ccs insight

SAMSUNG

Mobilité et sécurité

How to do bigger things in business*

Le RGPD et l'évolution de la sécurité –
de nouvelles opportunités en matière de mobilité et de productivité

Avril 2018

*Comment faire les choses en grand pour vos projets.

Auteur : Nicholas McQuire
Vice-président, Enterprise Research

Nick a plus de 15 ans d'expérience en conseil technologique à destination des entreprises, notamment en tant que directeur général de la Global Enterprise Mobility Alliance (GEMA). Il a également été vice-président de l'IDC, où il était chargé de la division Stratégies de mobilité des entreprises à Londres. Nick dirige notre activité de recherche dédiée aux entreprises, axée sur l'espace de travail digital, la mobilité, la sécurité, l'intelligence artificielle et le cloud computing. Régulièrement cité par la BBC, CNBC et Reuters, il intervient dans de nombreux événements tels qu'InfoSecurity Europe, AI Tech World, le Mobile World Congress, le Cloud and DevOps World Forum et bien d'autres.

@nickmcquire

« Nous devons arrêter de croire que le RGPD est une contrainte et commencer à le voir comme une opportunité. »
Le PDG d'une grande entreprise française

Résumé analytique

À partir d'une analyse des nouvelles menaces et des principaux changements réglementaires, nous avons établi une série de recommandations à l'intention des DSI, directeurs des opérations, responsables informatiques et cadres dirigeants sur les sujets de la sécurité, de la mobilité et de la productivité.

- Les entreprises doivent voir le Règlement Général sur la Protection des Données (RGPD) comme une opportunité de faire évoluer leurs processus informatiques, d'investir et d'améliorer leurs mesures de sécurité.
- Les dernières fuites de données très médiatisées prouvent qu'investir dans des appareils mobiles récents est le moyen le plus simple de se protéger contre ces menaces.
- Il est important, tout en répondant à ce besoin de sécurité, de trouver une solution qui ne nuit pas à la productivité des employés.
- Investir dans ses employés est peut-être la meilleure dépense qu'une entreprise puisse faire en matière de sécurité.
- L'entreprise doit à la fois équiper ses employés avec un matériel mobile efficace et les sensibiliser aux risques sur la gestion des données personnelles de leurs clients.
- Remplacer les technologies obsolètes réduit les risques, augmente la satisfaction des employés et améliore l'image de l'entreprise auprès de ses clients.
- Avec l'arrivée du RGPD, une sécurité mobile moderne permet aux entreprises d'être plus agiles et plus sûres, ce qui en retour améliore la satisfaction et la fidélité de ses clients.

Avec l'arrivée du RGPD, une sécurité mobile moderne permet aux entreprises d'être plus agiles et plus sûres, ce qui en retour améliore la satisfaction et la fidélité de ses clients.

Introduction

Ce rapport est le deuxième d'une série en trois parties intitulée « How to do bigger things in business » qui explore l'impact des technologies mobiles sur les performances des entreprises.

Nos recherches pour le premier rapport « Big+Small* » nous ont permis de conclure que la réussite future des grands groupes et des petites startups allait dépendre de leur faculté à comprendre et à apprendre les uns des autres tout en surmontant leurs différences.

Ce rapport « Mobilité et sécurité » passe en revue les principales questions de sécurité liées à la mobilité professionnelle.

