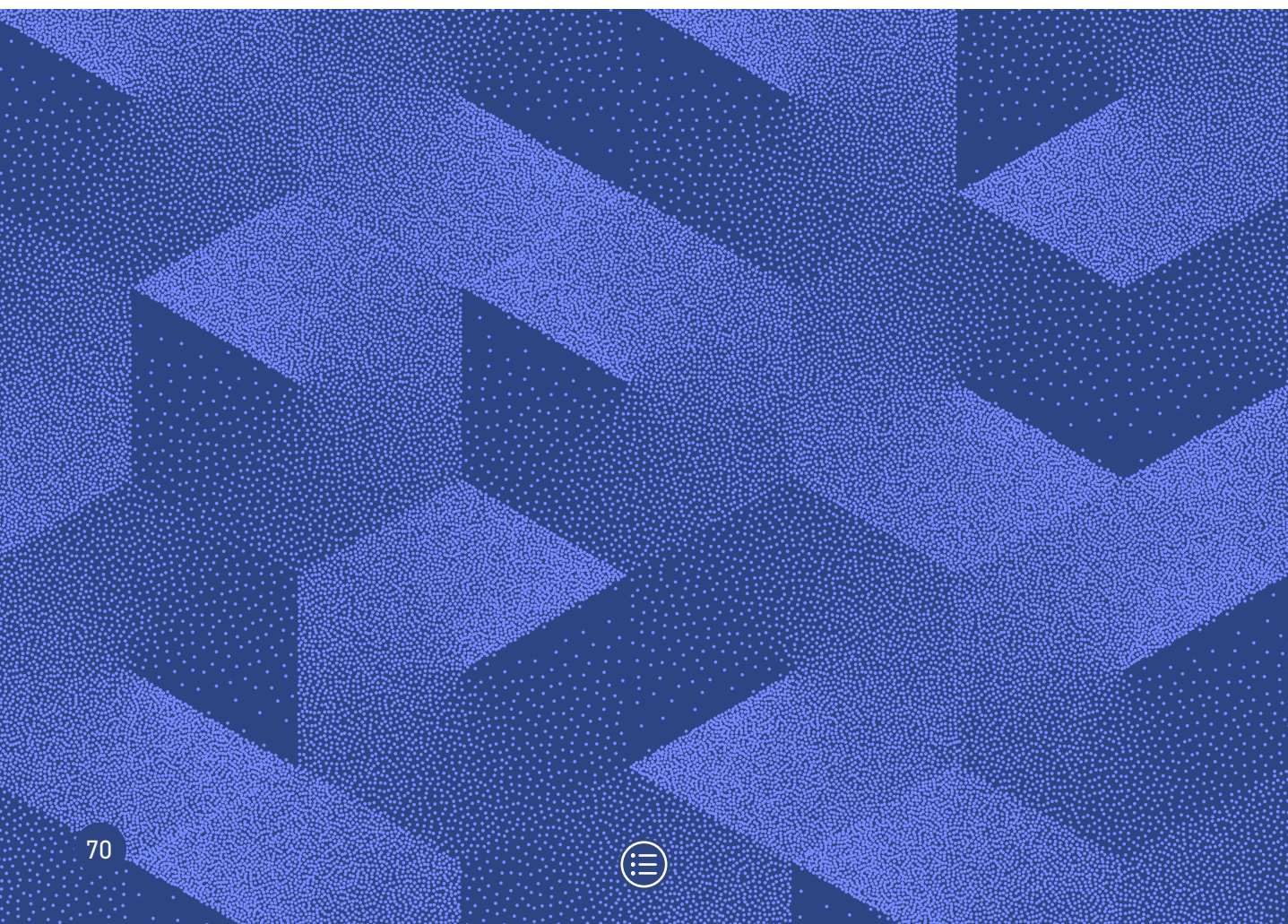
Dans cette hypothèse, il est fortement recommandé de mettre en place des mesures visant à réduire le risque résiduel à un niveau plus faible, et ce en limitant la vraisemblance du risque :

- **mettre en place une politique de gestion des accès stricte** et ne permettre uniquement des accès nécessaires pour la réalisation des missions,
- **mettre en place des techniques de surveillance et de sécurité,** tel que l'emploi de techniques de chiffrement des dossiers les plus sensibles ou la mise en place d'un SOC,
- **établir des politiques de confidentialité et de non-concurrence dès l'arrivée** d'un membre au sein du cabinet,
- **établir une charte informatique du cabinet.**

