# Les défis pour la sécurité de la main-d'œuvre mobile : présentation et solution

#KingstonIsWithYou

# Les défis pour la sécurité de la main-d'œuvre mobile : présentation et solution

## Avant-propos

Il est temps pour vos collaborateurs de prêter un peu plus attention à la sécurité des données. Vous savez déjà que le télétravail est bénéfique pour votre activité. Toutefois, les défis que cette pratique représente pour la sécurité de votre réseau et votre conformité avec le RGPD sont bien trop importants pour être ignorés. Nombreuses sont les entreprises qui considèrent que la mise en place d'un contrôle sérieux de l'écosystème informatique implique obligatoirement de gros investissements. Ce n'est pas nécessairement le cas. Vous ne pouvez pas vous retrancher derrière l'argument du coût.

Les systèmes, les services et les produits existent et ils coûtent moins cher que vous ne le croyez. Le fait est que ce défi de la sécurité n'est pas seulement financier ou technique. Il est également culturel. Vous pouvez mettre en place un environnement informatique adéquat pour le télétravail sans trop de difficultés. Mais si vos collaborateurs n'adoptent pas l'attitude et le comportement adéquats vis-à-vis de la sécurité et de la conformité des données, votre activité rencontrera des difficultés. Les coûts potentiels d'une divulgation sont astronomiques.

**Les produits existent.**
**Mais c'est l'éducation qui va faire toute la différence.**

## Sommaire

Ce bref ebook a été rédigé par trois experts de la sécurité des données et du télétravail.

**Rob Allen**
@Rob_A_kingston

Rob occupe les fonctions de Directeur du marketing et des services techniques. Il travaille chez Kingston Technology depuis 1996. À ce titre, Rob est chargé de la supervision des relations publiques, des réseaux sociaux, du marketing des canaux de distribution avec les médias et la création du marketing numérique pour tous les produits et marques Kingston.

**Rafael Bloom**
@rafibloom73

Rafael est directeur de Salvatore ltd. Il aide les société à gérer les défis et les opportunités au niveau de la stratégie, des ventes et des procédures qui résultent de l'évolution des technologies et des réglementations.

**Sarah Janes**
@SarahkJanes

Sarah occupe les fonctions de Directrice générale chez Layer 8 Ltd depuis 2014. Cette société aide les responsables de la sécurité à créer et maintenir une culture de cybersécurité efficace dans toutes les organisations, depuis les petites activités familiales jusqu'aux grandes entreprises.

# Les défis pour la sécurité de la main-d'œuvre mobile : présentation et solution

## Table des matières



# Section 1 – Le problème

## L'accès à distance est critique

L'époque où le travail s'effectuait uniquement depuis un bureau centralisé est révolue. Les membres du personnel consultent leur courrier professionnel sur leur smartphones privés. Votre directeur d'exploitation passe plusieurs journées à travailler depuis chez lui ou depuis son café préféré. Les commerciaux accèdent aux données de l'entreprise indispensables à leur activité depuis les installations des clients. Le télétravail est devenu la nouvelle norme.

Il donne un coup de pouce à la productivité et à la rétention du personnel.[1] Il réduit les frais généraux.[2] Il contribue à la protection de l'environnement.[3] Des études indiquent que **70% des professionnels travaillent à distance au moins une fois par semaine.**[4]

Ceci étant dit, une seule personne suffit pour compromettre la sécurité de l'ensemble de votre organisation si elle n'adhère pas aux protocoles de sécurité nécessaires.