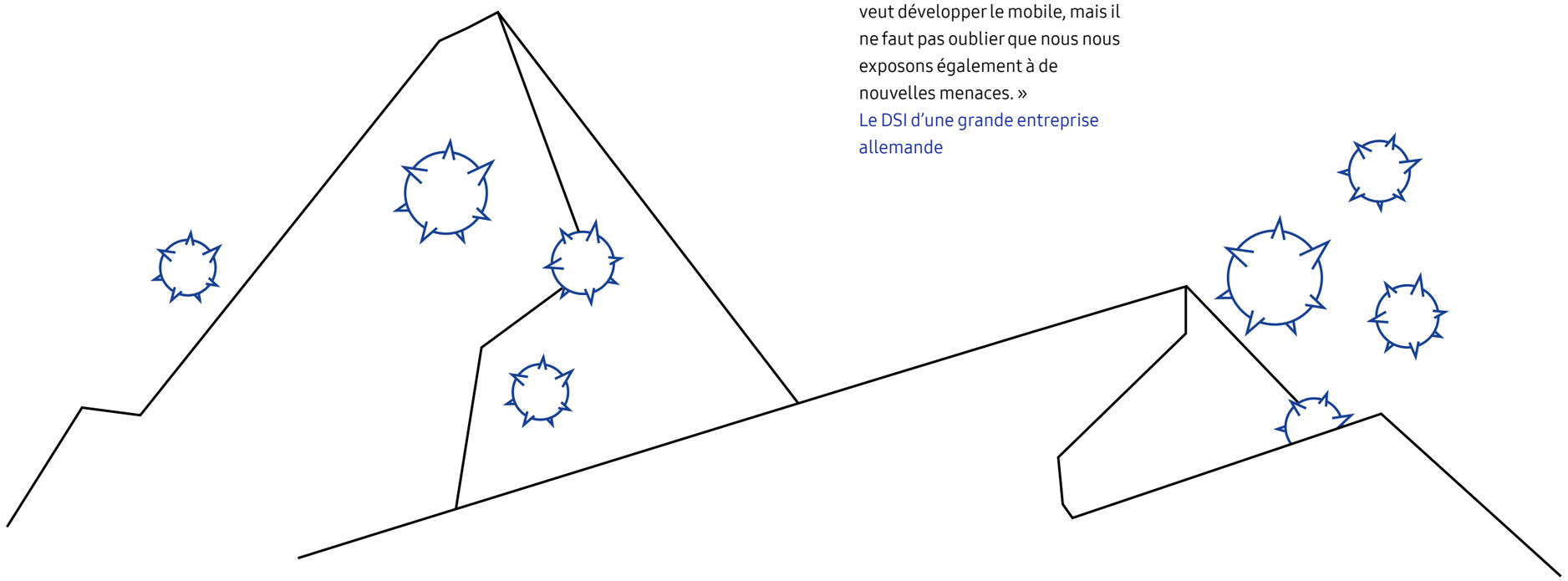
Il a pour but de présenter des conseils pratiques à l'intention des DSI, responsables informatiques et décideurs dans un contexte marqué par les cyberattaques et la nécessité de se conformer au Règlement Général sur la Protection des Données (RGPD).

Les résultats et les citations présents dans ce rapport proviennent d'une étude réalisée en 2017 auprès de grandes entreprises et de startups.

Les participants étaient des décideurs expérimentés travaillant dans des entreprises de toute taille dans divers secteurs, basées en France, en Allemagne, en Italie, en Espagne et au Royaume-Uni.

Afin de formuler des recommandations pratiques, nous avons concentré notre analyse sur trois domaines:

*Grandes + Petites entreprises



« Je m'inquiète du nombre d'appareils mobiles que nous avons. De nos jours, tout le monde veut développer le mobile, mais il ne faut pas oublier que nous nous exposons également à de nouvelles menaces. »
Le DSI d'une grande entreprise allemande

01

L'arrivée de nouvelles menaces

La sécurité est la principale priorité des décideurs informatiques en 2018.

Les décideurs chargés d'implémenter de nouvelles solutions technologiques sont davantage sous pression pour justifier l'efficacité de leurs choix contre la prolifération des cybermenaces.

Dans ce chapitre, nous présentons plusieurs menaces externes qui ont transformé le domaine de la sécurité au cours des dernières années.

On y retrouve la complexification des cyberattaques (malwares, ransomwares et tentatives de phishing), l'augmentation des coûts liés aux violations de données et l'impact des nouvelles réglementations.

Entre 4 et

14%

des failles de sécurité et des incidents sont causés par la perte ou le vol d'un appareil professionnel.

(Violation des données. Enquête Verizon, 2017)

Les cyberattaques font les gros titres

Les grands médias parlent de plus en plus des violations de données, soulignant leur impact pour les entreprises qui en sont victimes.

Après les attaques des ransomwares WannaCry et NotPetya en 2017, la cybersécurité s'est imposée comme l'une des principales menaces auxquelles font face les entreprises.

L'année 2018 a vu l'apparition de deux nouvelles failles affectant presque tous les processeurs fabriqués ces 20 dernières années.

Surnommés Spectre et Meltdown, ces défauts de fabrication ont permis aux cybercriminels de récupérer des données, dont des mots de passe et des informations de cartes bancaires, auparavant réputées sécurisées.

Des chercheurs spécialisés dans la sécurité ont découvert ces failles mi-2017, mais celles-ci n'ont pas été portées à l'attention du public avant janvier 2018.

Depuis, Apple, Google, Intel, Microsoft et d'autres fabricants et développeurs majeurs ont publié de nombreux patchs. Et de nouvelles mises à jour devraient suivre dans les mois à venir.

Pour se protéger contre ces risques, les entreprises devront appliquer ces correctifs de sécurité en effectuant des mises à jour fréquentes, aussi bien au niveau logiciel que matériel.

1/3

Un tiers des managers senior ont admis que des appareils mobiles de leur société ont déjà été piratés ou compromis.

