Les enjeux de gouvernance et de sécurité dans Microsoft 365

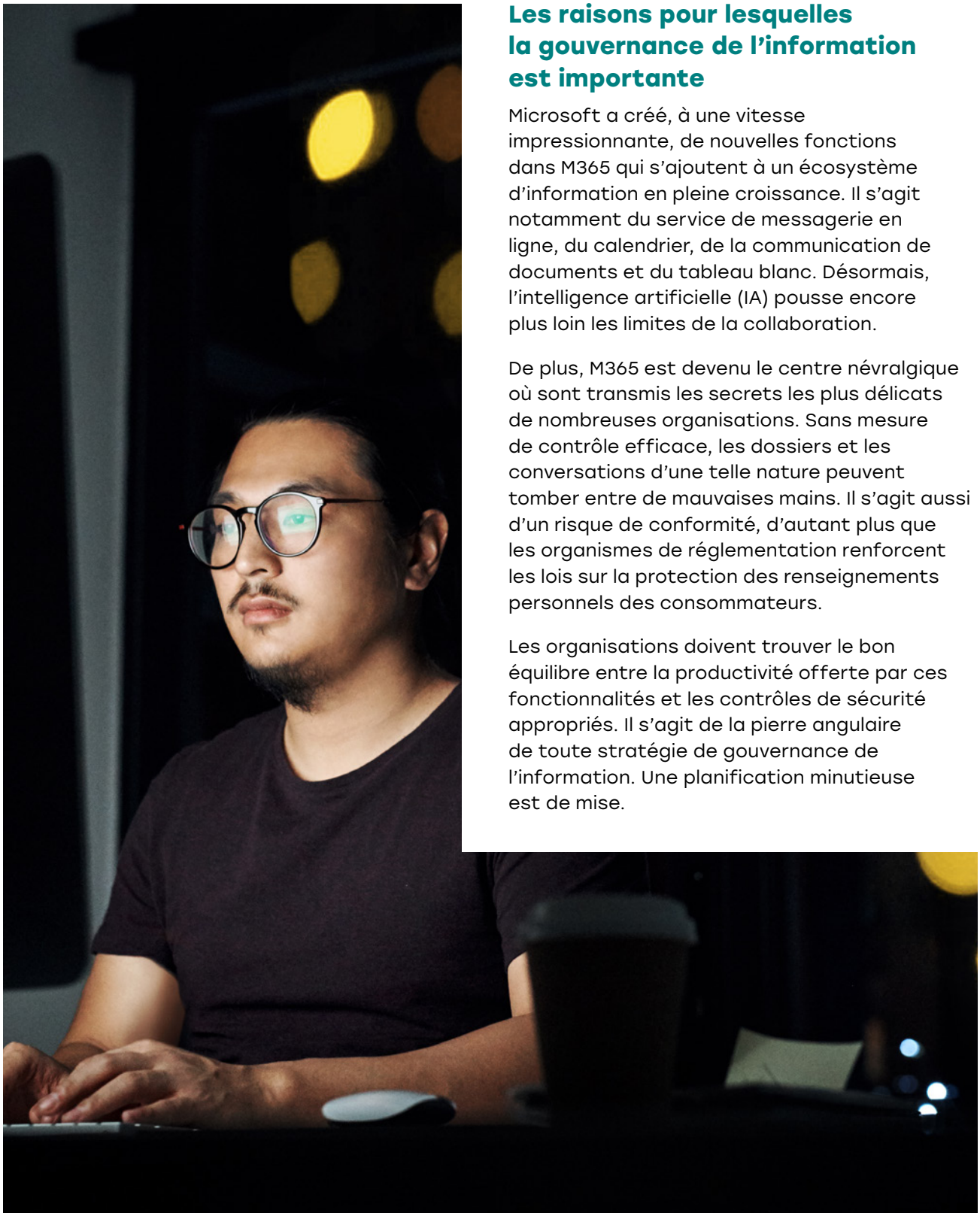
Microsoft Office a fait son apparition en 1990, sept mois avant la première page Web. À l'époque, tout se passait sur l'ordinateur de l'utilisateur.

