

LE RESPONSABLE DES RISQUES TECHNOLOGIQUES



Introduction au risque technologique

Presque toutes les entreprises modernes utilisent la technologie dans une certaine mesure pour améliorer la gestion de leurs produits et de leurs services. Bien que l'élimination des méthodes manuelles atténue certains risques opérationnels en soi, elle introduit également d'autres menaces.

Le risque technologique désigne la probabilité d'une panne logicielle qui peut nuire au paysage système d'une entreprise. Grâce à une évaluation adéquate, les entreprises peuvent atténuer ces risques technologiques et optimiser leur veille d'affaires .

Qu'est-ce que le risque technologique?

Dans le domaine de l'entreprise, le risque technologique est la menace d'une défaillance de la technologie de gestion qui pourrait compromettre la cybersécurité et le renseignement décisionnel. Ce cyber risque peut prendre de nombreuses formes, notamment des inefficacités, des vols et des logiciels malveillants. Cependant, les principales menaces concernent l'architecture logicielle, l'outillage, la livraison et la maintenance.

Ces types de risques rendent la gestion des risques technologiques essentielle pour les entreprises modernes qui utilisent des processus internes automatisés. La gestion proactive des risques technologiques permet d'identifier et d'atténuer les menaces émergentes avant qu'elles n'aient une chance de compromettre l'intelligence décisionnelle. Cela minimise l'effet de boule de neige lorsque des erreurs mineures inaperçues s'accumulent jusqu'à des dommages irréconciliables.

Architecture logicielle

Selon la solution, l'architecture logicielle peut être obsolète, créant des inefficacités inutiles. L'ancienne infrastructure peut siloter les données, dissocier les services et restreindre le partage des données, ce qui rend impossible la compilation précise des données.

Lorsque les systèmes stockent des informations séparément, ils ont tendance à différer dans leur format et à exposer l'entreprise à des risques gonflés de vol. Les données non traitées rendent encore plus difficile la génération de rapports et de diagnostics.

Outillage

De nombreux systèmes hérités utilisent également l'outillage, qui établit un vaste ensemble de fonctionnalités diverses applicables à différents services. Bien qu'un large éventail d'outils puisse sembler attrayant, il est également coûteux et peut rendre difficile la formation des employés. Certains outils peuvent même nécessiter un matériel supplémentaire à utiliser, ce qui ajoute des dépenses d'exploitation supplémentaires.

Livraison et entretien

Les solutions qui nécessitent une intervention humaine intensive pour mettre en œuvre augmentent le risque d'erreur humaine et d'erreurs de connexions. Cela suppose une maintenance future importante, qui peut consommer beaucoup de temps, d'énergie et de ressources. Par conséquent, les entreprises peuvent avoir de la difficulté à s'adapter à l'évolution de la technologie.

Avantages d'une évaluation des risques technologiques

En effectuant régulièrement des évaluations des risques technologiques, les entreprises peuvent minimiser l'impact des menaces et renforcer la sécurité logicielle. Toutefois, les évaluations des risques de l'entreprise procurent également plusieurs autres avantages aux organisations.

Coûts réduits

Les entreprises qui tiennent un calendrier d'évaluation des risques technologiques peuvent éviter des coûts inutiles pour résoudre les problèmes technologiques. Les responsables informatiques peuvent également effectuer des évaluations avant d'implémenter un système pour s'assurer qu'il répond aux besoins actuels de l'entreprise. Sinon, les entreprises pourraient finir par payer pour plusieurs systèmes qui reproduisent certains processus et négligent d'autres.

Risques minimisés

Les systèmes automatisés reposent sur la technologie sous-jacente que les entreprises doivent tenir à jour pour éviter que des faiblesses ne se forment dans les pare-feu. Un logiciel obsolète peut également déclencher des problèmes supplémentaires s'il se connecte à d'autres systèmes existants. Cela peut créer un goulot d'étranglement, retardant les opérations séquentielles et allongeant les temps d'arrêt du système. Grâce à l'évaluation des risques technologiques, les gestionnaires peuvent rapidement détecter et éliminer les risques.

Agilité améliorée

De nombreuses entreprises craignent qu'avec l'automatisation, elles perdent leur autorité et leur contrôle sur les systèmes internes. Toutefois, les évaluations des risques opérationnels accroissent l'agilité et la réactivité des entreprises aux activités internes. En fait, l'automatisation donne aux propriétaires la possibilité de standardiser diverses tâches afin de rationaliser les opérations et le flux de travail.

Étapes de l'évaluation des risques technologiques

La réalisation d'une évaluation des risques technologiques est exhaustive, mais nécessite du temps et de l'attention aux détails.

1. Liste des applications potentielles

Tout d'abord, les chefs de projet doivent décrire tous les systèmes internes établis, y compris les intégrateurs de solutions et d'autres technologies sous-jacentes. Les services informatiques adéquats devraient disposer d'un document permanent qui enregistre chaque logiciel au moment de la mise en œuvre. En définissant le nouveau paysage technologique, les entreprises peuvent examiner chaque élément au cours de l'évaluation.

2. Évaluer le logiciel

Les gestionnaires doivent ensuite évaluer les versions des logiciels utilisés par chaque ministère. Certaines entreprises se procurent la technologie d'un seul fournisseur de services principal qui dispose de plusieurs versions du même logiciel de base. Grâce à la même infrastructure, les entreprises peuvent implémenter des solutions de comptabilité, de gestion des stocks et de points de vente. Cela garantit que tous les systèmes peuvent s'intégrer de manière transparente et partager des données.

3. Évaluer les serveurs et les centres de données

Ensuite, les responsables doivent évaluer leurs serveurs de données et leurs centres pour déterminer leur capacité et leurs limites. De nombreux fournisseurs recommandent d'affecter des piles technologiques à chaque serveur afin d'optimiser les fonctionnalités des centres de données. Une pile technologique, ou écosystème de données, répertorie tous les

4. Connecter les logiciels et les applications

Après avoir localisé toutes les solutions, il est temps de cartographier le flux de données dans toute l'entreprise. En illustrant le paysage technologique, les développeurs peuvent connecter des logiciels et des serveurs disjoints pour un échange de données efficace. Cela permet également aux gestionnaires de définir les dépendances, les goulets d'étranglement et les inefficacités.

5. Déterminer l'impact du logiciel

Enfin, les entreprises doivent définir la probabilité et l'impact potentiel des risques sur leur infrastructure. Par exemple, si les entreprises ne sont pas en mesure de relier leurs systèmes existants, elles risquent de manquer des données qui se situent entre les secteurs. D'autres organisations peuvent être exposées à un risque de détérioration des données à moins qu'elles ne mettent à jour leur logiciel.