Kensington®

Sécurisez vos appareils, protégez vos données.

Comment la sécurité physique peut prévenir votre prochaine violation de données

Introduction

Le paysage de la sécurité a considérablement évolué au cours des dernières années, en raison de changements majeurs dans nos modes et lieux de travail. La pandémie de COVID-19 a été le principal moteur de cette évolution : elle a accéléré l'adoption de modèles de travail hybrides et flexibles et modifié fondamentalement les priorités en matière de sécurité des appareils.

Kensington a commandité une étude réalisée par Vanson Bourne, spécialiste indépendant des études de marché, auprès de 1 000 décideurs informatiques seniors, responsables de la sécurité physique (matérielle) de leur entreprise aux États-Unis et dans la zone EMEA. Presque toutes les personnes interrogées (**92%**) ont renforcé leurs politiques de sécurité en réponse à la pandémie, reconnaissant les risques accrus associés aux environnements de travail décentralisés. Dans la perspective de 2025, les modèles de travail plus flexibles devraient se développer, soulignant qu'il est temps de repenser les stratégies de sécurité des appareils.

Les violations de données ne sont pas seulement un problème numérique : chaque appareil volé ou non sécurisé représente une porte d'entrée potentielle pour un accès non autorisé à des informations confidentielles, présentant des risques importants pour les entreprises. Le fardeau financier d'une violation de données atteignant désormais en moyenne des millions d'euros, les enjeux n'ont jamais été aussi élevés. À mesure que les entreprises continuent d'adapter leurs modèles de travail, l'urgence d'aborder les problèmes de sécurité des appareils a considérablement augmenté. Des exigences plus strictes en matière de protection des données et une recrudescence des violations de données ont encore renforcé l'importance de protéger à la fois les appareils physiques et les informations confidentielles qu'ils contiennent. Ce rapport met en évidence le rôle essentiel que jouent les câbles de sécurité dans la réduction de ces risques et souligne pourquoi il est essentiel d'agir maintenant pour anticiper les défis émergents.

Grâce à ces résultats, nous examinerons les impacts concrets du vol d'appareils, montrerons comment des solutions simples mais efficaces comme les câbles de sécurité peuvent aider à réduire les risques et soulignerons comment la sécurité physique offre une tranquillité d'esprit dans un monde où les modèles de travail évoluent constamment. Ce rapport fournit des informations pratiques pour les entreprises évoluant dans le paysage complexe de la sécurité d'aujourd'hui. Il explique les conséquences importantes du vol d'appareils et montre comment les câbles de sécurité peuvent être à la fois rentables et rassurants.

Principales constatations:

76% des personnes interrogées déclarent que leur entreprise a été touchée par des incidents de vol au cours des deux dernières années, les incidents étant plus fréquents dans les organisations qui ont des modèles de travail plus flexibles. Par exemple, notre étude a révélé que **85%** des entreprises avec des modèles de travail flexibles ont connu un incident de vol au cours des deux dernières années, contre **71%** de celles dont les employés sont entièrement sur site.

Les conséquences du vol d'appareils vont au-delà de la perte matérielle et incluent notamment :

- Nécessité de renforcer les mesures de sécurité existantes (**33%**)
- Conséquences juridiques ou réglementaires dues à la compromission de données sur des appareils volés (**33%**)
- Baisse de productivité des employés due à la perte ou au vol d'appareils (**32%**)

Les organisations utilisant des câbles de sécurité ont été **37%** moins susceptibles de subir une violation de données due à un appareil non sécurisé (**38%** contre **60%** parmi celles qui n'en utilisent pas).

Les entreprises qui utilisent actuellement des câbles de sécurité ont été également plus susceptibles d'adopter une double approche de la sécurité, les trois quarts (**76%**) ayant recours à des mesures numériques telles que les empreintes digitales ou les clés de sécurité pour l'authentification à deux facteurs, contre **62%** de celles qui n'utilisent pas du tout de câbles de sécurité.

84% estiment que les câbles de sécurité sont rentables pour réduire les violations de données potentielles, offrant un bénéfice significatif pour un investissement relativement faible.

- **42%** considèrent que les câbles de sécurité sont extrêmement rentables, offrant une protection élevée à faible coût, les cadres supérieurs étant plus susceptibles de reconnaître leur valeur (**56%**) que les cadres intermédiaires (**36%**).

Presque toutes les personnes interrogées (**97%**) pensent que les câbles de sécurité peuvent empêcher le vol, réduisant ainsi le risque d'accès non autorisé aux données confidentielles de l'entreprise.

Le vol d'appareils : des conséquences stupéfiantes

Il est rare qu'un jour se passe sans que l'on entende parler d'un incident de sécurité, qu'il s'agisse d'une attaque à grande échelle contre un conglomérat mondial ou d'une exploitation plus ciblée d'une infrastructure ou d'un service critique. Et bien que ces exemples suggèrent que les cyberincidents soient souvent les plus largement discutés, ou du moins présumés l'être, il est important de reconnaître que les menaces sur la sécurité physique peuvent être tout aussi critiques.

On parle peu des incidents de sécurité physique, où des personnes non autorisées accèdent à des zones sécurisées ou compromettent des biens, ce qui a des conséquences tout aussi désastreuses qu'une attaque par rançongiciel typique. Selon notre étude, plus des trois quarts (**76%**) des personnes interrogées déclarent que leur entreprise a été touchée par des incidents de vol d'appareils au cours des deux dernières années.

