



Comprendre le cyberrisque

Sondage sur la culture du cyberrisque

Diagnostic de la culture des sociétés destiné à atténuer le risque

La majorité des atteintes à la sécurité informatique résultant d'une erreur ou d'un comportement humain (qu'il s'agisse d'actes négligents ou malveillants), de nombreuses organisations ont intérêt à cerner les causes profondes de ce comportement et les aspects de la culture organisationnelle qui peuvent contribuer à compromettre la sécurité informatique. Forte de son expertise combinée en matière de capital humain et de solutions de gestion des cyberrisques, Willis Towers Watson offre un aperçu du risque lié aux personnes et elle est bien placée pour aider ses clients à faire face aux failles informatiques créées par leur main-d'œuvre.

Les sources de cyberrisque peuvent comprendre le manque de sensibilisation des employés, un sens des responsabilités insuffisant, une mauvaise compréhension des étapes prises par l'organisation pour s'occuper de la cybersécurité et un faible « cyber-QI », tout cela entraînant des comportements qui augmentent l'exposition au risque des systèmes et des processus internes. Les défauts de sécurité peuvent être présents à l'échelle de l'organisation ou dans certains secteurs.

Comment le comportement des employés peut entraîner un cyberrisque

- La négligence et les actes malveillants des employés sont la source de cinquante-huit pour cent des cyberattaques¹.
- Certains aspects cruciaux de l'expérience des employés font défaut chez les sociétés victimes de cyberattaques, notamment :
 - la poursuite d'un objectif fondé sur l'orientation client (se traduisant, par exemple, par le souci de répondre aux attentes et d'améliorer les processus);

- une exécution du travail rapide et une souplesse dans la prise de décisions et la gestion d'équipes;
- des pratiques de gestion des ressources humaines qui permettent au personnel de se faire entendre, de se faire respecter et de soutenir le travail d'équipe;
- une formation sur le stress et un perfectionnement en fonction de la rémunération et du rendement².
- La perception qu'ont les entreprises de leur capacité à faire face aux cyberrisques et de leur gouvernance ne se traduit pas par des actions concrètes des employés. Par exemple, près de la moitié des employés pensent qu'ils peuvent ouvrir sans risque n'importe quel courriel reçu sur un ordinateur au travail³.

Ce n'est qu'en enquêtant sur les failles, en sensibilisant les employés et en les faisant passer de la conformité à l'adoption de nouveaux comportements que les organisations pourront commencer à acquérir une compréhension du risque. Prenez les mesures préventives appropriées et progressez sur la voie de l'engagement durable.

¹ Indice des sinistres déclarés en 2017 de Willis Towers Watson.

² Analyse exclusive de Willis Towers Watson des données de sondages auprès des employés en fonction de la norme relative aux entreprises mondiales à rendement élevé et de la norme des fonctions TI des entreprises mondiales.

³ Sondages sur le cyberrisque auprès des employeurs et des employés de 2017 de Willis Towers Watson.

Sondage sur la culture du cyberrisque de Willis Towers Watson

Fruit de la vaste expérience de Willis Towers Watson dans la recherche auprès des employés et la gestion du cyberrisque, son Sondage sur la culture du cyberrisque recueille de l'information directement auprès des employés sur la fréquence des comportements témoignant d'une cybercompétence et sur leurs perceptions des défis que représente le cyberrisque en milieu de travail.

Les résultats obtenus donnent un aperçu de la situation actuelle sur la sensibilisation à la cybersécurité et les actions des employés à l'échelle de l'organisation, et ils indiquent la voie à suivre pour constituer une main-d'œuvre cyberintelligente. Ils procurent aussi de manière précise des renseignements sur la culture du risque dans l'organisation et permettent à la haute direction de prendre des mesures décisives pour la création de solutions.

Options de mise en œuvre :

1. Indice de vulnérabilité (compris dans le sondage existant sur la mobilisation des employés)
2. Sondage éclair (à effectuer vous-même, il peut être distribué à des groupes précis)
3. Sondage complet (plus de 100 questions qui peuvent être personnalisées)

Des rapports peuvent être créés pour la haute direction.

Fournir à la direction des renseignements clés

- Fournissez à vos dirigeants des données comparatives sur l'atteinte à la sécurité des données qui permettent de hiérarchiser les enjeux liés à la culture organisationnelle

Base de données mondiale regroupant les données recueillies auprès de **1,3 million** de répondants issus d'entreprises ayant subi un **cyberincident**.



