DRC · DATASHIELD RISK CONSULTING

CODEX

ÉDITION DIRIGEANTS

L'essentiel de la cybersécurité
pour décider

Pour les dirigeants de TPE, PME et petites organisations — comprendre, gouverner, réagir. Une lecture de vingt minutes.

DRC — DATASHIELD Risk Consulting

LA MAÎTRISE DU RISQUE NUMÉRIQUE

DATASHIELD
RISK CONSULTING

CODEX — Édition Dirigeants

VERSION CONDENSÉE · 2026

Les données chiffrées reflètent l'état de la menace connu en 2025-2026 (sources : ANSSI, ENISA, CERT-FR) ; elles sont appelées à évoluer.

CODEX · ÉDITION DIRIGEANTS

Sommaire

Avant-propos 1

I. Comprendre 1

II. Gouverner 3

III. Réagir 5

IV. Ce que la réalité enseigne 6

Mémento — pour agir dès cette semaine 7

Repères — principes pour décider 8

DRC, à vos côtés 8

Version condensée du Codex DRC. Pour aller plus loin, l'édition complète développe chacun de ces sujets.

Avant-propos — Pour vous, dirigeant

> *Vous n'avez pas besoin de devenir expert en cybersécurité. Vous avez besoin de savoir décider.*

Ce livret n'est pas un manuel technique. Il ne parle ni de pare-feux, ni de configurations, ni d'outils. Il s'adresse à celles et ceux qui dirigent une **TPE, une PME ou une petite organisation** — une entreprise de quelques salariés, une collectivité, une association, un cabinet. Des structures qui, le plus souvent, n'ont pas de responsable sécurité, confient leur informatique à un prestataire, et découvrent le sujet le jour où il devient un problème.

Il tient en une idée simple. La cybersécurité n'est pas une affaire de technique : c'est une affaire de **décision**. Et les décisions qui comptent — que protéger, quoi exiger de son prestataire, comment réagir quand l'incident survient, faut-il payer une rançon — ne se délèguent pas. Elles reviennent au dirigeant.

Ce livret est la version resserrée du *Codex DRC*, notre doctrine complète. Il en retient l'essentiel, réécrit pour une lecture de vingt minutes. Il se lit en trois temps : **comprendre** ce qui est réellement en jeu, **gouverner** avant que la crise n'arrive, **réagir** avec justesse le jour où elle arrive. Il se termine par un **mémento** que vous pouvez détacher, afficher, et confronter à votre prestataire dès la semaine prochaine.

Les chiffres et exemples cités s'appuient sur les travaux publics de l'ANSSI, de l'ENISA et du CERT-FR (2025-2026). Nous décrivons le risque tel qu'il est, non tel qu'on l'imagine.

PARTIE I

Comprendre

> *Avant de se protéger, il faut savoir de quoi, et pour quoi.*

La cybersécurité est une décision, pas une technologie

On croit souvent que se protéger, c'est acheter le bon logiciel. C'est une illusion rassurante. Les outils comptent, mais ils ne décident rien. Ils n'établissent pas ce qui est vital pour votre activité, ils n'arbitrent pas entre ce que vous acceptez de risquer et ce que vous refusez, ils ne préparent pas votre organisation à tenir un lundi matin où plus rien ne fonctionne. Ces choix-là sont des choix de direction.

La maturité d'une organisation ne se mesure pas au nombre de ses solutions de sécurité, mais à la **qualité des décisions** qu'elle prend face au risque numérique. Une petite structure qui a compris cela, et qui applique quelques gestes simples avec constance, est mieux protégée qu'une grande qui a tout acheté sans jamais décider.

Principe DRC — La maturité d'une organisation ne se mesure pas au nombre de solutions de sécurité qu'elle possède, mais à la qualité des décisions qu'elle prend face au risque numérique.

Ce que vous protégez vraiment : la confiance et la mission

Un incident cyber n'abîme pas d'abord des machines. Il abîme la **confiance** — celle de vos clients, de vos usagers, de vos partenaires, de vos équipes — et il menace votre capacité à **poursuivre votre mission**. Une mairie qui ne peut plus délivrer d'actes d'état civil, un cabinet dont les dossiers clients sont menacés de publication, une PME qui ne peut plus facturer : dans chaque cas, ce qui est en jeu dépasse l'informatique.

Protéger une organisation, ce n'est donc pas protéger des serveurs. C'est protéger sa capacité à tenir sa promesse, malgré l'incident. C'est pourquoi le sujet est stratégique, et non technique.