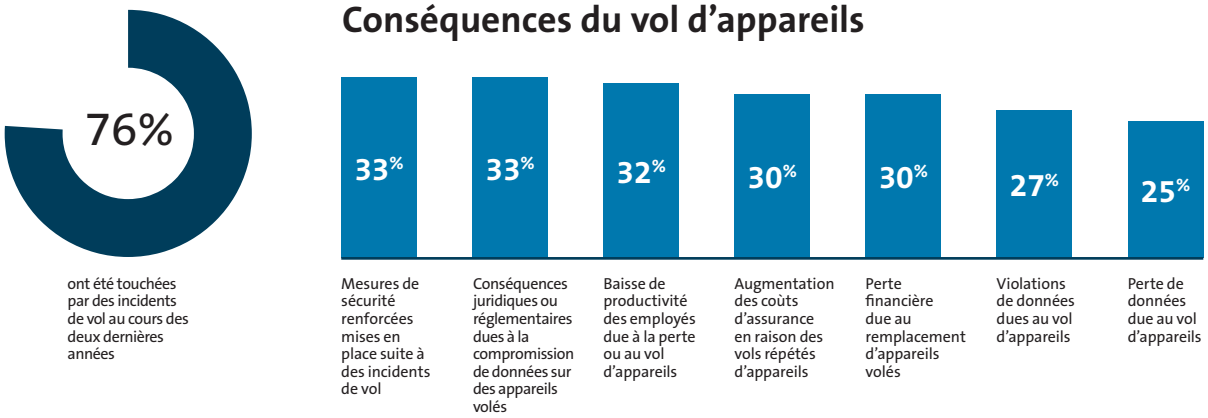


Fig. 1: *comment votre entreprise a-t-elle été touchée par des incidents de vol d'appareils au cours des deux dernières années ? [Toutes les personnes interrogées : 1000]*

Ce n'est pas seulement le coût évident du remplacement d'un appareil auquel les entreprises sont confrontées (**30%**). Les conséquences les plus courantes sont une augmentation des mesures de sécurité mises en place à la suite de ces incidents (**33%**) et des conséquences juridiques ou réglementaires dues à la compromission de données (**33%**), ces dernières étant souvent clairement décrites. Par exemple, les amendes au titre du RGPD[1] peuvent atteindre jusqu'à 20 millions d'euros ou **4%** du chiffre d'affaires global d'une entreprise, les violations même moins graves pouvant coûter jusqu'à 10 millions d'euros, ce qui présente des risques financiers importants en cas de non-conformité. Aux conséquences financières s'ajoute le coût de la baisse de productivité des employés due à la perte ou au vol d'appareils (**32%**). Au-delà de l'une de ces conséquences, il y a une implication financière ou temporelle claire sur les résultats de l'entreprise. Ainsi, ce ne sont pas seulement les incidents de sécurité numérique qui requièrent une attention particulière, les menaces physiques présentent aussi des risques importants. En approfondissant leur compréhension de ces vulnérabilités, les entreprises peuvent prendre des mesures simples et rentables pour protéger leurs appareils. Les mesures de sécurité physique étant à la fois abordables et faciles à mettre en place (comme nous le verrons plus loin), elles représentent une première étape pratique dans le renforcement de la sécurité globale.

"Outre les mesures de cybersécurité, **la sécurité physique est tout aussi importante.** Les câbles de sécurité font partie d'une stratégie de cybersécurité renforcée."

Cadres supérieurs ; fabrication et production ; 1 000 employés ou plus ; modèle de travail entièrement sur site ; France

1 GDPR Fines/Penalties, Intersoft Consulting, https://gdpr-info.eu/issues/fines-penalties/

De nos jours, il ne s'agit pas de savoir si une violation de données se produira, mais quand. En fait, chaque vol d'appareil représente une violation de données potentielle, et les implications financières sont énormes pour les entreprises. Selon le rapport le plus récent d'IBM sur le coût des violations de données[2], le coût moyen global d'une violation de données en 2024 s'élevait à 4,88 millions de dollars US, soit une augmentation de **10%** par an par rapport à la moyenne de 2023. Ce chiffre varie selon le secteur et la taille de l'entreprise, certaines organisations pouvant donc être confrontées à des chiffres encore plus élevés.

Analyse des données:

- **Secteur:** les entreprises des secteurs des services aux consommateurs (**95%**), de l'énergie, du pétrole/gaz et des services publics (**90%**), de la construction et de l'immobilier (**89%**) sont les plus susceptibles d'avoir été touchées par le vol d'appareils. La forte mobilité des employés et des appareils dans ces entreprises les expose à un risque accru de vol.
- **Taille:** la probabilité de vol d'appareils a augmenté de **82%** dans les petites entreprises (100–249 employés) contre **69%** dans les grandes entreprises (plus de 1 000 employés), soulignant les conséquences plus importantes pour les petites entreprises où les ressources sont plus limitées.
- **Niveau hiérarchique:** ceux qui occupent des postes plus élevés sont beaucoup plus susceptibles de déclarer avoir été touchés par des incidents de vol (**87%**) que les cadres intermédiaires (**67%**). Il est probable que les responsables de la gestion quotidienne d'une entreprise soient mal informés des menaces potentielles liées aux appareils non sécurisés. Accroître leur sensibilisation aux menaces et aux répercussions associées encouragera les entreprises à intégrer les câbles de sécurité dans leurs besoins culturels et à harmoniser les perspectives à tous les niveaux pour soutenir une stratégie de sécurité globale.

