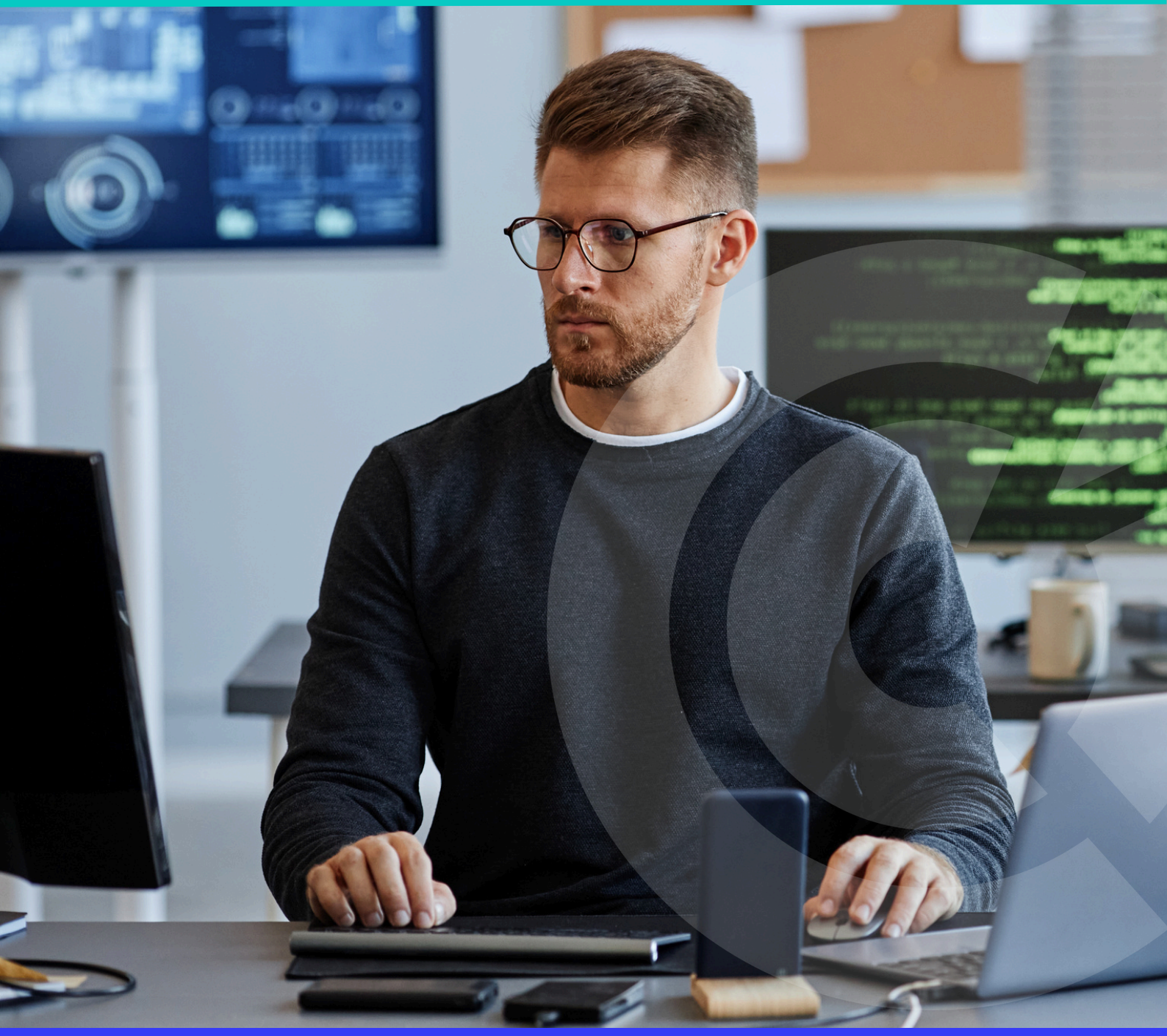
GUIDE DU NUMÉRIQUE

Jeunes créateurs :
Sécuriser son activité numérique



SOLUCCIO Numérique

Les offres

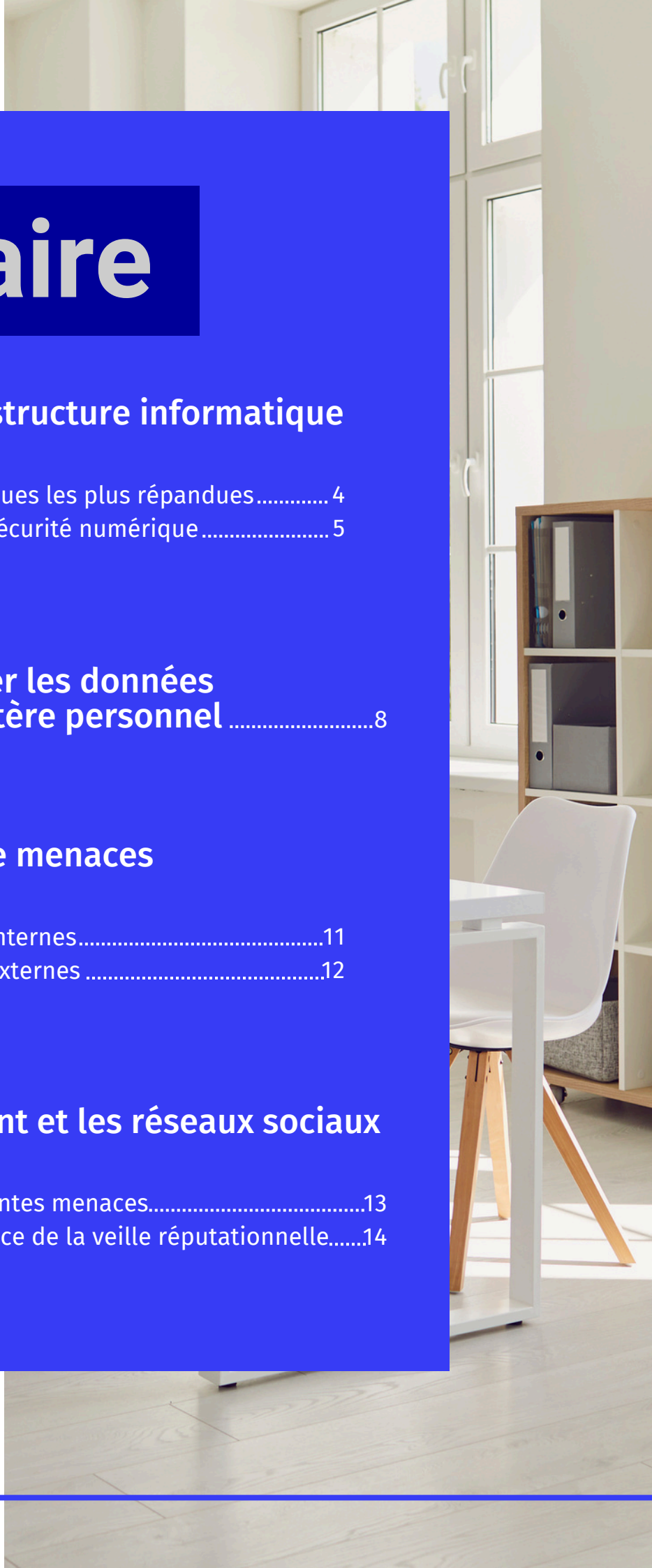
CCI PARIS ILE-DE-FRANCE ENTREPRISES

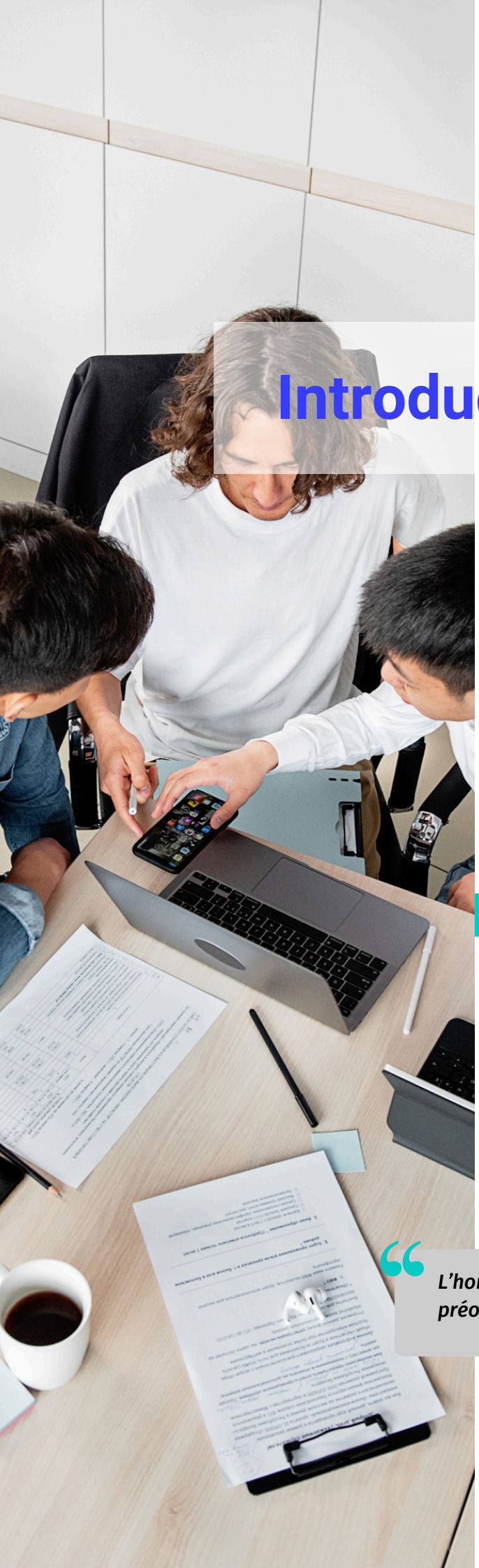
Sommaire

Protéger son infrastructure informatique

Les autres types de menaces

Le jeune dirigeant et les réseaux sociaux





Introduction

Pour un jeune entrepreneur, la sécurité numérique est un élément fondamental. Une fois son entreprise créée, celui-ci doit protéger ses systèmes informatiques, les données personnelles collectées conformément à la réglementation, se protéger contre les intrusions, veiller à sa réputation en ligne...

