Risque positif dans le cadre de la cybersécurité

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Risque positif dans le cadre de la cybersécurité

Table of Contents

Introduction 1
Avantages des risques positifs 3
Promotion des résultats positifs 3
Renforcement de la sécurité 4
Modification du langage des risques 6
Augmentation de l'adoption 7
Exemples de risques positifs 8
Risque positif en matière de technologie 8
Risque positif en matière de gestion de projet 8
Risque positif en matière de cybersécurité 8
Réponse aux risques liés à la cybersécurité 10
Étapes suivantes 13
FAQ 14
Risque à la hausse et positif 14
Importance 14
Ressources 15
Historique du document 16
..... xvii

Risque positif dans le cadre de la cybersécurité

Greg Bell, Amazon Web Services (AWS)

Mai 2022 (historique du document)

Généralement, le risque est perçu de manière négative, comme l'exposition à une perte ou la gestion d'un événement défavorable. Cependant, l'Organisation internationale de normalisation (ISO) définit le risque comme « l'effet de l'incertitude sur les objectifs ». Dans ce cas, l'effet peut être positif ou négatif.

Les risques réels peuvent varier d'un secteur à l'autre, mais cette définition standard s'applique à tous, et chaque secteur d'activité présente à la fois des risques négatifs et positifs. Dans le secteur de la cybersécurité, le risque négatif fait référence à une perte potentielle, tandis que le risque positif fait référence au gain potentiel d'actifs, de connaissances, d'améliorations ou de données.

Les domaines de la gestion de projet et de l'informatique ont adopté la stratégie qui consiste à évaluer les risques positifs dans les rapports métier et les décisions métier. Cependant, le secteur de la cybersécurité ne l'a pas encore adoptée comme pratique courante, et de nombreuses méthodologies de gestion des risques continuent de se concentrer sur les risques négatifs. Si elles parlent d'un risque positif, ce n'est que brièvement.

Traditionnellement, la cybersécurité considère le risque uniquement sous un angle négatif. Voici les deux types courants de risque négatif dans le domaine de la cybersécurité :

- Risque à la baisse : exposition à des pertes dues à des facteurs externes, tels qu'une menace. Par exemple, les cybercriminels peuvent introduire un incident de sécurité ou en augmenter la probabilité.
- Risque à la hausse : exposition à une perte dans le but de réaliser un gain, comme une vulnérabilité résultant du changement. Par exemple, lors de l'implémentation d'une stratégie informatique, vous risquez d'augmenter par inadvertance le risque d'incident de sécurité. Le risque à la hausse n'est pas la même chose qu'un risque positif. Même s'il survient dans le but de réaliser un gain, le risque à la hausse se concentre sur le potentiel de perte.

Jusqu'à récemment, la cybersécurité ne prenait en compte que le risque négatif, tandis que la définition du risque était axée sur un résultat négatif potentiel. Les risques positifs mettent l'accent sur le résultat positif potentiel dès le début de l'identification des risques. L'exclusion des risques positifs empêche de reconnaître les résultats positifs en matière de cybersécurité. En raison de l'importance

accordée aux risques négatifs, les dirigeants considèrent généralement la cybersécurité comme réactive plutôt que proactive et sous-estiment sa contribution aux résultats métier positifs.

Ce document définit les risques positifs pour le secteur de la cybersécurité et décrit les avantages et l'importance d'inclure les risques positifs dans votre stratégie de cybersécurité.

Avantages des risques positifs

En particulier dans un secteur tel que la cybersécurité, qui vise à protéger l'entreprise contre les pertes potentielles, il est facile de cerner le risque lié à une perspective négative. Il peut être bénéfique de cerner les risques en matière de cybersécurité en fonction de leurs gains potentiels pour l'activité en promouvant des résultats positifs, en renforçant la sécurité de l'organisation, ainsi que la confiance des clients.