Comment les modèles de travail jouent-ils un rôle ici ?

Nous avons mentionné, en introduction de cette étude, le changement radical des modes de travail au cours des dernières années, l'adoption de modèles de travail plus flexibles, en dehors d'un lieu de travail fixe, ayant été accélérée par la pandémie de COVID-19.

Alors que plus des trois quarts (**76%**) des personnes interrogées déclarent que leur entreprise a été touchée par un vol d'appareils au cours des deux dernières années, cela devient plus évident encore lorsque les modèles de travail sont plus flexibles, passant à plus de 9 sur 10 (**94%**) lorsque les employés travaillent entièrement à distance.

Ampleur du vol d'appareils au cours des deux dernières années, selon le modèle de travail actuel

Fig. 2: *proportion des personnes interrogées dont l'entreprise a été touchée par des incidents de vol d'appareils au cours des deux dernières années. [Toutes les personnes interrogées, données réparties par modèle de travail actuel, chiffres de base dans le graphique]*

2 Cost of a Data Breach Report 2024, IBM, juillet 2024, https://www.ibm.com/reports/data-breach

Bien qu'il soit important pour toute entreprise de veiller à la sécurité physique des appareils et de se méfier des conséquences du vol d'appareils, les modèles de travail flexibles et à distance amplifient considérablement le risque de vol, rendant des mesures de sécurité robustes plus importantes que jamais.

Il faut noter que les vols d'appareils sont généralement nombreux, même lorsque les employés sont entièrement sur site. Les entreprises ne peuvent se permettre aucune complaisance, quel que soit le lieu de travail de leurs employés. La menace de vol d'appareil n'est pas nouvelle et n'est pas apparue uniquement après la pandémie. Notre étude de 2016[3] a examiné les risques de sécurité causés par le vol de matériel informatique en entreprise. Les professionnels de l'informatique interrogés ont classé le risque de vol d'appareils au bureau (**23%**) presque aussi élevé que le risque de vol dans les voitures et les transports (**25%**), et supérieur au risque de vol dans les aéroports et les hôtels (**15%**) ou les restaurants (**12%**). Cela montre que le vol d'appareils demeure une menace constante, même dans des environnements entièrement sur site, soulignant la nécessité d'une vigilance accrue et de mesures de sécurité physique proactives, quel que soit le lieu de travail.

Ce défi a été encore amplifié dans le monde post-COVID-19, **93%** des entreprises signalant une augmentation des risques de sécurité en raison du passage à des modèles de travail flexibles et hybrides. Ces risques ne se limitent pas au vol d'appareils physiques, ils incluent aussi des vulnérabilités accrues en matière de protection des données, des accès non autorisés et des violations causées par des réseaux domestiques non sécurisés et des environnements de travail décentralisés.

"**C'est le moyen, le plus simple** de s'assurer que nos appareils sont littéralement verrouillés ! **Nous avons ainsi la certitude que tout est en sécurité.**"

Membre du conseil d'administration/cadre de direction ; informatique, technologies et télécommunications ; 100–249 employés ; modèle de travail flexible ; États-Unis

Les risques de sécurité augmentent en raison des environnements de travail hybrides ou à distance

35% Risque accru de vol d'appareils en dehors des environnements de bureau securisés

35% Manque de contrôle sur l'environnement physique dans lequel les appareils sont utilisés *(par exemple, les appareils sans surveillance)*

34% Plus grande vulnérabilite aux violations de données dues à des réseaux domestiques non sécurises

34% Augmentation des cas de piratage visuel dans les espaces publics *(par exemple, espionnage physique de l'écran d'une personne dans les cafés, les aéroports, etc.)*

34% Risque accru d'acces non autorisé aux appareils de l'entreprise dans les espaces publics ou partages

34% Dépendance accrue a l'égard d'appareils personnels susceptibles de ne pas être conformes aux normes de sécurité de l'entreprise

32% Absence de mesures de sécurité physique appropriées pour les appareils situés dans des lieux distants *(par exemple, câbles de sécurité)*

32% Plus grande difficulté à appliquer les stratégies de sécurité des appareils à distance

Fig. 3: *selon vous, quels risques de sécurité ont augmenté en raison des environnements de travail hybrides ou à distance suite à la pandémie de COVID-19 ? [personnes interrogées dont l'entreprise a connu un passage au travail hybride/à distance suite de la pandémie de COVID-19 : 494]*

Dans cette optique, la meilleure approche de la sécurité consiste à combiner des mesures physiques robustes avec des protections numériques avancées afin de garantir une protection complète des appareils et des données dans un monde de plus en plus décentralisé.