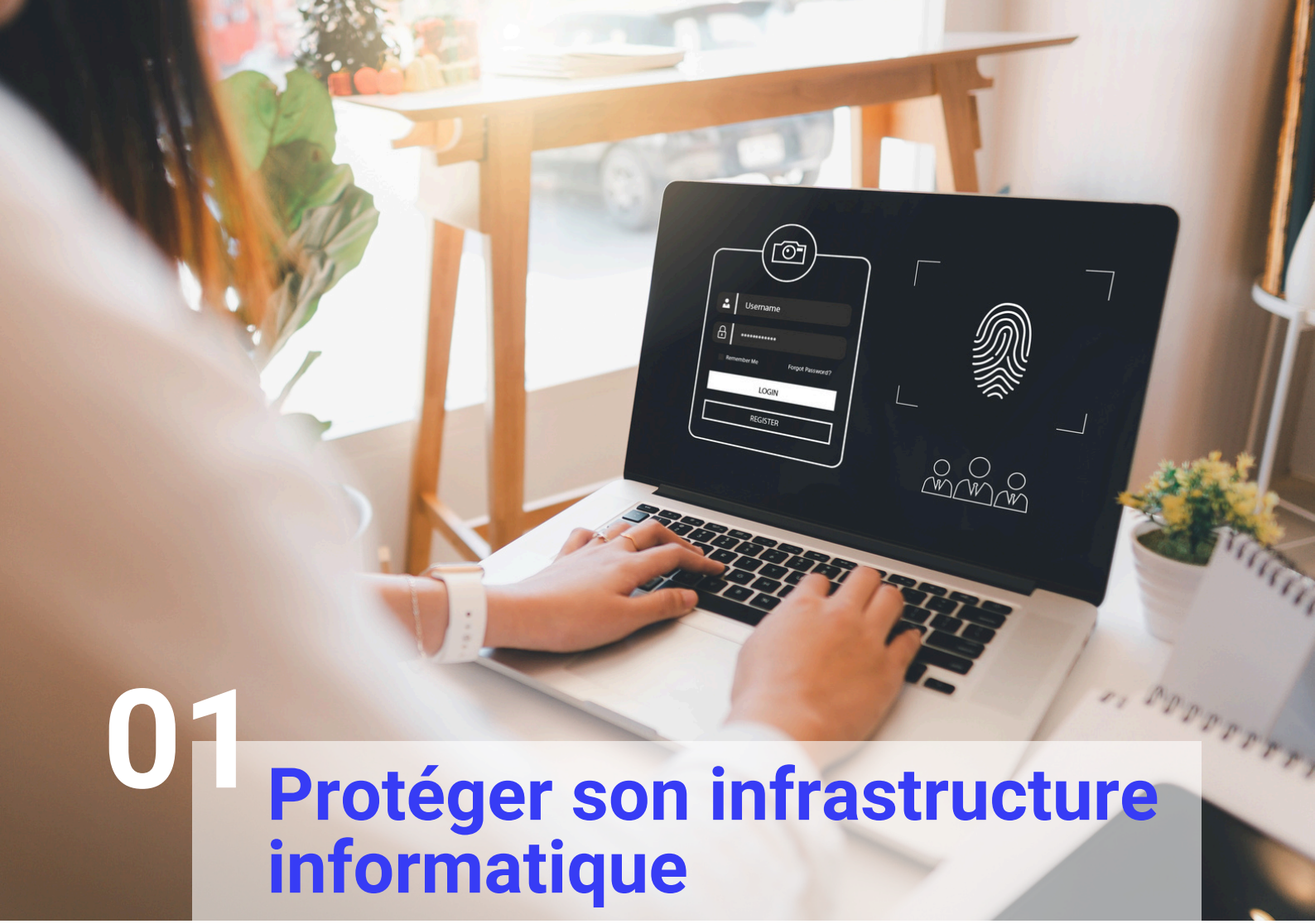
Il existe divers types de menaces, assurer sa sécurité et celle de son entreprise est à la fois un devoir et une obligation légale pour le jeune dirigeant. Tout manquement à ces obligations l'expose à des sanctions financières et pénales et met en péril la pérennité de son activité.