Promotion des résultats positifs

L'adoption d'un risque positif permet à l'organisation d'évaluer et de reconnaître la contribution du domaine aux résultats métier positifs. Selon Cybersecurity In The C-Suite and Boardroom (rapport de recherche d'Enterprise Strategy Group) :

- 69 % des chefs d'entreprise et des responsables technologiques estiment que la cybersécurité est entièrement ou principalement un domaine technologique peu ou pas lié à l'activité.
- 11 % des chefs d'entreprise et des leaders technologiques assimilent cybersécurité et conformité réglementaire.
- 82 % des entreprises affirment que les risques liés à la cybersécurité ont augmenté au cours des deux dernières années en raison de facteurs tels que l'augmentation des cybermenaces, l'intégration accrue de la technologie au sein de l'activité et l'augmentation de la surface d'attaque.

Lorsque les responsables de la cybersécurité intègrent les risques positifs dans les conversations et les rapports, cela contribue à promouvoir la valeur des opérations informatiques sécurisées au sein de l'entreprise.

Supposons, par exemple, qu'une entreprise ait été victime d'une violation de données il y a plusieurs années, en raison de l'absence de processus de gestion des correctifs. L'incident est toujours évoqué par les médias et il affecte la perception des clients à l'égard de l'entreprise et leurs interactions avec celle-ci. L'entreprise souhaite surmonter l'incident et élargir son offre de services, mais la confiance des clients bloque les ventes. La cybersécurité utilise le risque positif pour convaincre les dirigeants d'investir dans un processus de gestion des correctifs qui met à jour les applications en permanence. Le nouveau processus réduit considérablement le risque de violation de données, en améliorant le niveau de sécurité de l'entreprise. Les informations concernant le processus de gestion des up-to-the-minute correctifs parviennent aux médias et aux clients potentiels. Les clients se sentent

désormais à l'aise lorsqu'ils achètent auprès de l'entreprise, et les ventes augmentent à un niveau impressionnant.

Le fait de ne pas prendre en compte les risques positifs lors de l'identification des risques peut fournir une évaluation incomplète et affecter la décision métier. Pour des exemples concrets de risques positifs susceptibles d'affecter les décisions métier, veuillez consulter Exemples de risques positifs.

Renforcement de la sécurité et de la confiance des clients

La cybersécurité fait partie intégrante de la sécurité de l'entreprise. Les violations de données peuvent nuire à la confiance des clients, mais une sécurité et une réputation solides peuvent également renforcer la confiance des clients et créer des opportunités métier.

Comme indiqué dans Promotion des résultats positifs, des recherches montrent que les dirigeants sont conscients des risques négatifs associés à la cybersécurité, mais qu'ils ne comprennent souvent pas les risques positifs ou la valeur métier. Cependant, des recherches montrent que les dirigeants dans le domaine de la cybersécurité comprennent les avantages qu'un solide niveau de sécurité peut apporter à l'organisation.

Dans La recherche sur la cybersécurité : l'accélérateur de l'innovation (livre blanc de Vodafone), Vodafone a interrogé 1 434 décideurs internationaux dans le domaine de la cybersécurité. Selon les données :

- 73 % des personnes interrogées pensent qu'une sécurité renforcée génère des opportunités métier.
- 89 % ont déclaré que l'amélioration de leur sécurité accroîtrait la fidélité et la confiance des clients.
- 90 % ont également déclaré avoir été en mesure d'améliorer leur image, d'atteindre de nouveaux clients potentiels et d'en faire de véritables clients.
- 89 % pensent qu'une cybersécurité efficace constitue un avantage concurrentiel pertinent, qui les aide à se différencier de leurs concurrents.
- 24 % ont indiqué avoir augmenté leurs revenus en utilisant les technologies cloud et l'Internet des objets (IoT), mais aussi en adoptant des contrôles de sécurité informatique ciblés.
- Au lieu d'utiliser des résultats négatifs potentiels lorsque vous communiquez avec la direction, vous pouvez également utiliser le risque positif pour expliquer la valeur métier que représente l'amélioration de la confiance des clients. Les dirigeants peuvent faire preuve de prudence lorsqu'ils financent des programmes. Dans certains cas, la cybersécurité ne reçoit que le strict minimum nécessaire à son fonctionnement. La communication interne des risques positifs dans

les demandes de financement peut aider vos dirigeants à comprendre la valeur métier liée à la cybersécurité. Cela peut entraîner une augmentation du financement des initiatives de cybersécurité et générer des recettes pour l'entreprise.