(Se conformer au RGPD dans un environnement 100% mobile, Lookout, 2017)

86%

Aux États-Unis et en Europe de l'Ouest, 86 % des employés utilisent régulièrement des applications mobiles pour le travail, avec 4,2 applications par employé en moyenne.

(Employee Mobile Technology Survey, CCS Insight, 2016)

La prolifération des malwares, des ransomwares et des tentatives de phishing

Les appareils mobiles sont de plus en plus vulnérables aux malwares, notamment en raison de la démocratisation des applications professionnelles basées dans le cloud telles que Microsoft Office 365, WhatsApp et LinkedIn.

Des utilisateurs peu scrupuleux misent sur le manque de connaissances des utilisateurs qui téléchargent ces applications.

Les applications malveillantes imitent des applications célèbres pour inciter l'utilisateur à les télécharger, causant ainsi des dégâts aux appareils, aux entreprises ou aux deux.

Les applications qui envoient des SMS payants ou espionnent les actions des utilisateurs sont particulièrement dangereuses.

Même si leur nombre reste relativement restreint, il suffit qu'un seul employé installe une application malveillante pour que les données de l'entreprise tombent entre de mauvaises mains.

Des règles strictes doivent être mises en place afin d'éviter l'installation d'applications non autorisées sur des appareils professionnels.

Malgré les efforts déployés par Apple et Google, respectivement sur l'App Store et Google Play, certaines attaques passent entre les mailles du filet, comme lors de la récente fuite de données personnelles ayant touché l'Agence des transports suédoise. Des bases de données du gouvernement et de la police ont été touchées.

Les hackers sont de plus en plus ingénieux pour arriver à leurs fins, ciblant les individus par le biais de tactiques d'ingénierie sociale pour donner plus de crédibilité à leurs e-mails.

Un bon exemple concerne le PDG de Barclays, Jes Staley, qui a admis en 2017 s'être fait berner par un e-mail frauduleux relativement basique.

L'escalade des coûts

Selon une estimation du Forum économique mondial, la cybercriminalité coûte actuellement 445 milliards de dollars à l'économie mondiale chaque année.

Le groupe danois Maersk, spécialisé dans le transport et la logistique, a annoncé dans son rapport financier du deuxième trimestre publié en août 2017 que l'attaque NotPetya lui avait coûté à elle seule entre 200 et 300 millions de dollars.

Outre le coût financier lié à ces attaques, les failles de sécurité peuvent nuire considérablement à la réputation des entreprises et des personnes.

Et comme nous allons le voir, le RGPD peut vous exposer à des dépenses supplémentaires.

En cas de violation sérieuse de données, les amendes peuvent s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel de l'entreprise, la valeur la plus importante étant retenue.

Évolution de la législation

Avec l'entrée en vigueur du Règlement Général sur la Protection des Données, les 12 mois à venir s'annoncent décisifs pour les entreprises européennes.

Selon ses auteurs, la rédaction du nouveau règlement a notamment été motivée par l'augmentation du nombre d'appareils mobiles présents sur le marché.

Le RGPD stipule que le vol ou la perte de données personnelles doivent être signalés dans les 72 heures suivant la découverte.

Par conséquent, les entreprises doivent absolument savoir où et comment ces données client sont créées, transmises et stockées.

En théorie, les attaques de grande ampleur devraient pouvoir être évitées plus facilement à mesure que les entreprises investissent pour améliorer leur sécurité et le contrôle de leurs données pour se conformer au RGPD.

