Situation de l'industrie

Sécurité de l'information

2016 À L'ÉCHELLE MONDIALE

Shred-it MD

Table des matières

2 Introduction

4 Analyse de la situation

6 Résumé infographique *Security Tracker*

7 Pratiques d'excellence en matière de sécurité de l'information sur le lieu de travail

9 Soyez prêt pour l'avenir : Préparez-vous au défi du travailleur nomade

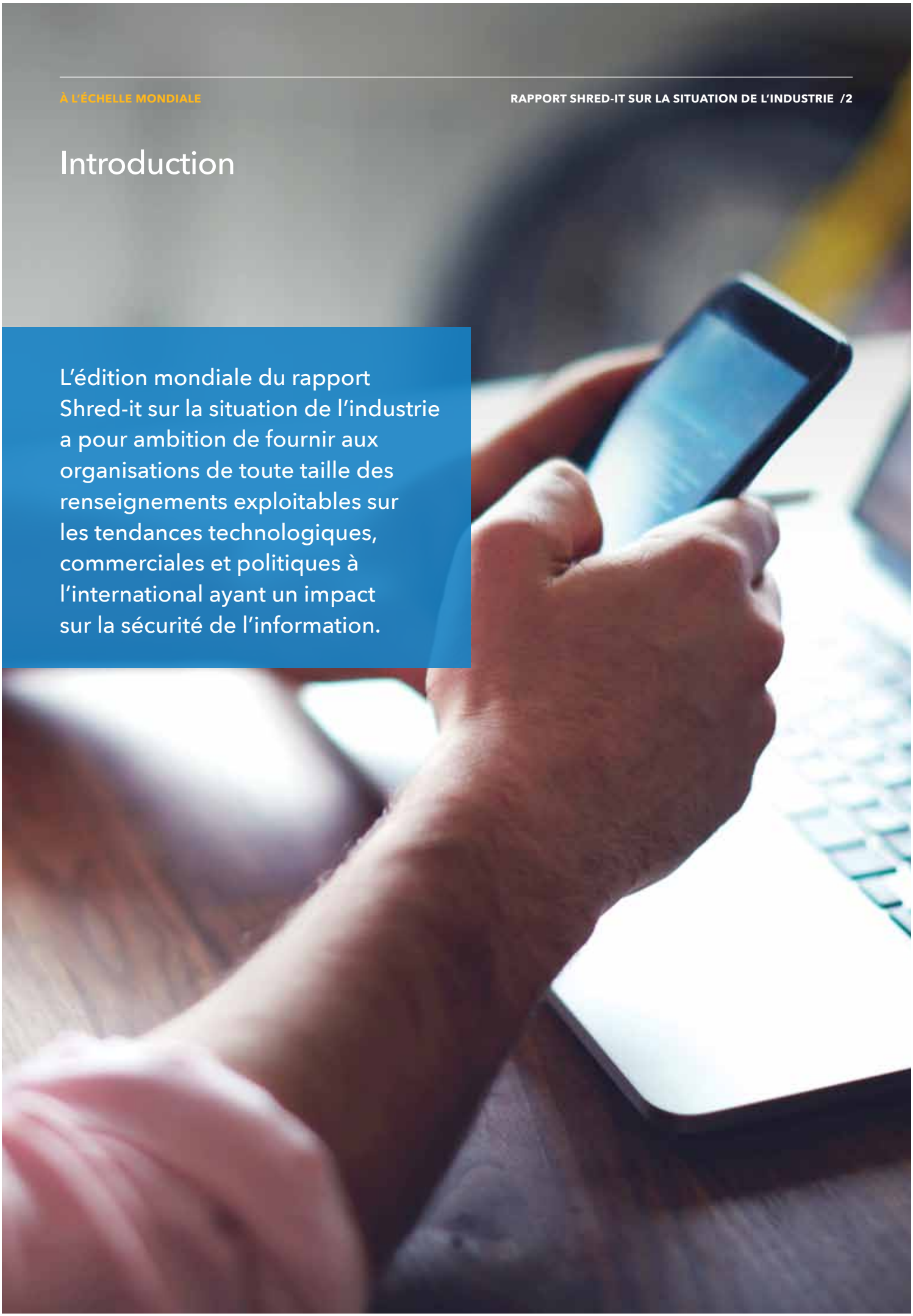
11 Posez vos questions à l'expert

13 Protection de la vie privée – Pensez à l'échelle mondiale et agissez à l'échelon local

16 Résumé

Introduction

L'édition mondiale du rapport Shred-it sur la situation de l'industrie a pour ambition de fournir aux organisations de toute taille des renseignements exploitables sur les tendances technologiques, commerciales et politiques à l'international ayant un impact sur la sécurité de l'information.



Introduction

Le rapport se fonde sur les résultats détaillés du sondage annuel Shred-it *Information Security Tracker* (Sécurité de l'information), une étude approfondie et ciblée menée par Ipsos pour Shred-it.

L'étude *Security Tracker* (Suivi sur la sécurité) donne une vision globale sur les politiques et procédures en matière de sécurité de l'information aux propriétaires de petites entreprises (PPE) et cadres supérieurs (CS) des quatre coins du monde. Ces données offrent une perspective internationale unique et donnent un aperçu des risques émergents, tout en soulignant la manière dont les différentes zones géographiques hiérarchisent la protection des données et la sécurité de l'information.