A quoi sert ce guide ?

Vous venez justement de créer votre entreprise ? Ce guide vous informe sur les éléments à considérer en matière de sécurité numérique et vous aide à adopter une approche préventive.

Pour plus d'informations, nous vous recommandons de vous faire accompagner. Contactez votre CCI de proximité pour échanger avec un expert.

> *L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique.*
>
> **Albert Einstein**



01 Protéger son infrastructure informatique

Face à l'explosion des volumes de données, à une connectivité accrue, à des attaques de plus en plus lucratives et à des techniques ultra perfectionnées, les cyberattaques sont en constante augmentation. Ainsi, selon l'ANSSI*, le nombre d'attaques par ransomware (attaques les plus répandues) signalées en 2023 a augmenté de 30% par rapport à 2022.

Faute de temps et de moyens, avec des systèmes informatiques plus modestes et des budgets réduits en matière de sensibilisation, les petites structures sont particulièrement visées. En se sentant moins exposées aux risques cyber que les grands groupes, en raison de leur taille et de leur visibilité moindre par rapport aux grandes structures, mais aussi parce qu'elles sous-estiment la valeur de leurs données et de leurs systèmes informatiques, elles deviennent des cibles prioritaires pour les cybercriminels. Ainsi, en 2023, les plus petites entreprises sont les principales victimes des cyberattaques en France avec 60% des attaques les ciblant (source : l'ANSSI*).

60%
des cyberattaques visent les PME

En cas de doute : faites-vous accompagner par des experts juridiques

*Agence nationale pour la sécurité des systèmes d'information

Pour accéder aux systèmes informatiques, voler les données ou perturber les services, les cyberattaquants utilisent diverses techniques.

Les cyberattaques les plus répandues

Hameçonnage
Phishing

Les attaquants envoient des mails ou des messages qui semblent provenir de sources légitimes pour inciter les victimes à divulguer des informations sensibles, comme des mots de passe ou des numéros de carte de crédit. Par exemple: un mail prétendant venir de votre banque demandant une vérification immédiate de vos informations de compte

Logiciels malveillants
Malwares

Logiciels conçus pour endommager, perturber ou obtenir un accès non autorisé à un système informatique (virus, cheval de Troie, *ransomwares*, *spywares*, *adwares*...). Le plus connu est le *ransomware* (rançongiciel) qui chiffre les fichiers d'un utilisateur et demande une rançon pour les déchiffrer.

Attaque de l'homme au milieu
Men In The Middle (MITM)

Procédure qui permet à un attaquant de s'interposer entre vous et l'ordinateur avec lequel vous communiquez pour lire la conversation ou la modifier. L'attaquant interpose ses propres communications entre les parties, leur faisant croire qu'elles communiquent directement entre elles alors qu'en réalité, il est en train de capter, modifier ou injecter des messages. L'objectif de cette attaque est de récupérer des données confidentielles telles que des détails de compte bancaire, des numéros de carte de crédit ou des informations de connexion, qui peuvent être utilisées pour commettre d'autres crimes comme le vol d'identité ou les transferts de fonds illégaux.

Attaque par déni de service
Distributed Denial of Service (DDoS)

Type de cyberattaque dans lequel un acteur malveillant vise à rendre un appareil indisponible pour ses utilisateurs en interrompant son fonctionnement. Pour cela, les attaquants envoient au réseau ou au serveur ciblé un flot constant de trafic, tel que des demandes frauduleuses, qui submerge le système et l'empêche de traiter le trafic légitime. Ces attaques ressemblent aux *ransomwares* mais visent le service de la victime plutôt que ses données.

Usurpation d'identité
Spoofing

Technique de falsification utilisée par des attaquants pour se faire passer pour une entité légitime afin de tromper des systèmes ou des utilisateurs. Cette méthode permet aux attaquants de contourner des mécanismes de sécurité, de voler des informations ou de lancer d'autres types d'attaques. Il existe plusieurs formes de spoofing, chacune exploitant différents aspects des communications et des systèmes informatiques.

Hameçonnage ciblé
Spear phishing

Technique où l'attaquant se concentre sur une personne spécifique ou un groupe restreint d'individus au sein d'une organisation. Contrairement au phishing classique, qui envoie des emails en masse à un large public, l'hameçonnage ciblé implique une recherche approfondie pour personnaliser les messages et rendre l'attaque plus crédible et difficile à détecter. Depuis l'arrivée de l'IA, les attaques de ce type se sont sophistiquées. Désormais, des mails de phishing ultra personnalisés sont envoyés de manière individuelle, reprenant les informations personnelles de la personne ciblée dans le but de lui soutirer des données sensibles.

Toutes ces attaques ont des répercussions sur le bon fonctionnement de l'entreprise : interruption des opérations, perte des données, coûts significatifs, atteinte à la réputation auprès des clients, partenaires et investisseurs, baisse des ventes...