## La conformité avec le RGPD est incontournable

La mise en place de mesures de sécurité adéquates n'est pas négociable. La sécurité est indispensable pour garantir l'intégrité de votre organisation et éviter les violations du RGPD. Et le RGPD est à prendre au sérieux. L'Information Commissioner's Office (ICO, bureau du Commissariat à l'information) a récemment imposé à British Airways et à la chaîne d'hôtel Marriott des amendes d'un montant de près de 300 millions de livres sterling suite à des divulgations de données.[5]

**70%** des professionnels travaillent à distance au moins une fois par semaine.[4]

## Quels sont les types d'activité exposés au risque ?

Si des membres de votre personnel travaillent à distance ou s'ils accèdent aux systèmes de l'entreprise depuis leur propre dispositif, votre activité est exposée. C'est aussi simple que cela.

[1] **Inc.com: A 2-Year Stanford Study Shows the Astonishing Productivity Boost of Working From Home -** www.inc.com/scott-mautz/a-2-year-stanford-study-shows-astonishing-productivity-boost-of-working-from-home.html

[2] **PGi: What are the cost savings of telecommuting? -** www.pgi.com/blog/2013/03/what-are-the-cost-savings-of-telecommuting/

[3] **FlexJobs: 5 stats about telecommuting's environmental impact -** www.flexjobs.com/blog/post/telecommuting-sustainability-how-telecommuting-is-a-green-job/

[4] **CNBC: 70% of people globally work remotely at least once a week, study says -** www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html

[5] **The Guardian: GDPR fines: where will BA and Marriott's £300m go? -** www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog

# Section 2 – Les défis de l'accès à distance

## Le télétravail présente plusieurs défis en matière de sécurité.

Ils peuvent être difficiles à relever mais ils doivent être pris au sérieux pour l'intégrité de votre organisation.

**Sarah Janes**
@SarahkJanes

**Directrice générale**
**Layer 8 Ltd**

« Une des grandes préoccupations pour les entreprises depuis l'entrée en vigueur du RGPD est le contrôle des données à caractère personnel en leur possession. Aucune entreprise ne peut prétendre pouvoir contrôler ces données si elle ne sait pas où elles sont stockées. »

Les entreprises éprouvent des difficultés à faire évoluer leurs systèmes internes et leurs dispositifs au même rythme que la technologie en général.

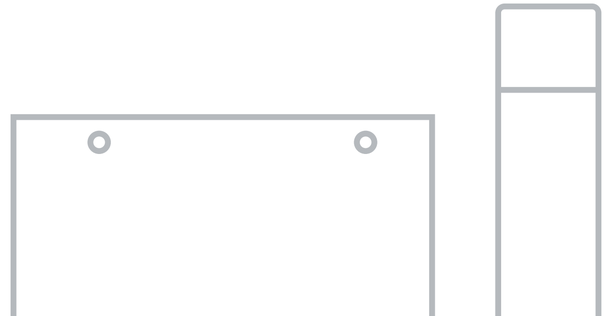
Ainsi, 38% des employés en télétravail engagés par les P.M.E. considèrent qu'ils ne disposent pas du support technique ou de l'expertise requis lorsqu'ils travaillent depuis leur domicile ou un espace public.

Dans ces conditions, les employés règlent les problèmes comme ils le peuvent et ce faisant, sapent vos efforts de protection des données et compromettent la sécurité de votre activité. Si vos protocoles de sécurité ne sont pas au service de l'efficacité de vos collaborateurs, ceux-ci trouveront des solutions alternatives telles que le stockage d'informations sensibles sur des sites comme Slack ou Dropbox, dans leur messagerie privée ou sur des clés USB personnelles. Et comme si cela ne suffisait pas, vous instaurerez une culture de confrontation entre votre équipe de sécurité de l'information et le reste de vos collaborateurs. Votre activité coure un risque.