> **Principe DRC** — La cybersécurité protège avant tout la confiance nécessaire au fonctionnement des organisations. Les technologies ne sont que les instruments de cette confiance.

La menace réelle, en quelques chiffres

La menace n'est ni abstraite ni lointaine. En 2025, l'ANSSI a traité **plus de 3 500 événements de sécurité** en France. À l'échelle européenne, l'ENISA recense près de **4 900 incidents** vérifiés sur un an, et classe le **rançongiciel** comme la menace la plus destructrice. Surtout, l'**hameçonnage** — le courriel piégé — reste à l'origine d'environ **60 % des intrusions** : la première porte d'entrée n'est pas un exploit sophistiqué, c'est un humain qui clique.

Deux évolutions méritent l'attention d'un dirigeant. D'abord, l'**intelligence artificielle** abaisse le coût de la fraude : des courriels d'hameçonnage plus crédibles, des usurpations d'identité (y compris vocales et vidéo) « pour quelques dizaines de dollars ». Ensuite, la bascule vers l'**extorsion sans chiffrement** : de plus en plus, l'arme n'est plus de bloquer vos données, mais de les **voler et menacer de les publier**. On ne peut pas restaurer une fuite depuis une sauvegarde.

Pourquoi les petites structures sont visées

Beaucoup de dirigeants pensent : « nous sommes trop petits pour intéresser qui que ce soit ». C'est faux, et c'est dangereux. Les attaques ne sont pas des vendettas ciblées ; elles sont **opportunistes et industrialisées**. Un attaquant ne choisit pas une victime prestigieuse : il ratisse, et frappe ce qui est **visible et mal défendu**.

Les chiffres publics le confirment. En 2024, l'ANSSI a traité **218 incidents** touchant des collectivités — dont **144 visant des communes**. Les petites structures ne sont pas épargnées : elles sont ciblées **précisément parce qu'elles sont accessibles**. Leur fragilité tient rarement à un manque d'outils sophistiqués, mais à l'absence des fondamentaux — moindre maturité, moyens limités, forte dépendance à un prestataire, sauvegardes non isolées.

Le risque : le regarder en face, pas l'éliminer

Il n'existe pas de risque zéro. Chercher à supprimer tout risque conduit à dépenser sans fin, ou à se rassurer à bon compte. La bonne posture est autre : **comprendre** les risques qui pèsent réellement sur votre activité, les **hiérarchiser**, et décider lesquels vous réduisez, lesquels vous transférez (assurance, prestataire), lesquels vous acceptez en connaissance de cause. C'est un travail de direction, proportionné à vos moyens.

Principe DRC — La cybersécurité n'a pas pour but de supprimer le risque, mais de permettre aux organisations de le comprendre, de l'évaluer et de le maîtriser pour poursuivre leur mission.

L'essentiel de la Partie I — La cybersécurité est une décision de direction, pas un achat de logiciel. Ce que vous protégez, c'est la confiance et la continuité de votre mission. La menace est réelle, industrialisée, et vise en priorité les structures visibles et mal défendues — donc les petites. On ne supprime pas le risque : on le regarde en face et on le maîtrise.

PARTIE II

Gouverner

> *Les décisions les moins chères et les plus efficaces se prennent avant la crise, à froid.*

Partir des missions, pas des outils

La première question n'est pas « quel logiciel installer ? » mais « **qu'est-ce qui, chez nous, ne doit jamais s'arrêter, ou fuiter ?** ». Pour une PME, ce sera peut-être la facturation, le fichier clients, les coordonnées bancaires. Pour une collectivité, l'état civil et la paie. Pour un cabinet, la confidentialité des dossiers. Identifiez ces quelques missions vitales : elles décident où porter l'effort en priorité. Une organisation mature protège d'abord ses missions ; les moyens numériques ne sont protégés que parce qu'ils les rendent possibles.

Principe DRC — Une organisation mature protège d'abord ses missions. Les actifs numériques ne sont protégés que parce qu'ils rendent ces missions possibles.

Les fondamentaux qui arrêtent la grande majorité des attaques

Vous n'avez pas besoin d'un arsenal. Une poignée de mesures simples, appliquées avec constance, ferme la porte à l'immense majorité des attaques opportunistes qui frappent les petites structures. Cinq d'entre elles comptent plus que tout le reste.