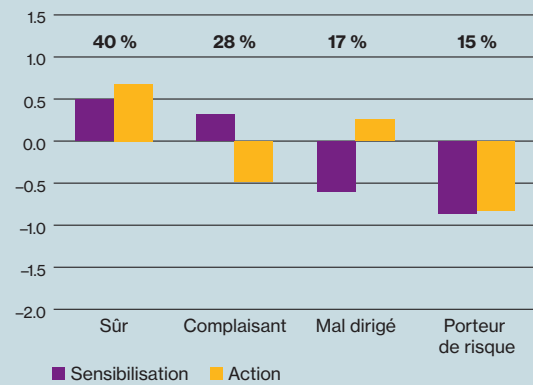
- Obtenez des suggestions d'amélioration directement auprès des employés

Deux questions à développement sur mesure :

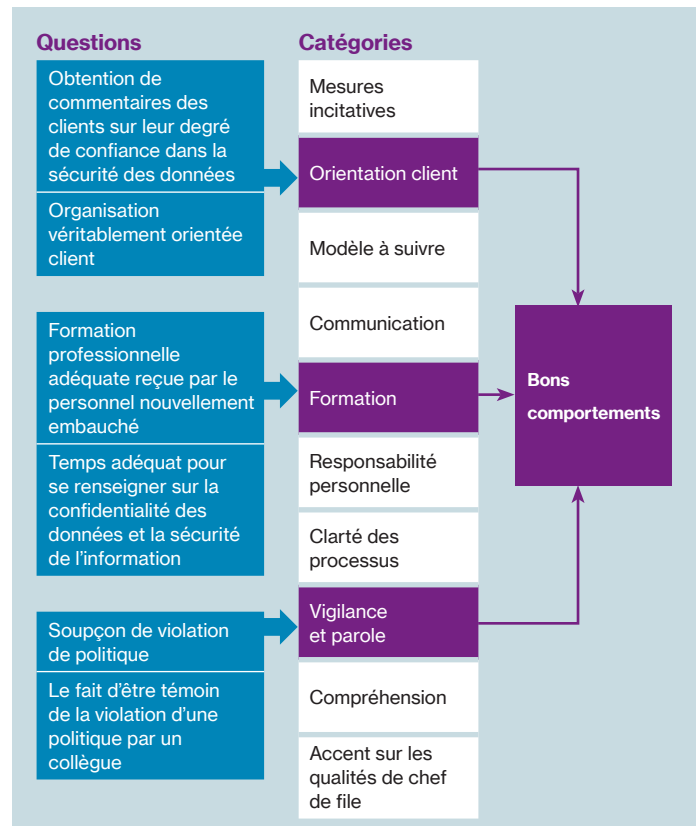
1 Que faisons-nous actuellement qui fonctionne bien pour gérer les risques liés à la confidentialité des données et à la sécurité de l'information?

2 Quelles mesures devrions-nous prendre au cours des 12 prochains mois pour réduire ces risques?

- **Segmentez votre main-d'œuvre pour cibler les employés qui sont porteurs de risque**

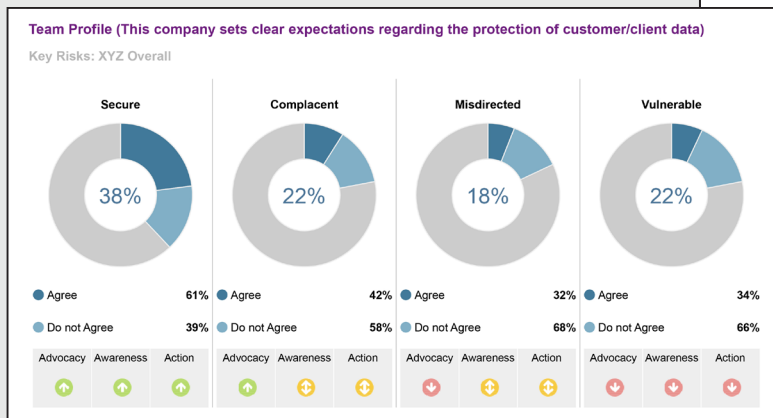
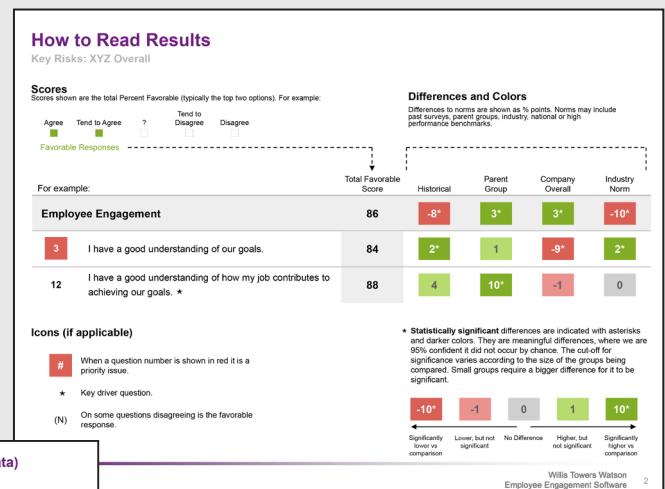
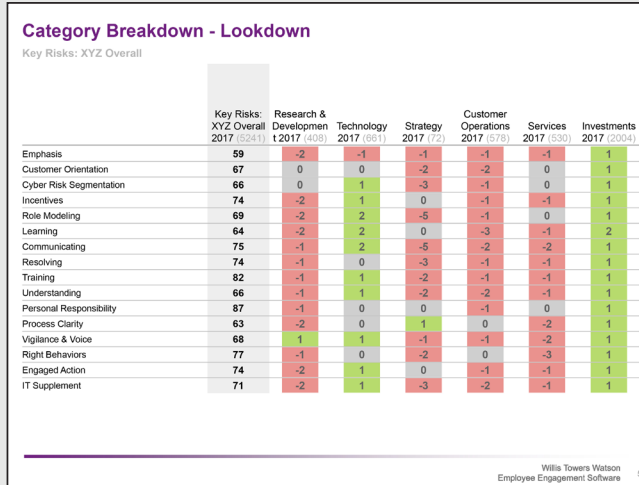