Modification du langage des risques en matière de cybersécurité

Le défi que pose l'adoption d'un risque positif pour la cybersécurité tient en partie au fait que la terminologie technique et propre au domaine est axée sur les risques négatifs, tels que les menaces, les vulnérabilités et les contrôles de sécurité. Le secteur de la cybersécurité doit évoluer et élargir son vocabulaire pour inclure un langage qui met l'accent sur les résultats métier positifs (ou les risques positifs) que la cybersécurité apporte à l'entreprise. Des termes tels qu'avantage métier, bénéfices et valeur métier soulignent la contribution de la cybersécurité à l'organisation.

Changer le langage de la cybersécurité contribue à modifier la perception selon laquelle la cybersécurité est un domaine technologique exclusivement axé sur les menaces et les vulnérabilités et qu'elle n'est pas liée à l'activité de l'entreprise. Les dirigeants d'entreprise sous-estiment souvent la contribution de la cybersécurité aux résultats métier positifs. Pour plus d'informations sur la perception de la cybersécurité par les dirigeants, veuillez consulter Promotion des résultats positifs.

Augmentation de l'adoption dans les domaines liés

L'inclusion du risque positif suscite un intérêt croissant dans de nombreux domaines, car elle reconnaît les contributions du domaine aux résultats métier. Le concept de risque positif a récemment été adopté dans les processus et définitions courants de gestion de projet.

En 2013, le Project Management Institute (PMI) a intégré la définition du risque positif (également appelé opportunités) dans la cinquième édition du Project Management Body of Knowledge (PMBOK). Le PMBOK définit le risque individuel comme « une condition ou un événement incertain qui, s'il se produit, a un effet positif ou négatif sur un ou plusieurs objectifs du projet ». Il définit globalement le risque du projet comme « l'effet de l'incertitude sur le projet dans son ensemble… plus que la somme des risques individuels au sein d'un projet, puisqu'il inclut toutes les sources d'incertitude du projet… représente l'exposition des parties prenantes aux implications des variations des résultats du projet, qu'elles soient positives ou négatives ».

Malheureusement, l'inclusion par le PMI des résultats positifs dans ses définitions du risque ne s'applique pas encore au secteur de la cybersécurité.

Exemples de risques positifs

Voici quelques exemples de risques positifs pour la technologie, la gestion de projet et la cybersécurité.

Risque positif en matière de technologie

Un exemple de risque positif en matière de technologie est que l'implémentation d'une technologie pourrait entraîner une réduction du coût salarial. Par exemple :

1. L'implémentation de cette technologie pourrait améliorer l'efficacité des entreprises.
2. Ces gains d'efficacité pourraient entraîner une réduction de la main-d'œuvre.
3. La réduction de la main-d'œuvre pourrait entraîner une réduction du coût salarial.

Risque positif en matière de gestion de projet

Un exemple de risque positif en matière de gestion de projet est qu'une erreur de calcul du budget d'un projet pourrait entraîner des économies ou le financement de projets supplémentaires. Par exemple :

1. L'implémentation précoce d'un projet technologique peut entraîner une erreur de calcul des coûts liés au projet par le chef de projet.
2. Une erreur de calcul des coûts liés au projet pourrait entraîner un financement excessif du projet.
3. Un financement excessif du projet pourrait permettre de réaliser des économies ou de financer des projets supplémentaires.

Risque positif en matière de cybersécurité

Un exemple de risque positif en matière de cybersécurité est l'implémentation de la gestion des correctifs, qui pourrait renforcer la confiance des clients. Par exemple :

1. L'implémentation de la gestion des correctifs pourrait réduire les vulnérabilités de l'application.
2. La suppression des vulnérabilités pourrait réduire les risques liés aux applications et les rendre plus sûres.
3. L'amélioration de la sécurité des applications pourrait réduire les pertes de données.