À retenir

L'étude « Risques cyber analyse de la sinistralité : quels enseignements ? » réalisée par BESSE et Stelliant en 2022 met en évidence une augmentation significative des risques de faillite pour les entreprises victimes de cyberattaques. Selon cette analyse, **les entreprises attaquées voient leurs risques de faillite augmenter d'environ 50% dans les six mois suivant l'incident.**

Renforcer sa sécurité numérique

Heureusement, il existe des outils à la portée du jeune entrepreneur pour renforcer sa sécurité numérique et réduire les risques associés aux cyberattaques :

La formation et la sensibilisation à la cybersécurité

Vous pouvez vous former, ainsi que vos collaborateurs, sur les bonnes pratiques en matière de cybersécurité comme par exemple reconnaître une tentative de phishing, choisir un mot de passe robuste, gérer de façon sécurisée les données...

La protection des données

Faire des sauvegardes régulières des données sensibles et les stocker hors site et dans le cloud permet de protéger les données en cas de cyberattaque ou de tout autre incident. Pour vous aider, vous pouvez **appliquer la règle du 3-2-1 pour la sauvegarde**.

La règle du 3-2-1

3 copies de vos données

2 supports différents

1 copie hors site

Au minimum 3 copies de vos données (2 sauvegardes en plus des données principales de la production), sur 2 supports différents, dont 1 copie hors site (sur le cloud ou sur un équipement situé sur un autre site par exemple.)

Les logiciels de sécurité

Installez et maintenez à jour tous vos logiciels sur l'ensemble de votre parc :

- systèmes d'exploitation,
- outils de sécurité (antivirus, antimalwares, firewalls...)
- sans oublier ceux utilisés quotidiennement : logiciels de bureautique et navigateurs.

MON DIAG NUM'

Réaliser un état des lieux de sa maturité numérique

Pour connaître le niveau de sécurité de votre activité sans disposer de compétences techniques particulières, il est important de se faire accompagner. Un expert numérique pourra vous proposer un plan d'actions personnalisé.

En savoir plus

L’analyse des contrats de prestation

Dans votre vie de chef d’entreprise, vous aurez recours aux services de tierces personnes et établirez probablement un contrat de prestation. **L'analyse de ces contrats est essentielle pour définir clairement les attentes, les responsabilités et les niveaux de service attendus (SLA).**

Les SLA cadrent la manière dont doit se dérouler un projet informatique, notamment en ce qui concerne le niveau de sécurité de stockage et de gestion des données personnelles. Elles permettent de préciser les délais de réponse, la gestion des sauvegardes, le niveau de sécurité, la gestion admin, les temps de disponibilité, les procédures de récupération en cas de panne...

Si la plupart des fournisseurs de services présentent leurs propre SLA, il est vivement conseillé de les étudier avec attention, et si possible avec l’aide d’un expert juridique.

S’assurer que les SLA correspondent bien aux besoins et aux attentes de l’entreprise permet de **minimiser les interruptions de service et les pertes de données.**

Les plans de reprise ou de continuité après sinistre

En cas d'incident majeur, il existe deux types de plans de gestion des risques visant à assurer la résilience et la continuité des activités :

Proactif

Catastrophes naturelles

Erreurs humaines

PLAN DE REPRISE D’ACTIVITÉ (PRA)