L'édition mondiale du rapport 2016 sur la situation de l'industrie dévoile un certain nombre de thèmes communs et de nouveaux défis auxquels les entreprises sont confrontées, parmi lesquels :

Une prise de conscience croissante – Les gouvernements aux quatre coins de la planète promulguent des réglementations strictes portant sur la sécurité de l'information. Alors que la prise de conscience ne cesse de croître parmi les CS et les PPE quant aux prescriptions légales relatives au stockage et à la destruction des données confidentielles, quelques pays nagent toujours en pleine confusion en ce qui concerne les exigences juridiques et se retrouvent face à la nécessité d'inciter leur gouvernement à donner des orientations plus claires en termes de responsabilités organisationnelles.

Des lieux de travail flexibles – La culture d'entreprise est en pleine évolution de par le monde. Les lieux de travail de plus en plus flexibles, associés à un nombre croissant de travailleurs à distance et mobiles, peuvent à l'avenir poser un risque considérable dans le domaine de la sécurité de l'information pour les entreprises. La capacité d'une organisation à gérer efficacement les outils modernes (clés USB, ordinateurs portables et autres terminaux mobiles) de ses effectifs travaillant à distance et éparpillés aux quatre coins du monde aidera à déterminer la réussite globale de son approche de la sécurité de l'information.

La formation continue – La formation continue des employés ayant pour objectif de les familiariser avec les politiques et procédures en matière de sécurité de l'information contribuera à l'atténuation du risque d'erreurs humaines et au maintien de la sécurité de l'information au sommet des priorités. La fréquence des formations et un programme d'employés ambassadeurs peuvent être la clé de l'efficacité de ce point de vue.

La gestion du matériel – La mise en place de politiques et de protocoles stricts régissant le mode de stockage du matériel électronique existant est cruciale pour l'approche de gestion de la sécurité de l'information d'une organisation. L'étude mondiale révèle que bon nombre de grandes organisations ne s'arrêtent plus au simple stockage de leurs équipements et dispositifs existants, mais les détruisent de plus en plus fréquemment. Parmi celles-ci, les organisations de premier plan misent sur l'expertise d'une tierce partie pour détruire régulièrement leur matériel.

En plus des thèmes et des nouveaux défis identifiés ci-dessus, l'étude a également démontré que les deux groupes sondés continuent à être parfaitement conscients des risques de pertes financières des suites d'une brèche de données. Ce constat est étayé par les récents résultats de l'étude 2016 sur le coût de la violation de données menée conjointement par IBM et l'Institut Ponemon qui a conclu que le coût total moyen d'une brèche de données a augmenté de 29 % depuis 2013[1].

Les deux groupes sont également conscients des aspects immatériels tels que la confiance des clients, la réputation de l'entreprise et le développement durable. La confiance et la réputation, des notions universelles, figurent parmi les biens les plus précieux d'une entreprise et doivent donc être protégés en fonction.

Pour garantir que leurs politiques en matière de sécurité de l'information suivent l'évolution, les CS et les PPE doivent avoir une vision plus large des risques et des impacts sur l'information. L'édition mondiale du rapport Shred-it 2016 sur la situation de l'industrie constitue le point de départ.

1 Étude 2016 sur le coût de la violation de données de l'Institut Ponemon, page 1

Analyse de la situation

À L'ÉCHELLE MONDIALE

À l'échelle mondiale, les chefs d'entreprise reconnaissent l'importance croissante de la sécurité des données au sein de leurs organisations. Avec la disparition des frontières et une plus grande mobilité parmi les employés, les entreprises doivent combler le fossé entre la prise de conscience et l'action en donnant aux employés les formations et les outils dont ils ont besoin pour protéger les informations confidentielles.

Impact d'une brèche de données

Dans quelle mesure les sociétés prennent-elles au sérieux la menace d'une brèche de données ? Alors que les sociétés semblent comprendre que les brèches de données représentent une possibilité réelle, beaucoup d'entre elles continuent à penser que la perte de données confidentielles n'aura pas un impact significatif sur la capacité de fonctionnement de leur organisation. Selon le sondage 2016 Shred-it *Security Tracker*, seulement un peu plus de la moitié (52 %) des personnes interrogées de par le monde estiment qu'une perte ou un vol de données aurait un impact considérable sur leurs activités. Plus surprenant encore, seul un quart (24 %) des personnes conscientes de l'impact d'une éventuelle brèche considèrent que le principal dommage concernerait la crédibilité ou la réputation de leur entreprise, et placent les impacts légal et financier en deuxième et troisième positions respectivement. Des résultats de l'étude 2016 sur le coût de la violation de données menée par l'Institut Ponemon, il ressort cependant que les dommages causés à la réputation d'une société peuvent rapidement se traduire par des pertes financières[2]. Après une brèche de données, la direction d'une entreprise doit prendre les mesures qui s'imposent pour garder la confiance des clients afin de minimiser l'impact financier de la perte d'activités.

Origine d'une brèche de données

À l'échelle mondiale, les sociétés prennent conscience que les agissements de leurs employés peuvent mettre en péril leurs données confidentielles. Notre étude révèle que 45 % des personnes interrogées au monde pensent que l'erreur humaine ou une perte accidentelle du fait d'un employé ou d'un initié de la société est l'origine la plus probable d'une brèche de données.

Malgré cette prise de conscience, la majorité des entreprises ne

2 Étude 2016 sur le coût de la violation de données de l'Institut Ponemon, page 1

mettent pas en place les protocoles requis aidant les employés à sécuriser les informations des clients et celles de nature concurrentielle. Près de la moitié (40 %) des chefs d'entreprise mondiaux ne disposent pas de directives pour le stockage et la destruction d'informations confidentielles et ne donnent aucune instruction en ce sens à leurs employés qui travaillent hors site ou à domicile. Ce manque de protection est d'autant plus préoccupant au vu des résultats de l'étude Ponemon qui fait état que la plupart des brèches de données (48 % dans l'étude de cette année) sont toujours la conséquence d'attaques criminelles et malveillantes, alors qu'un quart (25 %) seulement étaient dues à une erreur humaine[3].