4. La réduction des pertes de données pourrait renforcer la confiance des clients.

Un autre exemple de risque positif en matière de cybersécurité est l'implémentation d'une réponse aux incidents, qui pourrait augmenter la productivité des employés. Par exemple :

1. L'implémentation de la réponse aux incidents pourrait permettre de détecter une augmentation du trafic réseau.
2. L'augmentation du trafic réseau pourrait permettre de détecter l'utilisation abusive des ressources par les employés accédant à des contenus non liés au travail, tels que des services de diffusion de musique et de vidéos. Ces activités consomment la bande passante du réseau et peuvent avoir un impact négatif sur les performances du réseau et des applications.
3. La détection d'une utilisation abusive des ressources de l'entreprise par les employés pourrait entraîner le blocage de ces services.
4. Le blocage de ces services pourrait réduire la consommation de la bande passante du réseau et augmenter la productivité des employés.

Enfin, le dernier exemple de risque positif en matière de cybersécurité est l'implémentation d'un plan de réponse aux incidents qui pourrait accroître les opportunités métier et renforcer le respect des lois sur la confidentialité. Par exemple :

1. L'implémentation d'un plan de réponse aux incidents peut permettre de détecter et d'identifier rapidement les logiciels malveillants et les rançongiciels.
2. L'identification des logiciels malveillants et des rançongiciels pourrait réduire l'impact et atténuer la menace pour les ressources de l'entreprise.
3. L'atténuation de la menace qui pèse sur les ressources de l'entreprise pourrait créer des opportunités métier et aider l'entreprise à rester en conformité avec les lois sur la confidentialité.

Réponse aux risques liés à la cybersécurité

Les réponses aux risques positifs et négatifs sont très différentes. Pour les risques négatifs, vous prenez des mesures pour minimiser l'impact sur le résultat, tandis que pour les risques positifs, vous prenez des mesures pour maximiser l'impact sur le résultat. Le tableau suivant montre les réponses potentielles aux risques positifs et négatifs.

Type de risque	Réponse	Définition
Risque positif	Exploiter	Maximisez la probabilité que le risque se produise afin que son effet positif se concrétise.
	Partager	Attribuez une partie de la propriété ou de la responsabilité du risque à une autre partie. C'est la même approche qu'avec un risque négatif, et elle essaie de contrôler les pertes ou les gains potentiels.
	Améliorer	Augmentez les conditions qui créent le risque afin de maximiser les opportunités.
	Ignorer	Ignorez la possibilité que ce risque se présente et ne prenez aucune mesure. Cette réaction est courante lorsque la probabilité du risque est très faible ou lorsque les avantages d'un résultat positif potentiel sont minimes.
Risque négatif	Atténuer	Minimisez la probabilité que le risque se produise.

Type de risque	Réponse	Définition
	Transférer	Transférez la responsabilité du risque à une autre partie, par exemple en souscrivant une police d'assurance pour transférer le risque à une compagnie d'assurance.
	Éviter	Éliminez les conditions à l'origine du risque.
	Accept	Reconnaissez l'existence du risque, mais ne prenez aucune mesure.

En ce qui concerne les risques négatifs, les organisations évitent, transfèrent, atténuent ou acceptent le risque, en fonction de leur tolérance au risque et de leur appétit pour le risque. Elles essaient de prévenir le risque et, si tel est le cas, de minimiser son impact sur l'ensemble de la mission.

