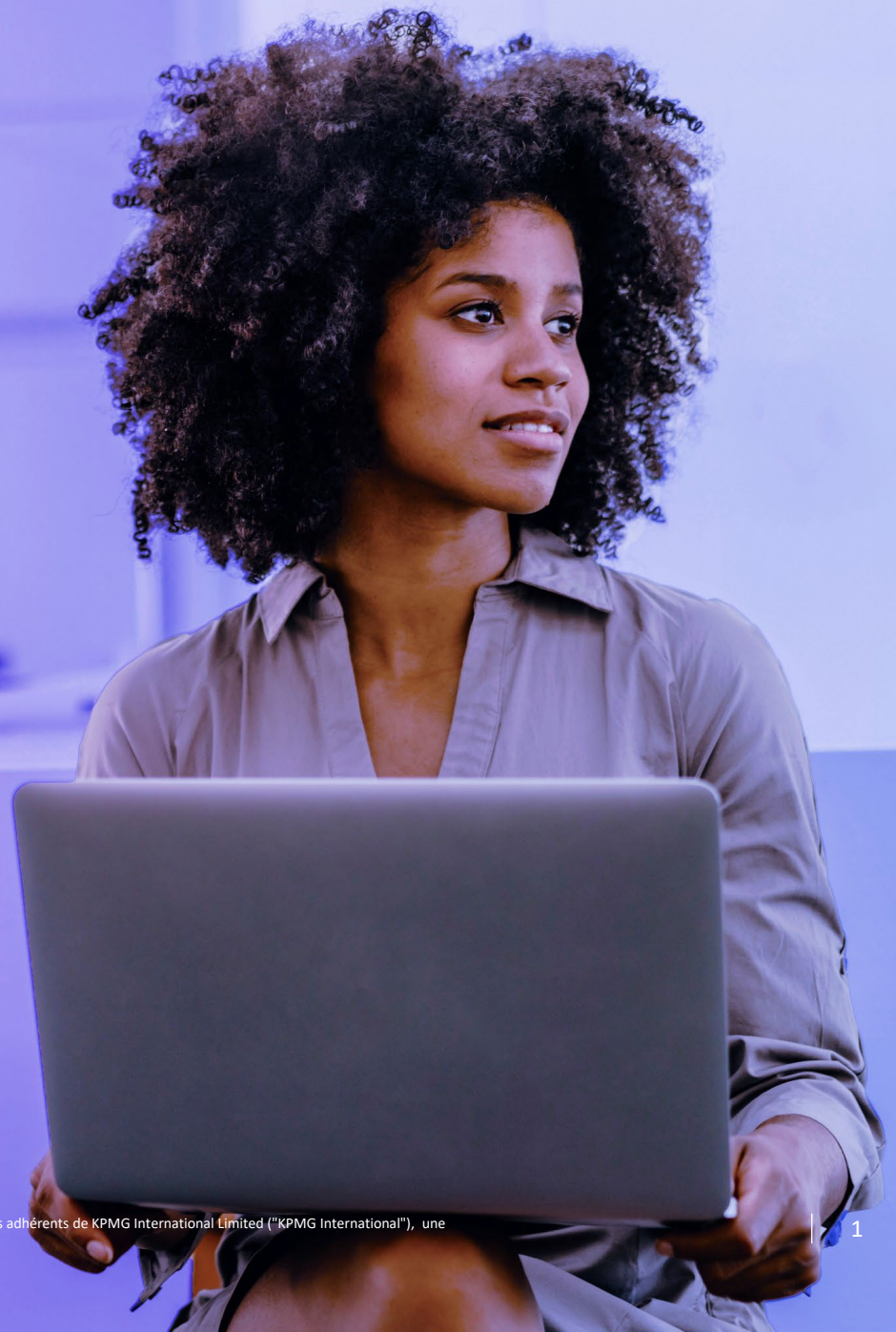
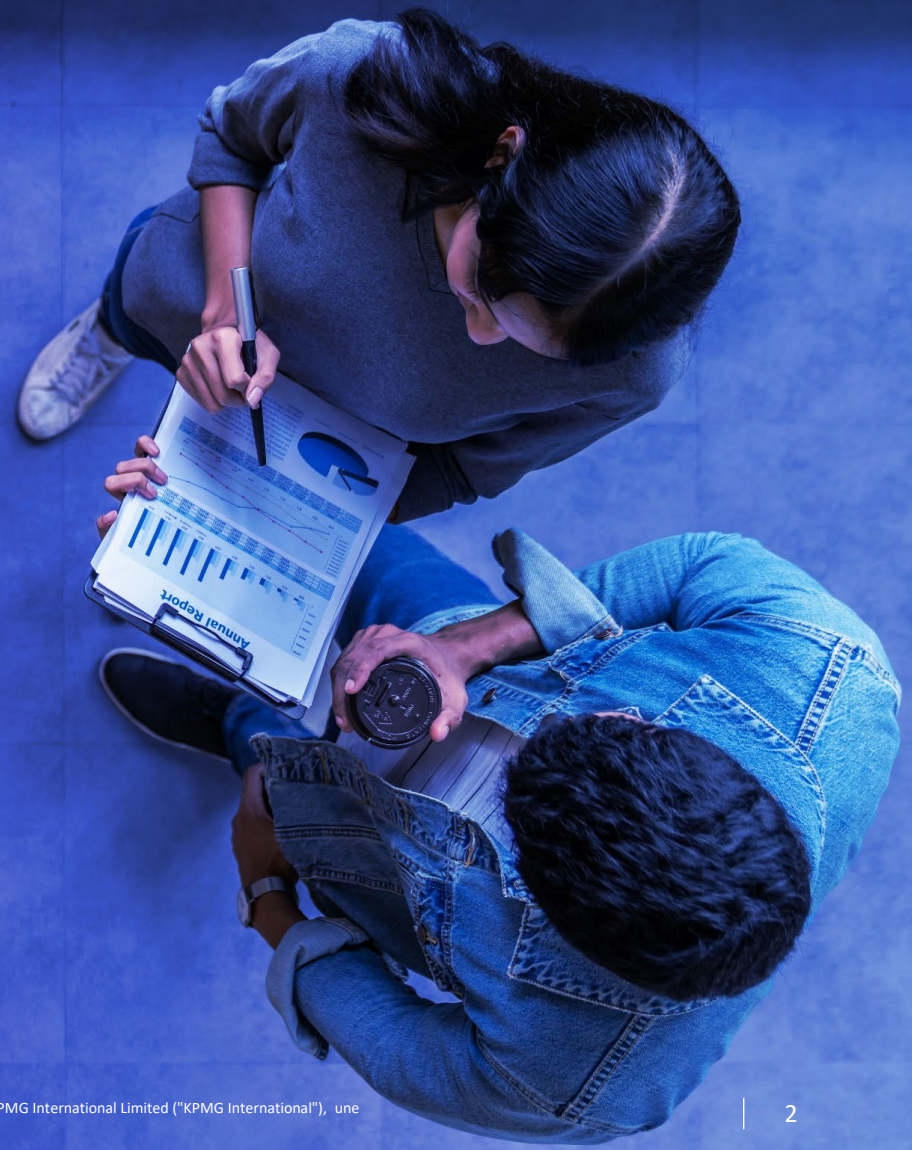
Cybersécurité des Sociétés de Gestion