- **Établissez quelles expériences suscitent un comportement exemplaire**



Les rapports sont riches de renseignements sur la culture du cyberrisque grâce auxquels vous pouvez :

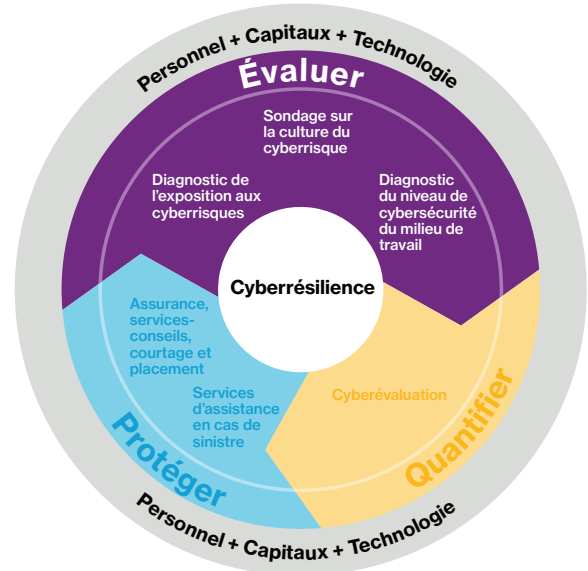
- Cibler les employés les plus susceptibles de causer un cyberincident et prédire la fréquence des cybercomportements à risque élevé.
- Catégoriser ces employés géographiquement et selon leur fonction, leur titre ou leur rôle – ce qui permet de définir efficacement un plan d'atténuation des risques approprié.
- Donner la priorité à l'action afin d'encourager la main-d'œuvre à devenir « cybercompétente » au lieu d'être motivée uniquement par l'obligation de se conformer à des politiques.
- Définir le « risque humain » dans la chaîne d'approvisionnement en incluant les fournisseurs et d'autres partenaires commerciaux dans vos considérations.



	Total Favourable	Breached Companies Norm
Training	82	11*
40 I have adequate time at work to learn about data privacy and information security risks.	87	n/a
41 I receive regular training on how to protect customer/client information.	96	n/a
42 I have been well trained in understanding the data privacy and information security risks relevant to my job.	94	n/a
43 Employees new to my department receive adequate training for their jobs.	67	n/a
44 The training I have received has adequately prepared me for the work I do.	67	3*
45 There are sufficient opportunities for me to receive training to increase my eligibility for a better job.	82	19*

Pourquoi Willis Towers Watson?

Plus de la moitié des cyberincidents ont pour cause première les employés, de sorte qu'il s'agit d'un problème d'origine humaine. Comme les cyberattaques coûtent en moyenne quatre millions de dollars, le problème est également de nature financière. Personne ne comprend mieux cette réalité complexe que Willis Towers Watson. À titre de société mondiale de premier plan en matière de solutions axées sur le capital humain, de services-conseils en gestion des risques et de courtage, nous sommes en mesure d'évaluer vos failles en matière de cybersécurité, de vous protéger au moyen de solutions de pointe et d'améliorer considérablement votre capacité à surmonter avec succès des attaques futures. Prenez connaissance de nos solutions de cybersécurité complètes à l'adresse willistowerswatson.com/cyber.



À propos de Willis Towers Watson

Willis Towers Watson (NASDAQ : WLTW) est une société mondiale de premier plan en services-conseils, en courtage et en solutions qui aide ses clients partout dans le monde à transformer le risque en parcours de croissance. Nos racines remontent à 1828, et Willis Towers Watson compte 45 000 employés dans plus de 140 pays et marchés. Nous concevons et réalisons des solutions qui permettent de gérer le risque, d'optimiser les avantages sociaux, de cultiver les talents et d'augmenter la capacité des capitaux afin de protéger les organisations et les personnes, et de les rendre plus solides. Notre vision unique nous permet de reconnaître ce qui se trouve aux carrefours stratégiques entre les talents, les actifs et les idées, la formule dynamique qui favorise les résultats d'entreprise. Ensemble, réalisons votre potentiel. Consultez notre site à l'adresse willistowerswatson.com.

Pour en savoir plus

Patrick Kulesa

+1 212 309-3746

patrick.kulesa@willistowerswatson.com

Kelly Harkcom

+1 312 288-7131

kelly.harkcom@willistowerswatson.com



<https://www.willistowerswatson.com/fr-CA/social-media>

© Willis Towers Watson, 2019. Tous droits réservés.
WTW-NA-2019-WTW222047

willistowerswatson.com

Willis Towers Watson