axé sur la récupération de données et des accès après une interruption

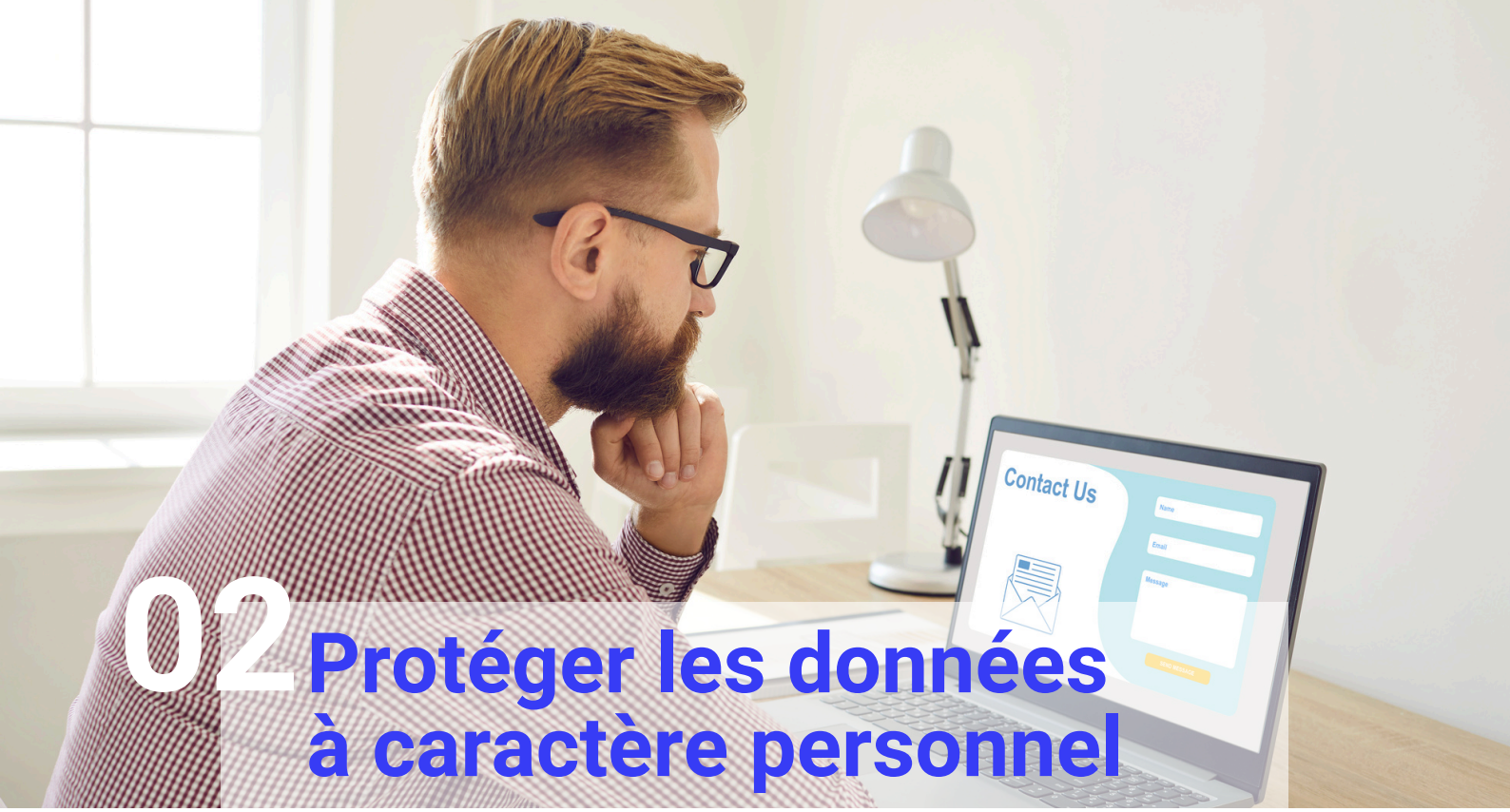
Peut exiger des mesures de sécurité supplémentaires pour les employés

PLAN DE CONTINUITÉ D’ACTIVITÉ (PCA)

vise à assurer que les activités critiques de l’entreprise continuent de fonctionner malgré l’incident

Limite les temps d’arrêt des opérations

Ces documents internes à l’entreprise permettent de mieux gérer une interruption d’activité pouvant entrainer des conséquences financières, juridiques en cas de non-respect des obligations contractuelles, ou encore nuire à la réputation de l'organisation. A noter qu’ils peuvent accompagner un contrat mais ne font pas partie des SLA.



02 Protéger les données à caractère personnel

En tant que jeune dirigeant, vous conformer au RGPD (Règlement Général sur la Protection des Données) dès la création de votre entreprise est obligatoire pour protéger les données personnelles de vos clients, employés, partenaires.

Définition

Le RGPD est une réglementation de l'Union Européenne entrée en vigueur en 2018. Elle établit des règles strictes sur la **protection des données personnelle des citoyens** de l'Union européenne tout en permettant aux professionnels de développer leurs activités numériques. Le RGPD est une obligation légale **pour toute entreprise qui collecte des données personnelles**, mais aussi pour les sous-traitants qui traitent des données personnelles au nom et pour le compte d'autres entreprises.

Pour un jeune dirigeant, se conformer au RGPD ne doit pas être perçu comme une contrainte juridique et technique mais plutôt comme **une stratégie essentielle pour sécuriser son activité numérique**. C'est une opportunité pour l'entreprise qui présente plusieurs intérêts :

- Respecter les droits des personnes concernées valorise l'image d'une entreprise sérieuse et responsable, gage d'une relation de confiance
- Une gestion rigoureuse des données collectées simplifie les démarches de prospections, de gestion des facturations, et *in fine* de vente de produit
- Respecter le principe de minimisation des données et tenir à jour la liste des fichiers, permet d'identifier les besoins et données réellement nécessaire pour l'entreprise
- Améliorer la sécurité des données collectées permet de garantir aux personnes concernées que leurs données sont protégées contre les atteintes extérieures.

Toutefois, toutes les entreprises n'étant pas soumises aux mêmes contraintes, les dispositifs mis en place doivent être proportionnels et raisonnables au regard du but et des moyens de la structure.

Quels risques en cas de non-conformité ?