En ne s'assurant pas que leurs employés comprennent et respectent les politiques en matière de sécurité, les entreprises pourraient bien mettre en danger leur organisation et leur réputation en exposant leurs données de grande valeur sur les clients, employés et activités à des risques tant internes (erreur humaine) qu'externes (attaques malveillantes ou pirates informatiques).

Dans le même temps, les organisations n'évaluent pas seulement les risques auxquels elles sont confrontées aujourd'hui, elles explorent également ceux auxquels elles devront faire face à l'avenir. Avec des employés de plus en plus mobiles et compte tenu de la dépendance croissante par rapport à l'accès à distance, il n'est pas surprenant que 35 % des personnes interrogées au monde estiment que la principale menace pour la sécurité de leur organisation d'ici cinq à dix ans se manifestera en ligne, suivie de près par deux autres préoccupations de taille que sont le manque de connaissances en interne ou l'erreur humaine découlant de connaissances insuffisantes (16 %) et l'informatique en nuage (14 %). En plus d'admettre les risques émergents dans le domaine de la sécurité de l'information, associés à un environnement professionnel en mutation, les entreprises doivent également veiller à ce que leurs politiques et procédures évoluent en fonction des origines potentielles d'une brèche de données.

Types de documents les plus exposés

Lorsque les sociétés commencent à examiner sérieusement les différentes manières dont les données peuvent être violées, il semble que la menace devient plus réelle. En les interrogeant sur l'impact sur différents types de documents, la majorité des entreprises mondiales sondées (71 %) reconnaissent que le vol de documents et / ou de données pourrait avoir un impact sur la stabilité de leur société. Dans chaque pays, les informations des clients furent choisies par le plus grand nombre de sociétés (40 % à l'échelle mondiale) comme celles encourant le plus grand risque en cas de violation, suivies de près par les pièces comptables (29 % à l'échelle mondiale).

3 Étude 2016 sur le coût de la violation de données de l'Institut Ponemon, page 2

Résumé infographique Security Tracker (MONDIAL)

L'IMPORTANCE DE LA SÉCURITÉ DES DONNÉES

À L'ÉCHELLE MONDIALE,

LES CHEFS D'ENTREPRISE COMMENCENT À RECONNAÎTRE L'IMPACT D'UNE BRÈCHE DE DONNÉES.

SI DES DONNÉES ÉTAIENT PERDUES OU VOLÉES :

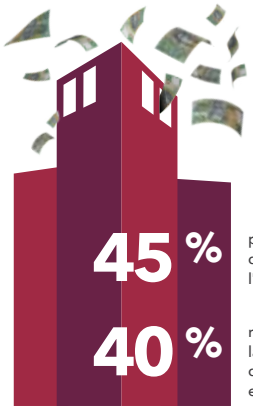
52 % estiment que cela pourrait avoir un impact significatif sur leur organisation.

24 % sont d'avis que cela pourrait nuire à la crédibilité et à la réputation de leur entreprise.

14 % pensent que cela pourrait leur causer un préjudice financier.

13 % considèrent que des conséquences juridiques s'ensuivraient.

MAIS LES SOCIÉTÉS NE FOURNISSENT PAS LES FORMATIONS NI LES OUTILS PERMETTANT À LEURS EMPLOYÉS DE SÉCURISER LES INFORMATIONS DES CLIENTS ET CONCURRENTIELLES



45 % pensent que l'erreur humaine ou une perte accidentelle du fait d'un employé ou d'un initié de la société est l'origine la plus probable d'une brèche de données.

40 % ne disposent pas de directives pour le stockage et la destruction d'informations confidentielles et ne donnent aucune instruction en ce sens à leurs employés qui travaillent hors site ou à domicile.

CES PROCHAINES 5 À 10 ANNÉES,

les organisations considèrent ces éléments comme les plus grands risques :

- **MENACE EN LIGNE 35 %**
- **ERREUR HUMAINE 16 %** des suites de connaissances insuffisantes
- **INFORMATIQUE EN NUAGE 14 %**