Trente-cinq ans plus tard, le monde a changé. Son successeur, Microsoft 365 (M365), intègre une étroite collaboration entre les équipes dans l'expérience quotidienne de l'utilisateur.

L'augmentation de la productivité a créé de nouvelles difficultés. La plupart des gens ne sont pas préparés aux risques pour la sécurité associés à la transmission fluide de l'information, d'où le besoin de cadres pour trouver l'équilibre entre la sécurité et la productivité. Le présent livre électronique explique la façon dont une planification minutieuse et l'utilisation judicieuse des technologies d'assistance peuvent protéger les utilisateurs de M365 grâce à des mesures de protection numériques.

En collaboration avec

WeActis par Mondata



Les raisons pour lesquelles la gouvernance de l'information est importante

Microsoft a créé, à une vitesse impressionnante, de nouvelles fonctions dans M365 qui s'ajoutent à un écosystème d'information en pleine croissance. Il s'agit notamment du service de messagerie en ligne, du calendrier, de la communication de documents et du tableau blanc. Désormais, l'intelligence artificielle (IA) pousse encore plus loin les limites de la collaboration.

De plus, M365 est devenu le centre névralgique où sont transmis les secrets les plus délicats de nombreuses organisations. Sans mesure de contrôle efficace, les dossiers et les conversations d'une telle nature peuvent tomber entre de mauvaises mains. Il s'agit aussi d'un risque de conformité, d'autant plus que les organismes de réglementation renforcent les lois sur la protection des renseignements personnels des consommateurs.

Les organisations doivent trouver le bon équilibre entre la productivité offerte par ces fonctionnalités et les contrôles de sécurité appropriés. Il s'agit de la pierre angulaire de toute stratégie de gouvernance de l'information. Une planification minutieuse est de mise.

Productivité et sécurité dans Microsoft 365

L'équilibre entre la productivité et la sécurité est en soi une tâche qui comporte des risques. Si les contrôles de sécurité sont trop permissifs, des fuites de données pourraient se produire. Au contraire, s'ils sont trop stricts, les utilisateurs risquent de contourner les politiques pour rester productifs et mener à bien leur travail. Le problème potentiel est donc le ***shadow IT.***

Les entreprises ne peuvent pas compter sur Microsoft pour trouver un équilibre entre la productivité et la sécurité. Les fonctionnalités de M365 se concentrent surtout sur l'échange d'information, et moins sur la gestion des risques. Les besoins de chaque organisation étant différents; puisqu'ils dépendent du secteur industriel et de la région administrative d'appartenance, ainsi que de la taille de l'entreprise, les paramètres par défaut ne permettent pas d'atteindre l'équilibre parfait entre productivité et sécurité. Chaque organisation doit trouver son propre profil de risque et fixer les contrôles de sécurité de façon appropriée.

Pour trouver cet équilibre délicat, les entreprises doivent corriger plusieurs lacunes communes en matière de gouvernance de l'information:

