D’une approche « case à cocher » à une approche « cadres de référence »

Le point de vue des RSSI : recentrer les programmes de cybersécurité sur le risque et non la conformité

IBM

IBM **Center for Applied Insights**
ibm.com/ibmcai | ibmcai.com

Le risque lié à la cybersécurité constitue une menace majeure. C'est aussi une priorité des COMEX. L'augmentation des financements alloués aux initiatives de sécurité reflète la gravité de l'enjeu.

Les responsables de la sécurité se sont rendu compte que « cocher des cases » pour répondre aux exigences de conformité avait cessé d'être une stratégie suffisante. Pour leur part, les sociétés plus matures ont entrepris de transformer leurs programmes en les recentrant réellement sur le risque, et appliquent une approche sophistiquée pour déterminer les risques et hiérarchiser les investissements en matière de sécurité.

Le risque de cybersécurité est une menace majeure pour les entreprises toutes tailles confondues. Sa gestion est désormais prioritaire au niveau des Directions des Organisations. Le financement des initiatives de sécurité est en hausse, signe de l'importance de cet enjeu. Toutefois, le nombre grandissant de vols de données publiquement révélés, en dépit d'une meilleure visibilité, a conduit de nombreux RSSI (responsables de la sécurité des systèmes d'information) et d'autres spécialistes de la sécurité à examiner leurs propres motivations et hypothèses de départ. Ils recherchent depuis peu des approches fondamentales permettant d'influencer et d'améliorer leurs propres programmes de sécurité, ainsi que des bonnes pratiques permettant de définir et d'appliquer efficacement la gestion du risque.

Le présent rapport de l'IBM Center for Applied Insights, qui s'inspire de l'étude « Identifying How Firms Manage Cybersecurity Investment, » sponsorisée par IBM et réalisée par la Southern Methodist University, montre comment les RSSI font monter en puissance les projets de cybersécurité. Leur objectif est de trouver une réponse à l'une des principales difficultés sous-jacentes : les programmes de sécurité sont principalement orientés sur la conformité plutôt que sur la gestion des risques des différents métiers qu'ils sont censés servir.[1] En un mot, les RSSI savent que la conformité pure et simple n'est pas acceptable pour une entreprise correctement gérée.

Notre programme de sécurité est axé sur la conformité. Comment le recentrer sur le risque ?

Comment communiquer au mieux la notion de risque aux organisations et gérer les attentes ?

Ai-je à disposition les compétences, les processus et les outils nécessaires pour mettre en œuvre les contrôles indispensables pour réussir ?

Pour répondre à ces questions, les RSSI choisissent des approches plus sophistiquées pour qualifier les menaces, hiérarchiser et financer les initiatives de sécurité. De plus en plus souvent, les Leaders de la sécurité utilisent des cadres de référence personnalisés comme outils stratégiques pour transformer l'entreprise et la recentrer sur le risque réel lié à la cybersécurité.

À propos de l'étude

Le présent rapport de l'IBM Center for Applied Insights s'inspire de l'étude « Identifying How Firms Manage Cybersecurity Investment, » sponsorisée par IBM et réalisée par le Darwin Deason Institute for Cyber Security, qui fait partie de la Lyle School of Engineering de la Southern Methodist University de Dallas, au Texas. Les chercheurs ont interrogé plusieurs dizaines de Responsables Sécurité de différents secteurs d'activité, principalement dans les services financiers, la santé, la distribution et le secteur public.

Ils ont organisé des entretiens approfondis en s'appuyant sur une approche semi-structurée, afin d'évaluer plusieurs dimensions : exploration des grands risques liés à la cybersécurité, méthodes de définition des risques, soutiens apportés par l'entreprise aux initiatives de cybersécurité et hiérarchisation des financements.

A propos de l'IBM Center for Applied Insights

ibm.com/ibmcai | ibmcai.com

L'IBM Center for Applied Insights introduit de nouvelles façons de penser, de travailler et de diriger. Grâce à une étude basée sur des données probantes, le Centre apporte aux dirigeants des orientations pragmatiques et des arguments en faveur du changement.

Quelles difficultés pour les RSSI ?

Privilégier l'aspect stratégique

Traditionnellement, les décisions d'investissement en cybersécurité étaient en général déterminées par les obligations de conformité, et y répondaient avec des solutions mettant en œuvre les meilleures pratiques et des technologies reconnues sur marché. C'était l'approche « case à cocher » qui prévalait pour répondre aux exigences de base.

Les meilleures pratiques sectorielles constituaient un banc d'essai permettant aux RSSI de juger s'ils avaient apporté une réponse efficace aux principaux facteurs de risque dans leur entreprise. Si leurs homologues avaient mis en place des mesures, ils savaient qu'ils avaient intérêt à en faire de même. Et si l'entreprise était en conformité, l'affaire était classée. Le défi des RSSI consiste dans le fait que trop souvent, une approche axée sur la conformité ne protège pas l'organisation des risques de sécurité réels auxquels elle est confrontée.