445 Mrd $

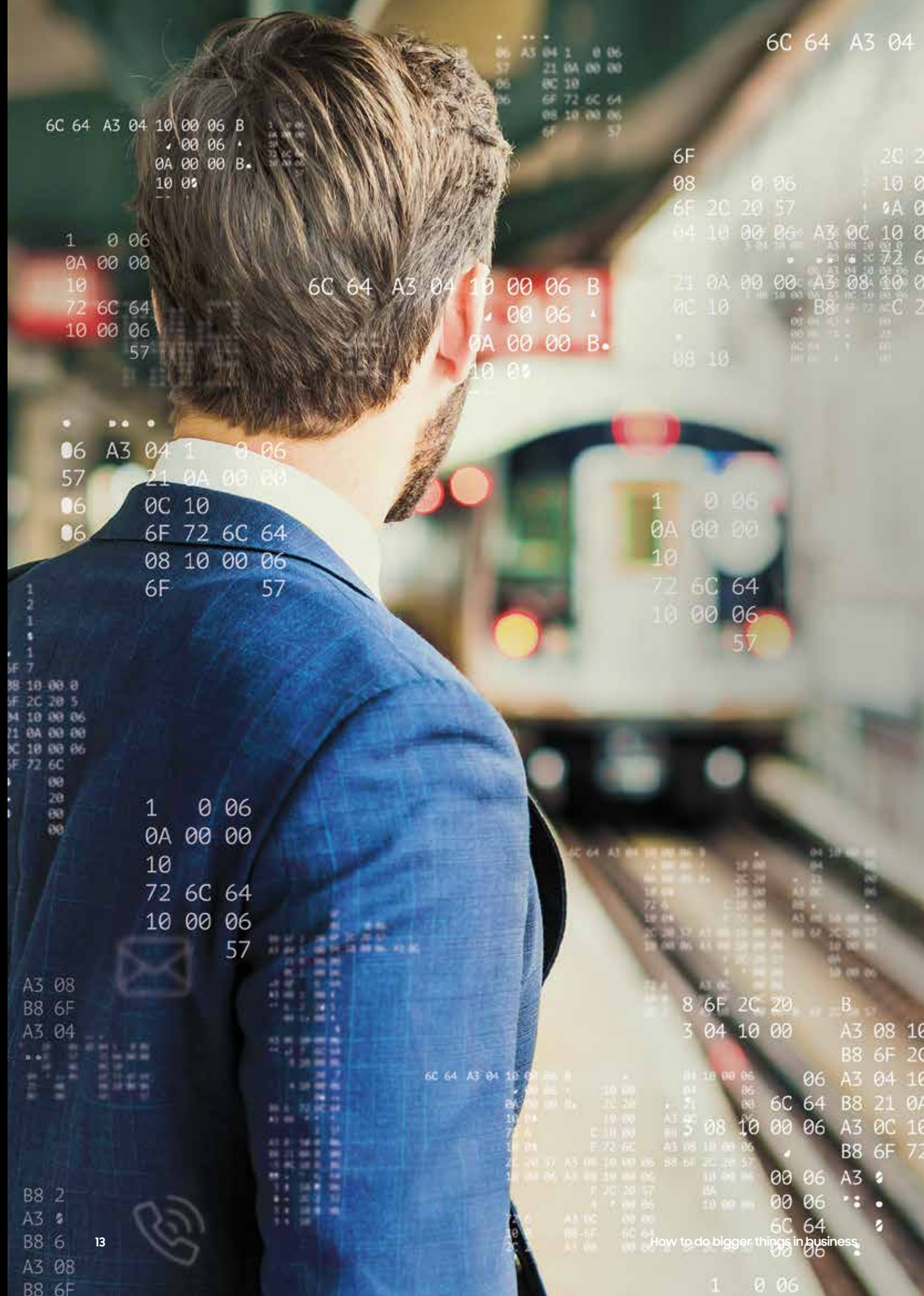
La cybercriminalité coûte chaque année 445 milliards de dollars à l'économie mondiale

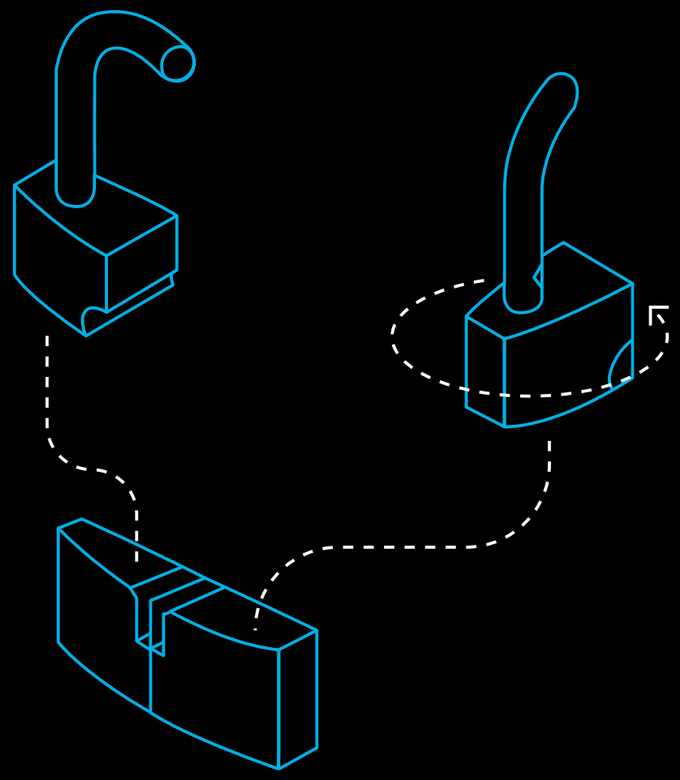
(Forum économique mondial)

72 %

des entreprises vont augmenter leurs dépenses de cybersécurité dans les deux prochaines années

(CCS Insight, 2017)





02

Les défis sécuritaires des entreprises

Les menaces externes s’appuient sur divers défis sécuritaires internes.