La CNIL (la Commission Nationale de l'Informatique et des Libertés) peut prononcer une sanction financière allant jusqu'à 20 millions d'euros du chiffre d'affaires ou 4% du CA annuel global pour les manquements les plus graves ! Dans ce cas, c'est le montant le plus élevé qui est retenu. Cette sanction peut être associée à une communication publique, portant préjudice à l'image de l'entreprise, et dans certains cas à des condamnations pénales visant les dirigeants d'entreprise à titre personnel.

En savoir plus

Pour que le Règlement Général sur la Protection des Données n'ait plus aucun secret pour vous, consultez notre dossier thématique en ligne.

1/3

des sanctions comporte un manquement à la sécurité des données personnelles

+101 M€

de sanctions infligés par la CNIL en 2022

18

dossiers européens examinés par la CNIL

Pour se conformer au RGPD, le dirigeant doit mettre en place plusieurs mesures et pratiques pour garantir que toutes les données personnelles sont traitées de manière légale, sécurisée et transparente. La démarche se fait en plusieurs étapes clés :

1. **Cartographier les données et les traitements**
2. **Analyser l'impact**
3. **Mettre en place un registre des traitements**
4. **Implémenter dans les processus métiers des considération liées aux données personnelles** *protection "by design" et "by default")*
5. **Respecter les droits des administrés**

Le jeune dirigeant peut décider d'entamer sa démarche seul, en suivant les recommandations disponibles sur le site de la CNIL, ou faire appel à un prestataire.

03 Les autres types de menaces

Tout au long de sa vie, le jeune dirigeant doit protéger son entreprise contre diverses formes de menaces. Celles-ci peuvent provenir de l'interne comme de l'externe. Chacune de ces menaces présente des risques distincts et nécessite d'être traitée spécifiquement.

Les menaces internes

Le vol de matériel ou de données

Par des salariés pour en tirer un avantage financier, servir un concurrent, ...
Ou encore un employé mécontent qui chercherait à nuire à l'entreprise.

Les négligences et erreurs humaines

Erreurs de traitement des données, erreurs décisionnelles, erreurs de communication, erreurs de sécurité...

Formez régulièrement vos collaborateurs à la sécurité, clarifiez vos process, proposez un environnement de travail propice à la concentration... Le contrôle des accès, des politiques de sécurité strictes, l'utilisation d'outils de surveillance et de systèmes de détection des menaces permettent de mettre en place des mesures de protection robustes.

Les menaces externes

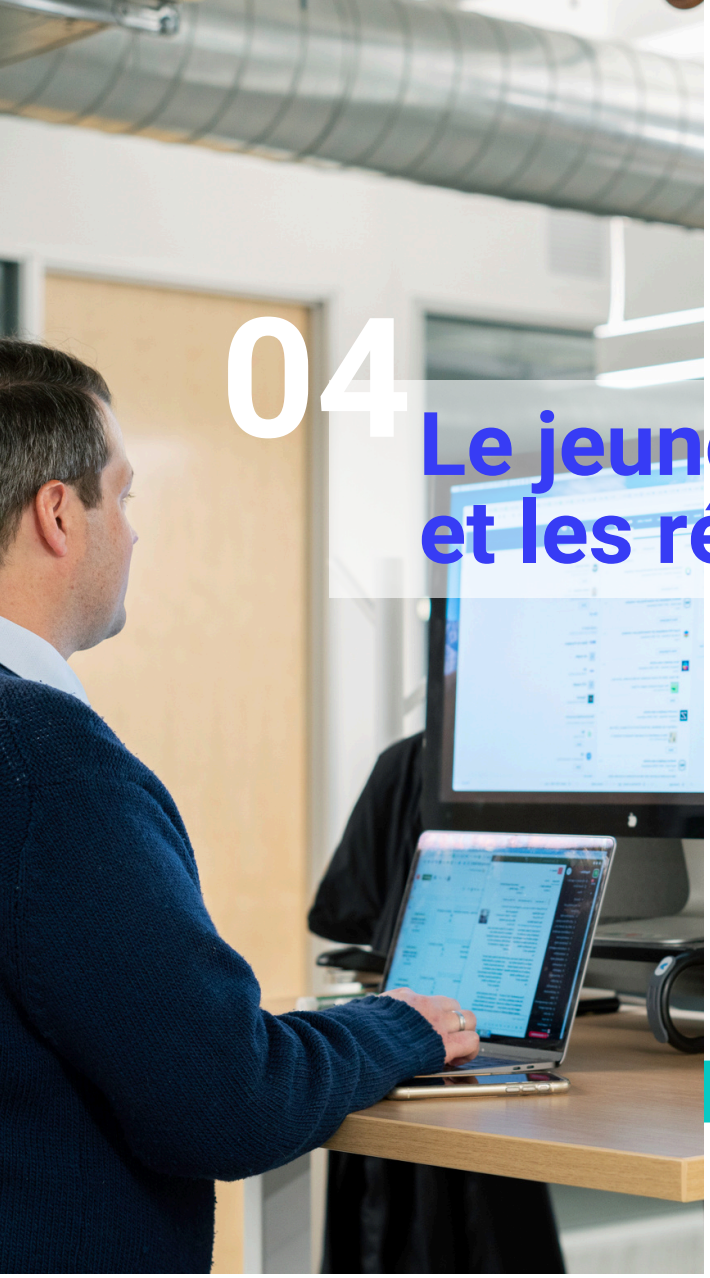
Les intrusions dans les locaux, les actes de vandalisme

Les actes de malveillance

Les incendies, vagues de chaleur, inondations..

