ivanti

Évaluer objectivement le cyber-risque :

Guide d'évaluation des risques basée sur les données

Sommaire

À propos de cet e-book

La gestion de l'exposition envisage les risques dans le contexte de l'appétence au risque de l'entreprise. Les responsables de sécurité sont ainsi en mesure de formuler des recommandations de sécurité éclairées, compréhensibles par la direction et susceptibles de susciter l'adhésion de l'ensemble des parties prenantes.

Ce e-book vous propose des outils pratiques pour maîtriser un pilier essentiel de la gestion de l'exposition : **l'évaluation des risques basée sur les données.**

Vous découvrirez une méthode simple pour évaluer les riques et en présenter les résultats en démontrant l'impact direct des décisions prises sur les actifs critiques de l'entreprise, selon que vous choisissez de réduire le risque ou de l'accepter.

Nous vous accompagnons pas à pas dans l'application de ce processus, avec des exemples concrets et des astuces pratiques pour enrichir vos analyses et proposer des actions d'atténuation pertinentes. Enfin, ce guide vous fournira des clés pour établir un langage commun avec les autres dirigeants afin d'améliorer la compréhension mutuelle et la prise de décision en matière de gestion des risques et d'exposition.

Introduction

Vous êtes conscient des cyberattaques qui menacent votre entreprise, des « fissures » récurrentes qui engendrent des vulnérabilités, ainsi que des initiatives qui pourraient renforcer votre posture de sécurité.

Les autres parties prenantes de l'entreprise connaissent leurs objectifs et les risques calculés qu'elles sont prêtes à assumer pour y parvenir.

En somme, vous êtes tous animés par un objectif commun : une entreprise saine et profitable. Cependant, sans compréhension commune des risques, vous risquez de passer à côté des véritables enjeux.

Pour parvenir à un alignement, il est indispensable de disposer d'une évaluation des cyber-risques détaillée, objective et quantifiable.

Les conclusions de cette évaluation et ses résultats sont présentés dans un langage compréhensible par tous les dirigeants de l'entreprise, ce qui facilite leur adhésion à vos initiatives de sécurité.

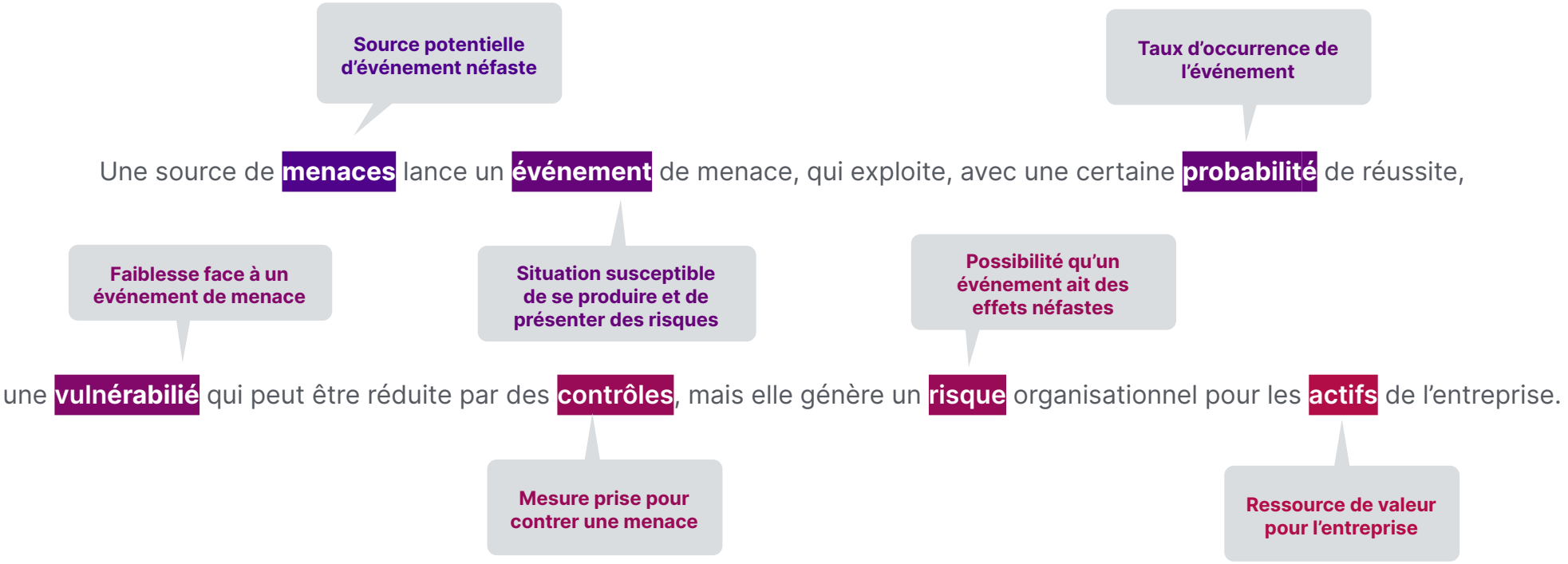
De plus, cette évaluation pourrait remettre en question certaines de vos hypothèses concernant les risques à atténuer ou à accepter.

Mais alors, comment déterminer une valeur chiffrée pour un événement de sécurité qui ne s'est pas encore produit ? C'est précisément ce que nous allons explorer ensemble.

Évaluation des risques

Termes clés et modélisation générale des risques

Voici typiquement à quoi ressemble un modèle de gestion des risques :



Ce modèle correspond à des situations réelles, par exemple :

Le groupe **ALPHV** a été à l'origine de nombreuses **attaques par ransomware**, qui ont **réussi** à toucher plusieurs entreprises aux États-Unis, en Europe et en zone APAC. Ces attaques ont exploité des **failles dans les contrôles d'accès et ont tiré parti du manque de formation des utilisateurs**, provoquant des **interruptions de service** de plusieurs jours. Pour certaines entreprises, ces interruptions ont entraîné d'importants retards dus à l'absence de **sauvegardes** fréquentes, générant des risques financiers, **réputationnels et juridiques**, d'autant que des **informations** sensibles auraient pu être compromises et divulguées publiquement.

Étapes d’évaluation des risques

Dans cette section, nous présentons les 5 étapes essentielles pour évaluer les risques.

1. Identifier les actifs concernés par votre évaluation des risques.
2. Attribuer une valeur à ces actifs.
3. Identifier les vulnérabilités et les menaces.
4. Calculer les risques (probabilité x impact).
5. Analyser les coûts et les avantages.

Vous pourrez alors proposer des recommandations pour répondre aux risques, en vous appuyant sur les données de votre évaluation. Nous aborderons plus tard en détail les quatre types de réponses possibles.

Éviter
le risque en mettant fin à l’activité risquée, ou en arrêtant totalement le système vulnérable.

Accepter
le risque et décider de vivre avec, sans aucune action.

Transférer
le risque, généralement en souscrivant une assurance qui couvrira les risques financiers.

Atténuer
le risque en appliquant des protections supplémentaires.

Étape 1
Identifier les actifs

Quels sont les actifs qui nous intéressent ?

Les actifs peuvent être classés comme **tangibles** (bâtiments, personnes, équipements) ou **intangibles** (informations, brevets, marque, licences, fichiers clients, R&D).

Vous pouvez également classer les actifs d'après leur propriétaire. À un niveau élevé, l'on trouve les **actifs métier** (liquidités, terrains, stocks, usines, expertise des collaborateurs) ou les **actifs IT** (logiciels, serveurs, pare-feux, ordinateurs portables, outils de surveillance).

Mais les actifs IT n'existent pas pour eux-mêmes : ils sont en fait destinés à protéger les actifs métier. Votre entreprise peut posséder un secret de fabrication (actif métier intangible) résidant sur un serveur (actif IT tangible). Les contrôles de sécurité appliqués à ce serveur peuvent à eux seuls déterminer la survie ou la chute de votre entreprise.

Supposons que vous vous intéressiez à la prévention des pertes de données. Vous devez évaluer ce qui entre dans le périmètre concerné (ordinateurs portables professionnels, BYOD, téléphones, imprimantes), puis déterminer leur nombre (idéalement, ces informations proviennent d'un inventaire à jour). Vous pouvez alors expliquer pourquoi sécuriser x postes client revient à sécuriser des actifs métier stockant des informations confidentielles, comme des données client, des informations de carte bancaire ou les salaires des collaborateurs.