Quelle place tient la Cybersécurité dans la Gestion de Portefeuille?

kpmg.mc | cyber

En bref



KPMG Monaco accompagne les entreprises monégasques sur un large éventail de sujets de management, financiers, règlementaires, et maintenant renforce sa présence locale en Cybersécurité.

Ce document s'adresse particulièrement aux sociétés de gestion de portefeuille, à leurs problématiques métier et aux défis technologiques qu'elles ont à relever.

De nombreuses sources s'accordent pour dire que les **principales menaces cyber** redoutées par les **sociétés de gestion de portefeuille** sont:

- **Exfiltration des informations clients** ou informations personnelles des clients (CID) par des employés mécontents, vengeurs ou démissionnaires,
- **Infiltration des systèmes de passage d'ordre** ou les boites mails pour passer des opérations frauduleuses par des cybercriminels,
- **Les attaques *Ransomware*** par des cybercriminels, conduisant à des fuites d'informations, des coûts de remise en état du système et parfois des pertes de sauvegardes, et pertes d'image.

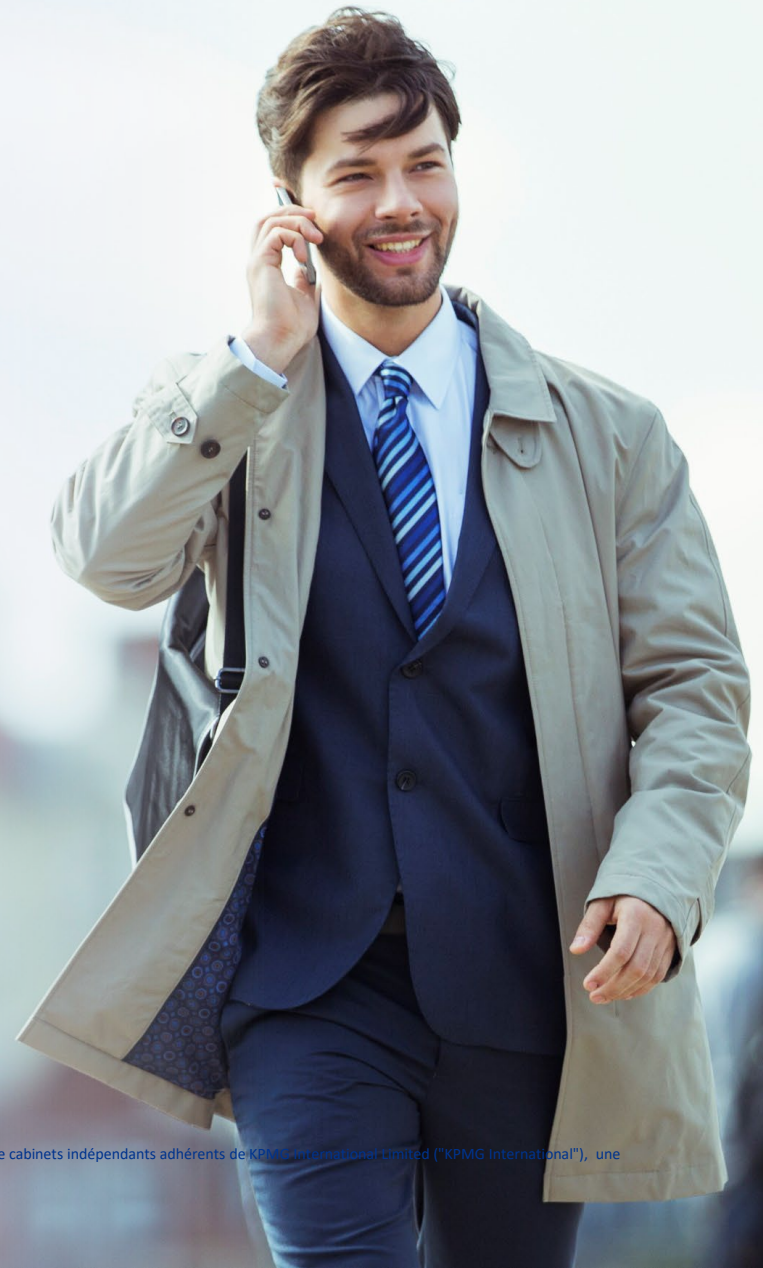
Pour faire face à ces menaces internes et externes et éviter des surcoûts de remédiation et de sanctions règlementaires, il est nécessaire d'être accompagné par des personnes qui connaissent votre métier. KPMG Monaco dispose d'experts cyber locaux pour vous apporter des réponses pertinentes grâce à nos connaissances métier et technique issues de nos diverses activités d'expertise et d'audit.