D'abord, l'**authentification multifacteur (MFA)** sur tout ce qui est accessible depuis Internet — messagerie, accès distants, comptes d'administration. C'est la mesure au meilleur rapport effort/protection qui existe. Ensuite, des **sauvegardes hors ligne, testées** : une sauvegarde restée connectée au réseau est chiffrée avec le

reste le jour de l'attaque ; une sauvegarde qu'on n'a jamais essayé de restaurer n'est pas une sauvegarde. Puis les **mises à jour** régulières, qui referment les failles connues par lesquelles entrent les attaquants. La **journalisation** ensuite : sans traces, on ne peut ni comprendre ce qui s'est passé, ni le prouver. Enfin, le **moindre privilège** : chacun n'accède qu'à ce dont il a besoin, et les comptes qui peuvent tout faire sont rares et surveillés.

Ces gestes ne sont pas spectaculaires. Ils sont décisifs.

La continuité : tenir quand la panne arrive

La question n'est pas seulement d'éviter la crise, mais de **fonctionner malgré elle**. Que faites-vous si, demain matin, vos systèmes sont inutilisables pendant une semaine ? Une organisation résiliente a pensé cela à l'avance : quelles activités basculer en mode dégradé (l'état civil repart sur papier, la paie reste prioritaire), qui prévenir, dans quel ordre redémarrer. Le vrai plan de continuité n'est pas celui qui est écrit dans un classeur : c'est celui qui **fonctionne** quand les procédures habituelles cessent de fonctionner.

Principe DRC — Une organisation résiliente n'est pas celle qui évite toutes les crises, mais celle qui reste capable de poursuivre sa mission malgré elles.

Vos dépendances : le prestataire, le cloud

Si votre informatique est confiée à un prestataire, retenez ceci : l'externalisation transfère des **opérations**, jamais votre **responsabilité**. Le jour de l'incident, c'est votre organisation qui rend des comptes à ses clients, à la CNIL, à ses usagers. Vous devez donc exiger de votre prestataire ce qu'un dirigeant a le droit d'exiger : où sont vos sauvegardes et sont-elles isolées, qui fait quoi en cas d'incident, sous quel délai il intervient, comment il préserve les preuves plutôt que de « nettoyer » dans l'urgence. Ces points s'écrivent dans le contrat, pas dans la panique. Votre sécurité ne dépasse jamais celle de vos dépendances critiques.

Principe DRC — L'externalisation transfère des opérations. Elle ne transfère jamais la responsabilité stratégique de la continuité, de la confiance et de la résilience.

Ce que la loi attend désormais de vous

La réglementation a changé de logique : elle place la responsabilité chez le **dirigeant**, pas chez le technicien. Le **RGPD** impose, en cas de violation de données personnelles, une notification à la CNIL sous **72 heures**, et l'information des personnes concernées lorsque le risque est élevé. La directive européenne **NIS 2** étend les obligations de cybersécurité à environ **15 000 entités** en France, sur dix-huit secteurs, avec une responsabilité explicite des organes de direction ; sa transposition française est en cours, mais son périmètre et ses grandes exigences sont déjà connus. Le message est clair : attendre « la date » pour s'y mettre est une faute. Ce que la loi demande — savoir où sont ses données, se préparer à notifier, documenter ses décisions — relève de toute façon d'une bonne gouvernance.

L'essentiel de la Partie II — Partez de vos missions vitales. Appliquez avec constance cinq fondamentaux (MFA, sauvegardes hors ligne testées, mises à jour, journalisation, moindre privilège). Préparez le mode dégradé avant d'en avoir besoin. Encadrez votre prestataire par écrit — vous gardez la responsabilité. Et sachez que la loi vous tient désormais, vous, dirigeant, pour comptable.

PARTIE III

Réagir

> *Le jour de l'incident, quelques bons réflexes dans les premières heures pèsent plus que tout le reste.*

Le premier réflexe : qualifier sans détruire

Face à l'incident, la tentation est double : tout éteindre, ou tout réinstaller au plus vite pour « repartir ». Les deux détruisent l'information dont vous aurez besoin pour décider — et, le cas échéant, pour porter plainte. Le bon premier geste est de **qualifier sans détruire** : isoler ce qui doit l'être pour stopper la propagation, sans tout couper à l'aveugle, et **préserver les traces** (journaux, horodatages, message de rançon, systèmes touchés). C'est aussi le moment de **coordonner votre prestataire** plutôt que de le laisser nettoyer dans l'urgence — un réflexe fréquent qui efface les preuves. En investigation, le temps détruit les preuves : la première décision consiste à identifier ce qui disparaîtra en premier.