3 lÉtude sur la sécurité informatique et le vol d'ordinateurs portables, Kensington, août 2016, https://www.kensington.com/news/news-press-center/2016-news--press-center/kensington-survey-data-reveals-that-it-theft-in-the-office-ranks-nearly-as-high-as-theft-in-cars-and-more-than-in-airports-or-restaurants/?srsltid=AfmBOooRTMdZ4gjmcNB3viXIJcIL4GY47Xx-O5I08AldLhLEB5LjnH0Ts

Des câbles de sécurité qui empêchent les pertes et réduisent les coûts

"L'absence d'un câble de sécurité sur l'équipement a entraîné une violation de données, **engendrant des pertes importantes pour l'entreprise.**"

Cadre intermédiaire ; informatique, technologies et télécommunications ; 1 000 employés ; modèle de travail flexible ; États-Unis

Jusqu'à présent, nous avons mis en évidence les conséquences du vol d'appareils et à quel point il peut être répandu, quel que soit l'environnement de travail. Pourtant, ce n'est pas la seule préoccupation de nos décideurs informatiques seniors interrogés. Un large éventail d'aspects les inquiète en matière de sécurité, dans les domaines physique et numérique.

Certaines de ces préoccupations présentent de nouveaux facteurs en matière de sécurité physique. Par exemple, près d'un quart (**23%**) sont préoccupés par le piratage visuel, où les données confidentielles sont à la merci de quiconque si l'écran d'une personne est exposé dans un lieu public, par exemple dans un café ou dans les transports en commun. En fait, ceux qui travaillent de manière flexible (**48%**) sont plus susceptibles de signaler le piratage visuel comme une préoccupation que ceux qui opèrent dans des environnements entièrement à distance (**3%**) ou hybrides (**33%**). Cela souligne que le piratage visuel n'est pas seulement associé au travail à domicile, mais plutôt à l'octroi de libertés excessives qui sont plus difficiles à contrôler. Les entreprises devront prendre en considération la protection de leurs données lorsque les employés sont en déplacement, grâce à des solutions de dissuasion supplémentaires telles que les filtres de confidentialité.

Aspects les plus préoccupants de la sécurité des appareils

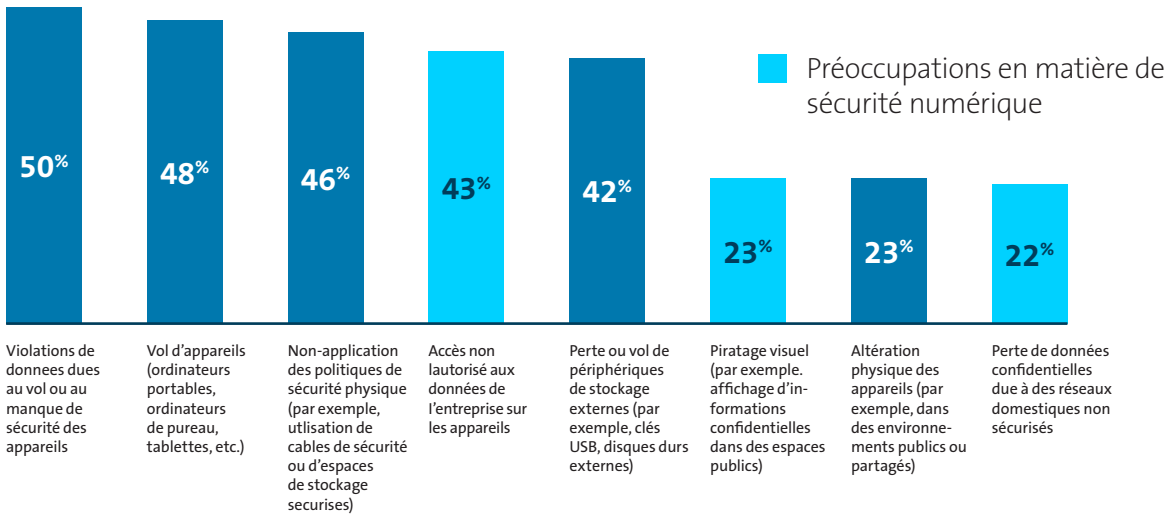


Fig. 4: *quels sont les aspects de la sécurité des appareils qui vous préoccupent le plus dans votre entreprise ? [Toutes les personnes interrogées : 1 000, combinaison des réponses classées en première, deuxième et troisième position]*

Les violations de données restent néanmoins la principale préoccupation, ce qui est justifié car une proportion notable (**46%**) a subi une violation de données comme conséquence directe d'un appareil non sécurisé.

C'est là qu'un câble de sécurité peut être utile. Les entreprises qui en utilisent sont **37%** moins susceptibles d'avoir subi une violation de données due à un appareil non sécurisé par rapport à celles qui n'en utilisent pas.

Entreprises ayant subi une violation de données ou une perte de données confidentielles à cause d'un appareil non sécurisé

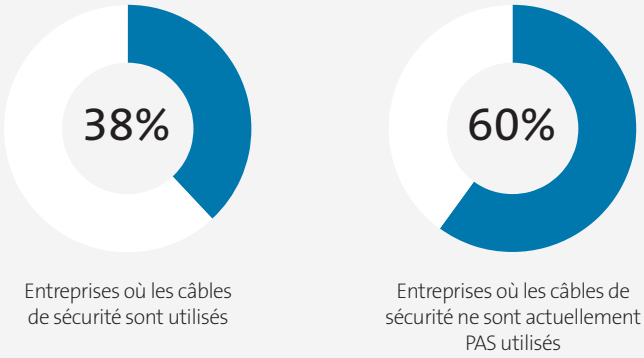


Fig. 5: *votre entreprise a-t-elle subi une violation de données ou une perte de données confidentielles comme conséquence directe d'un appareil non sécurisé ? [Toutes les personnes interrogées, données réparties entre ceux qui utilisent actuellement des câbles de sécurité : 629 ; et ceux qui n'en utilisent aucun : 371]*

Le résultat est clair : démontrer une réduction mesurable des violations ou pertes de données renforce la valeur des câbles de sécurité comme élément essentiel d'une protection complète des appareils. Ces preuves convaincantes soulignent comment les câbles de sécurité réduisent directement les risques, les positionnant comme un investissement indispensable pour les entreprises qui s'engagent à protéger leurs données et minimiser les vulnérabilités de sécurité.