Faire évaluer la sécurité élémentaire de son système d'informations (audit sécurité généraliste ou test d'intrusion) représente bien souvent un coût inférieur à 10 000€.

Vous **retrouverez nos conseils et notre approche dans les pages suivantes**.

Pour nous contacter, écrivez à notre responsable de BU Cybersécurité à l'adresse cmaillioux@kpmg.mc.

Sommaire



Les challenges business à relever

Les sociétés de gestion de portefeuilles font face à de nombreux défis en matière de business.

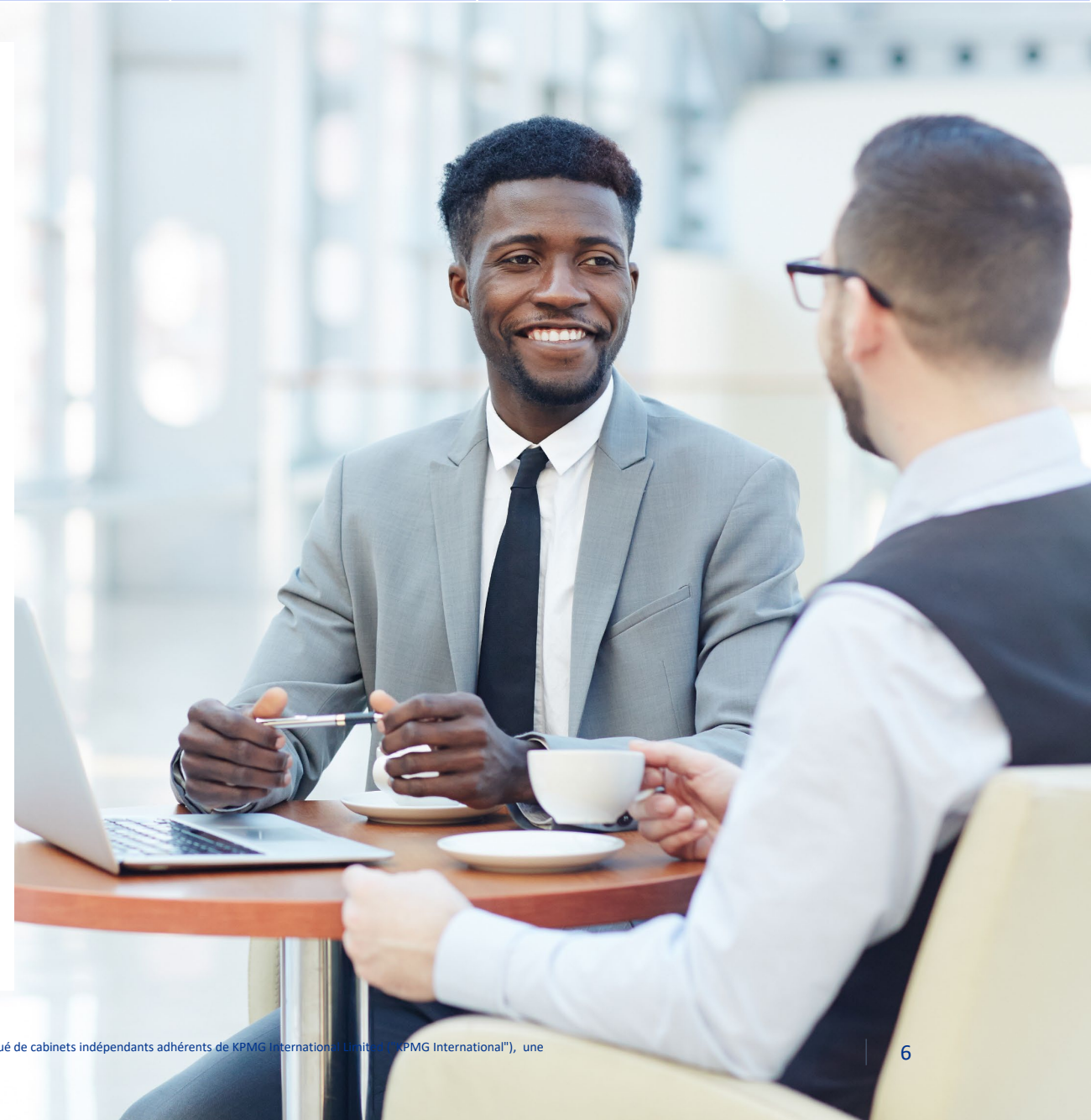
Le secteur de la gestion de portefeuilles est **hautement concurrentiel** : vous devez trouver des moyens de vous différencier et de générer des rendements optimaux pour vos clients.

L'air du temps fait que **les attentes des clients évoluent** ; ils recherchent des solutions de gestion de portefeuilles plus personnalisées, et des options d'investissement socialement plus responsables, par exemple. Dans le même temps, **la pression pour réduire les coûts tout en maintenant une qualité de service constante** est toujours présente.

