proofpoint.

EBOOK

Les indicateurs qui comptent :

Le guide du RSSI – Évaluer, hiérarchiser et justifier des budgets de cybersécurité adaptés à l'entreprise

proofpoint.com/fr

SECTION 1

De bouc émissaire à stratège

Pour comprendre à quel point le rôle du RSSI a évolué au cours des dernières années, il suffit de lire le témoignage d'un dirigeant lors d'une récente table ronde de Proofpoint.

« Lorsque j'ai commencé dans le secteur, le rôle du RSSI s'apparentait à celui d'un bouc émissaire », se souvient-il. La direction avait besoin de quelqu'un à blâmer si les choses tournaient mal. Mais la plupart du temps, elle privilégiait les polices d'assurance génériques aux investissements dans les équipes et solutions de sécurité. En d'autres termes, les RSSI étaient des experts en technologie qui ne disposaient que de ressources limitées.

Mais les choses sont en train de changer. Les menaces sont de plus en plus complexes et peuvent affecter bien davantage que quelques systèmes isolés au sein d'une entreprise. Et lorsque les cyberattaques se transforment en compromissions de données de grande ampleur, elles peuvent rapidement ternir ou détruire une marque.

Cela a modifié la façon dont la direction considère les investissements dans la cybersécurité, ainsi que le rôle du RSSI. Les conseils d'administration prêtent aujourd'hui bien plus d'attention aux activités des RSSI. Et comme l'indique le terme « Responsable » de leur titre, les RSSI sont étroitement impliqués dans la stratégie globale de l'entreprise. De plus en plus souvent, ils orientent sa transformation numérique de manière à gérer les risques, à optimiser les processus métier et à réduire les pertes évitables.

« Lorsque j'ai commencé dans le secteur, le rôle du RSSI s'apparentait à celui d'un bouc émissaire. ».

De nouveaux défis entraînent de nouveaux coûts

Cette évolution s'accompagne de nouveaux besoins budgétaires. Selon une étude récente de Forrester, 60 % des décideurs en matière de sécurité d'entreprise ont augmenté leurs budgets de sécurité en 2020[1].

Et ceux qui ne dépensent pas plus s'efforcent de tirer le maximum des fonds dont ils disposent. Les budgets de cybersécurité actuels doivent couvrir de nombreux défis :

- Évolution des réglementations et des exigences
- Migration progressive vers le cloud
- Adoption subite des modèles de travail à distance et hybride
- Évolution du paysage des menaces

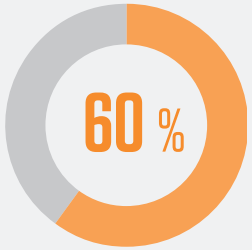
Préparer l'avenir

Tout en s'adaptant à ces changements, un grand nombre de RSSI s'attendent à ce que les budgets continuent d'augmenter (de 11 % en moyenne) afin de relever les défis à venir. Près de deux RSSI sur trois (65 %) pensent qu'ils seront mieux à même de résister aux cyberattaques et de s'en relever d'ici 2023[2].

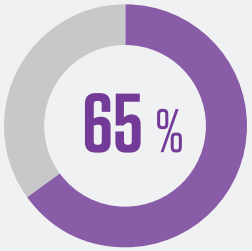
Le degré de préparation reste néanmoins une préoccupation majeure. Bien que les responsables se montrent optimistes quant à leur capacité à résister aux attaques et à s'en relever à moyen terme, ils semblent avoir moins confiance dans leurs capacités actuelles. En effet, le rapport Voice of the CISO 2021 a révélé que 66 % des RSSI estiment que leur entreprise n'est pas armée pour faire face à une cyberattaque ciblée[3].

En tout état de cause, ce sont les individus, et non plus les technologies réseau, qui constituent le nouveau périmètre. Par ailleurs, l'adoption de nouveaux modèles de travail (hybride ou en télétravail à temps plein) ne fait qu'ajouter aux défis et à la complexité de la sécurité.

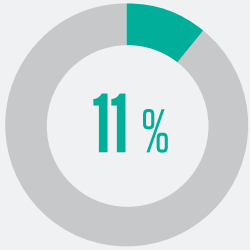
En tant que responsable de la sécurité, vous pouvez orienter votre budget de façon à gérer au mieux ces changements. Cet eBook décrit les bonnes pratiques pour évaluer les risques, déterminer la tolérance aux risques de votre entreprise, évaluer votre solution actuelle, hiérarchiser les dépenses et justifier votre budget auprès du conseil d'administration.



des décideurs en matière de sécurité d'entreprise ont augmenté leurs budgets de sécurité en 2020



des RSSI pensent qu'ils seront mieux à même de résister aux cyberattaques et de s'en relever d'ici 2023



d'augmentation des budgets pour relever les défis à venir

1 Forrester, « Global Security Budgets in 2021 » (Budgets de sécurité globaux en 2021), août 2021.
2 Proofpoint, « Voice of the CISO », mai 2021.
3 Proofpoint, « Voice of the CISO », mai 2021.