L'évolution de la réglementation

Le risque réputationnel : qu'il s'agisse d'une mauvaise communication, d'un concurrent qui cherche à déstabiliser votre entreprise, de critiques négatives sur vos produits ou services, ou d'un salarié mécontent, votre réputation peut être atteinte



04 Le jeune dirigeant et les réseaux sociaux

A l'ère de la communication en temps réel et de l'utilisation croissante des réseaux sociaux, les jeunes dirigeants n'ont d'autres choix que de s'intéresser à ces plateformes. Les réseaux sociaux ont pris une telle place qu'ils peuvent aider le jeune dirigeant à recruter, contrôler l'image de son entreprise, asseoir sa marque, établir des liens avec le public...

Les différentes menaces

Toutefois, il est recommandé de rester vigilant quant aux menaces que représentent les réseaux sociaux :

- **Vol de données**
- **Usurpation d'identité**
- **Diffamation *les "trolls"***
- **Divulgation d'informations confidentielles sur l'entreprise**

L'ingénierie sociale et l'arnaque au président

Vous et vos collaborateurs devez rester prudents dans l'utilisation des réseaux sociaux, et limiter la publication d'informations sur ces plateformes. En effet, certains fraudeurs identifient vos collaborateurs et collectent les données les plus confidentielles sur votre entreprise pour agir avec malveillance.

L'arnaque au président qui consiste à usurper l'identité d'un dirigeant ou à prétendre agir sur son ordre, figure parmi les plus grandes **techniques de fraude visant à mettre en confiance une victime** pour qu'elle réalise des transactions financières ou divulgue des informations confidentielles.

Elle peut se manifester par un coup de téléphone sur votre lieu de travail ou un mail dans lequel l'escroc se fait passer pour vous et demande à vos employés de réaliser expressément un virement, en prétextant une situation d'urgence (dette à régler, exécution d'un contrat...).

Les bons réflexes à adopter

- **Limitez la diffusion d'informations** (réseaux sociaux, sites internet, signatures, etc.)
- **Mettez en place des procédures internes sécurisées** (double contrôle, accès limité aux informations sensibles)
- **Sensibilisez vos collaborateurs**
- **Soyez vigilant en cas de procédure urgente** et confidentielle ne respectant pas les procédures internes
- **Méfiez-vous de tout virement inhabituel** que vous devriez signer

Les risques de deepfake

Cette méthode d'hypertrucage pour réaliser du **faux contenu vidéo ou audio ou falsifier des contenus existants grâce à l'intelligence artificielle** représente un fléau pour la sécurité des entreprises. Majoritairement sur les réseaux sociaux, les cybercriminels envoient des messages qui semblent provenir d'une source connue et dont la demande permet de pénétrer les systèmes, accéder aux données sensibles et les dérober.

L'importance de la veille réputationnelle

Faire une veille régulière permet de protéger la réputation de votre entreprise. La veille est un outil essentiel pour le dirigeant, elle permet :

- d'anticiper les risques en surveillant activement ce qui se dit sur votre activité, votre personne ou vos produits
- de mieux gérer une crise en suivant l'évolution de la situation en temps réel et en adaptant votre communication
- de surveiller vos concurrents
- de renforcer votre crédibilité et de rester engagé avec vos parties prenantes (clients, employés, investisseurs...)

Conclusion

Après avoir créé votre entreprise, vous ferez face à différentes menaces. Afin de réduire les risques et protéger votre entreprise, vous pouvez **mettre au point des pratiques simples d'hygiène informatique, former vos collaborateurs à la sécurité, vous conformer à la réglementation, protéger votre réputation et réaliser une veille régulière de vos activités**.

Vous pouvez aussi choisir de vous faire accompagner par des experts qui vous apporteront des conseils et des solutions personnalisées pour protéger vos actifs et assurer la pérennité et la croissance à long terme de votre entreprise.

VOUS SOUHAITEZ VOUS FAIRE ACCOMPAGNER ?

Les experts de la CCI Paris Ile-de-France sont à vos côtés, n'hésitez pas à les solliciter.

Contactez-nous

CCI PARIS ILE-DE-FRANCE
ENTREPRISES

Avec vous, à toutes les étapes de votre développement

CCI Entreprises

CCI Entreprises

entreprises.cci-paris-idf.fr