**Rob Allen**
@Rob_A_kingston

**Directeur du marketing et des services techniques, Kingston Technology**

« D'après mon expérience, plus une entreprise est grande, plus le télétravail est compliqué et soumis à des restrictions. Les employés doivent gérer de longs délais de connexion et des mesures de sécurité complexes. »



# Section 2 – Les défis de l'accès à distance

## BYOD (Apportez vos propres terminaux)

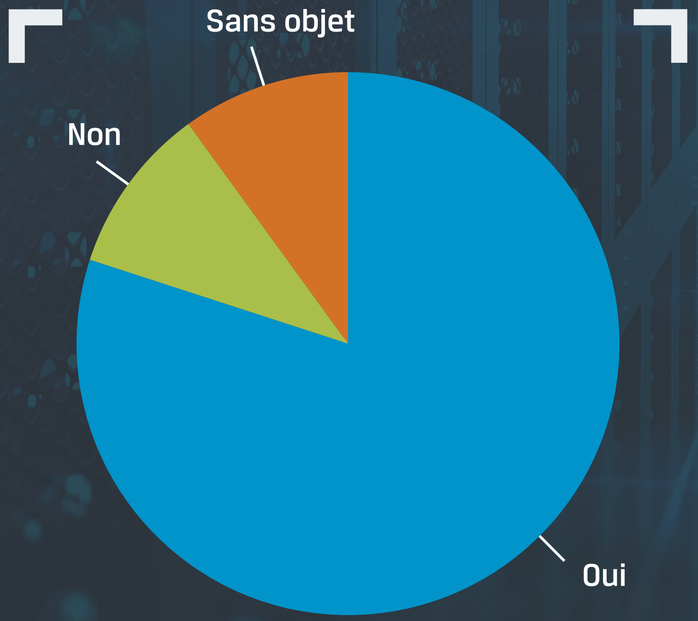
Il n'est pas rare de voir de nos jours des employés qui lisent leur courrier professionnel sur leur propre smartphone ou qui accèdent aux données de votre organisation depuis un ordinateur portable ou une tablette personnels. Ce comportement n'est pas sans danger. Votre équipe transfère-t-elle des données hors de l'organisation ? Le matériel et les logiciels utilisés sont-ils sûrs ? Ces questions méritent une réponse.

**Sarah Janes**
@SarahkJanes

**Directrice générale**
**Layer 8 Ltd**

« Pour les entreprises, le simple fait de savoir où leurs données sont stockées représente un important défi. »

## Avez-vous des raisons de croire que vos employés adoptent des pratiques inadéquates pour contourner les mesures de sécurité en place ?




Source : enquête Kingston 2019

## Réseaux Wi-Fi publics

Le problème ne se limite pas uniquement au travail depuis le domicile de l'employé. Qu'en est-il de ces employés qui aiment travailler depuis un café, en dégustant un latte ? Les réseaux Wi-Fi publics sont une véritable aubaine pour les pirates informatiques. Vous devez mettre à la disposition de vos collaborateurs tous les outils requis pour atténuer le risque.

## Cyberattaques et phishing sophistiqué

Les messages de phishing qui ciblent certains employés deviennent chaque jour plus élaborés et convainquant. Vos collaborateurs sont-ils en mesure de les identifier ? Et que dire de la menace en constante évolution que représentent les malwares et les ransomwares ? Tous vos dispositifs sans aucune exception doivent être protégés.

# Section 3 – L'infrastructure de l'accès à distance (et une note sur la mentalité de la sécurité)

**La technologie qui permet de relever les défis de la sécurité du télétravail existe. Et il n'est pas nécessaire d'investir une fortune.**

## Création de l'infrastructure adéquate

Les employeurs doivent tout entreprendre pour que leurs collaborateurs mobiles puissent accéder facilement et efficacement aux outils et aux données dont ils ont besoin pour réaliser leur tâches quotidiennes et être productifs. La solution ne consiste pas nécessairement à ajouter de nouveaux produits, mais bien à opérer les bons choix dès le départ. Par exemple, la majeure partie des entreprises ne peut se passer d'ordinateurs de bureau ou portables. Il convient donc de privilégier les disques durs ou les SSD chiffrés. Ainsi, en cas de perte ou de vol de données de l'entreprise, vous pourrez être certain qu'elles ne tomberont pas entre de mauvaises mains. De plus, en cas de divulgation de données, l'ICO fera preuve d'une plus grande compréhension si vous pouvez démontrer que vous aviez adopté des mesures concrètes pour protéger vos données.