Dans ce chapitre, nous vous présentons les problématiques critiques auxquelles les entreprises sont le plus souvent confrontées lors du déploiement de solutions de sécurité.

On retrouve parmi ces défis l’obsolescence technologique, les appareils non gérés et la diminution de la productivité.

L’obsolescence des technologies

Beaucoup d’entreprises disposent d’une infrastructure informatique, de systèmes back-end et de processus vieillissants qui constituent des obstacles considérables à l’innovation.

C’est d’autant plus évident lorsqu’on s’intéresse aux appareils des entreprises.

Selon une estimation de CCS Insight, plus de 300 millions d’ordinateurs utilisés par les entreprises dans le monde entier ont plus de quatre ans.

Les appareils et les systèmes les plus anciens sont généralement les plus vulnérables aux cyberattaques, comme l’ont démontré les attaques NotPetya et WannaCry en 2017.

+ de 300 M

Plus de 300 millions d’ordinateurs utilisés par les entreprises ont plus de quatre ans.

(Estimation CCS Insight)

Seules

54 %

des entreprises s'appuient sur une quelconque forme de gestion des appareils mobiles.

45 %

des entreprises n'ont aucune politique officielle en matière de sécurité des données client.

(CCS Insight)

Les appareils non gérés

Peut-être pour essayer de répondre au vieillissement de leurs technologies, de nombreuses entreprises ont multiplié ces dernières années le nombre d'appareils et d'applications qu'elles utilisent, 70 % d'entre elles prévoyant de poursuivre leurs investissements au cours des deux prochaines années.

Les employés ont tendance à ne pas faire de distinction entre leur téléphone professionnel et leur téléphone personnel : pour rester en contact avec des amis, prendre des photos, faire des achats et gérer leur compte bancaire, mais également pour accéder aux systèmes de l'entreprise lorsqu'ils sont en déplacement.

Plus les employés utilisent leurs appareils personnels, plus le risque est grand qu'ils y stockent des informations sensibles de l'entreprise.

Mais CCS Insight a découvert que seulement 54 % des appareils professionnels sont administrés.

Dans ce contexte, la gestion implique une protection contre les menaces de sécurité et l'application de politiques d'entreprise relatives aux données.

Notre enquête montre également que de nombreuses entreprises peinent à utiliser les fonctionnalités les plus basiques en matière de sécurité, telles que l'application d'un mot de passe ou le chiffrage de l'appareil.

Ces entreprises prennent donc le risque que des données sensibles ou des informations personnelles concernant leurs clients ou leurs employés tombent entre de mauvaises mains.

Cette réalité pose d'importantes questions à l'aune du RGPD.

Un même appareil contient souvent des données personnelles et professionnelles.

En théorie ce n'est pas un problème. Mais l'accès par un membre de l'équipe informatique à des informations personnelles lors d'une opération sur l'appareil professionnel constitue sous le RGPD une violation de la vie privée.

Pour de nombreuses entreprises, les employés constituent l'obstacle principal à la conformité au RGPD.

Quelles que soient les précautions mises en place, les gens continueront à perdre leur téléphone, et les employés continueront à se connecter involontairement à des points d'accès Wi-Fi non sécurisés ou à télécharger des applications ou du contenu non vérifiés.