LES SOCIÉTÉS DOIVENT ÉLABORER DES PLANS D'ACTION EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

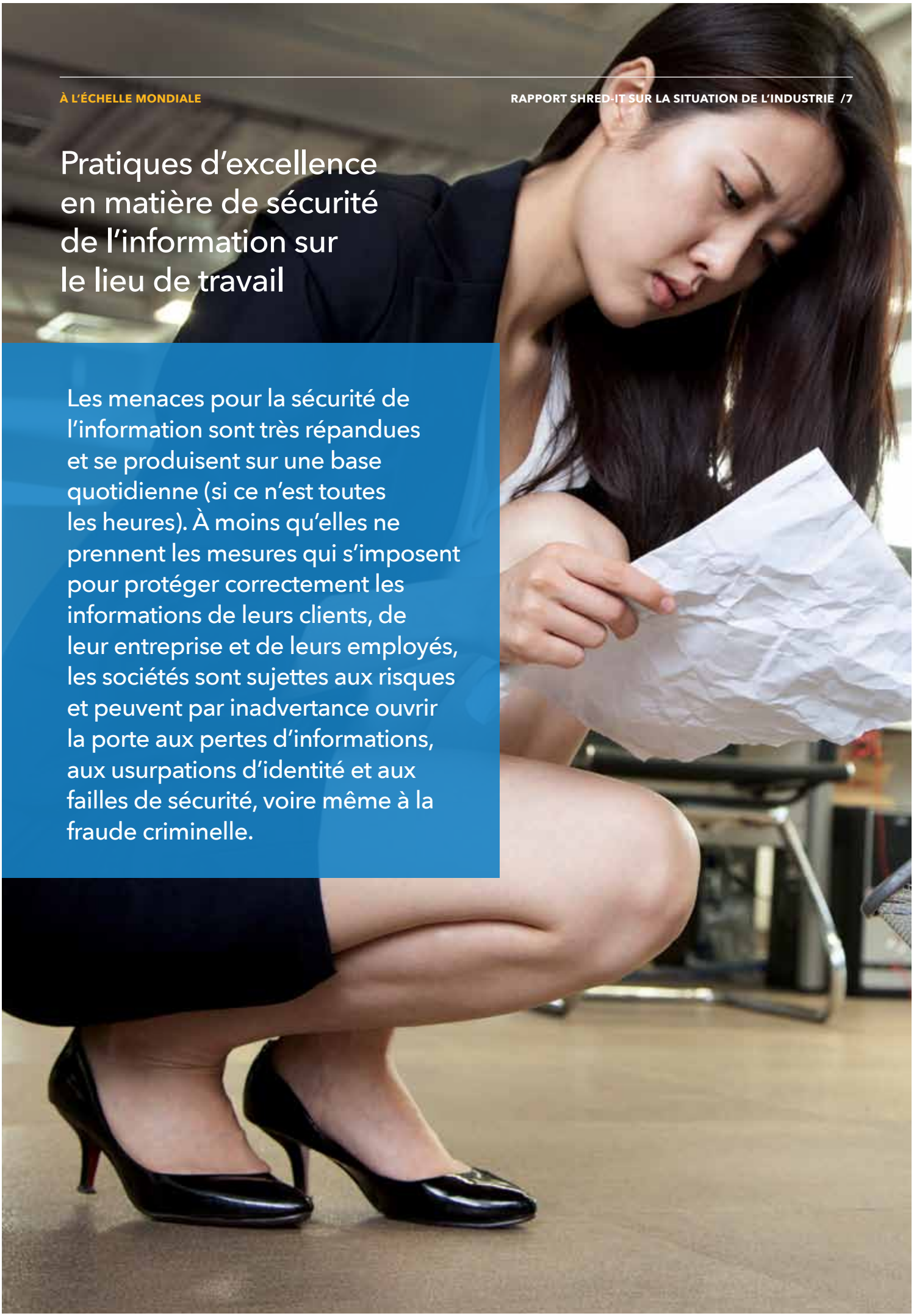
pour aider leurs employés à protéger les informations confidentielles.

Pour de plus amples informations sur la protection de votre environnement de travail,nous vous invitons à visiter le site shredit.fr.

Toutes les statistiques du sondage 2016 Shred-it Information Security Tracker sont fournies par Ipsos.

Shred-it

Pratiques d'excellence en matière de sécurité de l'information sur le lieu de travail



Les menaces pour la sécurité de l'information sont très répandues et se produisent sur une base quotidienne (si ce n'est toutes les heures). À moins qu'elles ne prennent les mesures qui s'imposent pour protéger correctement les informations de leurs clients, de leur entreprise et de leurs employés, les sociétés sont sujettes aux risques et peuvent par inadvertance ouvrir la porte aux pertes d'informations, aux usurpations d'identité et aux failles de sécurité, voire même à la fraude criminelle.

Pratiques d'excellence en matière de sécurité de l'information sur le lieu de travail

La mise en œuvre d'un plan de sécurité de l'information visant la protection des données est vitale pour la gestion des menaces relatives à la sécurité de l'information. C'est là une étape que les sociétés de toute taille aux quatre coins du monde doivent franchir pour atténuer le risque de brèche de données.

Shred-it a identifié 10 pratiques d'excellence en matière de sécurité de l'information que toutes les entreprises, quelles que soient leur taille, leur implantation géographique et leurs ressources, peuvent mettre en place pour protéger leurs clients, leur réputation et leur personnel :

Exercer le leadership de haut en bas – Lorsque les membres de la direction font montre de leur engagement à l'égard de la sécurité de l'information, les employés sont plus enclins à suivre leur exemple. Si les managers se comportent d'une façon susceptible d'ébranler les politiques et procédures en matière de sécurité, les employés ne les prendront pas au sérieux. Personne n'est au-dessus de la loi.

Éduquer les employés – Les employés ont besoin de formations régulières pour comprendre les politiques de leur organisation portant sur la sécurité de l'information et couvrant les informations en ligne, physiques et stockées électroniquement, pour garantir qu'ils sont conscients de la façon dont il convient de traiter et de détruire les informations confidentielles. Des effectifs bien formés sont essentiels pour protéger votre organisation d'une brèche de données potentiellement préjudiciable.

Ne jamais baisser la garde – Au fil du temps, les organisations changent et se développent. Il en va de même pour les risques dans le domaine de la sécurité de l'information. Il est primordial de réexaminer régulièrement les politiques et procédures de sécurité pour s'assurer qu'elles reflètent la réalité des activités commerciales en évolution constante.

Mettre en place une politique *Shred-it All* – Une politique *Shred-it All* élimine toute incertitude sur la question de savoir si les documents sont confidentiels ou non en rendant obligatoire le déchiquetage de tous les documents sur support papier avant leur recyclage ou leur destruction. Cette simple étape est le meilleur moyen pour éviter toute erreur humaine, y compris la manipulation sans précaution de documents et de fichiers confidentiels. Par ailleurs, le recyclage de tous les papiers déchiquetés ajoute un avantage environnemental à la solution de sécurité destinée aux entreprises.