L'objectif est d'éliminer tout risque de fuite d'informations. Cependant, en quantifiant ces risques, vous serez plus à même de concevoir une stratégie d'atténuation efficace et de convaincre les parties prenantes de l'adopter.

Les joyaux de la couronne

Les **joyaux de la couronne**, ce sont les actifs les plus précieux de l'entreprise. Parmi tous les actifs, ce sont ceux dont la compromission aurait l'impact le plus sévère sur l'entreprise.

Spontanément, vous avez certainement identifié les **informations** de l'entreprise comme l'un de ces joyaux. Et vous avez raison. Cependant, d'autres dirigeants ont peut-être une perception différente et considèrent que certains processus et systèmes d'entreprise constituent les actifs les plus précieux. Ce qu'ils ne réalisent pas toujours, c'est que sans les informations sous-jacentes, leur valeur est nulle. Les informations ayant une durée de vie bien plus longue que ces systèmes, elles doivent être protégées en priorité.

En fin de compte, vous faites référence aux mêmes actifs, car les processus métier et les systèmes d'information sont interdépendants et fonctionnent ensemble. Toutefois, pour maximiser l'efficacité de votre démarche, il est essentiel que votre analyse des risques soit très spécifique et parfaitement ciblée.

Imaginons que l'un des joyaux de la couronne de l'entreprise soit son système CRM, et les informations client qu'il traite. Voyez la différence entre ces deux affirmations :

« Nous risquons une perte ***d'informations*** *suite à une attaque par usurpation d'identité sur notre DNS. »*

« Une fuite de données survenue l'année dernière, qui a touché 45 % des entreprises de notre secteur, a entraîné la divulgation publique de ***données d'identification personnelle (PII) de clients*** *ainsi que des informations sur les transactions traitées dans Salesforce. Les conséquences potentielles sont préoccupantes : des sanctions estimées à 4,5 milliards d'euros, des coûts importants liés aux poursuites judiciaires, et une atteinte à notre réputation qui pourrait nécessiter entre 5 et 10 ans pour être pleinement restaurée. »*

Il est évident que la seconde formulation est plus puissante, car elle met en lumière les implications concrètes. Une évaluation des risques détaillée vous aidera à atteindre ce niveau de spécificité.

Étape 2
Déterminer la valeur des actifs

Qu'il s'agisse d'un actif tangible ou intangible, sa valeur doit être clairement définie. Bien que l'évaluation de cet actif puisse ne pas relever directement de l'équipe Sécurité, sa valeur constitue un paramètre crucial – voire le plus déterminant – lors de la prise de décisions stratégiques concernant la mise en place de mesures de protection adaptées à cet actif spécifique.

Pour déterminer la valeur d'un actif, il faut prendre en compte plusieurs éléments :

- Coût d'acquisition ou de développement de l'actif.
- Coût de maintenance et de protection de l'actif.
- Valeur de l'actif pour ses propriétaires et ses utilisateurs.
- Valeur de l'actif pour les pirates.
- Prix que d'autres sont prêts à payer pour cet actif.
- Coût de remplacement de l'actif en cas de perte.
- Activités opérationnelles et de production qui seraient affectées par la non-disponibilité de cet actif.
- Responsabilité juridique en cas de compromission de l'actif.
- Utilité et rôle de l'actif dans l'entreprise.

Chaque actif d'entreprise doit avoir un propriétaire, et la valeur de l'actif doit être déterminée par ce propriétaire, éventuellement avec les conseils de l'équipe Sécurité.

Se pose ensuite une question très importante : combien cela coûterait-il à l'entreprise de ne PAS protéger cet actif ? La réponse à cette question commence par une analyse d'impact business (BIA).

L'analyse d'impact business typique

L'analyse BIA est une étape essentielle dans le cycle de vie de la continuité d'activité. C'est un processus qui réunit les équipes technologiques et métier pour évaluer la criticité des activités et des actifs sous-jacents.

En posant des questions comme « Que se passerait-il exactement si ce processus cessait de fonctionner ? », les propriétaires de ces processus et les autres fonctions de l'entreprise sont amenées à réfléchir aux impacts potentiels (notamment financiers), ce qui permet d'obtenir des chiffres réalistes, exploitables dans votre évaluation des risques.

Une analyse BIA parfaite inclut :

- Objectif, propriétaires, entrées et sorties des processus.
- Impact d'une interruption, mesuré sur le plan financier, opérationnel, juridique/réglementaire et réputationnel.
- Identification des pires scénarios possibles et périodes critiques (pics d'activité, par exemple).
- Objectifs de délai de récupération (RTO, Recovery Time Objective), objectifs de point de récupération (RPO, Recovery Point Objective) et durée d'interruption de service maximale tolérable (MTD, Maximum Tolerable Downtime).
- Ressources nécessaires pour exécuter/soutenir le processus : recours à d'autres départements, informations, personnes, infrastructure, sites appartenant aux fournisseurs et actifs IT. Ces ressources devront être restaurées en priorité selon les objectifs définis pour le RTO et le RPO.

Astuces

De nombreux modèles de BIA ont déjà été publiés mais il n'y a pas de recette miracle. Vous trouverez ci-après un modèle simplifié (téléchargeable sous forme de diaporama modifiable), à utiliser comme point de départ.

La continuité des activités et la sécurité des informations peuvent dépendre des autres départements de l'entreprise. Dans ce cas, les informations doivent être partagées afin de garantir une approche cohérente de la gestion des risques.

Affectation d'une criticité aux actifs avec l'analyse BIA

L'analyse d'impact business (BIA) identifie, parmi les systèmes critiques de l'entreprise, ceux qui sont indispensables à sa survie. Elle estime ainsi la durée d'interruption de service que l'entreprise peut tolérer. C'est ce que l'on appelle la durée d'interruption de service maximale tolérable (MTD).

Exemples de MTD :

- **Non essentiel :** 30 jours
- **Normal :** 7 jours
- **Important :** 72 heures
- **Urgent :** 24 heures
- **Critique :** Quelques minutes ou heures

Chaque fonction de l'entreprise et chaque actif doivent être classés dans l'une de ces catégories, selon la durée pendant laquelle l'entreprise peut survivre sans eux. Cette estimation aide l'entreprise à déterminer les contrôles nécessaires pour garantir la disponibilité de ces ressources.

Par exemple, si l'indisponibilité d'un serveur Web pendant 4 heures est susceptible de coûter 120 000 euros à l'entreprise, ce serveur doit être considéré comme **critique**. Dans ce cas, l'entreprise devrait envisager d'installer un serveur Web redondant.

Par contre, si un outil de reporting sur l'occupation des bâtiments reste inacessible pendant 3 semaines et que le coût de l'indisponibilité ne dépasse pas 500 euros, l'on peut considérer que cet outil est **non essentiel**. Dans ce cas, vous pouvez vous appuyer sur le SLA du fournisseur ou prendre des mesures correctives.

Astuces

Le RTO des processus et des systèmes peut être corrélé au montant des pertes financières potentielles. Le résultat obtenu peut ensuite être utilisé par votre analyse quantitative des risques. Ces informations sont probablement déjà disponibles, recueillies lors d'analyses BIA existantes ou intégrées à votre plan de reprise après sinistre. Dans le cas contraire, il vous suffit de mener une analyse ciblée en la limitant au périmètre spécifique.

Voici à quoi ressemble une analyse BIA simplifiée.

Nom de processus	Interruption du processus	Impact financier	Impact juridique	Impact sur la réputation
Paiements le jour même	<4h	€-€€€	N/A	N/A
	4h-8h	€€€-€€€	N/A	Faible
	2-5 jours ouvrables	€€€-€€€€	Moyen	Moyen
	1-2 semaines	€€€-€€€€	Moyen	Élevé
	2-4 semaines	€€€€-€€€€€€	Élevé	Critique
Justification	▪ Perte de réputation et de confiance du public : ... ▪ Perte d'avantages concurrentiels : ... ▪ Augmentation des dépenses opérationnelles : ... ▪ Violation de contrats/accords : ... ▪ Non-respect d'obligations légales et réglementaires : ... ▪ Retards dans les revenus prévus : ... ▪ Perte de revenu : ... ▪ Perte de productivité : ... ▪ Autres : ...			
Ressources nécessaires	Personnel : Min 4 personnes semaine 1 ; min 6 personnes au bout d'une semaine Système de paiement : Doit être opérationnel, pas de solution de rechange Jetons de paiement : Au moins 2 Systèmes IT : Système de paiement (serveurs + base de données), Internet, connexion à la chambre de compensation, e-mail Lieu : Télétravail possible le premier jour, espace de bureau nécessaire ensuite Équipement de bureau : Imprimante			

Astuces

Vous pouvez télécharger ce modèle BIA sous forme de diaporama modifiable.