Principe DRC — Au début d'un incident, la priorité n'est pas de tout comprendre immédiatement. Elle est de conserver la capacité de comprendre davantage demain, sans avoir détruit les preuves, aggravé les conséquences ni perdu la maîtrise des décisions.

Ne pas payer : pourquoi

La question de la rançon se pose presque toujours. La doctrine, comme la position des autorités françaises, est claire : **on ne paie pas**. Payer n'offre **aucune garantie** — ni que vous récupérerez vos données, ni qu'elles ne seront pas publiées ou revendues malgré tout — et cela **finance le crime**, désignant votre organisation comme une proie qui cède. L'affaire du centre hospitalier de Corbeil-Essonnes, en 2022, le confirme *a contrario* : l'établissement n'a pas payé ; les données ont été publiées un mois plus tard — payer n'aurait rien empêché. La décision, si elle doit se poser, se prend **à froid, au niveau de la direction**, jamais sous le seul effet de l'urgence ou de l'émotion.

Notifier, signaler, porter plainte

Réagir, c'est aussi respecter vos obligations, et elles jouent en votre faveur. Si des données personnelles sont concernées, vous **notifiez la CNIL sous 72 heures**. Vous **signalez** l'incident au dispositif national d'assistance (cybermalveillance.gouv.fr pour les plus petites structures, l'ANSSI pour les entités concernées). Vous **déposez**

plainte. Loin d'être un aveu de faiblesse, le signalement est ce qui vous permet d'être **aidé**, et il nourrit la connaissance collective de la menace. Documentez vos décisions au fil de l'eau : cette trace vous protège.

Communiquer juste

En crise, le silence et le mensonge coûtent plus cher que la vérité. Communiquer ne consiste pas à protéger une image, mais à **protéger la confiance** : dire ce que l'on sait, ce que l'on ignore encore, ce que l'on fait, à qui de droit et au bon moment. Une information exacte, cohérente et sobre vaut mieux qu'une promesse rassurante que les faits démentiront.

Principe DRC — La communication de crise ne consiste pas à protéger l'image de l'organisation. Elle consiste à protéger la confiance, en fournissant une information exacte, cohérente et utile.

L'humain d'abord

Une organisation n'est jamais qu'un ensemble de personnes. En crise, ce sont des femmes et des hommes qui décident, coopèrent et tiennent — souvent sous forte pression. Les préserver, les informer, les soutenir n'est pas accessoire : c'est une condition de la résilience. Et lorsque l'incident touche des personnes vulnérables ou des données intimes, l'accompagnement humain compte autant que la réponse technique.

L'essentiel de la Partie III — Qualifier sans détruire. Ne pas payer — la décision se prend à froid, en direction. Notifier la CNIL sous 72 h, signaler, porter plainte : c'est ainsi qu'on est aidé. Communiquer avec exactitude pour protéger la confiance. Et se rappeler que l'on gouverne d'abord des personnes.

PARTIE IV

Ce que la réalité enseigne

> *Deux faits publics, documentés, pour vérifier que la doctrine tient sur le terrain.*

Corbeil-Essonnes (2022) : refuser la rançon, tenir la mission

Dans la nuit du 20 au 21 août 2022, le Centre hospitalier Sud-Francilien est frappé par un rançongiciel. Rançon réclamée : **10 millions de dollars**. L'hôpital bascule en **mode dégradé** — urgences perturbées, interventions reportées, retour partiel au papier — et **ne paie pas**. Un mois plus tard, des données sensibles sont publiées.

La leçon pour une petite structure est transposable : l'épreuve réelle n'a pas été technique mais **organisationnelle** — la capacité à poursuivre la mission en mode dégradé, préparée avant la crise. Et payer n'aurait offert aucune garantie. *(Sources : Le Monde Informatique, LeMagIT, Public Sénat, 2022.)*

Les collectivités face au rançongiciel

En 2024, l'ANSSI a traité **218 incidents** touchant des collectivités — dont **144 communes** —, parmi lesquels **25 rançongiciels** ; **21 sur 25** ont provoqué une perturbation significative de l'activité. Surtout, les petites communes **déclarent moins** : l'angle mort est donc plus large encore. La fragilité ne tient pas à un manque d'outils sophistiqués, mais à l'absence des **fondamentaux**. La leçon : appliquer les gestes simples vaut mieux qu'attendre l'outil parfait — et **déclarer** l'incident est ce qui permet d'être aidé. *(Source : ANSSI, Panorama de la cybermenace 2025 et bilan des collectivités 2024.)*

Ces deux cas réels prolongent les **cas d'école** — fictifs mais réalistes — développés dans l'édition complète du Codex, pensés pour la mairie, la PME, le cabinet et la petite structure médico-sociale.