SECTION 2

Évaluation de la tolérance aux risques

Tout d'abord, évaluez votre exposition aux menaces et déterminez votre tolérance aux risques à l'aide d'un cadre adapté à votre entreprise. Il existe de nombreux cadres pour vous y aider. Lors de la discussion concernant ces sujets avec la direction et les membres du conseil d'administration, veillez à mentionner le cadre utilisé en expliquant votre choix.

Le poids des chiffres

La quantification des risques n'est pas une science exacte et peut s'avérer complexe. Cependant, prendre le temps de quantifier les risques et la tolérance aux risques de votre entreprise vous aidera à justifier votre budget par la suite. Vous pouvez également analyser les risques en termes qualitatifs, mais les indicateurs pécuniaires trouveront un écho certain auprès des dirigeants et des membres du conseil d'administration.

Par ailleurs, il est essentiel que toutes les parties prenantes soient sur la même longueur d'onde. La tolérance aux risques exprimée par les dirigeants d'entreprise lors de la planification ne correspond pas toujours à leur tolérance réelle aux risques. Pensez à élaborer des scénarios réalistes avec la direction et les membres du conseil d'administration pour vous assurer que vous parvenez à la véritable appétence de votre entreprise pour le risque.

Principaux cadres de cybersécurité

Cadre de cybersécurité du NIST

Le NIST, une division du ministère américain du Commerce, fournit des conseils sur la gestion des risques de cybersécurité et l'amélioration des communications internes et externes en matière de cybersécurité.

NISTIR 8286 : Identification et estimation des risques de cybersécurité pour la gestion des risques d'entreprise

Ce document se concentre sur la gestion des risques de cybersécurité au niveau de l'entreprise dans le contexte de la mission et des objectifs métier.

People-Centric Security Framework (PCSF)

Développé par Proofpoint suivant un processus transparent et fondé sur le consensus regroupant des parties prenantes privées et publiques, ce cadre vise à favoriser de meilleures pratiques en matière de risque humain et à aider les entreprises à protéger la confidentialité, l'intégrité et la disponibilité de leurs environnements.

SECTION 3

Maîtrise des risques

Après avoir déterminé votre exposition aux menaces et votre tolérance aux risques, vous devez évaluer les protections actuellement en place contre ces menaces.

Voir au-delà des technologies

Vous serez peut-être tenté d'envisager les risques à travers le prisme de votre pile technologique existante. Tout le monde connaît les indicateurs clés de performance opérationnelle, tels que le délai de détection, le délai de réponse et le délai de correction.

Ces indicateurs sont utiles pour générer des rapports de bas niveau et pour comprendre les performances quotidiennes des solutions spécifiques implémentées. Cependant, ils ne sont pas aussi utiles pour évaluer et communiquer votre position globale face à des risques de plus haut niveau et vos priorités métier.

Modélisation des menaces

Lorsque vous planifiez un budget et le présentez à la direction, envisagez d'utiliser une approche de modélisation des menaces pour évaluer les indicateurs de risque clés de votre entreprise ainsi que vos performances par rapport à ces indicateurs. La modélisation des menaces est un processus permettant d'identifier les menaces et leur mode d'apparition, puis de hiérarchiser les mesures de réduction des risques en conséquence. Contrairement aux indicateurs clés de performance spécifiques à une solution, la modélisation des menaces vous permet d'appréhender les risques globaux auxquels votre entreprise est exposée et d'identifier les lacunes de votre protection.

La modélisation des menaces vous aidera à identifier ce que vous faites bien, les domaines dans lesquels vous devez investir davantage et ceux où vous êtes prêt à accepter un risque résiduel. Vous pouvez évaluer un large éventail de risques de la sorte. En voici quelques-uns à envisager.

Modélisation des menaces en pratique

Voici un exemple du fonctionnement de la modélisation des menaces en pratique. Considérons les risques réglementaires. La fuite de données fait partie des scénarios pouvant entraîner un risque réglementaire. Or, la fuite de données peut découler d'un large éventail de vecteurs de menaces, tels que :

- Fuite de données de messagerie
- Transfert dans le cloud
- Sauvegarde de données sur un disque local
- Utilisation de supports amovibles
- Transfert de données vers une zone non sécurisée
- Utilisation d'un site de partage de fichiers externe
- Copier-coller manuel
- Vulnérabilités dans les applications

Tandis que vous mettez à plat chacun de ces vecteurs de fuite de données, vous pouvez évaluer votre niveau de protection et décider comment combler les lacunes.