Relations entre BIA et évaluation des risques

L'analyse BIA est une composante de l'évaluation des risques basée sur la continuité des activités. Elle met en évidence l'impact d'éventuels scénarios ayant une incidence significative sur les activités de l'entreprise, et permet d'identifier clairement les priorités business. Ces résultats vous aident à définir les joyaux de la couronne de votre entreprise, y compris les systèmes d'information qui les soutiennent.

L'évaluation des risques repose généralement sur l'équation suivante : **risque = menace x impact x probabilité**. Cependant, l'analyse BIA enrichit cette approche avec un paramètre crucial : le temps. Elle met l'accent sur les menaces susceptibles d'interrompre rapidement des processus métier critiques. C'est pourquoi l'analyse BIA constitue un outil critique pour déterminer les contrôles nécessaires pour protéger le paramètre **Disponibilité** de la **triade Confiance-Intégrité-Disponibilité** (CIA, Confidentiality-Integrity-Availability).

Une **attaque par ransomware** s'inscrit parfaitement dans l'un de ces scénarios de continuité, car elle rend les données indisponibles. Cependant, certains risques de sécurité ne prennent pas en compte le paramètre **Disponibilité**.

Lors d'une **fuite de données** (exfiltration sans utilisation de ransomware), les systèmes et les processus restent fonctionnels, et les données, bien que compromises, demeurent accessibles, voire trop accessibles. Dans ce cas, c'est le paramètre **Confidentialité** de la triade CIA qui est mis en péril car les processus qui manipulent les données ayant fuité ne cessent pas brutalement de fonctionner.

La modification ou la divulgation à des fins malveillantes d'un secret de fabrication (n'oublions pas que les secrets de fabrication comptent parmi les joyaux de la couronne) touche le paramètre **Intégrité**. Il s'agit une fois de plus d'un exemple d'événement pouvant échapper à l'analyse BIA.

C'est pourquoi vous devez envisager votre évaluation des risques sous d'autres angles. Toutefois, l'analyse BIA reste un bon point de départ.

Évaluation du score CIA

L'analyse BIA nous a permis de déterminer les actifs sensibles au facteur temps. Avec **l'évaluation du score CIA**, vous ajoutez une dimension à cette analyse.

L'ISACA propose une méthodologie pour évaluer et catégoriser les actifs en pondérant la valeur d'un actif d'après sa sensibilité.

Vous affectez à chacun des trois paramètres de la triade CIA la valeur 1 (faible), 2 (moyen) ou 3 (élevé). Le score CIA est obtenu en additionnant ces trois valeurs (Confiance-Intégrité-Disponibilité, C-I-A) pour obtenir un résultat compris entre 3 et 9.

Chaque actif de l'entreprise reçoit un score CIA, directement lié à l'implémentation d'un contrôle basé sur les risques. Un actif classé C3-I2-A2 (7) nécessitera des contrôles différents d'un actif classé C1-I1-A2 (4).

Ces deux méthodes font intervenir les propriétaires métier, qui sont responsables des informations circulant à travers leurs actifs. C'est donc l'occasion de renforcer une sensibilisation commune à la valeur des actifs, et de réduire l'écart entre la compréhension des risques et l'orientation stratégique de l'entreprise.

Astuces

L'évaluation du score CIA n'est pas nécessaire pour tous les éléments de configuration ou VDI. Il convient de regrouper les actifs en procédant logiquement, par exemple, en regroupant ceux qui partagent un même objectif business.

Si votre entreprise a rédigé une déclaration d'appétence au risque, utilisez-la comme cadre de référence pour aligner les autres dirigeants sur les valeurs que vous attribuez dans votre évaluation du score CIA. (Vous n'en avez pas ? Rédigez-en une à partir de ce modèle personnalisable.)

Étape 3

Modéliser les menaces et évaluer les vulnérabilités

L'étape suivante consiste à déterminer les menaces et vulnérabilités prioritaires.
Bien que vous puissiez déjà avoir une idée des risques principaux, valider ces hypothèses avec des données concrètes renforce la fiabilité et la crédibilité de votre évaluation des risques.

Modélisation des menaces

La modélisation des menaces doit s'appuyer sur la threat intelligence : tenez compte du paysage global des menaces, des types de menaces utilisés contre d'autres organisations de votre secteur et des spécificités propres à vos activités. Vous pourrez ainsi concentrer vos efforts sur les menaces les plus probables, et éviterez de perdre de l'énergie sur des menaces moins fréquentes.

Il existe plusieurs méthodologies de modélisation des menaces.
Les deux méthodologies suivantes sont assez courantes :

Arbres d'attaque :
Une source de menaces peut emprûnter plusieurs routes pour atteindre son objectif. L'arbre d'attaque représente ces différents trajets sous forme de branches et de nœuds. Chaque branche illustrant une voie d'accès possible, tandis que chaque nœud décrit les étapes ou conditions nécessaires pour que le pirate atteigne son objectif. Vous évaluez les vulnérabilités de chaque nœud.

Analyse de réduction :
Cette approche complémentaire des arbres d'attaque consiste à rechercher des points communs entre les différents nœuds. Vous pouvez alors identifier les contrôles potentiellement à même d'atténuer plusieurs vulnérabilités en même temps.

Astuce

Les exemples d'attaque identifiés lors de l'exercice de modélisation des menaces peuvent être repris pour compléter votre analyse des risques et vos recommandations de remédiation. Ces menaces sont ainsi concrètes et facilement compréhensibles par les autres fonctions de l'entreprise.

Évaluation des vulnérabilités

Contrairement à la modélisation des menaces qui fonctionne de l'extérieur vers l'intérieur, en identifiant d'abord les menaces potentielles et les vecteurs d'attaque, l'évaluation des vulnérabilités fonctionne de l'intérieur vers l'extérieur. Elle repère les failles présentes dans votre surface d'attaque.

Un principe fondamental de la gestion de l'exposition aux cybermenaces est de considérer la surface d'attaque dans une acception large. Lorsque vous évaluez les vulnérabilités de votre surface d'attaque, ne vous limitez pas aux informations et aux vulnérabilités système. Vous pouvez également inclure les processus (ex. : application tardive ou incorrecte des correctifs) et le facteur humain (ex. : personnes sensibles à l'ingénierie sociale, utilisation de mots de passe trop simples).

Les logiciels comme les scanners de vulnérabilités réseau, les tests de sécurité des applications et les outils de gestion de la surface d'attaque externe récoltent de précieuses informations sur les vulnérabilités potentielles. Vous pouvez aussi disposer d'autres sources d'informations, comme les rapports d'audit, les registres de risques, les tests de contrôle, les résultats des tests d'intrusion, les rapports d'incident, les études de conformité et la simple observation de la culture d'entreprise.

Les scores de vulnérabilités fournis par les fournisseurs et les systèmes comme le CVSS (Common Vulnerability Scoring System) permettent de repérer les vulnérabilités critiques. Cependant, cette approche ne suffit pas. Pour compléter cette liste (et, potentiellement, révéler des vulnérabilités à faible score dont l'impact serait plus sévère pour votre entreprise), il convient d'ajouter deux dimensions clés : **le contexte de menaces** et le **contexte de risques.**

Le contexte de menaces examine le paysage de menaces :
Une vulnérabilité peut être classée Critique. Cependant, si elle n'est pas activement exploitée, son importance diminue. Cette recherche a déjà été effectuée lors du travail de modélisation des menaces.

Le contexte de risques s'intéresse à votre entreprise :
Si cette vulnérabilité était exploitée, quel serait l'impact sur notre entreprise ?
Une vulnérabilité jugée mineure (mais non exploitée) pourrait, si elle touchait un système critique, entraîner une interruption majeure. Elle mérite alors davantage d'attention. Grâce à votre évaluation de l'impact business, vous savez quels sont les actifs, les systèmes et les processus à protéger en priorité.