La meilleure façon d'illustrer les réponses positives aux risques est d'utiliser des exemples :

- Exploiter : un responsable de la sécurité apprend qu'un professionnel de la sécurité qualifié a récemment décidé de chercher un nouvel emploi et prévoit une généreuse prime à la signature pour inciter le futur employé à rejoindre son équipe.
- Partager : un responsable d'unité commerciale souhaiterait améliorer la sécurité en utilisant un produit de gestion des accès privilégiés, mais ne dispose pas d'un budget suffisant pour acheter les outils et les services au cours de l'exercice en cours. Le responsable collabore avec un responsable d'une autre unité commerciale qui achètera et implémentera l'outil dans le cadre d'un projet pilote, puis étendra l'installation pour soutenir les deux unités commerciales.
- Améliorer : un employé a identifié une opportunité d'automatiser un processus métier existant afin de réduire les menaces de cybersécurité, mais cela nécessite un investissement en temps et en équipement. En constatant les avantages d'un tel processus, le responsable approuve les heures supplémentaires pour développer les capacités et réutilise les ressources matérielles et logicielles existantes qui permettent au projet de se poursuivre.
- Ignorer : un responsable financier apprend qu'un employé du service commercial a développé une nouvelle application qui automatise une tâche manuelle et fastidieuse. L'utilisation de l'application a

récemment été autorisée uniquement dans le service commercial. Le responsable financier obtient une copie de la nouvelle application pour obtenir un avantage similaire dans son service, sans autorisation explicite.

Étapes suivantes

Les domaines de la technologie et de la gestion de projet ont intégré les risques positifs dans leurs processus d'évaluation des risques, mais le secteur de la cybersécurité les a historiquement exclus. Les risques positifs peuvent se traduire par des résultats métier positifs, et le secteur de la cybersécurité doit évoluer pour intégrer les risques positifs et en tirer parti.

Vous pouvez commencer à communiquer les risques positifs immédiatement dans toutes les communications. Par exemple, les évaluations des risques, les évaluations de la sécurité ou les rapports d'état devraient inclure une section sur les risques positifs. Les demandes de financement adressées à la direction doivent inclure des risques positifs, communiquer les avantages potentiels pour l'entreprise et mettre en évidence les avantages métier potentiels obtenus en approuvant la demande.

FAQ

Quelle est la différence entre le risque à la hausse et le risque positif ?

Même si risque à la hausse et risque positif semblent similaires, ils sont en réalité très différents. Dans le domaine du risque, il existe un résultat positif ou négatif, et dans le cas des résultats négatifs, il existe un risque à la hausse ou à la baisse.

Le risque positif est le gain potentiel d'actifs, de connaissances, d'améliorations ou de données. Par exemple, vous implémentez la gestion des correctifs et un processus permettant de supprimer rapidement les vulnérabilités, par exemple en une semaine. Au cours de l'année suivante, aucun incident de sécurité ne se produit.

Le risque à la hausse est l'exposition à une perte dans le but de réaliser un gain. Par exemple, l'entreprise déploie une nouvelle application et vous implémentez la gestion des correctifs et un processus permettant de supprimer rapidement les vulnérabilités, par exemple en une semaine. L'exposition à une perte (période pendant laquelle vous supprimez les vulnérabilités) se produit dans le but de réaliser un gain (une application plus sécurisée), ce qui est considéré comme un risque à la hausse. Vous pouvez augmenter le risque à la hausse en modifiant le processus de suppression des vulnérabilités sur un jour, ou en diminuant le risque à la hausse en portant la période à un mois. Fondamentalement, le risque à la hausse est la possibilité incertaine de réaliser un gain tout en essayant de minimiser une perte.

Pourquoi est-il important d'inclure le risque positif dans la cybersécurité ?

L'intégration des risques positifs dans les évaluations et les conversations portant sur les risques de cybersécurité contribue à promouvoir la valeur de la cybersécurité pour l'entreprise. Pour de plus amples informations, veuillez consulter Avantages des risques positifs.

Ressources

- Cybersecurity In The C-Suite and Boardroom (rapport de recherche d'Enterprise Strategy Group)
- Recherche sur la cybersécurité : l'accélérateur de l'innovation (livre blanc de Vodafone)
- Integrating Cybersecurity and Enterprise Risk Management (ERM) (publication du NIST)
- Clarifying “Upside” and “Positive” Risk (billet de blog de l'institut FAIR)

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un fil RSS.

Modification	Description	Date
Publication initiale	—	27 mai 2022

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.