## Travailler avec les bons vendeurs

Le secteur de la sécurité des technologies de l'information regorge de fabricants et de vendeurs. Faites vos recherches. Le secret consiste à disposer d'un système proposé par un fournisseur de solutions de confiance qui possède l'expertise adéquate pour faciliter le travail de votre main-d'œuvre mobile.

## VPN

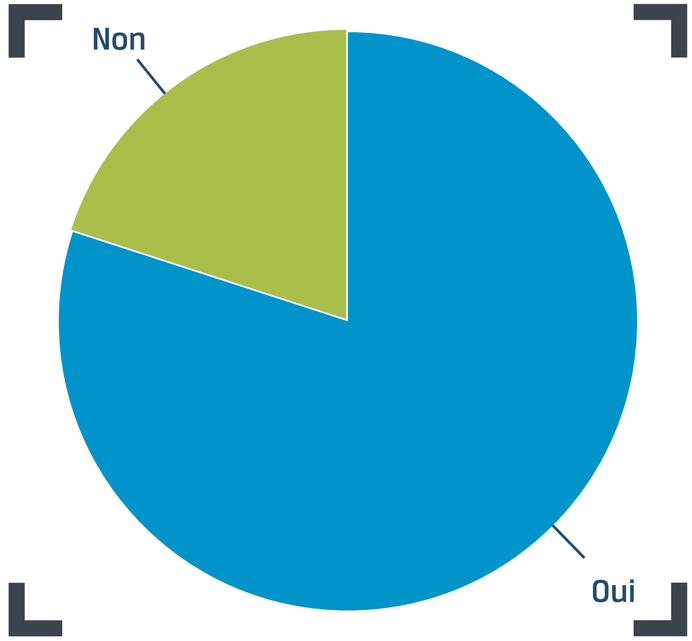
Si la protection de votre organisation passe par l'utilisation d'un réseau privé virtuel, l'accès des individus adéquats aux outils adaptés réduira considérablement vos risques. Les VPN sont particulièrement intéressants pour les collaborateurs qui accèdent aux données de l'entreprise via des réseaux Wi-Fi publics.

## Logiciel DLP

Presque toutes les suites logicielles DLP permettent de limiter l'accès au réseau tout en créant des listes blanches reprenant certains dispositifs comme des clés USB sécurisées qui ont été conçues dès le départ pour être uniques. Le coût d'une telle solution est minime. (Découvrez la gamme de solutions USB de Kingston, que vous pouvez personnaliser aux couleurs de votre organisation.)

## Avez-vous dû ou devez-vous introduire des modifications importantes dans votre entreprise pour garantir la conformité avec le RGPD ?