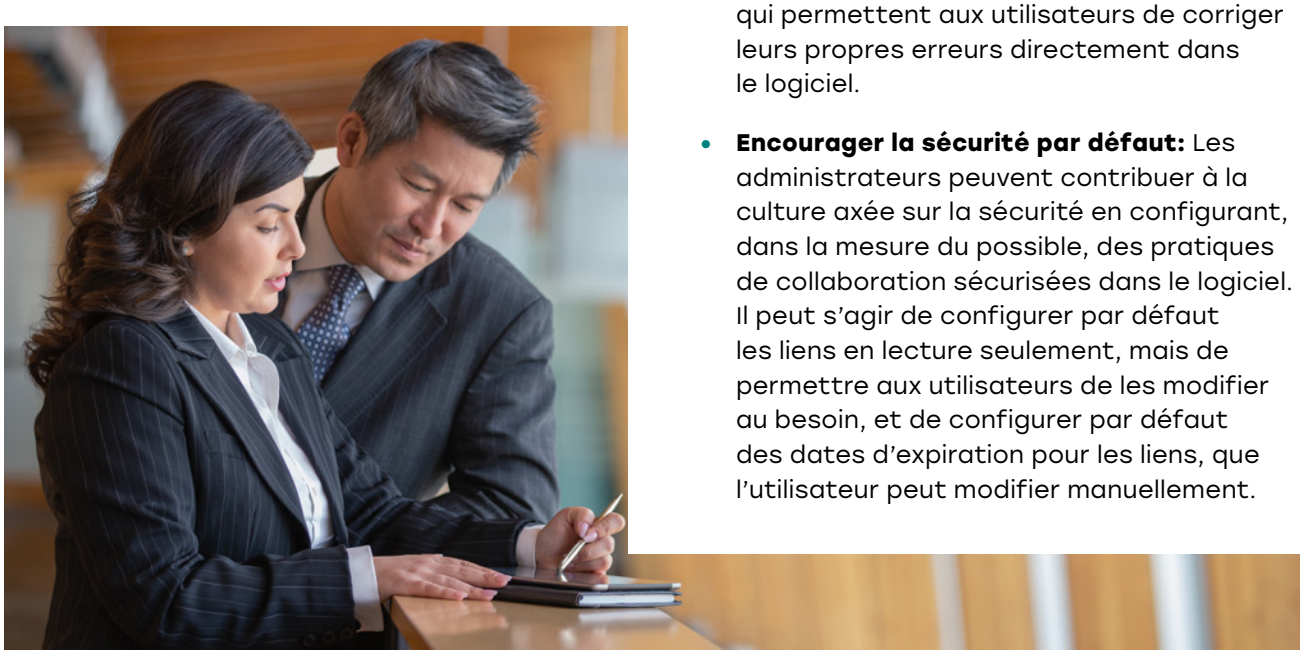
- **Surcharge de collaboration:** Les utilisateurs sont enclins à s'échanger des renseignements dans M365 parce que la plateforme leur permet de créer et d'échanger rapidement des fichiers sur SharePoint, sur OneDrive et dans Teams. Or, bon nombre d'utilisateurs ne connaissent pas les attributs comme la définition d'une date d'expiration pour les fichiers partagés, la restriction des autorisations de modification ou le contrôle des accès externes. Pour cette raison, il arrive parfois que des dossiers deviennent accessibles à un public beaucoup plus vaste que prévu. Un fichier destiné à quelques membres de l'équipe peut devenir accessible à toute l'organisation. Au fil du temps, un tel échange excessif de données non protégées constitue une accumulation ingérable pour les TI.
- **La prolifération de l'information:** M365 facilite la création de sites SharePoint et la communication de documents, mais il ne rend pas obligatoire leur gestion ou leur suppression, et il n'existe aucun moyen facile d'obtenir un aperçu clair de toutes les ressources partagées. Le nombre de sites non gérés et de documents partagés augmente au fil du temps et, dans la plupart des cas, la date d'expiration n'a pas été définie.
- **L'absence de classification des données:** De nombreuses entreprises ne disposent pas de cadre de classification des données qui les orientent dans la gestion en amont des données en fonction de leur sensibilité. De plus, elles n'ont pas non plus les compétences nécessaires pour mettre en œuvre un tel cadre.
- **Formation inadéquate des utilisateurs:** Souvent, les utilisateurs n'ont pas reçu de formation sur le traitement quotidien des données. Même dans le cas où les utilisateurs suivent une formation de sensibilisation, celle-ci est souvent peu fréquente, ce qui fait que les utilisateurs n'en tiennent pas compte dans leurs comportements quotidiens.
- **La culture du blâme:** Une culture où les utilisateurs sont blâmés pour des violations de la politique est source d'inquiétude et les dissuade de se dénoncer eux-mêmes. Il s'agit du même type de réaction néfaste qui caractérise les exercices relatifs à un faux hameçonnage conçus pour évaluer la sensibilisation des utilisateurs.