Astuce

Téléchargez cette checklist pour vérifier que toutes les facettes de votre surface d'attaque sont bien prises en compte.

Étape 4
Déterminer les risques

À ce stade, nous connaissons la valeur des actifs (AV), les menaces et les vulnérabilités. Il ne nous reste plus qu'à étudier la probabilité et l'impact pour calculer les risques. Deux méthodes distinctes permettent de mesurer le risque : l'approche **quantitative** et l'approche **qualitative**.

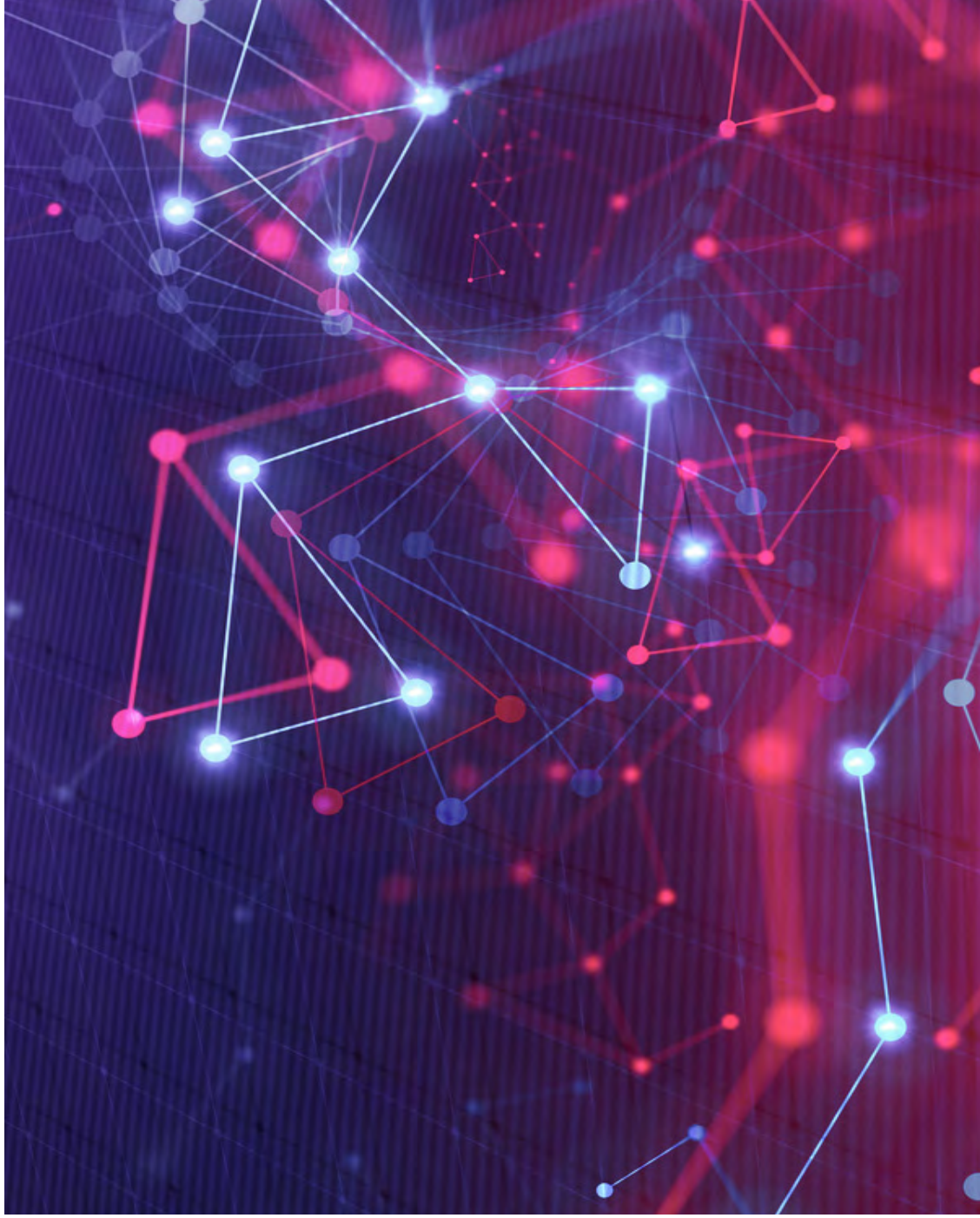
L'analyse quantitative des risques utilise des équations pour attribuer une valeur monétaire aux composants évalués.

L'analyse qualitative des risques utilise des valeurs et des scores (faible/moyen/élevé, 1 à 10 ou feux tricolores).

Choisissez la méthodologie la plus adaptée à votre entreprise. Dans cet e-book, nous nous concentrons surtout sur l'analyse quantitative des risques.

Astuce

Les outils automatisés d'analyse des risques peuvent servir à accélérer l'évaluation des risques, car ils évitent les opérations manuelles et indiquent les avantages des différents contrôles de sécurité.



Analyse quantitative des risques

Votre PDG et le conseil d'administration préfèrent recevoir une analyse quantitative et chiffrée. Savoir que le risque de cyberattaque est élevé n'est pas le plus important pour eux : ce qui les intéresse réellement, c'est de connaître l'impact concret d'une attaque. Par exemple, une attaque par ransomware réussie, cryptant 15 % des données d'un système critique, pourrait non seulement faire perdre un avantage concurrentiel, mais aussi entraîner la suspension des engagements stratégiques de l'entreprise pendant 4 jours. Résultat : un coût estimé à 225 000 euros par jour.

Les équations généralement utilisées pour quantifier les risques sont en réalité assez simples.

Perte annuelle estimée (ALE) = La perte simple estimée (SLE) x Taux d'occurrence annualisé (ARO),
où la SLE = Valeur des actifs (AV) x Facteur d'exposition (EF)

Le **facteur d'exposition (EF)** représente le pourcentage de perte qu'une menace pourrait entraîner pour un actif donné. Par exemple, en cas de fuite d'un secret de fabrication, la perte d'avantage concurrentiel peut atteindre 10 % de la valeur de l'actif. Dans ce cas, l'EF serait de 10 %. En supposant que la valeur d'actif (AV) de votre secret de fabrication est de 4 millions d'euros, vous pouvez utiliser une équation simple pour calculer la perte simple estimée (SLE) :

AV (4M €) x EF (10 %) = SLE (400 000 €)

Le **taux d'occurrence annualisé (ARO)** est l'estimation de la fréquence à laquelle une menace est susceptible de survenir au cours d'une année. Dans notre exemple, vous pouvez examiner des événements comparables dans des entreprises comme la vôtre, et estimer qu'une fuite de secret de fabrication se produit tous les 20 ans. Autrement dit, son ARO est de 0,05 (1 an/20 ans). L'on peut alors calculer la **perte annuelle estimée (ALE)** :

SLE (400 000 €) x ARO (0,05) = ALE (20 000 €)

L'ALE obtenue permet à l'entreprise de décider si elle doit mettre en place des contrôles pour atténuer le risque ou simplement l'accepter.
Dans notre exemple, des contrôles de sécurité peuvent être justifiés si leur coût est inférieur à 20 000 euros par an.

Les résultats d'une analyse quantitative des risques vous seront utiles pour monter un business case de stratégie d'atténuation des risques. Ils permettent également d'écarter les stratégies d'atténuation dont le coût dépasse l'ALE.

Exemples de résultats d'analyse quantitative des risques

Actif	Menace	SLE	ARO	ALE
Secret de fabrication	Fuite	4 M €	0.05	20 000 €
Serveur de fichiers	Corruption	13 500 €	0.1	1 350 €
Usine	Incendie	250 000 €	0.1	25 000 €
Données	Malware	7 500 €	1	7 500 €
N° de carte bancaire des clients	Divulgation	300 000 €	4	1,2 M €

Prenons un autre exemple.

Fraîchement recruté comme Responsable IT et Sécurité dans une start-up d'IA en pleine croissance, vous êtes conscient d'un risque imminent d'attaque par hameçonnage. Dans le pire scénario, des cyber-attaquants pourraient exfiltrer et divulguer les algorithmes exclusifs développés par votre entreprise. Les conséquences seraient terribles : perte d'avantage concurrentiel et perte de valeur. De plus, vos premières campagnes de sensibilisation sur l'hameçonnage révèlent une statistique inquiétante : 10 % des collaborateurs cliquent encore sur des liens ou ouvrent des pièces jointes.