Source : enquête Kingston 2019



# Section 3 – L'infrastructure de l'accès à distance (et une note sur la mentalité de la sécurité)

## Clés USB et SSD

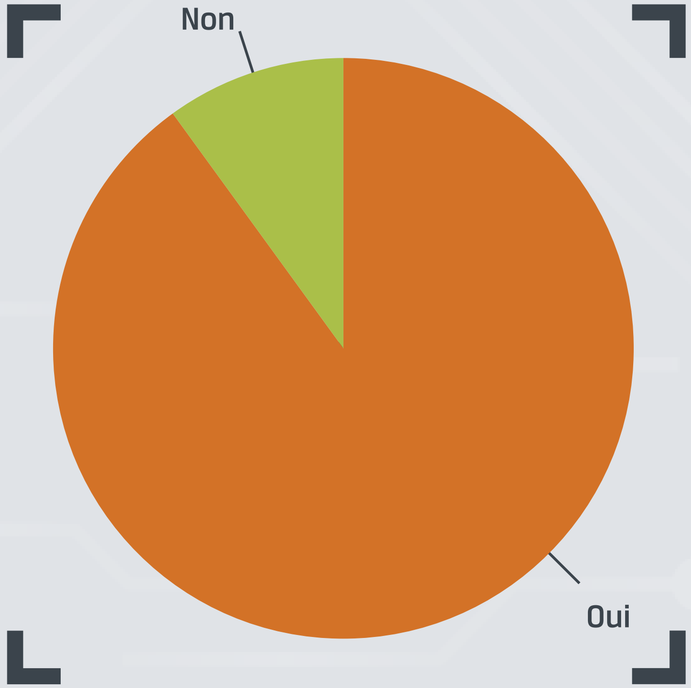
L'utilisation de clés USB sécurisées et l'équipement de vos ordinateurs portables avec des SSD chiffrées aident à résoudre les problèmes de travail à distance. En utilisant des clés USB sécurisées et des SSD chiffrés (avec ou sans Wi-Fi), vos données sont protégées et accessibles à tout moment et en tout lieu. Et en cas de perte ou de vol d'un dispositif, vous serez certain que personne ne pourra accéder aux fichiers chiffrés. Vous pouvez même détruire les clés USB à distance.

## Toujours s'attendre au pire

Parfois, un état d'esprit optimiste dissimule en fait une foi aveugle. Une équipe de sécurité digne de ce nom doit toujours imaginer le pire. Certes, il faut avoir confiance dans le comportement des collaborateurs et dans les mesures de sécurité. Mais il est bon de développer des hypothèses basées sur le pire des scénarios. L'intégrité de votre réseau a tout à gagner si vous supposez qu'il peut être attaqué et qu'il le sera.

## Ajoutez-vous un logiciel de sécurité sur les appareils mobiles de votre entreprise ? Par exemple, clés USB, ordinateurs portables, etc.

Source : enquête Kingston 2019



# Section 4 – La formation du personnel comme unique solution

Utiliser la technologie adéquate n'est pas le fin mot de l'histoire. Le véritable défi se situe au niveau des actions de vos collaborateurs quand ils se retrouvent seuls, face à leurs dispositifs. Voilà pourquoi les défis liés à la sécurité sont tout autant une question de culture du lieu de travail que de technologie. Sans la formation adéquate, le RGPD, la PECR et autres 'règles seront toujours vus comme des complications et rien d'autre pour vos collaborateurs.

**Voici quelques astuces.**

## Pas de règles sans raison

**« N'allez pas derrière cet arbre. »**
**« N'allez pas derrière cet arbre car il y a un lion. »**

Laquelle des deux sera plus facilement mémorisée ? L'être humain ne réagit pas bien face aux règles sans raison. Aidez vos employés à comprendre la raison d'être des règles.

## Personnalisation

De la même manière, vos collaborateurs comprendront mieux les défis pour la sécurité si vous les présenter sous une forme pertinente pour eux. Prenons le cas du RGPD par exemple. Pour aider les membres de votre équipe à comprendre que derrière chaque ensemble de données se trouve une personne, demandez-leur comment ils réagiraient face à une organisation qui adopterait une attitude nonchalante au traitement des données qu'ils leur ont confié. Quelle serait leur réaction si ces données tombaient entre de mauvaises mains ?