Si vous passez directement à l'évaluation des performances de technologies spécifiques, telles qu'une solution CASB, un agent de protection des endpoints ou un réseau privé virtuel (VPN), vous risquez de négliger les failles dans la couverture des vecteurs de fuite de données que ces produits ne couvrent pas.

En utilisant une approche de modélisation des menaces pour évaluer vos indicateurs de risque clés, vous pouvez dresser un tableau plus complet et plus stratégique du degré de préparation de votre entreprise face aux différents risques.

SECTION 4

Choix de solutions

Vous pouvez ensuite vous appuyer sur votre évaluation de la tolérance aux risques et votre analyse des indicateurs de risque clés pour identifier les principaux domaines nécessitant de nouveaux investissements.

Lors de l'examen de solutions spécifiques susceptibles de répondre à ces besoins, posez-vous les questions suivantes :

- La solution réduit-elle un risque particulier ?
- La solution résout-elle un problème métier ?
- La solution permet-elle d'améliorer l'activité ? (Permet-elle l'adoption de nouveaux outils ou processus ?)
- La solution nous permet-elle de simplifier et de rationaliser nos opérations de sécurité ?
- La solution s'aligne-t-elle sur nos objectifs métier et notre tolérance aux risques ?

Vous pouvez et devez vous poser les mêmes questions pour les solutions existantes. Avant de continuer à investir dans une technologie particulière, assurez-vous qu'elle répond toujours à vos besoins.

Quantification du retour sur investissement

Pour justifier vos investissements, ainsi que le budget nécessaire pour les pérenniser, auprès du conseil d'administration, vous devez quantifier le retour sur investissement de chaque solution.

Il n'est pas toujours facile de quantifier le retour sur investissement des solutions de sécurité, mais cela peut faciliter l'adhésion de la direction. Il faut pour cela mettre en balance les avantages de la solution avec son coût.

Veillez à évaluer les coûts cachés de la solution, par exemple :

Matériel

Mise en œuvre

Logiciels

Gestion continue

Pour chaque solution, comparez le coût aux avantages, qui peuvent inclure la réduction des risques et l'amélioration de l'efficacité du personnel. Il convient également de présenter l'option consistant à ne rien faire en détaillant l'exposition aux menaces et en donnant des exemples.

Par exemple, si vous choisissiez de ne pas réduire l'impact d'un ransomware ou d'un malware, les coûts potentiels pourraient inclure :

- Perturbation des activités
- Perte de productivité des utilisateurs finaux
- Temps consacré à l'investigation des menaces et à la création de rapports
- Temps consacré à la neutralisation des menaces
- Temps consacré à l'exécution manuelle de tâches telles que la suppression de messages d'une boîte email ou la réponse aux messages de phishing signalés

Documentation des risques résiduels

Veillez également à identifier votre cyberassurance et votre risque résiduel, c'est-à-dire l'exposition aux menaces qui subsiste après vos investissements. Il est pratiquement impossible d'amener votre entreprise au risque zéro et, si c'était possible, cela n'en vaudrait probablement pas la peine. Vous devez néanmoins vous assurer que votre risque résiduel respecte le niveau de tolérance aux risques de votre entreprise.

SECTION 5

Calcul et communication des besoins budgétaires

Une fois que vous avez déterminé vos besoins budgétaires et vos domaines d'investissement, vous devez communiquer ces besoins et investissements de manière convaincante à la direction et aux membres du conseil d'administration. Vous aurez probablement plusieurs publics différents, notamment :

- Le conseil d'administration
- Les responsables opérationnels, tels que le directeur de l'exploitation ou le directeur des systèmes d'information
- Les responsables financiers, tels que le directeur financier

Un message adapté

Il est judicieux d'adapter l'analyse de rentabilité de vos investissements en matière de sécurité à chaque public. Concentrez-vous sur l'impact sur les secteurs de l'entreprise supervisés par chacun d'entre eux. C'est un peu comme dire la même chose dans trois langues différentes :

- **Le conseil d'administration —** Lorsque vous vous adressez au conseil d'administration, insistez sur la façon dont votre plan répond à la tolérance aux risques de l'entreprise. Et identifiez le risque résiduel que l'entreprise est prête à accepter.
- **Les responsables opérationnels —** Lorsque vous vous adressez au directeur de l'exploitation ou au directeur des systèmes d'information, insistez sur l'aspect opérationnel de votre message. Concentrez-vous sur les lacunes, les vulnérabilités restantes et la façon dont votre plan compensera les risques pour les opérations métier.
- **Les responsables financiers —** Avec le directeur financier, soulignez comment vous avez équilibré les dépenses ou comment vous prévoyez de corriger les domaines en déséquilibre.