Vous êtes désormais face à un défi de taille : convaincre le PDG et les investisseurs — actuellement focalisés sur les progrès en ingénierie — d'allouer des ressources à des mesures essentielles telles qu'un outil anti-hameçonnage et des programmes de formation et de sensibilisation à la cybersécurité. Ces initiatives permettraient de réduire ce risque critique. Il ne vous reste plus qu'à vous lancer dans une analyse quantitative des risques (RA).

Déterminer la SLE :

D'après le rapport « 2024 IBM Cost of a Data Breach Report », les attaques par hameçonnage sont le deuxième vecteur de menace le plus coûteux (à égalité avec la compromission des e-mails d'entreprise, et derrière les actes malveillants perpétrés en interne). Leur coût moyen en 2024 s'élève à **4,88 millions** de dollars. Ce montant correspond à la **SLE** moyenne. Pour reprendre notre exemple, il est nécessaire de l'ajuster en fonction de vos variables **EF** et **AV**.

Nous allons donc commercer par ajuster la SLE en fonction de la taille de votre entreprise. Dans votre cas, c'est une petite entreprise. Votre **EF**, à savoir le pourcentage des données susceptibles d'être compromises, resterait probablement constant. Cependant, l'**AV** est sans doute bien plus faible, disons 10 % du montant. Vous obtenez alors une SLE de **488 000 euros.**

Déterminer l'ARO :

Au fil de votre analyse, vous avez découvert que les entreprises de taille comparable, opérant dans le même secteur, subissent des attaques par hameçonnage chaque semaine, soit 52 par an. Si 10 % de ces attaques réussissent (ce qui coïncide avec le résultat de vos campagnes de hameçonnage), l'**ARO** est de **5,2.**

Déterminer l'ALE :

SLE (488 000 €) x ARO (5,2) = ALE (2,5 M €)

(Montants arrondis.)

Il est évident qu'accepter le risque associé à cette ALE serait peu judicieux. Ces chiffres fournissent une base solide pour monter un business case en faveur d'une stratégie d'atténuation des risques plus agressive.

Analyse qualitative des risques

L'analyse qualitative des risques utilise une échelle pour évaluer les risques (ex. : de très faible à très élevé et/ou de 1 à 10).
Une matrice d'analyse qualitative des risques a généralement la forme suivante :

		Probabilité				
		1 Rare	2 Peu probable	3 Possible	4 Probable	5 Presque certain
Impact	5 Très élevé	5	10	15	20	25
	4 Élevé	4	8	12	16	20
	3 Moyen	3	6	9	12	15
	2 Faible	2	2	6	8	10
	1 Très faible	1	2	3	4	5

Légende des risques	Faible	Moyen	Élevé	Extrême

Reprenons votre analyse qualitative des risques. Ce scénario d'attaque par hameçonnage est considéré comme probable : en tant que petite entreprise, vous n'êtes pas ciblés à la même fréquence que des entreprises plus grandes et plus médiatisées. Toutefois, vous savez que l'hameçonnage est l'un des vecteurs de menace les plus répandus. Vous estimez que l'impact est moyen : le pire scénario aurait des conséquences extrêmement dommageables pour votre réputation et, par conséquent, pour la valeur de l'entreprise. Mais un scénario plus réaliste impliquerait une exposition moins élevée. Vous concluez donc que le risque est **élevé**.

Pour améliorer la rigueur et la reproductibilité de cette analyse, vous pouvez définir la **probabilité** à partir d'une fourchette réaliste fondée sur des événements historiques, en identifiant les scénarios plausibles (du plus probable au moins probable). Il ne reste plus qu'à attribuer une valeur financière pour chaque **catégorie d'impact**.

L'analyse quantitative et l'analyse qualitative des risques présentent chacune leurs avantages et inconvénients. Les combiner permet d'intégrer les risques plus difficiles à chiffrer — tels que les risques financiers ou opérationnels— mais aussi les risques pouvant avoir de graves conséquences comme les risques réglementaires ou les risques réputationnels.

Vous pouvez utiliser un tableau de ce type dans lequel vous attribuerez un coût indirect aux risques non financiers :

Impact	Monétaire	Réglementaire	Réputationnel
Très élevé	> 10 M d'euros	Poursuites pénales ; risque de retrait de licence ; responsabilité personnelle de la direction	Perte totale de confiance ; couverture médiatique négative continue au niveau local/mondial ; image de marque ternie
Élevé	1 à 10 M €	Amendes importantes, poursuites judiciaires et accords avec le ministère public ; possible restriction de licence d'exploitation	Confiance gravement atteinte, qui ne pourra jamais être entièrement rétablie ; couverture médiatique négative croissante, qui se propage au niveau international
Moyen	100 000 à 1 M €	Avertissements publics et amendes ; actions immédiates requises pour remédier à la situation	Confiance diminuée, mais possible à rétablir pour un coût considérable ; augmentation de la couverture médiatique négative
Faible	10 000 à 100 000 €	Avertissements non publics de la part des régulateurs/superviseurs	Confiance perdue mais récupérable avec le temps ; couverture médiatique nationale partiellement neutre
Très faible	< 10 000 €	Peu ou pas d'attention des régulateurs ou superviseurs	Confiance mise en doute mais récupérable rapidement ; couverture médiatique locale ponctuelle

Quelle que soit l'approche choisie, l'évaluation des risques doit toujours composer avec un défi majeur : l'incertitude.

Les deux méthodes d'analyse des risques (quantitative et qualitative) présentent des limites. Même lorsqu'elles s'appuient sur des données chiffrées, elles comportent un certain degré de subjectivité, étroitement lié à l'incertitude.

Ce terme désigne le manque de confiance que vous pouvez avoir dans une estimation. Intégrer le niveau d'incertitude dans votre évaluation est essentiel, car cela indique le niveau de confiance que vous accordez aux résultats.

Il est quasiment impossible de réaliser une analyse totalement objective. L'incertitude apparaît lorsque les données historiques ou les études disponibles sont insuffisantes, quand le temps manque pour collecter davantage d'informations, ou face à l'imprévisibilité d'événements « cygne noir ».

Identifier précisément les zones d'incertitude vous permet de mieux qualifier votre niveau de confiance et de cibler les domaines où il est possible de la réduire.

Prenons l'exemple d'une stratégie BYOD.

Dans un secteur à tolérance au risque très faible — comme la Défense — l'adoption du BYOD sera sans doute écartée. Pourtant, si les collaborateurs sont de plus en plus demandeurs et que la direction envisage cette solution pour améliorer la satisfaction au travail, il faut alors évaluer si le risque additionnel est justifié, et quels contrôles peuvent être mis en place pour l'atténuer.

Quelles questions faut-il se poser ?

- Si vous travaillez pour une agence gouvernementale ou êtes entrepreneur, des changements réglementaires futurs pourraient-ils impacter la stratégie de votre entreprise ?
- Combien de collaborateurs seront concernés par cette stratégie ? Quels sont les postes concernés ?
- Combien d'heures faudrait-il à l'équipe IT pour inscrire les périphériques et assurer leur support ?

Vous n'aurez peut-être pas toutes les réponses immédiatement, mais il est possible de réduire l'incertitude. Par exemple, en menant une enquête interne pour mieux anticiper le taux d'adoption du BYOD.

Étape 5
Analyser les coûts/bénéfices

Une fois le niveau de risque défini, vous pouvez étudier les différentes options d'atténuation. Même si ce document se concentre sur les contrôles de sécurité, ces principes s'appliquent également à d'autres mesures, telles que l'application de correctifs logiciels ou la correction des erreurs de configuration.

Coût des contrôles de sécurité

Pour formuler une recommandation éclairée en matière de réponse aux risques, vous devez répondre à une question essentielle : quel est le coût réel (coûts cachés inclus) de l'atténuation de ce risque ?

Un contrôle de sécurité peut être de nature purement technique (comme l'implémentation de la DLP), administrative (comme un programme de sensibilisation à la sécurité de l'information) ou physique. Stratégiquement placés entre les actifs et les menaces, les contrôles de sécurité permettent de réduire les vulnérabilités et d'atténuer l'impact d'une menace potentielle.