Analyse des données:

- **Secteur:** d'après les résultats de l'enquête, les entreprises des secteurs des services aux consommateurs (**65%**) et des soins de santé publics/privés (**57%**) sont plus susceptibles d'avoir subi une violation de données à cause d'un appareil non sécurisé. Le premier secteur est parmi les plus susceptibles d'avoir été touché par le vol d'appareils en général. En ce qui concerne le deuxième secteur, cela souligne peut-être des préoccupations plus importantes concernant la nature décentralisée des établissements de santé et le contact plus étroit du public avec les appareils. Le fait de disposer d'une telle richesse de données confidentielles expose ce secteur à un risque accru.
- **Taille:** soulignant davantage les ressources limitées des petites entreprises, elles sont plus susceptibles (**59%**) que les plus grandes (**40%**) d'avoir subi une violation de données à cause d'un appareil non sécurisé. Elles sont non seulement confrontées aux premières difficultés, mais aussi à l'effet boule de neige qui en découle.
- **Niveau hiérarchique:** ceux qui occupent des postes moins élevés sont moins susceptibles de signaler une violation de données ou une perte de données confidentielles à cause d'un appareil non sécurisé (**30%**) que leurs collègues membres du conseil d'administration ou cadres de direction (**59%**). Il y a un net décalage au sein des entreprises entre la compréhension réelle de la sécurité des appareils physiques et les conséquences de son manquement, ce qui nécessite une éducation et un partage des connaissances plus étendus.

"Un petit investissement initial dans des mesures de sécurité (câbles de sécurité) **peut contribuer grandement à éviter des remplacements coûteux d'appareils** ou des temps d'arrêt prolongés."

Cadres supérieurs ; éducation – secteur public ; 1 000 employés ou plus ; modèle de travail hybride ; États-Unis

Alors, comment les entreprises pourraient-elles surmonter ce problème?

Les entreprises sont confrontées à de nombreux problèmes de sécurité numérique et physique, et les conséquences du vol d'appareils sont stupéfiantes pour les entreprises et leurs résultats. Elles devraient rechercher la solution la plus rentable. Fort de son succès, un simple câble de sécurité pourrait être la réponse.

La majorité (**84%**) des décideurs informatiques seniors interrogés affirment que les câbles de sécurité sont rentables pour réduire les violations de données potentielles, soulignant leur valeur significative dans la prévention des vols et des violations. En outre, **42%** pensent qu'ils sont extrêmement rentables.

C'est une opinion universelle partagée par ceux qui utilisent déjà des câbles de sécurité et même ceux qui n'en utilisent aucun, ce qui soulève la question : pourquoi pas ? Les entreprises peuvent considérer les câbles comme des complications logistiques pour la gestion des appareils, ou peut-être qu'une plus grande attention accordée à la sécurité numérique plutôt qu'à la sécurité physique entraîne une sous-estimation de la valeur des câbles de sécurité, entravant ainsi leur adoption. Pourtant, comparé aux conséquences financières stupéfiantes du vol d'appareils, le coût d'un câble de sécurité (généralement entre 30 et 50 € par appareil seulement) représente un investissement minime pour réduire les risques. En approfondissant cette question, nous constatons une nette différence d'opinion au sein de la hiérarchie organisationnelle.