« Quand vous expliquez à un employé l'importance de la sécurité et du RGPD pour leurs intérêts en dehors de la vie professionnelle, il commence à comprendre pourquoi les organisations sont obligées de protéger ces données. »

**Rafael Bloom**
@rafibloom73
**Directeur chez Salvatore Ltd**

« En fin de compte, la meilleure manière d'améliorer la prise de conscience de la sécurité est de discuter avec les employés afin d'identifier les stratégies qui sont à la fois sûres et productives. »

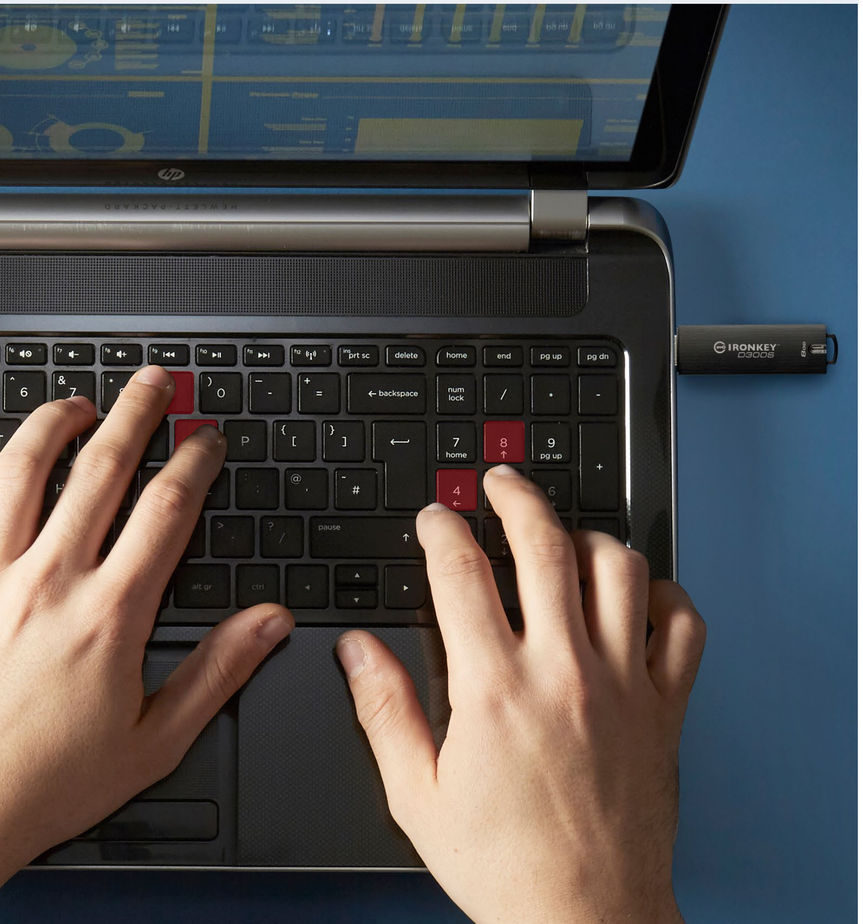
**Sarah Janes**
@SarahkJanes
**Directrice générale Layer 8 Ltd**

Source : enquête Kingston 2019

Réalisez-vous régulièrement un audit sur l'utilisation de solutions de stockage externe par vos employés ?

| 71% | 11% | 9% | 9% |
|---|---|---|---|
| Oui | Non | Pas sûr | Sans objet |

# Section 4 – La formation du personnel comme unique solution



## La formation est le début, pas la fin.

Étant donné que la majorité des organisations ne possède pas les ressources internes pour la formation sur la sécurité, d'autres entreprises doivent venir combler les lacunes. Mais il faut faire attention aux faux prophètes. Les formations assurées par des consultants externes sont trop souvent axées sur les exigences de conformité de cette activité (car c'est ce pourquoi ils obtiennent leur financement). Cela signifie que vos collaborateurs ne sortiront pas de ces formations avec une compréhension et une appréciation complètes de la cybersécurité. Les comportements dangereux persisteront.

**Sarah Janes**
@SarahkJanes

**Directrice générale**
**Layer 8 Ltd**

« Les organisations qui veulent véritablement modifier les comportements doivent oser arrêter les formations sur la sécurité à choix multiple. Elles doivent réfléchir à une formation qui permet aux collaborateurs de comprendre les bases de la sécurité et de la cybersécurité en général. »

La formation n'est pas la panacée. C'est trop facile de penser que votre personnel va automatiquement adopter des comportements sûrs et embrasser la conformité simplement parce qu'il a suivi une formation en la matière. Ce serait d'une naïveté dangereuse. La réussite requiert un travail continu pour changer la culture et les comportements.