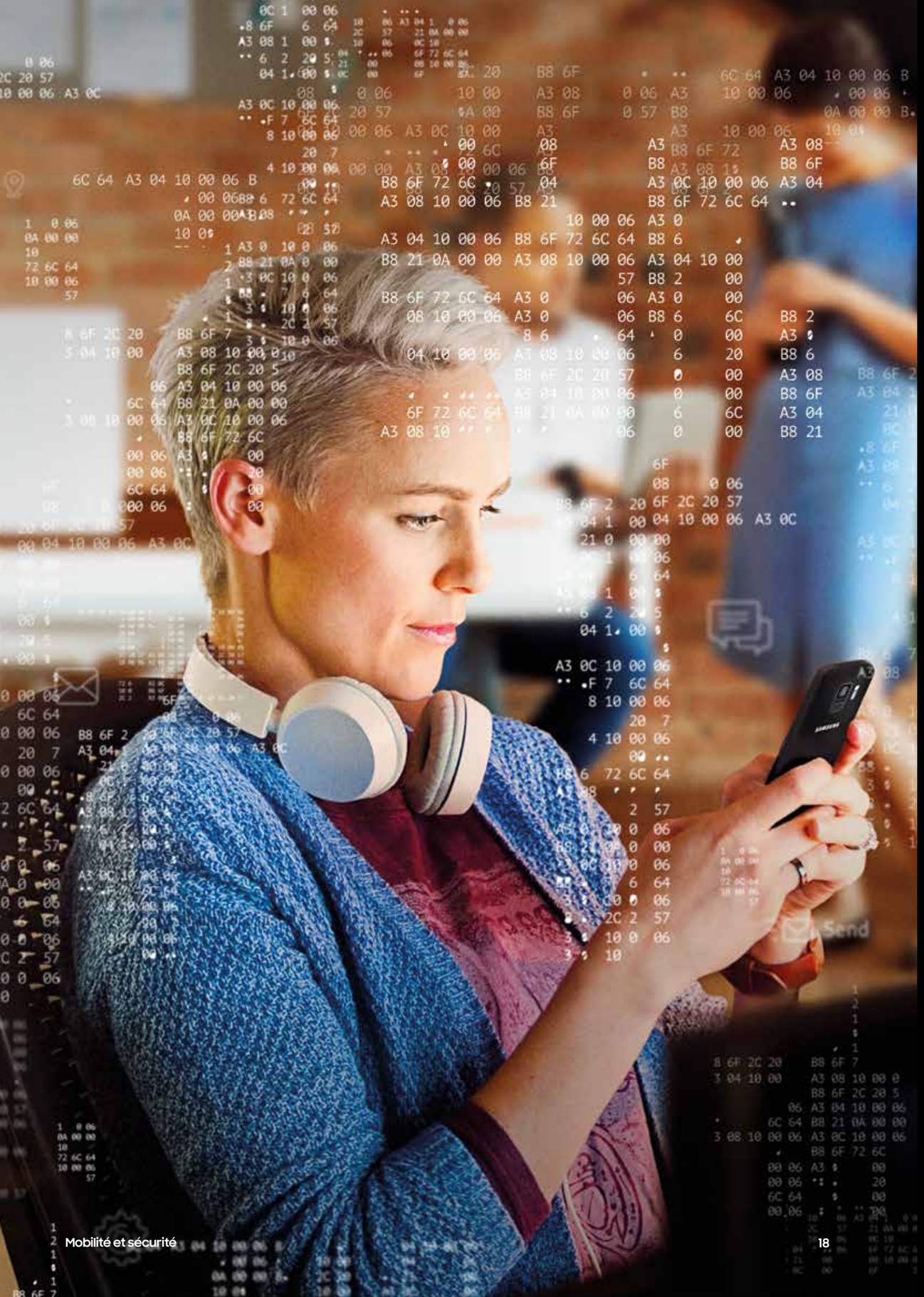
Diminution de la productivité

Pour de nombreuses entreprises, en particulier les grands groupes, l'un des principaux défis en matière de sécurité informatique est de trouver le bon équilibre entre la protection des données d'entreprise et le niveau de productivité des employés lorsqu'ils sont en déplacement.

Des compromis sont inévitables lorsque l'on veut protéger les données d'entreprise sans impacter trop négativement la productivité des employés.

Les entreprises doivent également tenir compte des questions liées au respect de la vie privée lorsqu'elles avancent sur le sujet de la sécurité mobile, en particulier lorsque des appareils personnels sont impliqués.

En 2017, 63 % des participants à l'étude Technologie et Mobilité avaient déclaré qu'ils seraient inquiets pour le respect de leur vie privée si leur employeur leur demandait d'installer un logiciel de sécurité sur un appareil personnel utilisé dans un cadre professionnel.



11 %

des entreprises n'imposent pas de mot de passe.

25 %

ne chiffrent pas les données sur leurs appareils.

42 %

des entreprises ont déclaré le vol ou la perte d'au moins un appareil au cours d'un trimestre.

(CCS Insight)

45 %

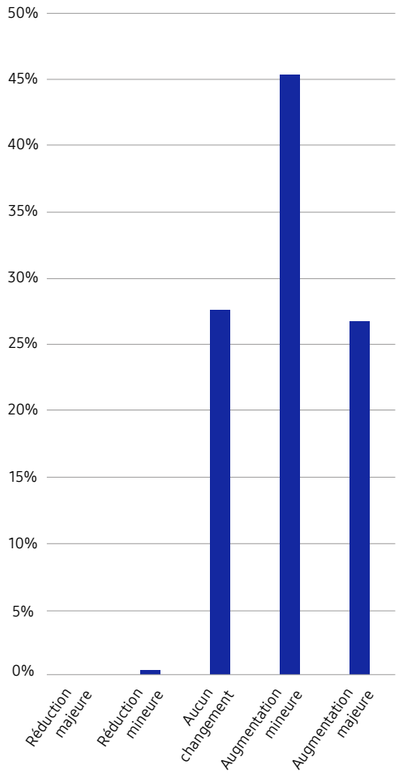
des entreprises pensent qu'elles seront touchées par une cyberattaque au cours des deux prochaines années.