Rentabilité perçue des câbles de sécurité

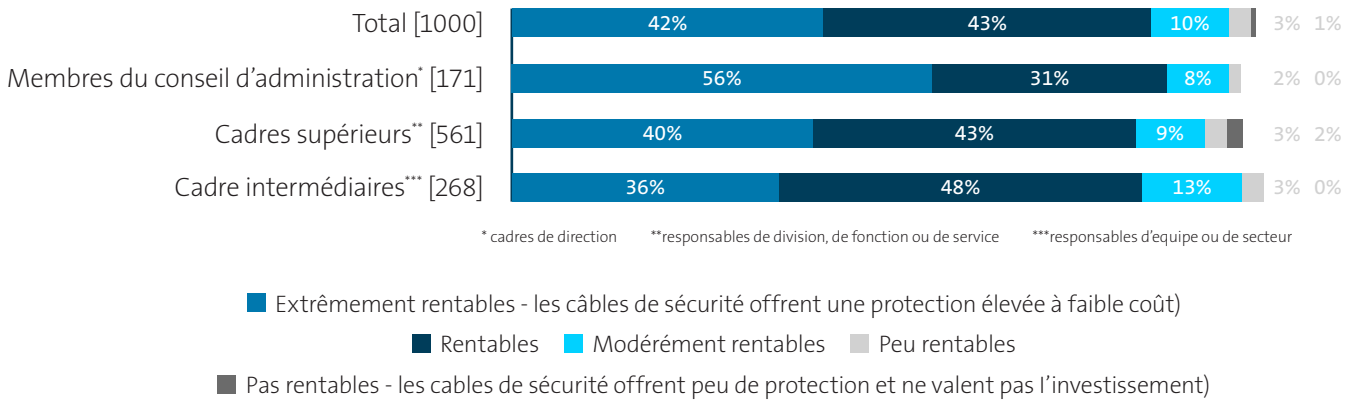


Fig. 6: *en termes de rentabilité, comment considérez-vous les câbles de sécurité dans la réduction des violations de données ou des vols d'appareils potentiels ? [Toutes les personnes interrogées, données réparties par niveau hiérarchique, chiffres de base dans le graphique]*

Ces résultats soulignent la nécessité cruciale de s'attaquer aux causes profondes du vol d'appareils et à ses répercussions plus larges dans l'ensemble de l'entreprise. Alors que les cadres supérieurs sont plus susceptibles de considérer les câbles de sécurité comme extrêmement rentables (**56%**), cette croyance diminue aux niveaux inférieurs de la hiérarchie. En fin de compte, les cadres supérieurs seront toujours plus axés sur les implications plus larges (par exemple, amendes réglementaires, réputation), tandis que les cadres inférieurs se concentreront sur les conséquences quotidiennes (par exemple, perte de productivité).

Ce décalage souligne l'importance de l'alignement organisationnel et de la sensibilisation à l'impact des câbles de sécurité, non seulement en tant qu'outil rentable, mais aussi en tant que solution proactive pour éviter des pertes importantes. Combler ces écarts de perception assurera une approche unifiée et efficace pour réduire les risques de vol d'appareils et protéger les données confidentielles.

"Une fois perdu, cet appareil causera des pertes importantes. Nous devons **résoudre ce problème à la source.**"

Cadre intermédiaire ; soins de santé – secteur privé ; 1000 employés ou plus ; modèle de travail hybride ; États-Unis

Les câbles de sécurité protègent et rassurent

Nous avons poursuivi notre analyse pour montrer que les câbles de sécurité ne sont pas seulement efficaces pour prévenir le vol, mais qu'ils constituent aussi une solution rentable pour réduire les risques de sécurité plus larges. Leurs diverses applications mettent en évidence leur polyvalence pour relever les défis de sécurité dans divers environnements, un avantage que de nombreuses entreprises réalisent déjà.

Beaucoup utilisent déjà des câbles de sécurité pour protéger les appareils électroniques dans leur entreprise. Les appareils les plus souvent sécurisés sont les ordinateurs portables (**44%**), les ordinateurs de bureau (**43%**) et les serveurs (**42%**), ce qui reflète la priorité accordée à la protection du matériel critique qui contient souvent des données confidentielles. Cette adoption généralisée témoigne de la reconnaissance des câbles de sécurité en tant qu'outil essentiel de protection contre le vol et l'accès non autorisé.

Rentabilité perçue des câbles de sécurité

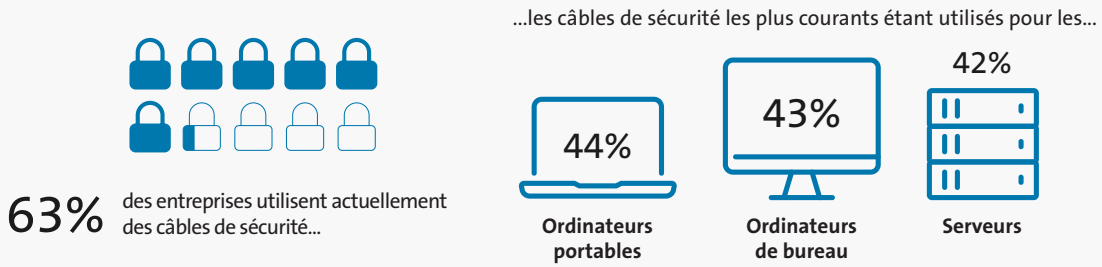


Fig. 7: *Parmi les appareils électroniques suivants, lesquels sont équipés de câbles de sécurité dans votre entreprise ? [Toutes les personnes interrogées : 1000]*

Cependant, le fait que près de 4 personnes interrogées sur 10 déclarent que leur entreprise n'utilise aucun câble de sécurité suscite des préoccupations quant aux vulnérabilités des stratégies de sécurité des appareils, en particulier pour les équipements fréquemment utilisés dans les environnements de travail mobiles ou hybrides.

Pour les entreprises, ces données soulignent la nécessité d'évaluer leurs mesures de sécurité actuelles de manière exhaustive. Bien que les câbles de sécurité soient une solution fiable et répandue, étendre leur utilisation à un plus large éventail d'appareils et les associer à des protections numériques complémentaires peut aider à combler les failles de sécurité existantes et à réduire les risques plus efficacement.

Presque toutes les personnes interrogées (**97%**) reconnaissent le rôle essentiel que jouent les câbles de sécurité dans la prévention du vol et de l'accès non autorisé qui en découle souvent. Cette reconnaissance généralisée reflète la confiance que les entreprises accordent à la sécurité physique en tant que mesure fondamentale pour protéger les appareils et les données confidentielles. Les câbles de sécurité agissent comme une première ligne de défense, réduisant les possibilités de vol et les risques associés au matériel compromis.