Il s'ajoute à ces challenges des facteurs exogènes au commerce : **les réglementations financières sont strictes et en constante évolution**; vous devez vous conformer à des normes et des exigences réglementaires précises, notamment la gestion des risques liés aux investissements. C'est un aspect crucial pour protéger les intérêts de vos clients, mais cela nécessite des ressources importantes pour la conformité.

Dans ces conditions, l'intégration de la technologie pour l'automatisation des opérations, l'analyse des données et la gestion des investissements est devenue essentielle. Et avec elle, la sécurité des données et la protection contre les cybermenaces sont des préoccupations majeures.

En synthèse il faut rester agile, s'adapter aux changements, investir dans la technologie, proposer des services innovants à vos clients et enfin s'assurer du respect des nombreuses réglementations en maintenant la pérennité des affaires face aux nouvelles menaces informatiques.



Les risques cyber & leurs impacts

La cybersécurité devient un sujet crucial pour les sociétés de gestion de portefeuilles. Parmi les risques cyber les plus importants auxquels vous pourriez être confrontés, se trouvent notamment :

Le vol de données : Les informations sensibles des clients, telles que leurs comptes et données financières, pourraient être volées.

Les attaques de phishing : Les employés pourraient être la cible d'e-mails de phishing visant à obtenir des informations confidentielles. Dans ce cas, des cybercriminels envoient des e-mails ou des messages frauduleux qui incitent les employés à divulguer des informations sensibles, telles que des mots de passe ou des données d'identification.

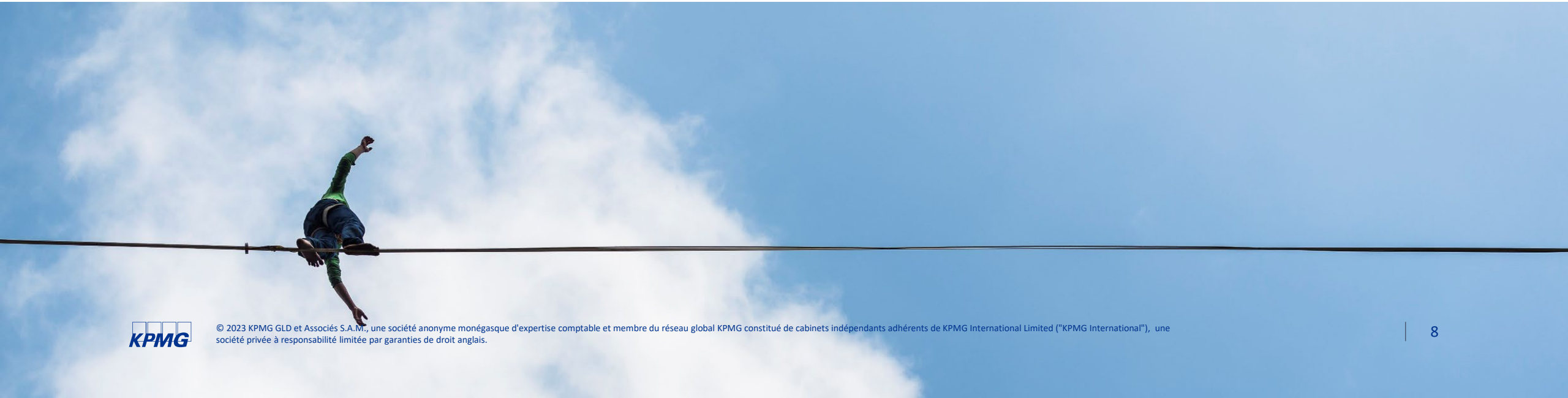
Les ransomwares : Les infections par des logiciels de rançon sont tristement célèbres ces dernières années, ce qui pourrait entraîner la perte de données ou le paiement d'une rançon. Si vous payez la rançon, il n'y a aucune garantie que vos données seront restaurées, et les criminels auront toujours accès à vos informations.

L'exploitation de vulnérabilités logicielles : Les failles de sécurité dans les logiciels que vous utilisez pourraient être exploitées par des attaquants malveillants.

Partenaires malveillants ou employés mécontents : Les employés ou les sous-traitants ayant un accès aux systèmes pourraient causer des problèmes délibérés pour vous nuire directement, ou profiter de leurs accès aux données pour les voler, les divulguer ou les vendre.

Les attaques DDoS : Les attaques par déni de service distribué pourraient perturber vos opérations en ligne, ou les liens informatiques avec votre groupe.

Pour réduire ces risques, il est important de mettre en place des contrôles de sécurité solides, de former le personnel à la cybersécurité, de surveiller de près les activités suspectes et de disposer de politiques de sécurité strictes pour protéger vos données. Une veille constante est essentielle pour détecter les menaces potentielles à un stade précoce.



Certaines sociétés de gestion ont publiquement communiqué sur des incidents qu'elles ont subis, et notamment :

Azimut Group (2023) : La société a communiqué publiquement avoir reçu une demande de rançon d'un groupe cybercriminel, et ne coopérer sous aucun prétexte. L'établissement n'a heureusement pas souffert de compromission des positions des clients ni des conseillers, aucun ordre frauduleux n'a été passé, ni aucun problème de continuité d'activité relevé.

BlackRock (2020) : BlackRock, l'une des plus grandes sociétés de gestion d'actifs au monde, a subi une violation de données en 2020. L'origine de l'incident est une erreur humaine ayant entraîné l'envoi de données à de mauvais destinataires, et non un problème de sécurité.