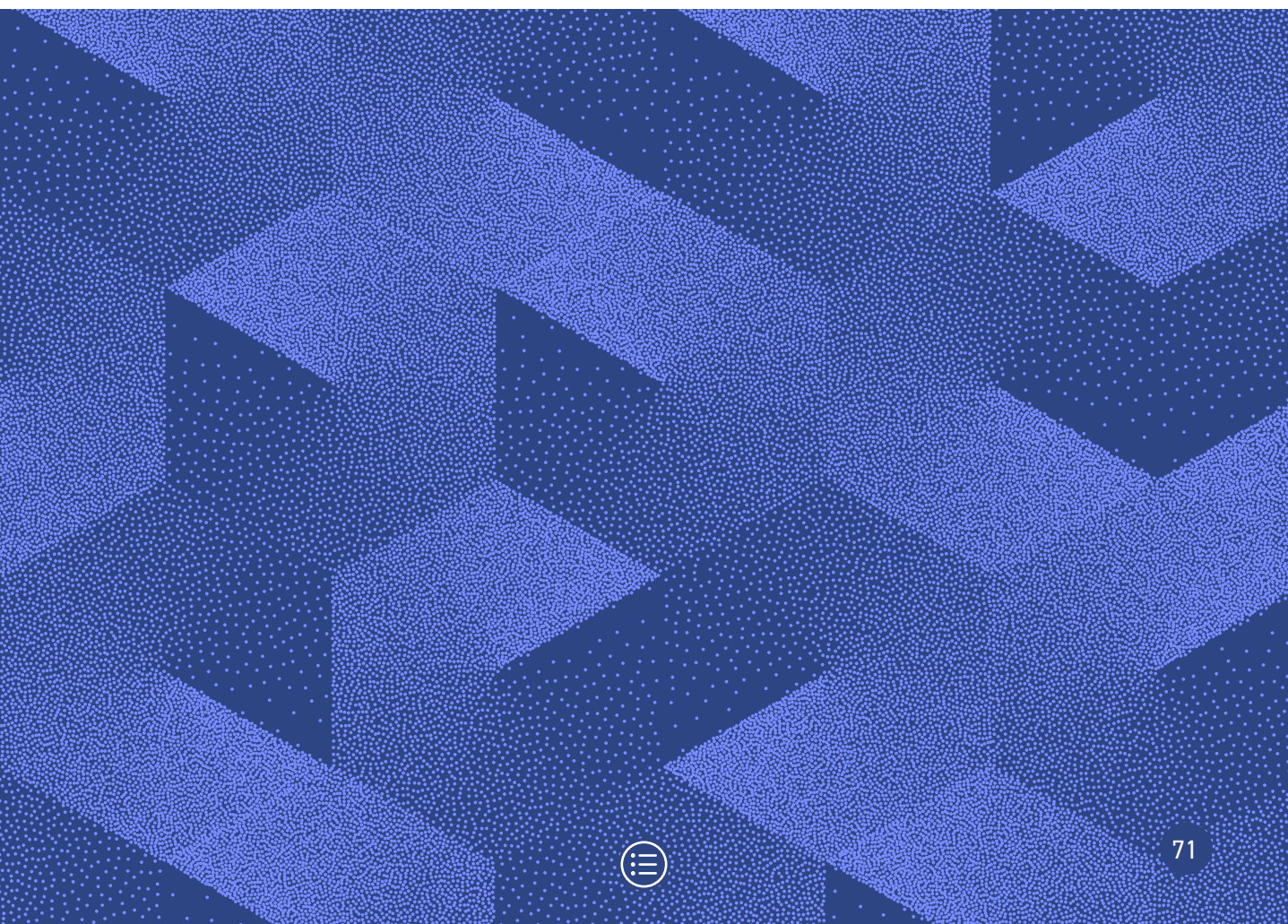
CALCUL DE VOTRE **RISQUE RÉSIDUEL**

→ Une fois ces mesures mises en place, votre niveau de risque résiduel serait **faible (niveau 2 : 1x2) :** la gravité du risque resterait significative, mais sa probabilité de réalisation deviendrait peu vraisemblable (V2)

→ Ces mesures de réduction du risque peuvent nécessiter des investissements dont l'opportunité peut être appréciée au moyen d'un raisonnement coût / bénéfice



REFERENCES



REFERENCES

- La méthode EBIOS Risk Manager – Le guide, ANSSI, édition 1.5, mars 2024 : https://cyber.gouv.fr/publications/la-methode-ebios-risk-manager-le-guide
- La sécurité numérique du cabinet d'avocat, Guide pratique, Conseil national des barreaux, octobre 2023 : https://encyclopedie.avocat.fr/GEIDEFile/CNB_2023-10-25_guide-cybersecurite[web-A].pdf?Archive=131763595994&verif=480312480316473152475325480314450536478530479433488826475274

Liste des personnes ayant contribué à l'élaboration du guide :

Membres de la commission Numérique du Conseil national des barreaux :

- Philippe Baron, Président ;
- Charlotte Hildebrand, Vice-présidente ;
- Guillaume Isouard, Vice-président ;
- Franck Dymarski, Membre ;
- Pierre Fonrouge, Membre ;
- Jérôme Gavaudan, Membre ;
- Isabelle Grenier, Membre ;
- Michel Guichard, Membre.

Permanents du Conseil national des barreaux :

- Thierry Berte, Responsable de la sécurité des systèmes d'information ;
- Géraldine Cavaillé, Directrice générale adjointe, Directrice juridique du CNB ;
- Axelle Deshaires, Juriste numérique au pôle Ecosystème de la profession, Direction juridique du CNB ;
- Johan Espinasse, Juriste numérique au pôle Ecosystème de la profession, Direction juridique du CNB ;
- Olivier Ziegler, Responsable du pôle Ecosystème de la profession, Direction juridique du CNB.

CONSEIL NATIONAL DES BARREAUX

LES AVOCATS

LE CONSEIL NATIONAL DES BARREAUX EST À VOTRE ÉCOUTE

Par téléphone au **01 53 30 85 60**
de 8 h 30 à 19 h 00
Par courrier électronique :
cnb@cnb.avocat.fr

Sur les réseaux sociaux

Au siège
180 boulevard Haussmann - 75008 Paris