"La présence de câbles de sécurité dans les bureaux ouverts, les espaces de coworking ou d'autres zones où plusieurs personnes peuvent être présentes, **réduit le risque de vol.**"

Membre du conseil d'administration/cadre de direction ; éducation – secteur privé ; 100–249 employés ; États-Unis

Conviction que les mesures de sécurité physique contribuent à empêcher le vol d'appareils

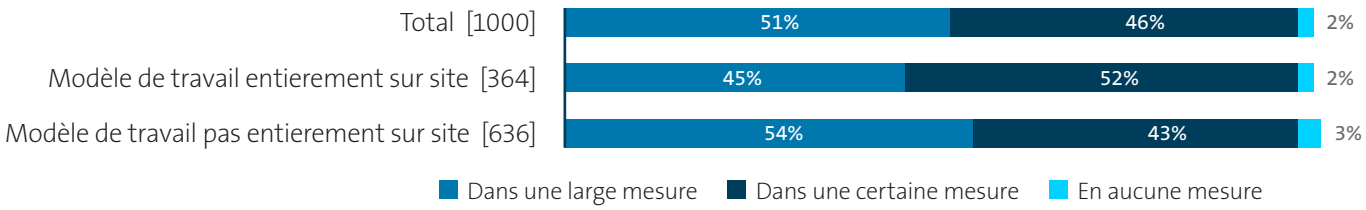


Fig. 8: *Dans quelle mesure pensez-vous que les mesures de sécurité physique telles que les câbles de sécurité contribuent à empêcher le vol d'appareils qui pourrait entraîner un accès non autorisé aux données de l'entreprise ? [Toutes les personnes interrogées, données réparties par type de modèle de travail, chiffres de base dans le graphique]*

Cette reconnaissance devient plus importante dans les entreprises qui ont adopté des modèles de travail flexibles et hybrides. Dans ces environnements décentralisés, les appareils sont de plus en plus utilisés dans des endroits non sécurisés, comme les bureaux à domicile ou les espaces publics, amplifiant le risque de vol ou d'exposition accidentelle. Les violations de données causées par des appareils non sécurisés sont beaucoup plus fréquentes dans les environnements de travail plus flexibles (**50%** combinés contre **39%** pour un modèle de travail entièrement sur site).

Conçus pour s'adapter à divers environnements, les câbles de sécurité offrent une protection fiable pour les appareils, qu'ils soient utilisés dans des bureaux, des espaces de travail à distance ou des environnements publics, garantissant ainsi la tranquillité d'esprit des entreprises dans tous les modèles de travail.