Instituer une politique du bureau propre – Une politique du bureau propre encourage les employés à ranger leur bureau et à mettre les documents sous clé dans une armoire de classement ou une unité de stockage lorsqu'ils quittent leur poste de travail pour une durée prolongée et à la fin de chaque journée de travail. Ceci inclut les documents, les classeurs, les notes, les cartes de visite et les supports numériques amovibles, tels que les clés USB. Les postes de travail en désordre et sans surveillance représentent un plus grand risque, puisque les informations sur feuille volante sont une cible facile pour les voleurs.

Instaurer une politique de conservation – Déterminez les documents qu'il convient de garder et leur durée de conservation. Indiquez clairement une date de destruction sur tous les dossiers stockés et n'oubliez pas que la conservation de certains documents pour une durée minimale peut être une obligation légale en soi. Dans le cadre de cette politique, les organisations devraient aussi procéder régulièrement au rangement de leurs locaux de stockage et éviter l'accumulation des disques durs obsolètes.

Protéger les espaces collaboratifs – Un lieu de travail collaboratif peut accroître la productivité et stimuler la réflexion novatrice. La sécurité de l'organisation peut cependant être compromise avec des informations confidentielles laissées sur des tableaux blancs, des bloc-notes ou des tableaux à feuilles mobiles, puisqu'elles sont exposées à la vue de tous dans les espaces communs. Les espaces collaboratifs doivent être débarrassés après utilisation. Les employés peuvent éventuellement prendre des photos des tableaux blancs ou des tableaux à feuilles mobiles et les sauvegarder sur un serveur sécurisé pour un usage ultérieur.

Crypter tous les dispositifs électroniques – Cryptez tous les dispositifs électroniques utilisés par les employés, indépendamment du fait qu'il s'agisse de leurs propres terminaux ou d'appareils fournis par la société. En cas de perte ou de vol de dispositifs électroniques, le chiffrement protégera les informations confidentielles sauvegardées sur chaque dispositif et atténuera toute activité compromettante.

Protéger les postes d'impression – Encouragez les employés et le personnel à ne laisser aucun document sans surveillance sur un poste d'impression partagé. Pour renforcer la sécurité autour des postes d'impression, il est recommandé d'envisager l'utilisation de mots de passe pour les travaux d'impression.

Limiter l'accès – Fixez des niveaux d'autorisation pour les personnes pouvant accéder à certains types d'informations confidentielles. Seules des personnes autorisées doivent manipuler les informations confidentielles.

Outre ces conseils, les entreprises doivent tout mettre en œuvre pour rester au fait de l'évolution des lois et de la législation sur la sécurité de l'information applicables à leur société, tout en veillant à ce que leurs politiques et procédures en matière de sécurité de l'information soient en conformité avec les politiques gouvernementales. En cas de non-conformité, les entreprises peuvent encourir des amendes considérables et être confrontées à de graves conséquences.

Soyez prêt pour l'avenir : Préparez-vous au défi du travailleur nomade

La mondialisation de l'environnement économique a boosté le nombre de travailleurs nomades qui deviennent ainsi le nouveau visage du salariat de demain. De récentes études, il ressort en effet que la main-d'œuvre mobile mondiale devrait atteindre 1,75 milliard d'individus d'ici à 2020, soit 42 % de la population active mondiale[4].

4 Strategy Analytics, 2015, *Global Mobile Workforce Forcast, 2015-2020*

Soyez prêt pour l'avenir : Préparez-vous au défi du travailleur nomade

En plus de permettre aux organisations d'accéder à un plus grand vivier de talents dans lequel puiser, une main-d'œuvre mobile offre plusieurs avantages aussi bien aux employés qu'aux entreprises, parmi lesquels une flexibilité accrue pour les travailleurs et une réduction des coûts indirects et administratifs pour les organisations.

Pour la main-d'œuvre mobile mondiale, la technologie est à la fois le catalyseur clé et le moteur de la croissance. Les smartphones et tablettes de plus en plus abordables, associés à l'acceptation croissante des programmes d'entreprise AVEC (Apportez votre équipement personnel de communication), simplifient comme jamais auparavant le travail à distance des employés. D'après la société International Data Corporation (IDC), la mobilité est désormais synonyme de productivité à l'intérieur comme à l'extérieur du lieu de travail, et l'adoption massive de la technologie mobile a créé un environnement où les travailleurs espèrent tirer le maximum de la technologie mobile au travail[5].

Il est néanmoins possible que de nombreuses organisations ne soient pas préparées aux défis inhérents à la sécurité de l'information allant de pair avec la gestion d'une main-d'œuvre mobile. Le sondage 2016 Shred-it *Security Tracker* dévoile singulièrement que 40 % des organisations ne disposent pas d'une politique en matière de sécurité de l'information pour les environnements de travail flexibles et hors site, et que seulement 31 % des entreprises ont adopté une politique touchant ces deux environnements. Ces chiffres démontrent que la majorité des sociétés ne fournissent pas à leurs employés les formations et les protocoles requis leur permettant de sécuriser les informations des clients et celles de nature concurrentielle dans un environnement mobile.