(CCS Insight, 2017)

03 Résoudre les défis en matière de sécurité

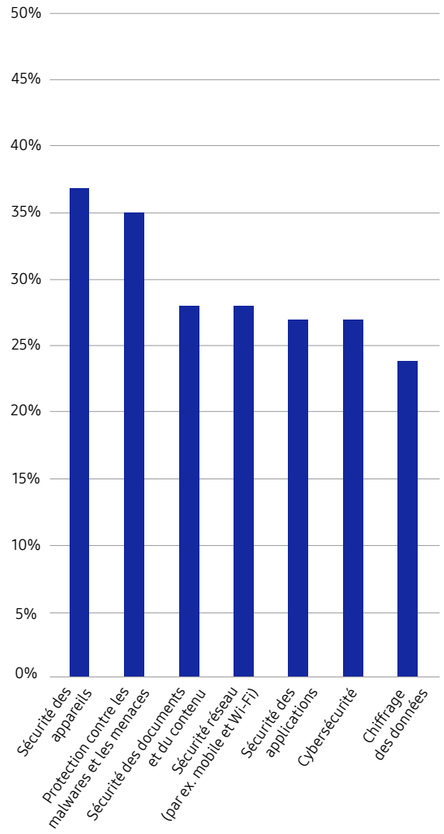
Les DSI cherchent de nouvelles approches pour répondre aux nouvelles menaces, tant internes qu'externes. Nous prévoyons trois tendances majeures en matière de sécurité au cours des 24 prochains mois. Nous les présentons dans ce chapitre : augmentation des investissements liés à la sécurité, exploration de nouvelles technologies et formation au traitement des données pour les employés.

La plupart des entreprises vont augmenter leurs dépenses en cybersécurité.



Dans quelle mesure vos dépenses en cybersécurité ont-elles évolué au cours des deux dernières années ?

Lorsque nous avons interrogé des décideurs informatiques sur leurs priorités en matière de sécurité mobile, ils ont notamment cité la sécurité des appareils et les malwares.



Investissements prioritaires en matière de sécurité mobile

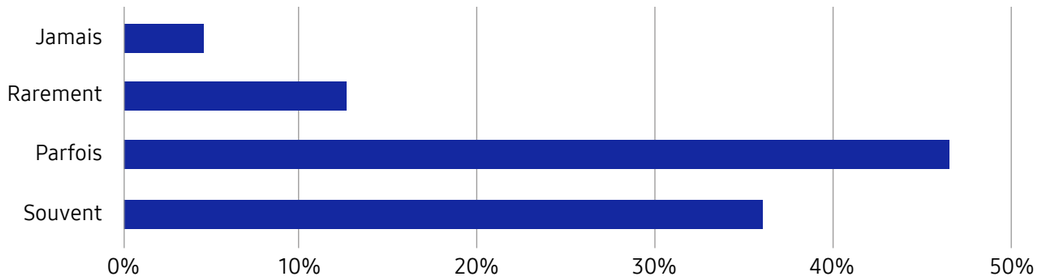
La cybersécurité est l'une des principales sources d'investissement

Les budgets augmentent indubitablement, et les entreprises cherchent à se protéger contre les menaces tout en se conformant aux réglementations telles que le RGPD.

Mais selon nous, les plus visionnaires ne se contentent pas de respecter le RGPD. Elles voient ce règlement comme une opportunité de renforcer la sécurité mobile, d'augmenter la productivité de leurs employés et d'obtenir un avantage sur la concurrence.

« Nous devons sensibiliser le public à l'importance des smartphones. Tout le monde en a un, mais personne ne voit le danger. »
Responsable informatique dans une PME

17 % des entreprises, notamment les startups et les petites entreprises, ne forment jamais (ou rarement) leurs employés au sujet de la sécurité des données.



À quelle fréquence proposez-vous des formations théoriques permettant à vos employés de comprendre comment ils peuvent protéger les données de l'entreprise ?

La formation des employés représente une énorme opportunité

La formation des employés impliqués dans le traitement d'informations sensibles représente l'un des principaux secteurs de croissance pour les investissements informatiques.

Les employés doivent comprendre l'impact d'éventuelles fuites de données, tant au niveau de la réputation de l'entreprise que des coûts occasionnés, notamment lorsque l'on tient compte des amendes considérables prévues dans le cadre du RGPD.