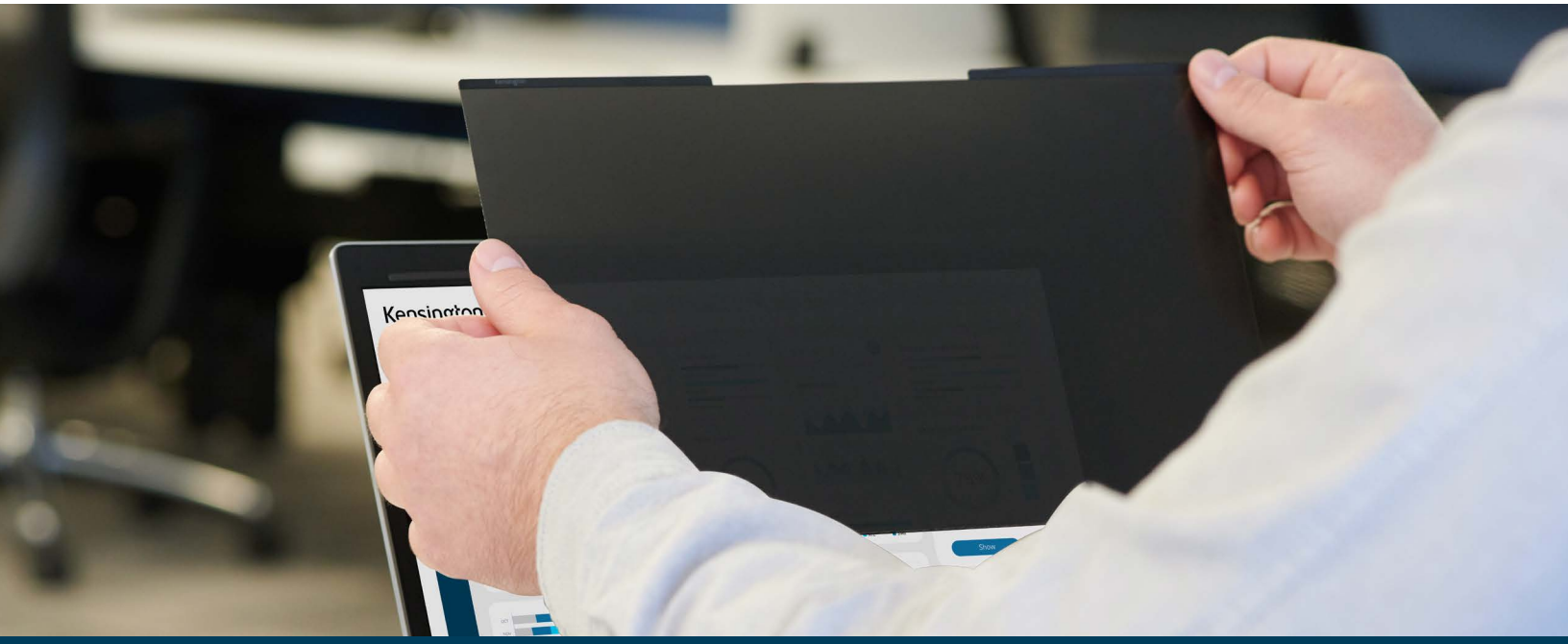
Conclusion

Les conséquences financières du vol d'appareils peuvent être énormes, le coût du remplacement du matériel volé étant souvent éclipsé par les impacts plus larges sur la productivité, la conformité réglementaire et les violations de données. Pour les entreprises, chaque appareil volé ou non sécurisé augmente le risque, non seulement pour les opérations, mais aussi pour les résultats financiers. Les câbles de sécurité offrent une solution éprouvée et rentable, déjà utilisée par beaucoup pour réduire la probabilité de vol et les conséquences financières et de réputation qui en résultent. En s'attaquant à ces risques à leur source, les entreprises peuvent adopter une attitude proactive pour protéger leurs biens et leurs données confidentielles.

Bien que les mesures de sécurité physique comme les câbles de sécurité soient efficaces, elles doivent faire partie d'une stratégie plus large pour faire face aux risques de sécurité en constante évolution associés au travail hybride. Combiner les câbles de sécurité avec des protections numériques complémentaires, telles que le chiffrement et l'authentification à deux facteurs, assure une couverture complète contre les menaces physiques et numériques. Des programmes de formation pour sensibiliser les employés à l'importance de cette approche intégrée peuvent renforcer davantage la sécurité organisationnelle. Pour les entreprises confrontées aux complexités des modèles de travail modernes, l'intégration de mesures de sécurité physiques et numériques est essentielle pour minimiser les risques, protéger leur personnel et maintenir la résilience opérationnelle.

Appel à l'action

Empêcher le vol d'appareils et les violations de données qui en résultent est beaucoup plus rentable que de faire face aux conséquences. Prendre des mesures préventives, telles que l'utilisation de câbles de sécurité pour ordinateurs portable dès aujourd'hui peut protéger votre entreprise contre d'importantes conséquences financières et opérationnelles à l'avenir. Afin d'assurer l'efficacité de ces mesures, l'alignement entre les cadres supérieurs, la direction et les équipes est essentiel. Un engagement commun envers les priorités de sécurité garantit que chacun comprend son rôle dans la protection des biens précieux et la réduction des risques.



Méthodologie

Kensington a chargé Vanson Bourne, spécialiste indépendant des études de marché, de réaliser l'étude sur laquelle ce rapport est basé. Au total, 1 000 responsables informatiques seniors impliqués ou ayant une influence sur la sécurité du matériel informatique physique dans leur entreprise ont été interrogés à l'automne 2024, aux États-Unis, au Royaume-Uni, en France et en Allemagne.

Les personnes interrogées devaient être issues d'entreprises comptant 100 employés ou plus et d'un éventail de secteurs privés et publics.

Les entrevues ont été menées en ligne et un processus rigoureux de présélection à plusieurs niveaux a été utilisé afin de s'assurer que seuls les candidats appropriés aient la possibilité de participer. Sauf indication contraire, les résultats présentés sont basés sur l'échantillon total.

À propos de Kensington

Kensington est l'un des principaux fournisseurs mondiaux d'accessoires pour ordinateurs de bureau et appareils mobiles plébiscité depuis plus de 40 ans par les services informatiques, les enseignants, les entreprises et les professionnels en télétravail. Kensington s'efforce d'anticiper les besoins et défis des entreprises en évolution constante, et de développer des solutions de haute qualité récompensées, destinées aux organisations souhaitant proposer aux professionnels les plus exigeants les outils qui leur serviront à prospérer. L'entreprise est fière d'être le choix des professionnels et de ses valeurs fondamentales en matière de design, de qualité et d'assistance.

Dans les environnements de bureau et mobiles, la vaste gamme de produits primés de Kensington permet d'offrir à ses clients une sécurité, optimale, des innovations en matière de productivité au bureau, une visioconférence professionnelle et un bien-être ergonomique.

Basée à Burlingame, en Californie, Kensington est l'entreprise pionnière et un des leaders mondiaux des solutions de sécurité pour ordinateurs portables. Kensington est une filiale d'ACCO Brands, « The Home of Great Brands Built by Great People », qui conçoit, fabrique et commercialise des produits grand public et utilisateurs finaux qui permettent aux utilisateurs de travailler, d'apprendre et de jouer. En plus de Kensington®, les marques largement reconnues d'ACCO Brands sont AT-A-GLANCE®, Five Star®, Leitz®, Mead®, PowerA®, Swingline®, Tilibra et bien d'autres. Pour plus d'informations sur ACCO Brands Corporation (NYSE : ACCO), consultez le site www.accobrands.com.

FOR MORE INFORMATION CONTACT: sales@kensington.com

Kensington
The Professionals' Choice™