Changement d'approche en matière de cybersécurité

Pour corriger des lacunes en matière de gouvernance comme celles que nous avons mentionnées, les entreprises doivent changer leur approche relative à la sécurité de l'information et au rôle que jouent les employés.

Les administrateurs peuvent éviter de nombreux problèmes d'accès et d'échange d'information en s'assurant que les utilisateurs disposent des autorisations appropriées. Ils peuvent surveiller régulièrement les autorisations pour s'assurer qu'elles conviennent aux rôles attribués aux utilisateurs et révoquer les autorisations abusives.

Pour aller plus loin, les organisations doivent repenser leur perception des utilisateurs. Au lieu de les considérer comme faisant partie du problème, pour ce qui est de la gouvernance de l'information, il est temps qu'elles les considèrent comme faisant partie de la solution. Pour ce faire, il faut créer une culture collaborative fondée sur la gestion collective des risques, où les utilisateurs partagent la responsabilité en lien avec les risques.



La promotion d'une culture de sécurité et de gestion collective des risques comporte plusieurs changements:

- **Habiliter les utilisateurs:** Faire participer les utilisateurs à la prise de décisions relatives aux risques liés à l'information qu'ils communiquent.
- **Faciliter la tâche:** Faire en sorte qu'il soit facile pour les utilisateurs de suivre les bonnes pratiques en matière d'échange sécurisé de renseignements au moment de la communication. Envisager d'utiliser des outils qui stimulent un changement de comportement (voir l'encadré).
- **Récompenser au lieu de punir:** Au lieu de punir les utilisateurs pour leurs erreurs, il faut les récompenser pour les gestes positifs qu'ils posent. La ludification est un outil puissant qui permet aux gens de souligner leurs bons coups. Il faut toutefois faire attention de ne pas l'utiliser pour attacher de la honte aux échecs.
- **Se concentrer sur l'apprentissage des erreurs:** Mieux encore, utiliser des outils de collaboration sécurisés faciles à utiliser qui permettent aux utilisateurs de corriger leurs propres erreurs directement dans le logiciel.
- **Encourager la sécurité par défaut:** Les administrateurs peuvent contribuer à la culture axée sur la sécurité en configurant, dans la mesure du possible, des pratiques de collaboration sécurisées dans le logiciel. Il peut s'agir de configurer par défaut les liens en lecture seulement, mais de permettre aux utilisateurs de les modifier au besoin, et de configurer par défaut des dates d'expiration pour les liens, que l'utilisateur peut modifier manuellement.

Le facteur de l'IA: méthodes de gouvernance relatives à l'IA et à Microsoft 365 Copilot

L'intelligence artificielle est devenue omniprésente dans M365, au point que, en janvier 2025, Microsoft a renommé sa suite pour Microsoft 365 Copilot. La mise en œuvre de cette technologie offre de nouvelles fonctionnalités puissantes, notamment dans des domaines tels que la recherche d'information. Cela dit, ces fonctionnalités comportent également des risques..

Comment l'IA amplifie les risques liés à l'information

M365 Copilot compte beaucoup sur une structure de données de type graphe et sur la recherche sémantique, ce qui en fait un puissant outil de recherche d'information. De cette manière, il peut trouver des données auxquelles l'utilisateur avait accès sans le savoir, en se fondant sur l'appartenance à différentes équipes et sur les relations avec les autres utilisateurs. Sa capacité à chercher des éléments dans des données non structurées le rend encore plus performant dans la recherche de données sensibles, comme des documents financiers ou des dossiers des ressources humaines (RH). Cela ouvre la porte à une vaste gamme de documents sensibles qui avaient été communiqués il y a longtemps, qui peuvent être découverts par inadvertance.