Pour mieux gérer le risque croissant de la main-d'œuvre nomade, les entreprises de toute taille doivent se montrer proactives en prodiguant des formations pour sécuriser les données des employés, des clients et de la société afin d'éviter en fin de compte toute violation de la sécurité de l'information. Voici 6 conseils qui aideront les organisations à gérer la sécurité de l'information en ce qui concerne leurs travailleurs mobiles :

1. Formez les travailleurs mobiles – Il peut s'avérer complexe pour une organisation de veiller à ce que les travailleurs nomades détruisent des informations confidentielles en toute sécurité. Encouragez les pratiques ad hoc par le biais de formations visant spécifiquement les politiques destinées aux employés à distance. Assurez-vous que les terminaux mobiles obsolètes sont détruits adéquatement en concluant un partenariat avec un fournisseur de destruction de documents fiable et ordonnez à vos employés de ramener sur le lieu de travail tous les documents sur papier et sur support numérique pour garantir leur élimination et leur destruction dans les règles de l'art.

2. Méfiez-vous des connexions non sécurisées – N'utilisez jamais de points d'accès Wi-Fi publics pour traiter ou consulter des informations sensibles. L'utilisation de connexions partagées ou publiques dans les salons d'affaires ou des bars / bistrots peut conduire à des brèches de données. Établissez des politiques incitant vos employés à ne se connecter qu'à des réseaux fiables dans le cadre de leur travail.

3. Soyez prudent en voyage – Les voyages d'affaires sont une réalité dans la vie d'aujourd'hui, à tel point qu'ils font partie de la routine de bien des façons. Selon les experts en cybersécurité, il est de plus en plus facile pour les fraudeurs et les pirates informatiques de lire les codes-barres des cartes d'embarquement et d'accéder aux données de contact des passagers, aux futurs plans de voyage et aux comptes grands voyageurs. Les organisations devraient envisager l'instauration de politiques exigeant des employés qu'ils détruisent leurs cartes d'embarquement, leurs itinéraires et autres documents liés aux vols en avion. Les organisations peuvent également encourager leurs employés à utiliser des étuis anti-RFID pour protéger leurs cartes de crédit et leur identité lorsqu'ils voyagent.

4. Préservez la confidentialité – Le piratage informatique visuel de terminaux mobiles peut se produire pratiquement partout. Mettez à la disposition de vos employés des écrans de confidentialité pour leurs ordinateurs portables, tablettes et autres terminaux mobiles pour protéger les informations confidentielles des regards indiscrets.

5. Protégez les dispositifs – Veillez à ce que tous les ordinateurs portables et autres terminaux mobiles soient cryptés et protégés par un mot de passe. La protection d'un ordinateur portable ou autre dispositif n'est assurée que s'il n'est jamais laissé sans surveillance dans un lieu public, une voiture ou une chambre d'hôtel. Il convient par ailleurs de crypter les dossiers d'informations que vous emportez.

6. Ne baissez jamais la garde – La protection permanente des informations est un défi de taille en constante mutation. Les risques sont bien réels et omniprésents. Par conséquent, les organisations doivent combattre le laisser-aller et s'assurer de propager une culture de responsabilisation au sein de leur entreprise.

5 IDC, 2015, *IDC Forecasts U.S. Mobile Worker Population to Surpass 105 Million by 2020*

Posez vos questions à l'expert

Andrew Lenardon, le Directeur mondial de Shred-it International, partage sa vision sur l'importance d'une politique globale en matière de sécurité de l'information et sur les mesures à prendre par les organisations des quatre coins du monde pour protéger leur lieu de travail.

Pourquoi les entreprises devraient-elles se soucier de leurs habitudes quant à la sécurité de l'information ?

A. L. : En l'absence de protocoles ad hoc visant à protéger les informations, qu'il s'agisse de documents ou de matériel informatique, les sociétés courent quotidiennement le risque de s'exposer elles-mêmes et d'exposer leurs clients à de sérieuses brèches de données. À l'échelle mondiale, le coût moyen d'une brèche de données est de 4 millions USD en termes de manque à gagner et le coût moyen pour chaque dossier perdu est de 158 USD[6]. En prenant ceci en compte et en considérant les éventuelles interruptions d'activités des suites d'une violation, un seul incident de sécurité peut avoir un impact considérable sur la santé financière d'une organisation.

Le préjudice financier n'est cependant pas la seule question qui devrait préoccuper les chefs d'entreprise. Une brèche de données peut aussi fortement affecter des aspects immatériels tels que la confiance des clients, la réputation de l'organisation et le développement durable. La confiance et la réputation figurent parmi les biens les plus précieux d'une entreprise et, si celles-ci sont ébranlées, elles peuvent fortement compromette la capacité d'une société à développer une relation positive avec les parties prenantes.

6 Étude 2016 sur le coût de la violation de données de l'Institut Ponemon, page 1

Posez vos questions à l'expert

Comment une brèche de données peut-elle affecter la réputation d'une organisation ?

A. L. : C'est bien simple, tout repose sur la confiance. Les organisations aux quatre coins du monde traitent quotidiennement des données de clients et ces derniers sont en droit d'attendre que leurs informations personnelles soient protégées. Une violation des informations est également un abus de confiance qui peut sérieusement porter atteinte à la réputation d'une organisation. La formation des employés et les protocoles aident à atténuer ce risque, mais il n'existe pas de remède miracle. Les organisations doivent en tout temps se montrer vigilantes pour protéger leur réputation et garder la confiance de leurs clients.

Quels sont les principaux obstacles à la sécurité de l'information au sein d'une organisation ?