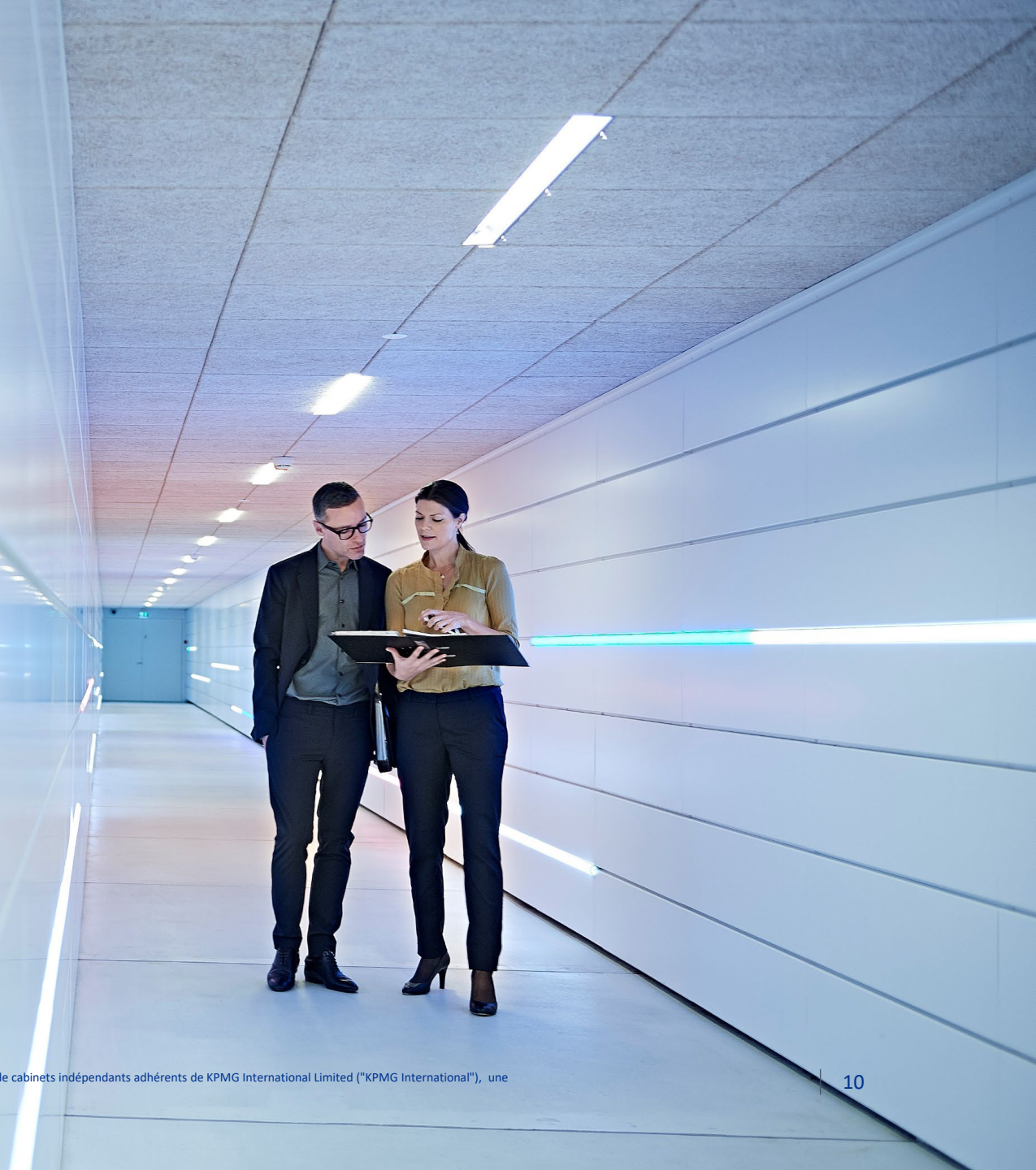
JP Morgan (2014) : JP Morgan aurait subi une attaque concentrée sur des serveurs hébergeant des informations sensibles de clients ayant accédé aux sites chase.com ou jpmorgan.com. Les données dérobées semblent être des données de contact (nom, email, etc.) mais pas de données sensibles (n° de comptes, mots de passe, par exemple).

ETRADE Financial (2013) : ETRADE a été confronté à une cyberattaque en 2013 qui a compromis les données personnelles de certains de ses clients (nom, email, etc.), les données sensibles ne semblant pas concernées.

Ainsi, les sociétés de gestion de portefeuilles ne sont pas épargnées par les cybermenaces. Elles doivent alors réagir pour restaurer leur réputation et **investissent alors massivement dans la sécurité après l'incident**, en plus de **risquer des amendes** liées aux fuites de données, et **au coût de remédiation de l'attaque**.

De façon proactive, rester vigilants et **investir pour prévenir de tels incidents et protéger les données des clients comme la réputation de l'entreprise** est primordial.

Prévenir le risque Cyber



Pour protéger votre société des risques cyber, les experts recommandent entre autres de mettre en œuvre les actions élémentaires suivantes :

Formation et sensibilisation à la cybersécurité : Offrez une formation régulière à vos employés pour les sensibiliser aux menaces cyber et les aider à reconnaître les attaques de phishing ou d'autres tentatives de vol de données.

Mise à jour des logiciels et correctifs : Assurez-vous que tous les logiciels et systèmes utilisés dans votre entreprise sont régulièrement mis à jour avec les derniers correctifs de sécurité pour réduire les vulnérabilités techniques exploitables.

Pare-feu et antivirus : Installez des pares-feux et des logiciels antivirus de qualité pour protéger votre réseau contre les attaques et les logiciels malveillants.

Gestion des accès : Mettez en place des contrôles d'accès stricts pour garantir que seules les personnes autorisées ont accès aux données dont elles ont besoin.