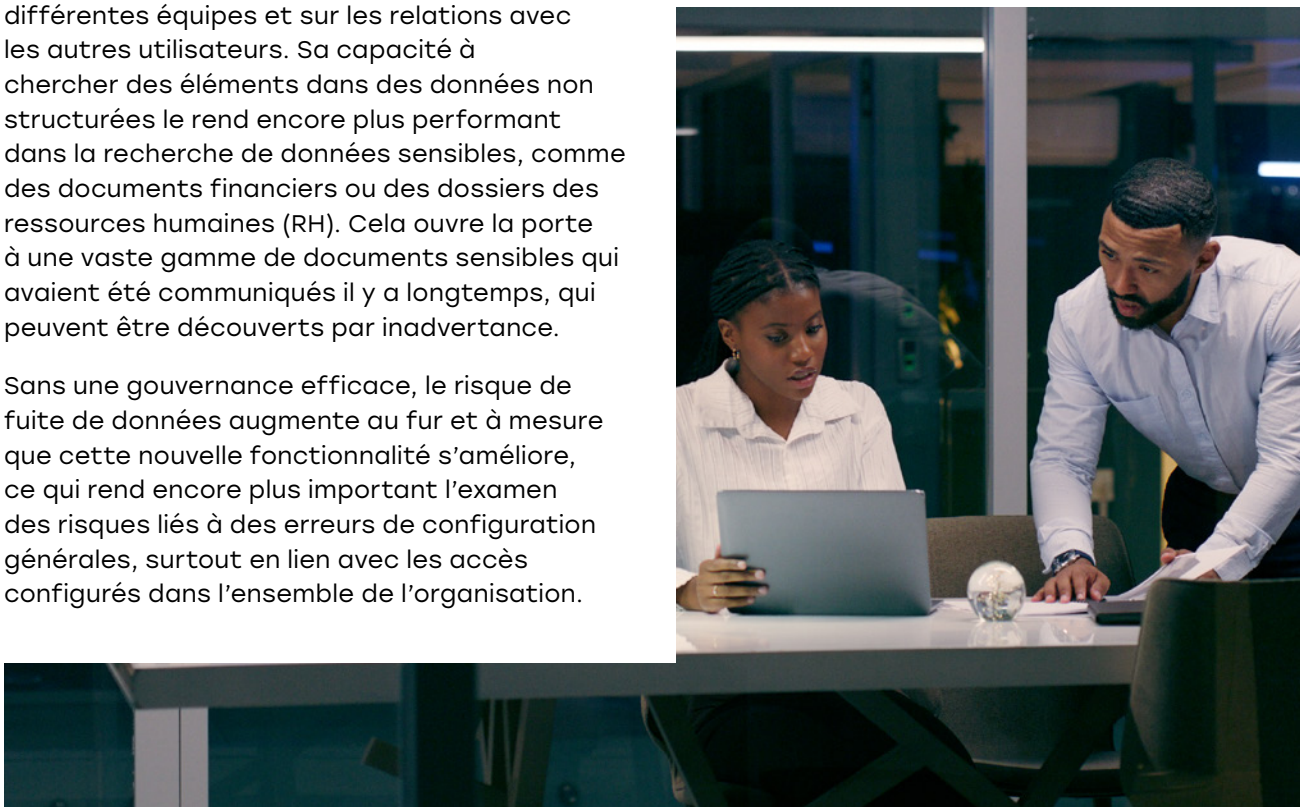
Sans une gouvernance efficace, le risque de fuite de données augmente au fur et à mesure que cette nouvelle fonctionnalité s'améliore, ce qui rend encore plus important l'examen des risques liés à des erreurs de configuration générales, surtout en lien avec les accès configurés dans l'ensemble de l'organisation.