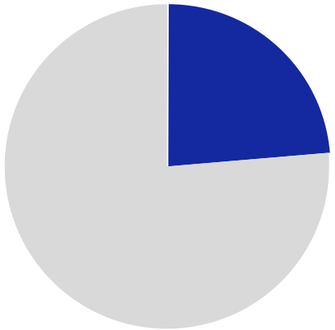
Bien que coûteuse, la formation protège les entreprises contre les menaces, les fuites de données et les violations en levant toute ambiguïté sur la façon dont les données doivent être protégées.

Les employés comprenant les risques et sachant comment les gérer seront bien plus attentifs et confiants lors du stockage de données sensibles.

Ils se sentiront en position de prendre les bonnes décisions.

357 M

de nouvelles variantes de malwares ont été détectées par Symantec en 2016.



Près d'un quart des participants ont déclaré que leur entreprise avait l'intention de s'appuyer sur l'intelligence artificielle pour se protéger contre les cybermenaces.

(CCS Insight, 2017)

L'émergence des nouvelles technologies telles que l'intelligence artificielle

En réalité, les services de sécurité ne peuvent pas faire face à toutes les menaces existant aujourd'hui. Selon Symantec, 357 millions de malwares différents ont été identifiés en 2016. Les entreprises commencent à se tourner vers de nouvelles technologies telles que l'intelligence artificielle pour automatiser la détection des menaces, aider les techniciens chargés de la sécurité à analyser les comportements inhabituels et répondre plus rapidement aux menaces.

Grâce à ces technologies, les techniciens disposent également de plus de temps pour réduire les risques sur le long terme.

2018 devrait être une année charnière dans l'adoption de l'intelligence artificielle, tandis que les entreprises comprennent de mieux en mieux ses avantages et trouvent de nouvelles façons de l'intégrer à leurs opérations. Cependant, au cours des 12 prochains mois, la détection automatisée des menaces sera l'une des principales utilisations de l'intelligence artificielle.

76%

des entreprises testent ou utilisent déjà l'intelligence artificielle.

44%

des entreprises s'attendent à ce que l'IA joue un rôle important pour elles dans les deux prochaines années.

(CCS Insight, 2017)

Recommandations

01

Faites du RGPD le moteur de votre changement

Les entreprises visionnaires profiteront du RGPD pour développer un avantage concurrentiel grâce à une approche plus moderne de la sécurité mobile.

Ce sera également pour elles un moyen d'améliorer la productivité et la mobilité des employés.

Les solutions de mobilité sécurisées impliquent des investissements continus sur le long terme.

Nous vous conseillons de réaliser des analyses de sécurité en continu en vous concentrant sur les outils et les processus qui auront un impact positif sur la productivité.

Si vous avez pris du retard dans votre préparation pour le RGPD, tournez-vous vers des solutions clé en main qui vous permettront de booster votre productivité.

02

Proposez des outils modernes et innovants à vos employés.

Investir dans vos employés est l'une des meilleures dépenses que vous puissiez faire en matière de sécurité. Donnez-leur des outils de pointe et des fonctionnalités leur permettant de travailler efficacement, de manière collaborative et productive.

Lorsque vous choisissez vos produits de sécurité mobile, optez pour des éditeurs leaders capables de vous proposer des formations, des bonnes pratiques et les nouvelles technologies offrant le bon équilibre entre une expérience utilisateur productive et une sécurité efficace.

03

Profitez-en pour former vos employés aux risques de sécurité

Première ligne de défense contre les menaces, les employés sont souvent oubliés en interne. De nombreuses entreprises, notamment les startups, ne forment pas suffisamment leurs employés aux risques de cybersécurité.

Des formations efficaces et régulières aux risques liés au traitement des données personnelles sont essentielles, tant pour la sécurité des données que pour la mise en conformité avec les réglementations telles que le RGPD.

Proposer un programme de formation complet et efficace à tous les employés vous permettra de réduire considérablement les risques sécuritaires.

04

Déterminez l'équilibre optimal entre sécurité et productivité

En plus de répondre à ce besoin de sécurité. Il est important de trouver une solution qui ne nuit pas à la productivité.

Comprenez les besoins de vos employés et évaluez ensemble les solutions de mobilité envisageables.

Les smartphones de nouvelle génération sont particulièrement adaptés à cette évolution des habitudes et des méthodes de travail.

Les leaders du marché doivent pouvoir vous proposer des formations, des bonnes pratiques et des fonctionnalités innovantes vous permettant de trouver le bon équilibre.

samsung.com/business

SAMSUNG