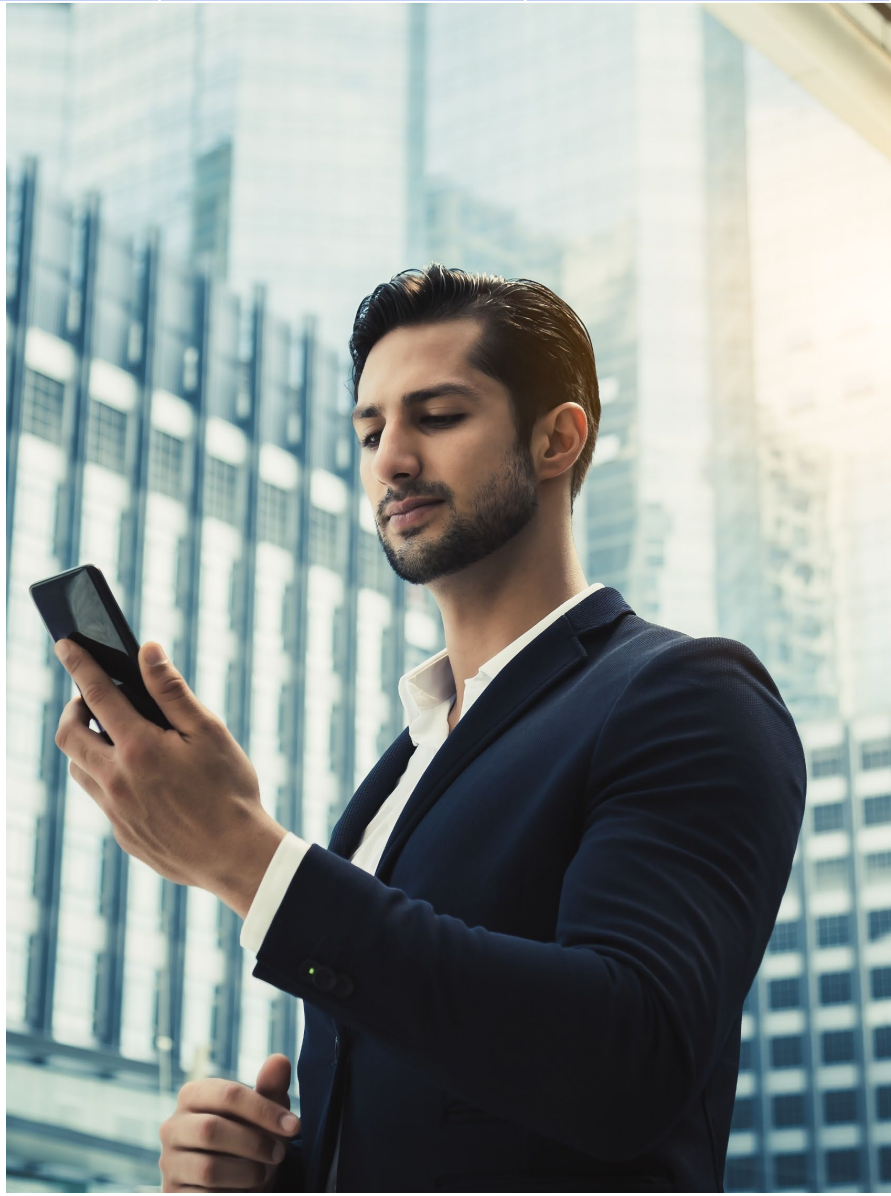
Plan de réponse aux incidents et gestion de crise : Élaborez un plan de réponse aux incidents pour savoir comment réagir en cas de violation de données, y compris pour la notification aux autorités compétentes et aux clients si nécessaire. Entraînez-vous à gérer la crise cyber.

Sauvegarde des données : Effectuez des sauvegardes régulières de toutes vos données critiques et assurez-vous qu'elles sont stockées en toute sécurité.