Gardez à l'esprit que toute atténuation a un coût. Par exemple, mettre un serveur hors ligne pendant la mise à jour des contrôles d'accès basés sur le rôle a un coût pour l'entreprise, tout comme l'implémentation d'un nouvel outil de sécurité. La différence réside dans la visibilité comptable : l'une des opérations est inscrite dans les comptes financiers, alors que l'autre est un coût caché — à moins, bien sûr, de veiller à le comptabiliser correctement.

En règle générale, le coût de sécurisation d'un actif doit être inférieur à la valeur de cet actif. Sinon, cette mesure d'atténuation est économiquement injustifiable.

Pour calculer le coût d'un contrôle de sécurité (en incluant les coûts cachés), vous devez prendre en compte divers éléments :

- Coût des logiciels
- Coûts de conception et de planification
- Coûts d'implémentation, y compris le coût des interruptions de service
- Modifications de l'environnement
- Compatibilité avec les mesures de sécurité déjà en place
- Maintenance
- Tests
- Coûts de réparation, remplacement ou mise à jour
- Coûts de fonctionnement et de support (formation du personnel incluse)
- Effets sur la productivité
- Coûts des abonnements
- Heures-personnes supplémentaires nécessaires pour la surveillance/réponse aux alertes

Valeur d'un contrôle de sécurité

Formule de calcul de la valeur d'un contrôle de sécurité :

(ALE avant implémentation du contrôle) - (ALE après implémentation) - (coût annuel du contrôle) = valeur du contrôle

Reprenons notre exemple précédent : prévenir l'exfiltration de données causée par une attaque de type hameçonnage en déployant un **outil anti-hameçonnage**, et en mettant en place une **campagne de sensibilisation à la sécurité de l'information.**

Pour déterminer la valeur de ces contrôles, il faut d'abord en calculer le coût. Supposons que, après avoir examiné tous les coûts directs et indirects, vous arriviez à un coût total de 90 000 euros.

Outil antihameçonnage	Campagne de formation
Déploiement (une seule fois)	Déploiement (une seule fois)
Intégration	Intégration
Frais de licence/d'abonnement	Frais de licence/d'abonnement
Formation des utilisateurs	Supports pour les campagnes de sensibilisation
Maintenance et support	Maintenance et support
Perte de productivité	Perte de productivité (temps que les collaborateurs passent en formation)
Estimation : 70 000 €/an	**Estimation : 20 000 €/an**

L'ALE initiale était :

SLE (488 000 €) x **ARO** (5,0) = **ALE** (2,5 M €)

(Montants arrondis.)

Pour déterminer la nouvelle ALE, il faut prendre en compte la réduction de l'ARO suite aux contrôles mis en place.

Votre ARO initiale reposait sur l'hypothèse suivante : des tentatives d'hameçonnage hebdomadaires avec un taux de réussite de 10 %, basé sur les résultats de vos campagnes précédentes. La fréquence des tentatives reste inchangée. Mais, après avoir examiné les offres de deux fournisseurs, vous estimez que l'utilisation combinée des deux solutions (l'outil anti-hameçonnage et la campagne de sensibilisation) ramènerait le taux de réussite à 2 %. En conséquence, cela réduirait votre ARO à 1/5 du calcul d'origine, à savoir 1,04.

Vous connaissez maintenant votre nouvelle ALE :

SLE (488 000 €) x nouvelle **ARO** (1,04) = **ALE** (507 500 €)

(Montants arrondis.)

Vous pouvez alors calculer la valeur du contrôle de sécurité :

ALE initiale (2,5 M €) - nouvelle **ALE** (507 500 €) - coût annuel du contrôle (90 000 €) = valeur du contrôle (1,9 M €)

(Montants arrondis.)

Risque total vs risque résiduel

L'implémentation de contrôles de sécurité vise à réduire le risque global (total) de l'entreprise à un niveau acceptable. Cependant, aucun système ou environnement n'étant sûr à 100 %, il reste toujours un certain niveau de risque à gérer : le risque résiduel.

L'ALE après implémentation des contrôles, aussi appelée ALE résiduelle, permet de quantifier ce risque résiduel.

Résidu quantitatif ALE = ARO résiduelle x SLE résiduelle

Dans notre exemple, la SLE reste inchangée après l'implémentation des contrôles mais l'on prévoit une réduction de l'ARO de 5,2 à 1,04, ce qui donne une ALE résiduelle bien inférieure à l'ALE initiale (inhérente). Cela démontre donc que la réponse apportée, à savoir l'atténuation du risque, était une décision pertinente.

Astuce

Vous pouvez utiliser les formules suivantes :

menaces x
vulnérabilité x
valeur de l'actif = **risque total**

menaces x
vulnérabilité x
valeur de l'actif x
écart dû aux contrôles = **risque résiduel**

Risque total -
contrôles = **risque résiduel**

Bénéfices potentiels d'un contrôle de sécurité

Les bénéfices d'un contrôle de sécurité dépassent souvent la simple atténuation d'une menace (comme décrit précemment à propos de la valeur d'un contrôle). En effet, ils permettent de réduire les **coûts de fonctionnement**, un facteur qui peut avoir une incidence sur votre analyse.

Exemple : **Automatisation des correctifs**

Supposons que décidiez d'automatiser le déploiement des correctifs. Ils seront déployés plus rapidement, ce qui réduira la durée d'exposition aux vulnérabilités tout en limitant le risque d'erreurs humaines.

Mais ses bénéfices ne s'arrêtent pas là. Prenons le cas suivant : votre entreprise gère 75 applications, chacune nécessitant un correctif toutes les deux semaines. Actuellement, l'équipe technique consacre en moyenne quatre heures pour packager et déployer un correctif, soit un total de 600 heures par an. Le coût horaire de votre équipe technique étant estimé à 100 euros, vous obtenez les économies de coûts de fonctionnement suivantes :

Nombre d'applications	75
Nombre de mises à jour bimensuelles par application	2
Nombre d'heures nécessaires pour packager et déployer une application	4
Nombre d'heures consacrées au packaging manuel	600
Coût horaire de l'équipe technique	100 €
Coût annuel du packaging manuel	**60 000 €**

Les gains de temps sont importants, surtout avec l'automatisation. Votre équipe peut ainsi se concentrer sur des tâches à valeur ajoutée, ce qui au final, engendrera des économies substantielles pour l'entreprise.

Voici d'autres exemples d'avantages quantifiables :

Bénéfice	Quantification
Détection des menaces : Détection anticipée des anomalies	Réduction du délai de détection des menaces potentielles
Réponse aux incidents : Réponse rapide aux alertes et aux incidents	Réduction du délai de réponse aux incidents
Surveillance en temps réel : La SIEM (Gestion des événements d'information de sécurité) n'attend pas qu'un administrateur vérifie les activités récentes	Amélioration de l'efficacité des collaborateurs (en temps)
Vue intégrée : Les données des périphériques compris dans le périmètre sont centralisées dans un tableau de bord	Réduction du temps passé à changer d'application, gain de temps dans la corrélation des événements
Précision : Moins de faux positifs	Gain de temps dans la distinction entre faux positifs et vrais événements
Conformité : Amélioration du reporting	Accélération de la génération de rapports à la demande lors d'un audit
Analyse a posteriori : Analyse plus rapide des incidents, traitement plus facile des demandes d'e-découverte	Gain de temps dans la reconstruction des journaux d'activité et le suivi des sources de menaces
Analyse de comportements : Découverte des schémas d'activité internes	Accélération de la distinction entre activités utilisateur normales et anormales

Réponse aux risques

Maintenant que vous avez collecté les informations pertinentes et réalisé votre analyse des risques, vous êtes en mesure de répondre au risque en formulant une réponse basée sur les données.

Options possibles

Comme nous l'avons dit, il existe quatre types de réponse aux risques :

Éviter
le risque en fermant l'activité/ le processus/le système/le site présentant un risque.

Accepter
le risque. Notez bien que ce choix vous impose de périodiquement repenser votre décision.

Transférer
le risque à l'assurance. Attention, cette option transfère uniquement le risque financier. L'entreprise reste responsable du risque matérialisé, et doit faire face aux autres types de perte, comme la perte de réputation.

Atténuer
le risque, en reconnaissant que le coût du risque matérialisé est supérieur au coût des contrôles.