Quel que soit le public, communiquez le retour sur investissement des solutions que vous avez quantifié pendant votre phase de planification. Aidez-le à comprendre ce que l'entreprise obtient pour l'argent que vous dépensez.

Retour sur investissement décroissant

Soyez prêt à expliquer le concept de « retour sur investissement décroissant ». Il se peut que vous deviez consacrer le même montant aux problèmes importants et manifestes qu'aux problèmes plus petits et moins évidents qui sont cependant tout aussi critiques. Une menace apparemment « mineure » peut exposer l'entreprise à un risque important, tel qu'une compromission de données, justifiant ainsi des dépenses considérables pour la compenser. Vous pouvez à nouveau vous référer à vos calculs de retour sur investissement pour mettre le coût de la solution en perspective par rapport au risque qu'elle réduit.

SECTION 6

Gestion des besoins hors cycle

Le processus de budgétisation suit un cycle annuel ou trimestriel. Cependant, il est inévitable que des problèmes surviennent en dehors du cycle standard, tels que des menaces émergentes ou de nouvelles tactiques des cybercriminels. Les incidents inattendus sont pratiquement impossibles à éviter, mais ils peuvent être l'occasion de réévaluer votre niveau de sécurité et de repenser vos priorités en matière de dépenses.

Coûts cachés

N'oubliez pas de prendre en compte tous les coûts associés à chaque solution que vous implémentez. La plupart des entreprises prévoient un budget pour les licences. Mais nombre d'entre elles oublient de prendre en compte le coût de la maintenance ou les ressources humaines nécessaires à la solution. Tenez compte de ces « coûts cachés » dès la planification pour éviter d'être pris au dépourvu.

SECTION 7

Accélération du processus

La budgétisation peut facilement s'avérer un processus laborieux. Cependant, il existe des moyens d'accélérer et de faciliter le processus.

Approche stratégique

Tout d'abord, embrassez pleinement votre rôle de partenaire stratégique et n'oubliez pas que le rôle même du RSSI évolue. Identifiez les objectifs poursuivis par les différentes parties prenantes et aidez-les à les atteindre à moindre risque.

Ne vous limitez pas aux opérations et au leadership technique et réfléchissez à la manière dont vous pouvez aider l'entreprise à mener sa transformation numérique et à atteindre les objectifs métier.

Équilibre entre risque et productivité

N'oubliez pas non plus que vous ne pouvez pas éliminer totalement le risque. En tant que professionnel de la sécurité, vous préférerez peut-être la prudence en matière de tolérance aux risques, mais le conseil d'administration et les autres dirigeants voudront trouver un équilibre entre l'exposition aux menaces et les objectifs métier. Par exemple, l'efficacité de votre passerelle de messagerie peut atteindre 99,1 %. Mais il suffit d'un seul email pour être victime d'une attaque de ransomware, ce qui laisse un risque résiduel de 0,9 %. Ce risque résiduel est généralement traité par l'ajout de couches de sécurité supplémentaires telles que l'isolation ou la prévention des fuites de données (DLP). Toutes les parties doivent toutefois comprendre que le risque zéro n'existe pas.

Trouvez un terrain d'entente et essayez d'éviter de devenir le « département qui dit non ». Votre budget et vos plans doivent équilibrer le risque par rapport aux priorités de l'entreprise et minimiser l'exposition aux menaces dans les limites de la tolérance aux risques de l'entreprise.

Attentes appropriées

Enfin, modérez les attentes au fur et à mesure. La plupart des départements d'une entreprise fonctionnent sur un modèle de production, dans lequel la production et des rendements élevés constituent des indicateurs clés de performance. En revanche, la cybersécurité repose sur un modèle de résilience.

C'est-à-dire que tout comme les pompiers sont payés qu'il y ait un incendie ou non, la cybersécurité nécessite un budget qui ne se traduit pas toujours par un rendement plus élevé. Or, personne n'arguera que les pompiers sont inutiles. C'est à vous qu'il incombe d'aider les autres parties prenantes à considérer la cybersécurité de la même façon.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0500-000-01-01 03/22