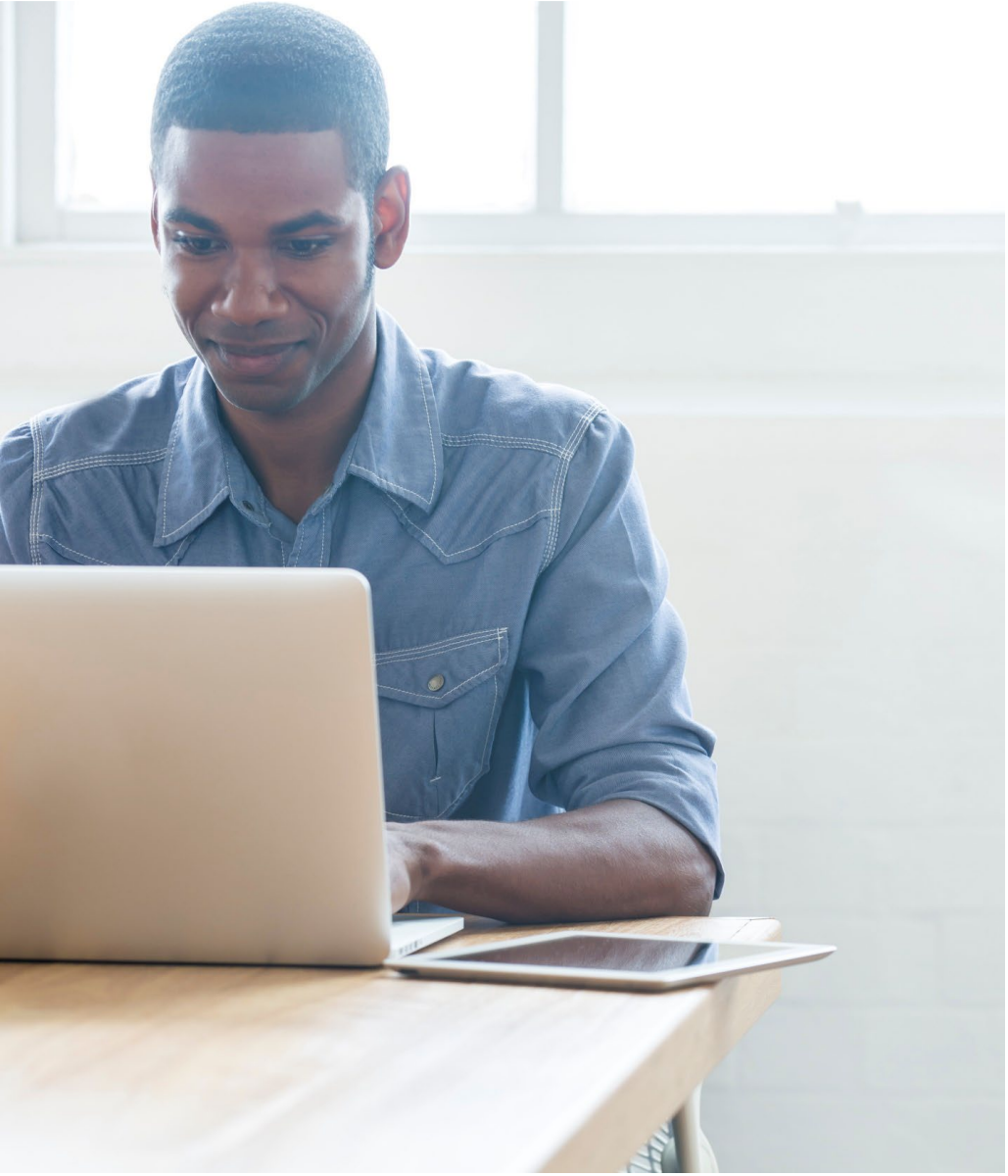
Chiffrement des données : Utilisez le chiffrement pour protéger les données sensibles, en particulier lorsqu'elles sont en transit (email, plateformes de transfert).

Évaluation et gestion de fournisseurs tiers : Si vous travaillez étroitement avec des fournisseurs ou partenaires, assurez-vous qu'ils respectent des normes de sécurité élevées. Ils peuvent être victimes d'incidents, impact alors vos données dans leurs systèmes.

Évaluations régulières de la sécurité informatique : KPMG dispose d'experts pour évaluer la cybersécurité de votre organisation. Nous pouvons identifier les vulnérabilités et les points faibles spécifiques à votre entreprise par des audits ou des tests d'intrusion, et proposer des recommandations adaptées. Il est important de travailler avec des experts en cybersécurité de confiance pour personnaliser votre approche en fonction des besoins spécifiques de votre entreprise, de vos impératifs business et des réglementations en vigueur.



Choisir KPMG Monaco



KPMG Monaco dispose d'une équipe cyber locale constituée de personnes passionnées, certifiée et disposant de l'expertise pour répondre à vos besoins.

Notre équipe locale nous permet de vous fournir la proximité et la connaissance des règlementations monégasques pour vous servir au mieux. Elles peuvent aussi s'appuyer sur le réseau KPMG international pour répondre à des problèmes d'expertise pointue ou sur des sujets internationaux. Voici un exemple de mission réalisée dans le secteur :

Société de gestion monégasque

Test d'intrusion interne

Nos experts ont mené des attaques sur le réseau interne (LAN) de la société à l'aide d'un ordinateur comportant les limitations associées à un profil stagiaire.