Revenons une fois de plus à notre exemple : prévenir l'exfiltration de données causée par une attaque de type hameçonnage. Nous avons calculé le risque total, le coût d'implémentation des contrôles et le risque résiduel après application de ces contrôles.

Éviter le risque impliquerait d'arrêter tous les échanges d'e-mails externes… Ce qui n'est absolument pas envisageable.

Accepter le risque est une décision raisonnable lorsque la valeur des actifs concernés est trop faible pour justifier le le coût de leur protection. Dans notre exemple, nous avons évalué le coût du risque matérialisé, à savoir l'ALE, à 2,5 M €. On peut réduire ce risque d'environ 80 % en investissant 90 000 €/an en contrôles… L'acceptation du risque n'est donc pas la meilleure option.

Transférer le risque à une compagnie d'assurance peut sembler intéressant en raison d'un coût initial relativement faible. Cependant, cette option n'est pas adaptée à notre situation. Bien que la couverture de cyberresponsabilité puisse couvrir les pertes financières, elle reste limitée et ne couvre pas d'autres types d'impacts. Dans notre exemple, nous devons prendre en compte l'impact sur notre prochaine campagne de financement, un risque réputationnel non couvert en cas de transfert du risque à une tierce partie.

Enfin, il est possible d'**atténuer** le risque en appliquant des contrôles de sécurité. Dans notre cas, nous avons choisi de combiner un outil antihameçonnage et une campagne de sensibilisation à la sécurité de l'information… une approche validée par les conclusions de notre évaluation des risques.

Intégrer l'appétence au risque

Il arrive qu'une évaluation des risques ne permette pas de dégager une réponse évidente, même lorsque le coût des contrôles est clairement inférieur à celui du risque matérialisé. En effet, les ressources disponibles étant limitées, toute stratégie d'atténuation s'accompagne d'un **coût d'opportunité**. Il ne s'agit donc pas simplement de choisir entre agir ou accepter le risque, mais plutôt d'arbitrer entre plusieurs investissements.

Comprendre l'**appétence au risque** de votre entreprise vous aide à trancher dans les situations limites, où l'analyse des risques justifie une stratégie d'atténuation alors que le coût d'opportunité est élevé.

L'appétence au risque est le niveau de risque qu'une entreprise est prête à accepter pour atteindre ses objectifs. Une **appétence au risque élevée** reflète une volonté d'accepter des risques plus importants dans le but d'en retirer des bénéfices supérieurs, tandis qu'une **faible appétence au risque** traduit une préférence pour la prudence.

L'appétence au risque varie beaucoup selon le secteur, la taille de l'entreprise, les objectifs de croissance, etc. Elle a aussi plusieurs dimensions : vous pouvez accepter un risque opérationnel élevé mais avoir une faible appétence au risque de non-conformité.

Généralement, une déclaration d'appétence au risque se présente comme suit :

Appétence générale au risque **[L'entreprise XYZ] adopte une approche équilibrée du risque. Elle reconnaît que tous les risques ne sont pas égaux, et qu'il faut accepter un certain niveau de risque pour atteindre les objectifs stratégiques.**	
Risque lié à l'innovation	Notre appétence au risque est élevée lorsqu'il s'agit d'investir dans des technologies de pointe et des solutions innovantes susceptibles d'offrir un avantage concurrentiel à nos produits. Nous reconnaissons que cela implique d'accepter un certain degré d'incertitude, notamment en matière de R&D et de développement produit.
Risque opérationnel	Notre appétence au risque est faible à modérée en matière de risque opérationnel. Tout en visant l'excellence opérationnelle, nous priorisons des initiatives qui optimisent l'efficacité et la qualité de service sans jamais compromettre nos standards.
Risque lié à la sécurité	Notre appétence au risque est très faible en matière de menaces et de failles de sécurité. La sécurité réseau et la protection des données sont notre priorité absolue. Nous investissons d'ailleurs massivement pour protéger nos systèmes et les données de nos clients.
Risque lié à la conformité	Notre appétence au risque est faible en matière de non-conformité aux obligations légales et réglementaires. Nous considérons qu'il est primordial de garantir l'application des lois, normes et meilleures pratiques en vigueur pour toutes les opérations.

Dans chacune de ces dimensions, il faut tenir compte de plusieurs facteurs clés :

- La **capacité de risque** est le niveau maximal de risque que l'entreprise peut supporter. Elle dépend généralement des ressources financières, des capacités opérationnelles et des contraintes réglementaires.
- La **tolérance aux risques** représente l'écart acceptable par rapport aux objectifs.
- Les **seuils de risque** définissent les limites acceptables au-delà desquelles un changement de stratégie est nécessaire.

Le seuil qui sépare la tolérance de la capacité, ou même les différents degrés de tolérance, vous aide à clarifier les zones d'incertitude, là où la réponse la plus appropriée au risque n'est pas immédiatement évidente.

Pour revenir à notre exemple, il existe potentiellement une situation où votre start-up à croissance rapide a une appétence au risque tellement élevée et un budget de cybersécurité tellement réduit que le risque de voir une attaque par hameçonnage réussir est tolérable, en dépit du faible coût relatif des contrôles.

Astuces

Si votre entreprise dispose d'une équipe spécialisée en gestion des risques d'entreprise, sollicitez son expertise, car elle a probablement documenté l'appétence au risque dans le cadre de son processus de gestion des risques.

Votre entreprise n'a pas encore rédigé de déclaration d'appétence au risque ? Rédigez-en une à partir de ce modèle personnalisable.

Exemples

Nous avons vu comment attribuer une valeur aux actifs, évaluer les menaces et les faiblesses, déterminer la probabilité et l'impact des menaces à l'aide de méthodes qualitatives, et déterminer le risque via l'ALE. Nous avons aussi estimé le coût des contrôles (et celui de leur absence).

Forts de ces connaissances, analysons quelques exemples du début à la fin.

Astuce

Téléchargez ce modèle personnalisable pour présenter votre propre évaluation dans ce format.

Exemple 1 : Prévenir les fuites de données liées au BYOD

Énoncé du problème :

Nos collaborateurs profitent de plus en plus de notre stratégie de BYOD, qui autorise l'utilisation professionnelle d'appareils personnels. Nous n'appliquons pas encore à ceux-ci les mêmes contrôles de sécurité qu'aux périphériques d'entreprise et nous nous inquiétons de la possibilité de sortie des données confidentielles.

Cette absence de contrôles peut inciter des collaborateurs à traiter les informations d'entreprise hors de notre environnement, par exemple en envoyant des données à des adresses e-mail ou des clouds personnels, à des sites de transfert de données, à des outils d'IA, etc.

Recommandation :

Étendre au BYOD la DLP (prévention des pertes de données) actuellement en place sur les périphériques appartenant à l'entreprise éviterait les incidents de fuite de données (involontaires ou intentionnels) et améliorerait la conformité.

Évaluation des risques :

AV : Notre analyse d'impact business (BIA) évalue la valeur d'actif des données sensibles de l'entreprise à 1 million d'euros.
EF : Nous considérons qu'en cas de fuite de données nous pourrions perdre 60 % de la valeur de nos données sensibles.
ARO : L'analyse du registre des risques et des tickets de support fait ressortir la probabilité de subir un incident dangereux deux fois par an.

AV × EF = SLE ⇒ 1 M € × 0,6 = 600 000 €
SLE × ARO = ALE ⇒ 600 000 € × 2 = 1,2 M €

Incertitude : Le niveau de confiance des données est de 85 %. Certains facteurs peuvent l'affecter, notamment :

- La nature et l'étendue des données sensibles ayant fuité.
- Le mécontentement potentiel des collaborateurs.
- La possibilité que les nouveaux collaborateurs ne suivent pas la formation de sensibilisation (mesure d'atténuation actuellement en place).