A. L. : Ils sont au nombre de deux. D'une part, si les membres de la direction ne font pas part de leur engagement par rapport à la sécurité, les employés ne prendront pas au sérieux les politiques en matière de sécurité de l'information. Les chefs d'entreprise doivent contribuer à la création d'une culture de la sécurité afin que les employés comprennent les protocoles mis en place pour la protection des informations confidentielles. D'autre part, la responsabilisation personnelle : chacun de vos employés sans exception doit comprendre comment ses agissements peuvent mettre en péril la société et ses clients. Un acte aussi simple que jeter inadéquatement dans le bac à recyclage un document pouvant contenir des informations sur les clients engage la responsabilité de l'entreprise et présente un risque pour cette dernière. Lorsque tous les employés ont bien saisi la manière de gérer et d'identifier les risques pour la vie privée, les chefs d'entreprise sont mieux à même de protéger leurs clients, leur réputation et leurs employés.

Comment les organisations peuvent-elles relever le défi d'une meilleure protection de leurs informations ?

A. L. : Les entreprises de toute taille doivent se montrer proactives lorsqu'il est question d'aborder les risques. En termes de sécurité de l'information, cela signifie la mise en place de protocoles pour une gestion adéquate des documents et du matériel informatique, de leur collecte à leur destruction finale, en passant par le stockage.

Les chefs d'entreprise doivent donner la priorité aux formations des employés et aux vérifications des politiques à intervalles réguliers pour protéger la sécurité de l'information sur le lieu de travail. Les formations et les vérifications régulières n'atténuent pas seulement le risque de brèches de données des suites d'une erreur humaine ou d'un manque de connaissances des pratiques de sécurité, mais elles constituent également un aide-mémoire utile pour le respect des politiques par les employés. Lorsque tous les employés ont bien saisi la manière de gérer et d'identifier les risques pour la vie privée, les chefs d'entreprise sont mieux à même de protéger leurs clients, leur réputation et leurs employés.

Pour sécuriser les données des employés, des clients et de la société, ces politiques doivent aborder les informations confidentielles à l'intérieur comme à l'extérieur des bureaux. L'information reste sensible, même si elle est électronique. Avec la généralisation des dispositifs électroniques, tels que les smartphones, les tablettes et les ordinateurs portables, il devient de plus en plus difficile d'empêcher le matériel confidentiel de quitter les bureaux.

Pourquoi les entreprises devraient-elles se préoccuper d'une main-d'œuvre mobile sans cesse croissante ?

A. L. : Plus les travailleurs deviennent mobiles et éparpillés à travers le monde, et plus les risques seront élevés. Les CS et les PPE doivent par conséquent surmonter ces nouveaux défis.

Dans un environnement de travail mobile, les informations commerciales sont stockées sur les disques durs d'ordinateurs portables, des clés USB, des disques durs externes ou des réseaux infonuagiques, et les employés emportent leur travail du bureau. Alors que l'utilisation de tels dispositifs permet aux employés de travailler hors site, cela signifie aussi qu'une énorme quantité d'informations confidentielles quitte le bureau avec eux. Il est tellement facile de perdre l'un de ces dispositifs technologiques ou de l'oublier dans la voiture, sans oublier qu'ils sont une proie de choix pour les pirates informatiques. Un seul ordinateur portable perdu ou volé est susceptible de nuire sérieusement à n'importe quelle entreprise.

Si l'on y ajoute que les employés accèdent désormais aux documents et aux e-mails d'affaires sur des ordinateurs et des terminaux mobiles qui n'appartiennent pas à la société, les employeurs ont un contrôle direct plus limité sur les informations de leur société, ce qui peut générer des risques d'atteinte à la vie privée, à la confidentialité et à la sécurité. Un employé travaillant sur son ordinateur personnel à domicile peut ne pas se montrer aussi empressé à installer les mises à jour de sécurité et les correctifs que l'employeur le ferait sur ses propres machines d'entreprise, ce qui peut rendre les systèmes de l'environnement de travail plus vulnérables aux logiciels malveillants ou espions.

Les sociétés doivent également avertir leurs employés de ne prendre ou de n'imprimer des informations confidentielles en dehors du lieu de travail qu'en cas d'absolue nécessité et leur donner des instructions sur leur destruction adéquate en toute sécurité. Les informations numériques ne sont pas les seuls éléments à quitter le bureau avec le personnel nomade et les employés doivent comprendre les risques et prendre les mesures qui s'imposent lorsqu'ils emportent des données de leur lieu de travail.

Protection de la vie privée – Pensez à l'échelle mondiale et agissez à l'échelon local

Le vieil adage selon lequel la meilleure défense, c'est l'attaque, se vérifie également lorsqu'il est question de la protection de la vie privée. Les législateurs des quatre coins du monde amendent régulièrement les règlements ou élaborent de nouvelles politiques en vue de protéger les citoyens et de garantir que leurs informations personnelles restent dans le domaine privé.

Protection de la vie privée – Pensez à l'échelle mondiale et agissez à l'échelon local

L'ampleur de la tâche est énorme. Pratiquement chaque entité gouvernementale ou entreprise privée dispose d'informations devant être stockées en toute sécurité et détruites une fois qu'elles ne sont plus nécessaires et ce, à des fins de protection de la vie privée et de respect de la réglementation.

Selon le cabinet d'avocats d'affaires international DLA Piper, nous nous trouvons dans une période d'activité sans précédent en termes de développement de réglementations sur la protection des données de par le monde, ce qui aura une incidence fondamentale sur l'approche que les entreprises mondiales doivent adopter vis-à-vis de la collecte et de la gestion des informations personnelles[7]. Par ailleurs, l'étude Data Protection Laws of the World menée par le cabinet suggère que l'émergence de lois dans des pays qui ne disposaient d'aucune loi sur la protection des données auparavant pourrait bien générer un risque considérable quant à leur application à l'avenir.