MÉMENTO

Pour agir dès cette semaine

> *À détacher, afficher, et confronter à votre prestataire dès cette semaine.*

Les dix gestes qui comptent

1. Activez le MFA partout où l'on se connecte depuis Internet (messagerie, accès distants, comptes d'administration). **2. Sauvegardez hors ligne, et testez la restauration** — une sauvegarde jamais restaurée n'en est pas une. **3. Mettez à jour** systèmes et logiciels sans traîner. **4. Limitez les droits** : chacun accède au strict nécessaire ; les comptes tout-puissants sont rares et surveillés. **5. Activez la journalisation** — sans traces, pas de compréhension ni de preuve. **6. Sensibilisez vos équipes** à l'hameçonnage : la première porte d'entrée est humaine. **7. Encadrez votre prestataire par écrit** : rôles, délais, preuves, sauvegardes. **8. Écrivez un plan de crise d'une page** : qui décide, qui prévient, dans quel ordre on redémarre. **9. Décidez à froid votre position sur le paiement** d'une rançon : non, et pourquoi. **10. Préparez vos contacts d'urgence** : prestataire, assurance, CNIL, cybermalveillance.gouv.fr, dépôt de plainte.

Les trois questions à poser à votre prestataire

Où sont nos sauvegardes, et sont-elles **isolées du réseau** et **testées** ? Qui fait quoi, et **sous quel délai**, en cas d'incident ? Comment **préservez-vous les preuves** plutôt que de tout réinstaller en urgence ?

La carte des 72 heures

Dès la découverte d'un incident touchant des données personnelles : **qualifier sans détruire** → **isoler** sans tout couper → **préserver les traces** → **notifier la CNIL sous 72 h** → **informer** les personnes si le risque est élevé →

signaler (cybermalveillance.gouv.fr / ANSSI) et **porter plainte** → **communiquer** avec exactitude → **reconstruire** depuis des sauvegardes saines, puis **corriger la cause**.

REPÈRES

Quelques principes pour décider

> *Extraits de la doctrine DRC. À garder en tête, non comme des slogans, mais comme des repères de décision.*

Principe DRC — Le cyberespace n'est plus un outil de l'organisation : il est devenu son environnement de fonctionnement.

Principe DRC — La cybersécurité ne relève pas d'un service. C'est une responsabilité de gouvernance portée collectivement par toute l'organisation.

Principe DRC — L'ingénierie sociale exploite moins les faiblesses humaines que les mécanismes normaux de la confiance. La meilleure défense est une culture de la vérification, non de la suspicion.

Principe DRC — La mission du dirigeant n'est pas d'éliminer le risque. Elle est de prendre des décisions proportionnées, documentées et assumées, malgré l'incertitude.

Principe DRC — Le véritable Plan de Continuité d'Activité n'est pas celui qui est écrit. C'est celui qui fonctionne lorsque les procédures habituelles cessent de fonctionner.

Principe DRC — La négociation ne consiste pas à convaincre l'attaquant. Elle consiste à empêcher l'attaquant de gouverner la décision de l'organisation.

Principe DRC — Une organisation ne doit jamais protéger ses moyens au détriment de sa mission. C'est la mission qui donne une valeur aux moyens, jamais l'inverse.

DRC, à vos côtés

Ce livret est la voix condensée d'une doctrine portée par **DRC — DATASHIELD Risk Consulting**, qui agit sous trois noms complémentaires.

Forterys porte le **conseil** : gouvernance, analyse du risque, continuité, conduite de crise — la doctrine au service de la décision. **DATASHIELD** porte l'**investigation** : preuve numérique, vérité des faits, renseignement — la doctrine au service de la vérité. **Après Piratage** porte l'**assistance** : l'accompagnement des victimes, le versant humain de l'incident — la doctrine au service des personnes.

Une conviction les relie : protéger une organisation, c'est protéger sa capacité à poursuivre sa mission malgré l'incertitude. Si ce livret vous a fait réfléchir à une seule décision, il a rempli son office. Pour aller plus loin, l'édition complète du *Codex* développe chacun de ces sujets — et nous sommes à votre disposition pour en parler.

La maîtrise du risque numérique.