<table>
<tr><th colspan="4">Réponse aux risques</th></tr>
<tr><th>Option</th><th colspan="2">Faisabilité</th><th>Risque résiduel</th></tr>
<tr><td>Évitement</td><td colspan="2">Possible : Avec l'évitement, le risque serait nul, mais il nous faudrait mettre fin à notre stratégie de BYOD, ce qui provoquerait le mécontentement des collaborateurs.</td><td>0</td></tr>
<tr><td>Acceptation</td><td colspan="2">Possible : Cette solution peut excéder notre appétence au risque. L'acceptation des risques revient à accepter les coûts financiers directs et indirects, notamment la perte de réputation, les poursuites judicaires, les amendes, les contrôles réglementaires, des avis négatifs sur les réseaux sociaux, etc.</td><td>ALE = 1,2 M €</td></tr>
<tr><td>Transfert</td><td colspan="2">Possible : Avec le transfert, l'assurance pourrait couvrir une partie des coûts. En général, la couverture cyber-responsabilité est limitée, entre 500 000 et 5 millions d'euros par occurrence. Cependant :
■ Les coûts liés à la perte de réputation, aux amendes réglementaires et aux poursuites judiciaires des clients viennent en sus, l'assurance ne les couvre pas.
■ Et, si aucun contrôle permettant d'atténuer les risques n'est mis en place, l'assurance peut cesser de nous couvrir si le problème se répète.</td><td>Incertitude. Dépend de la prime d'assurance et du nombre d'événements. Seul le risque financier est réduit.</td></tr>
<tr><td rowspan="7">Atténuation (action recommandée)</td><td colspan="3">Possible – voir ci-dessous</td><td rowspan="7">Réduction de 80 % de l'ARO, soit un nouvel ARO de 0,4. La SLE résiduelle reste identique.
Nouvelle ALE (résiduelle) = 600 000 € x 0,4 = 240 000 €</td></tr>
<tr><td colspan="2">Coûts</td><td>Bénéfices</td></tr>
<tr><td>Licences supplémentaires</td><td>30 000 €</td><td rowspan="5">Estimation : 80 % de réduction de la probabilité d'incidents de menace interne.</td></tr>
<tr><td>Heures-personnes nécessaires pour le déploiement</td><td>10 000 €</td></tr>
<tr><td>Formation des utilisateurs</td><td>10 000 €</td></tr>
<tr><td>Total année 1</td><td>50 000 €</td></tr>
<tr><td>Total pour les années suivantes</td><td>30 000 €</td></tr>
</table>

Exemple 2 : Remanier les contrôles d'accès basés sur les rôles

Énoncé du problème :

Les contrôles d'accès basés sur les rôles de notre système CRM n'ont pas été actualisés depuis 5 ans. Dans l'intervalle, notre structure organisationnelle a beaucoup changé. Par conséquent, les rôles et les privilèges associés ne correspondent plus aux rôles réels des utilisateurs du système. Ces derniers se retrouvent avec des privilèges inutiles ou excessifs, qui pourraient être exploités si un acteur de la menace récupérait des informations d'authentification.

Recommandation :

Bien que la refonte des accès basés sur les rôles représente un effort transversal significatif, ces changements ne causeront aucune interruption de service. La perte de productivité à court terme, liée à l'adaptation des utilisateurs à leur nouveau rôle, se résoudra rapidement. Ces coûts restant nettement inférieurs à la perte annuelle estimée (ALE), nous recommandons de poursuivre cet effort et nous demandons le soutien de nos collègues des équipes Ventes, Marketing et Opérations.

Évaluation des risques :

AV : Notre analyse d'impact business (BIA) évalue la valeur des données de notre système CRM à 1,5 M €.
EF : Compte tenu des autres contrôles en place (la journalisation et la surveillance, et l'authentification multifacteur), des cybercriminels pourraient accéder à environ 10 % des données sensibles et les exfiltrer.
ARO : D'après les résultats des tests d'intrusion de ces 5 dernières années (à raison de 2 tests de périmètre différent par an), nous concluons qu'il faut s'attendre à un incident/an impliquant l'utilisation d'un accès à privilèges.

AV × EF = SLE ⇒ 1,5 M € × 0,1 = 150 000 €
SLE × ARO = ALE ⇒ 150 000 € × 1 = 150 000 €

Incertitude : Le niveau de confiance des données est de 80 %. Certains facteurs peuvent l'affecter, notamment :

- La nature et la portée des données client ayant fuité.
- Le mécontentement potentiel des administrateurs.
- La fuite d'informations d'authentification due à une autre faille.

<table>
<tr><th colspan="5">Réponse aux risques</th></tr>
<tr><td>Option</td><td colspan="3">Faisabilité</td><td>Risque résiduel</td></tr>
<tr><td>Évitement</td><td colspan="3">Aucun : L'évitement réduirait le risque à 0, mais toute opération à privilèges dans notre système CRM serait impossible.</td><td>0</td></tr>
<tr><td>Acceptation</td><td colspan="3">Possible : L'acceptation est possible et peut correspondre à notre appétence au risque. Cependant, il faut aussi tenir compte des coûts indirects, comme la perte de réputation et le contrôle réglementaire.</td><td>ALE = 150 000 €</td></tr>
<tr><td>Transfert</td><td colspan="3">Possible : Le transfert à l'assurance couvrirait les coûts directs d'une occurrence (SLE = 150 000 €). En général, la couverture de la cyber-responsabilité est limitée, entre 500 000 et 5 millions d'euros par occurrence. Cependant, l'assurance peut refuser de la reconduire si le problème se répète parce qu'aucun contrôle n'a été mis en place pour atténuer la menace.</td><td>Incertitude. Dépend de la prime d'assurance et du nombre d'événements.</td></tr>
<tr><td rowspan="5">Atténuation (action recommandée)</td><td colspan="3">Possible – voir ci-dessous</td><td rowspan="5">ARO inchangé.

La réduction de 50 % du facteur d'exposition (FE) donne une SLE résiduelle de 75 000 €.

Nouvelle ALE (résiduelle) = 75 000 € × 1 = 75 000 €</td></tr>
<tr><td colspan="2">Coûts</td><td>Bénéfices</td></tr>
<tr><td>Temps de travail des équipes IT, Opérations, Marketing et Ventes pour définir les nouveaux rôles</td><td>10 000 €</td><td rowspan="3">Estimation : 50 % de réduction de l'exposition en cas d'attaque réussie.</td></tr>
<tr><td>Perte de productivité, le temps que les utilisateurs du système CRM s'adaptent à leur nouveau rôle</td><td>5 000 €</td></tr>
<tr><td>Total</td><td>15 000 €</td></tr>
</table>

Conclusion

Vous disposez désormais des outils nécessaires pour réaliser une évaluation des risques basée sur les données et présenter vos résultats d'une manière convaincante. Cet avancement majeur permet d'aligner les objectifs business de l'entreprise avec les objectifs de sécurité, tout en favorisant une compréhension mutuelle des risques entre les parties prenantes.

En outre, en adoptant un langage partagé avec le PDG et les membres du conseil d'administration, vous allez au-delà de votre objectif immédiat : vous êtes visible, écouté et soutenu financièrement.

Tout au long de cet e-book, nous vous avons proposé des outils et modèles supplémentaires. Ils vous aideront dans votre analyse. **Cliquez ici pour les télécharger :**

Modèle d'évaluation de l'impact business

Modèle de déclaration d'appétence au risque

Checklist Surface d'attaque

Modèle de rapport d'évaluation des risques

En vous souhaitant une bonne réussite !

À propos d’Ivanti

Ivanti Ivanti est un éditeur de logiciels d’entreprise qui propose une plateforme IT et Sécurité complète basée dans le Cloud. Ivanti fournit des solutions logicielles qui évoluent avec les besoins de ses clients, afin de permettre aux équipes IT et Sécurité d’améliorer l’efficacité opérationnelle tout en réduisant les coûts et en limitant proactivement les risques de sécurité. La plateforme Ivanti Neurons est native du Cloud. Elle est conçue comme base pour des services et outils unifiés et réutilisables, qui assurent la cohérence en matière de visibilité, d’évolutivité et de distribution sécurisée des solutions. Plus de 34 000 clients, dont 85 des entreprises Fortune 100, ont choisi Ivanti pour relever leurs défis grâce à ses solutions de bout en bout. Chez Ivanti, nous nous efforçons de créer un environnement où tous les points de vue sont écoutés, respectés et valorisés. Nous nous engageons aussi pour un avenir plus durable pour nos clients, nos partenaires, nos collaborateurs et la planète. Pour en savoir plus, visitez le site ivanti.com/fr et suivez-nous sur Twitter (@GoIvanti).

ivanti

Pour en savoir plus
ou pour contacter Ivanti,
visitez le site ivanti.com/fr