Les fondements de l'adoption sécuritaire de l'IA

Comme la plupart des technologies habilitantes, l'IA peut être une arme à double tranchant. Avec les bonnes mesures de gouvernance (voir l'encadré), l'IA peut stimuler la productivité. Étant donné la grande portée de cette technologie, la haute direction doit donner des instructions quant à sa mise en œuvre.

Et ensuite?

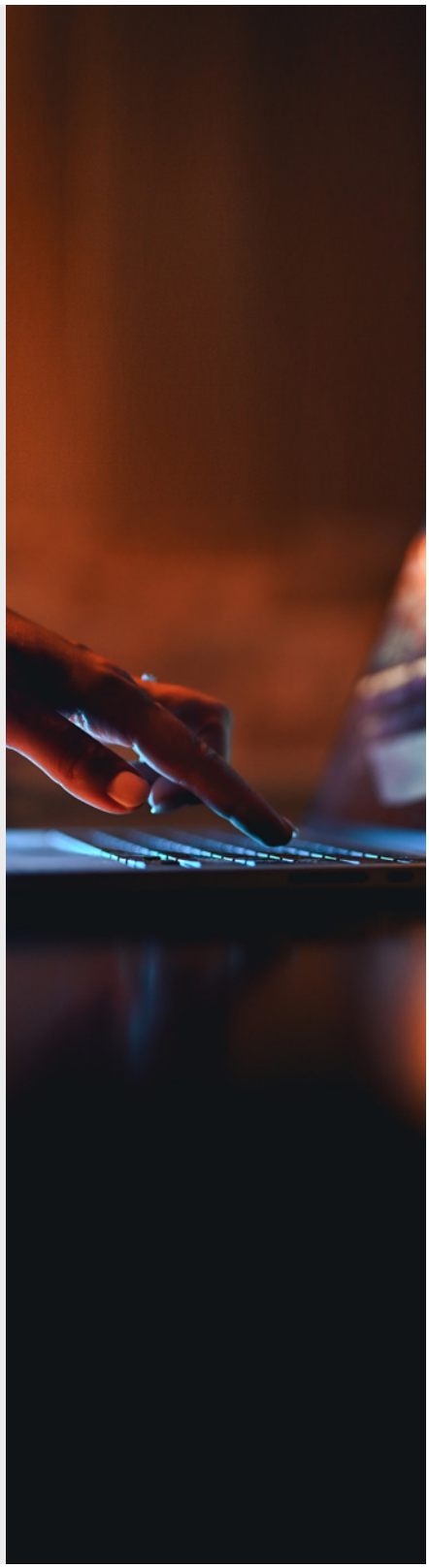
Les forces de Microsoft 365 en ce qui concerne la collaboration peuvent facilement devenir une faiblesse sans les bonnes mesures de gouvernance. Une gouvernance efficace doit faire des individus un élément essentiel de la culture de sécurité. Une telle façon de faire fonctionne mieux lorsque les individus reçoivent des messages contextuels qui les incitent à prendre les bonnes mesures, plutôt que des sanctions en cas d'erreur.



Liste de vérification: votre guide sur des mesures de gouvernance rapides à mettre en œuvre

La gouvernance de l'information peut être intimidante, mais si nous la divisons en ses éléments constitutifs, elle est plus facile à gérer. Votre stratégie devrait tenir compte des étapes suivantes:

- **Gérer les risques:** Harmoniser vos besoins en matière de conformité avec les besoins de gestion des risques propres à votre organisation pour créer une stratégie de gouvernance de l'information unifiée.
- **Dresser l'inventaire de l'information:** Répertorier les liens de partage actifs et recenser les données sensibles.
- **Créer des politiques:** Valider les bonnes politiques dans des domaines comme l'accès et l'expiration du lien, la classification des données et l'application automatisée des politiques. Adapter ces politiques en fonction du volume et de la sensibilité des données protégées.
- **Appliquer des pratiques de gestion collective des risques:** Après la mise en œuvre des politiques, commencer à partager la responsabilité de la gouvernance de l'information parmi les différents services.
- **Prévoir des mécanismes de collaboration sécuritaire:** Prévoir une formation efficace et facile à suivre à l'intention des utilisateurs qui interviennent dans des phases qui comportent des risques pour promouvoir une collaboration sécuritaire.
- **Adopter l'IA progressivement:** Après la conception d'une solide stratégie de gouvernance relative à l'IA, commencer à adopter progressivement cette technologie dans M365.
- **Assurer la surveillance et l'amélioration:** Enfin, créer une culture d'amélioration continue au moyen d'évaluations régulières et de correctifs apportés en lien avec des utilisateurs précis. Choisir des indicateurs représentatifs pour mesurer le changement de comportement.