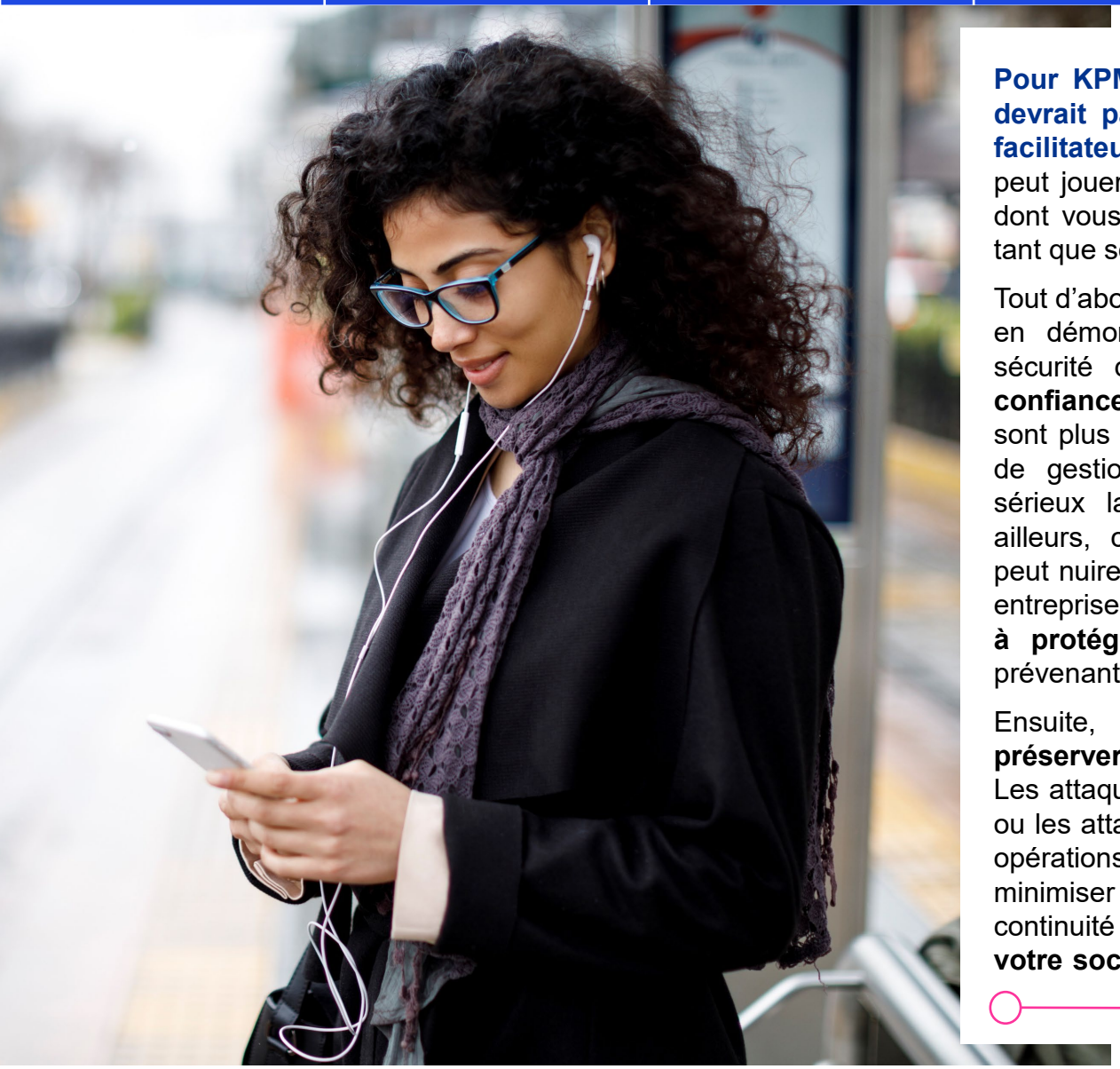
Ainsi les travaux ont permis de renforcer la confidentialité des données des clients en améliorant la sécurité des postes de travail et des services réseaux mais aussi en limitant certains droits des utilisateurs. L'investissement IT sera dirigé vers un gain réel de sécurité, notamment pour le choix d'un anti-virus plus performant et l'application de configurations durcies pour les utilisateurs du système d'informations.

Nous avons discuté les recommandations avec notre client lors d'une réunion de restitution pour **proposer des solutions adaptées à son contexte.** L'application de nos recommandations apportera comme **bénéfices directs** une **protection accrue** vis-à-vis de **menaces** comme les **ransomwares**, le déni de service, les impacts généralisés d'une **attaque par phishing** réussie et **l'exploitation de vulnérabilités techniques** par des personnes malveillantes.

Cela permet aussi à notre client de **communiquer sur le sérieux qu'il accorde à la protection des données de ses clients**, **d'éviter des accusations de négligences** de la part de régulateurs comme la CCIN en cas de de violation de données, et d'**investir judicieusement dans sa sécurité informatique**.

Nous disposons d'une palette d'autres services dédiés au secteur financier comme **l'évaluation de votre maturité cyber**, l'évaluation de **votre préparation aux ransomwares** ou **le conseil sur les bonnes pratiques et la simulation de gestion de crise cyber** pour vous aider à préparer votre société à ces incidents.

Cybersécurité & Business



Pour KPMG Monaco, la cybersécurité ne devrait pas être une contrainte, mais un facilitateur de business. La cybersécurité peut jouer un rôle essentiel dans la manière dont vous relevez les défis commerciaux en tant que société de gestion.

Tout d'abord, sur le plan de la communication, en démontrant un engagement envers la sécurité des données **vous renforcez la confiance de vos clients**. Les investisseurs sont plus susceptibles de choisir une société de gestion de portefeuilles qui prend au sérieux la protection de leurs actifs. Par ailleurs, comme une violation de données peut nuire gravement à la réputation de votre entreprise, **la cybersécurité peut vous aider à protéger votre image de marque** en prévenant les fuites de données.

Ensuite, la cybersécurité vous aide à **préserver votre efficacité opérationnelle**. Les attaques cyber, comme les ransomwares ou les attaques DDoS, peuvent perturber vos opérations. Une cybersécurité robuste peut minimiser ces perturbations et maintenir la continuité de vos services. **Vous préserverez votre société de coûts additionnels** en cas d'incidents, liés à la remédiation des incidents, à la perte de réputation, et aux investissements qui n'auront pas été planifiés pour renforcer la sécurité les années suivantes.

Pour aller plus loin, **de nouvelles opportunités d'usage peuvent être ouvertes à vos clients** grâce aux nouvelles technologies, et ces solutions sont de plus en plus axées sur la cybersécurité pour protéger les transactions financières et les données des clients dans ce nouveau contexte. **Les services innovants doivent être sécurisés pour emporter l'adhésion des clients**, et permettre aux entreprises de se différentier.

Nous pensons que la cybersécurité peut être un atout commercial en créant de nouvelles sources de revenus, en renforçant votre image de marque et en vous permettant de tirer parti de la croissance continue du secteur de la cybersécurité. Cela peut vous aider à diversifier vos activités et à rester compétitif sur le marché de la gestion de portefeuilles.

Contacts

KPMG GLD et Associés S.A.M.
Athos Palace
2, rue de la Lüjerneta
98000 Monaco

www.kpmg.mc

Sabina Debussy
Partner
Head of Advisory

sdebussy@kpmg.mc

Clément Maillioux
Senior Manager
Advisory IT | Cyber

cmaillioux@kpmg.mc