Sommaire

INTRODUCTION

Notre sujet est très pertinent au moment opportun et surtout dans le contexte de notre matière l'audit des systèmes d'informations.

La transformation digitale est devenue un incontournable pour une entreprise ou n'importe quel type d'organisation.

En effet, elle s'applique à tous les domaines et assure une optimisation de temps et d'argent en automatisant des tâches de plus en plus complexes.

Certes les systèmes d'informations ont énormément de bienfaits et d'avantages, or que ses derniers peuvent devenir une source très dangereuse de vulnérabilités à travers leurs inconvénients.

1- Définition de la transformation digitale d'une organisation :

La transformation digitale est le processus qui consiste à remplacer complètement les processus métier manuels existants par les toutes dernières alternatives numériques. Ce type de réinvention touche tous les aspects d'une entreprise, et pas seulement les technologies.

Avec une bonne stratégie de communication digitale, l'entreprise est en mesure de discuter avec un nombre conséquent de prospects instantanément. La transformation digitale permet donc de faciliter l'échange et les interactions avec les différents prospects et clients.

La transformation digitale aide une organisation à être plus compétitive dans un paysage économique qui change constamment au fur et à mesure que la technologie évolue.

2- les risques liés à la transformation digitale :

a. Les risques liés à la gouvernance des données

Les technologies digitales mobiles et réseaux sociaux favorisent la génération de données à l'insu de l'individu. La collecte, le partage et l'analyse de ces données constituent un risque pour l'entreprise surtout lorsqu'il s'agit de données médicales, financières ou autres données sensibles. Dans ce sens, une entreprise opérant dans le domaine du bâtiment utilise des drones pour inspecter les façades des édifices. ces objets connectés peuvent être intrusifs pour les citoyens et présenter des risques de non-conformité en termes de protection des données pour l'entreprise. Aussi, notre exploration du secteur de la santé a mis en évidence que cette problématique de confidentialité peut même entraver la collaboration entre les fournisseurs de soins et les développeurs de technologies spécialisées.

Par ailleurs, le problème de débordement par les données en cas de mauvaise gestion des canaux de génération et des flux de diffusion est très présent surtout dans le domaine de la banque-assurance. Un multinational leader dans le secteur a souligné que la technologie Cloud peut être utile pour piloter ce cycle d'exploitation des données, mais qu'en même temps elle soulève des défis de souveraineté des données.

b. Les risques liés aux relations avec des parties internes

Le digital ouvre à d'autres parties prenantes (client, fournisseur, partenaire, etc.), et donc à plus de risques en termes de gestion de ces relations. Dans ce sens, une entreprise en logistique maritime a mentionné que l'usage de la technologie blockchain pour établir des smart contracts a entraîné beaucoup de formalité et de rigidité dans ses relations client-fournisseur.

c. Les risques liés au pilotage des technologies digitales

La nature récente des technologies digitales met en difficulté la plupart des entreprises. La direction des systèmes d'information (DSI) doit rapidement maîtriser ces technologies pour répondre aux exigences instantanées des métiers, En effet, plusieurs départements ont déployé des solutions facilement accessibles pour subvenir à leurs besoins de transformation, ce qui a résulté en un souci de gouvernance de l'infrastructure technologique.

Cette maîtrise rapide des technologies digitales n'est pas toujours évidente, surtout que le développement de compétences digitales peut être rallongé en cas de pénurie d'experts, comme c'était le cas d'une entreprise opérant dans le secteur logistique. Ce développement de compétences implique des investissements conséquents en termes de temps, d'efforts et de coûts, qui peuvent rapidement être vains en raison de l'évolutivité et l'obsolescence fréquente des technologies digitales. Ce risque est hautement présent dans le secteur militaire, où les technologies digitales sont conçues sur mesure et doivent garantir un

minimum de durabilité pour amortir leurs coûts de développement, mais aussi dans le secteur agricole qui est caractérisé par une forte vulnérabilité des objets connectés utilisés.

3-Comment peut-on faire face à ces risques :

Il faut concevoir la maîtrise des risques comme un outil de gouvernance et pas comme une énième couche intermédiaire de procédures qui alourdissent le fonctionnement de l'entreprise. Le management des risques doit être structuré selon le triptyque suivant : avant, pendant et après.

Avant, on cherche de manière structurée et à fréquence optimisée à identifier les incertitudes et évaluer les risques associés aux événements avant que ceux-ci ne se produisent, pour prévenir les problèmes et en réduire l'impact et s'y préparer.

Pendant, c'est la gestion de crise

Après, c'est le retour d'expérience : apprendre de ses erreurs mais aussi apprendre de ses succès, et rendre ce savoir acquis disponible pour l'ensemble de l'entreprise.

Toute stratégie de gestion des risques numériques devrait intégrer les fondamentaux ci-après :

1. Prendre la mesure du risque numérique en tant que risque stratégique d'entreprise ;
2. Inscrire la sécurité numérique au cœur de sa gouvernance d'entreprise ;
3. Bâtir progressivement son socle de sécurité en termes de protection, défense et résilience ;
4. Piloter son risque (amélioration continue, veille sur la menace, audits de sécurité) ;

5. Tester régulièrement sa résilience grâce à des exercices de gestion de crise ;

6. Valoriser son cyber sécurité pour générer de la confiance auprès des clients et partenaires, et en faire un atout de compétitivité.

Le management des risques doit être explicite, inclusif et non punitif. Le pire c'est de cacher les problèmes. Et sans inclure l'ensemble des acteurs d'un système dans ce management, ça ne peut être que voué à l'échec : le management des risques est la résultante des efforts de chacun.

Conclusion

Ces trois classes de risques mettent ainsi en évidence des problématiques liées à certaines technologies digitales en particulier, mais aussi des défis induits par la nature interconnectée de ces technologies et leur usage simultané. Il est primordial de sensibiliser les praticiens envers ces risques à anticiper pour tirer profit de leurs investissements en transformation digitale. La transformation va justement au-delà de la pensée fonctionnelle et aborde les opportunités mais aussi les risques associés au changement.