Les entreprises et les organisations aux quatre coins du monde doivent garder à l'esprit les réglementations sur la protection de la vie privée régissant leurs opérations au niveau local. Tandis que les données relatives à la santé et les informations financières semblent être les catégories les plus citées en termes de réglementations, bon nombre d'entreprises comptent sur l'expertise d'une tierce partie spécialisée pour examiner les fonctions critiques et identifier les domaines clés à risque.

Le tableau ci-après reprend les fonctions classiques d'une entreprise pouvant être exposées à un risque lorsqu'il est temps d'appliquer les lois sur la protection de la vie privée.

DÉPARTEMENT	CE QU'IL FAUT PROTÉGER	RISQUES
Ressources humaines	• Demandes d'emploi • Documents liés à la santé et à la sécurité • Dossiers médicaux • Informations sur les salaires • Évaluations des performances • Informations et manuels de formation	La plupart des documents RH contiennent des informations confidentielles et personnelles sur les employés en fonction et potentiels.
Vente / Marketing	• Listes et contrats de clients • Informations financières • Dossiers de candidature • Plans stratégiques • Échantillons de produits • Calendriers de lancement • Budgets et prévisions	Les documents relatifs à la vente et au marketing contiennent souvent des informations privées et confidentielles sur les clients du moment et les prospects. Ils peuvent par ailleurs contenir des renseignements sur les stratégies commerciales et autres propriétés intellectuelles devant rester confidentielles.
Comptabilité	• Contrats • Factures • Listes de clients • Rapports internes • Fiches de paye • Informations sur les fournisseurs • Applications financières	Ces documents contiennent habituellement des informations financières pouvant occasionner des préjudices considérables s'ils sont compromis.
Technologies de l'information	• Disques durs • Clés USB • CD • Disques Zip • Détails de la configuration du réseau	Les actifs numériques peuvent contenir des millions de dossiers individuels et causer des dommages significatifs à une organisation s'ils sont perdus ou volés. Les dossiers électroniques sont en outre nettement plus faciles à transférer et à disséminer que les documents sur support papier.

7 DLA Piper, 2016, *Data Protection Laws of the World*

Protection de la vie privée – Pensez à l'échelle mondiale et agissez à l'échelon local

DÉPARTEMENT	CE QU'IL FAUT PROTÉGER	RISQUES
Approvisionnement	• Dossiers de l'entreprise • Bons de commande des fournisseurs • Dossiers des fournisseurs • Documents de spécifications des fournisseurs • Informations relatives aux cartes de crédit • Applications financières	Tout comme la comptabilité, le département de l'approvisionnement utilise intensivement des dossiers financiers et historiques se rapportant à l'entreprise ou à ses fournisseurs.
Recherche et développement	• Évaluations • Résultats des essais de produits • Formules • Plans de produits • Informations sur les nouveaux produits • Rapports • Dessins des spécifications • Prototypes	Ce département gère en continu des informations de nature concurrentielle qui peuvent sérieusement affecter l'avantage compétitif d'une organisation.
Direction	• Budgets • Correspondance • Listes de clients • Contrats juridiques • Prévisions • Plans stratégiques	Par essence, la direction traite des documents hautement confidentiels et sensibles.

Pratiques d'excellence

Dès que les organisations ont clairement compris leurs obligations légales locales et après avoir effectué une évaluation globale des risques, elles peuvent envisager l'intégration de plusieurs pratiques d'excellence, parmi lesquelles :

- la mise en place de politiques et procédures détaillées régissant les modes de collecte, de gestion, de conservation et de destruction des informations confidentielles de l'organisation,
- le développement de formations complètes sur les risques et les processus destinées aux membres du personnel pour les aider à comprendre leur rôle dans la sécurisation des informations à caractère privé,
- la sécurisation de tous les dispositifs électroniques, que ce soit pendant leur cycle de vie ou au terme de celui-ci,
- la réalisation d'audits à intervalles fixes pour contrôler l'efficacité et la conformité, tout en actualisant régulièrement les procédures et protocoles.

Résumé

Shred-it est particulièrement fier de fournir des renseignements exploitables sur les tendances technologiques, commerciales et politiques à l'international qui ont un impact sur la sécurité de l'information. Comme le montre l'édition mondiale du rapport 2016 sur la situation de l'industrie, la technologie mobile a fondamentalement transformé le lieu de travail. Les entreprises de toute taille doivent désormais relever de nombreux nouveaux défis liés à la flexibilité accrue des employés et à la croissance d'une main-d'œuvre mobile de plus en plus éparpillée aux quatre coins du monde.

Le rapport met en évidence un certain nombre de ces nouveaux défis tout en offrant des solutions basées sur des pratiques d'excellence de pointe. Parmi les leçons clés que doivent tirer les chefs d'entreprise, citons la formation continue des employés afin de les familiariser avec les politiques et procédures en matière de sécurité de l'information, le développement de politiques et de procédures pour faciliter la gestion des outils de la main-d'œuvre moderne à distance et l'intégration de pratiques ad hoc de gestion du matériel informatique dans une approche organisationnelle globale de la sécurité de l'information.

Lorsqu'il est question de la protection de la sécurité de l'information, le laisser-aller est l'un des risques clés dans toute organisation. Pour garantir que leurs politiques en matière de sécurité de l'information suivent l'évolution, les CS et les PPE doivent en permanence avoir une vision large des risques et des impacts sur l'information, tout en réexaminant leurs stratégies à intervalles réguliers.

Découvrez comment Shred-it peut aider votre organisation à améliorer sa sécurité de l'information en visitant le site shredit.com et en sélectionnant votre région.

Vous pouvez également vous tenir informé
en ligne sur les activités de Shred-it :

facebook.com/shredit

linkedin.com/company/shred-it

@Shredit