Les organisations qui comptent tirer parti de l'IA dans M365 doivent mettre en œuvre un régime de gouvernance en amont, car il s'agit d'une technologie qui amplifie les lacunes relatives à la configuration propres au logiciel. Il se peut que de nombreuses organisations ne sachent même pas que leurs utilisateurs aient déjà commencé à utiliser l'IA. Elles seront donc déjà en retard.

Communiquez avec WeActis aujourd'hui pour participer à une démonstration où nous vous montrerons la façon dont nous pouvons vous aider à renforcer l'hygiène des données dans M365, à réduire les risques liés à l'adoption de l'IA et à protéger votre organisation en encourageant vos employés à adopter des comportements sécuritaires. Grâce aux notifications de WeActis, envoyées directement à travers Microsoft Teams, vos employés prennent des actions concrètes telles que la révocation des accès ou des partages et la suppression de données sensibles sur leur poste de travail dont ils ne se servent plus.

L'aspect que revêt la sécurité axée sur le comportement dans la pratique:

Un directeur financier communique accidentellement une feuille de calcul qui contient tous les détails sensibles sur la rémunération des employés. Il oublie de limiter l'accès au service des RH, et toute personne ayant le lien peut consulter les données. Le fichier circule, perturbe le moral et cause des maux de tête aux RH.

Un outil de sécurité de l'information axé sur le comportement aurait rappelé au directeur financier de limiter les autorisations de communication à des personnes précises et de définir l'expiration automatique du lien.

L'importance des programmes de sécurité axés sur le comportement

Les programmes de sécurité axés sur le comportement aident à mobiliser les utilisateurs qui interviennent dans des phases qui comportent des risques et permettent d'atteindre des résultats positifs en matière de sécurité. Voici le fonctionnement de ces programmes:

- **Le contexte est essentiel:** Les programmes de sécurité axée sur le comportement utilisent des messages contextuels basés sur le principe du « coup de pouce », dans les phases qui comportent des risques. Il s'agit notamment de messages qui rappellent de configurer l'expiration.
- **La politique est intégrée dans le système:** La transmission de ces messages et suggestions vous permet d'appliquer les politiques de sécurité dans leur contexte. Une telle transmission s'adapte à des cas de figure opérationnels précis et facilite le processus pour les utilisateurs.
- **Meilleures mesures:** La collecte de mesures comportementales plus globales, comme le nombre de liens révoqués ou l'engagement par utilisateur, donne un meilleur portrait du rendement par rapport à la simple mesure du taux de clics durant de faux tests d'hameçonnage.

WeActis
par Mondata

À propos de WeActis

WeActis révolutionne la cybersécurité en transformant les employés en contributeurs actifs, et en faisant de la sécurité une responsabilité collective, et non pas un fardeau informatique. Intégrée à Microsoft Teams, l'application WeActis encourage les employés à prendre des actions sécuritaires simples permettant de diminuer les risques de leur organisation en moins de cinq minutes par semaine. En améliorant l'hygiène des données dans Microsoft 365, en renforçant la gouvernance et en simplifiant la réduction des risques, WeActis aide les organisations à bâtir une culture de cyberrésilience, ce qui améliore la conformité, réduit l'exposition des données et porte à des améliorations mesurables et durables en matière de sécurité.