**Rafael Bloom**
@rafibloom73

**Directeur chez Salvatore Ltd**

« J'ai vu des sociétés prétendument certifiées qui utilisent des feuilles de calcul ou des carnets pour sauvegarder les mots de passe ou d'autres sociétés dont les employés laissent dans leur voiture des copies non chiffrées de disque dur. À quoi bon posséder une certification si les principes de base n'ont pas été assimilés ? »

## Responsabiliser la base

Une stratégie potentielle pour introduire les changements de mentalité au sein de votre entreprise serait l'introduction de Champions de la sécurité qui se chargeraient de discuter des défis pour la sécurité et de proposer des protocoles de sécurité à la main d'œuvre à la base.

**Sarah Janes**
@SarahkJanes

**Directrice générale**
**Layer 8 Ltd**

« Des champions qui entament des discussions pour rendre la problématique de la sécurité plus pertinente au contexte de chaque employé avec, en parallèle, des formations en ligne pour faciliter les changements, représentent la meilleure méthode pour l'adoption de comportements sûrs. »

# Résumé

La protection des données et la cybersécurité peuvent représenter une lourde responsabilité. Ceci étant dit, les outils adéquats garantissent la simplicité et la sécurité du télétravail. Qui plus est, leur mise en œuvre est bon marché. Il ne faut cependant pas oublier que la mise en place d'une infrastructure de sécurité adéquate doit s'accompagner d'un changement de mentalité au sein de votre organisation si vous souhaitez que votre équipe adopte un comportement sûr.

**Voici un bref résumé.**

- Le télétravail est un acquis qui offre de nombreux avantages, notamment en matière de productivité, de loyauté du personnel et de réduction des frais généraux. Cependant, le télétravail présente plusieurs défis en matière de sécurité.
- Les violations de données sont une préoccupation certaine vu les grosses amendes imposées par l'ICO pour les violations du RGPD.
- Le concept BYOD, le matériel non sécurisé, l'utilisation inadéquate des logiciels et des réseaux Wi-Fi publics sont des menaces communes pour la sécurité.
- Une infrastructure de sécurité réussie doit promouvoir l'efficacité de vos collaborateurs et non pas la freiner. Dans le cas contraire, vos collaborateurs chercheront des raccourcis et des alternatives.
- Passez en revue les fabricants et vendeurs de solutions de technologie de l'information et choisissez ceux qui ont fait leur preuve.
- Les outils tels que les SSD et les clés USB sécurisées, les réseaux VPN et les logiciels DLP sont faciles à mettre en œuvre et ne coûtent pas cher.
- La réussite en matière de protection des données et de sécurité repose sur un changement de mentalité et de comportement au sein de votre organisation. Vous devez expliquer à vos collaborateurs pourquoi les règles ont été mises en place et non pas simplement leur dire de suivre aveuglément des protocoles.
- Vous pouvez certes compter sur l'aide de consultants externes pour la formation de votre personnel sur les questions de sécurité, mais il faudra veiller à ce que le contenu soit adapté et vous devez comprendre que vos collaborateurs ne vont pas adopter automatiquement le bon comportement simplement parce qu'ils l'ont entendu dans le cadre d'une formation.
- Introduisez les champions de la sécurité pour aborder les défis de sécurité et introduire les bons comportements à la base.

# À propos de Kingston

Kingston, avec ses 32 années d'expérience, dispose du savoir pour identifier vos défis en matière de télétravail et vous aider à les relever afin que vos collaborateurs puissent travailler en sécurité n'importe où, sans compromettre votre organisation.



**#KingstonIsWithYou**