Communiquer sur les priorités

Si la majorité des principaux dirigeants dans les entreprises sont conscients de l'importance de la cybersécurité, il reste aux RSSI à communiquer sur les besoins stratégiques et techniques dans un langage clair et accessible pour les membres du COMEX.

De leur propre aveu, il est aussi souvent difficile de démontrer le retour sur investissements (ROI) des projets de sécurité. En fait, de nombreuses entreprises considèrent désormais la sécurité comme une dépense nécessaire. Les indicateurs de mesure restent cependant précieux pour obtenir le soutien à certaines initiatives dépendant de la stratégie de cybersécurité.

Créer une stratégie de cybersécurité réalisable

Souvent, la principale préoccupation des membres du COMEX n'est pas de financer les initiatives de cybersécurité, mais de savoir si les équipes de sécurité sont capables de mettre correctement en œuvre les contrôles et de gérer une multitude de projets de soutien à l'entreprise.

Une partie de la difficulté provient du fait que la stratégie de cybersécurité n'est pas toujours réalisable. Pouvoir la relayer par le biais d'un plan d'implémentation clair, sélectionner les bonnes solutions et élaborer un planning de déploiement qui ne perturbera pas le fonctionnement de l'entreprise : ce sont autant de facteurs critiques qui entrent en jeu.

Les RSSI sont confrontés à la difficulté de trouver des candidats capables de gérer le déploiement : les profils requis doivent associer une combinaison rigoureuse de maîtrise technique et une bonne connaissance de l'activité métier. Les RSSI doivent de plus toujours se tenir au courant des tendances du marché, des meilleures pratiques sectorielles et de l'arrivée des nouveaux produits de sécurité.

« Une bonne conformité n'est pas synonyme de bonne sécurité. »

– Un RSSI dans le secteur public.

88 %

des responsables de la sécurité de l'information indiquent que leurs budgets de sécurité ont augmenté.

Trois grands défis pour les RSSI

Privilégier l'aspect stratégique

« J'essaie toujours de faire passer en dernier l'argument de la conformité. A mon avis, bien trop de solutions se contentent de faire le strict nécessaire et rien de plus. »

– Un RSSI du secteur de la distribution.

Communiquer sur les priorités

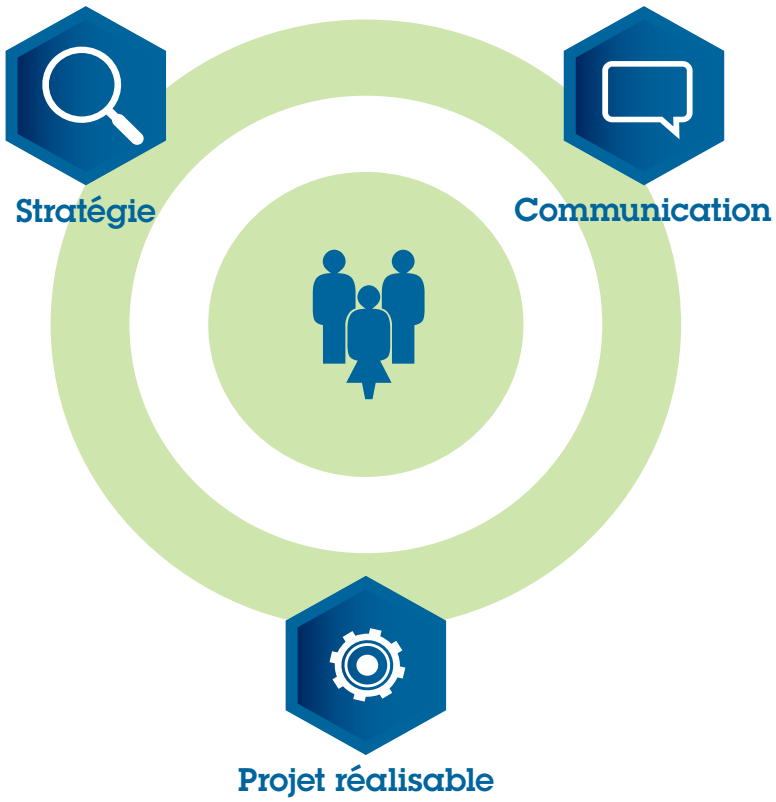
« Ma mission, pour la Direction, est d'expliquer la stratégie de sécurité en termes de projets et de coûts et dans un langage clair. »

– Un RSSI du secteur de la distribution.

Une stratégie de cybersécurité réalisable

« Peu importe que l'outil soit excellent si personne ne met concrètement en application le programme. »

– Un RSSI dans les services financiers.



Des cadres de référence centrés sur le risque qui représentent et mettent en œuvre la stratégie de cybersécurité

Pour relever les défis posés par la stratégie, la communication et la mise en œuvre, les RSSI favorisent de plus en plus souvent des cadres de référence adaptés qui formalisent leur approche de la cybersécurité.

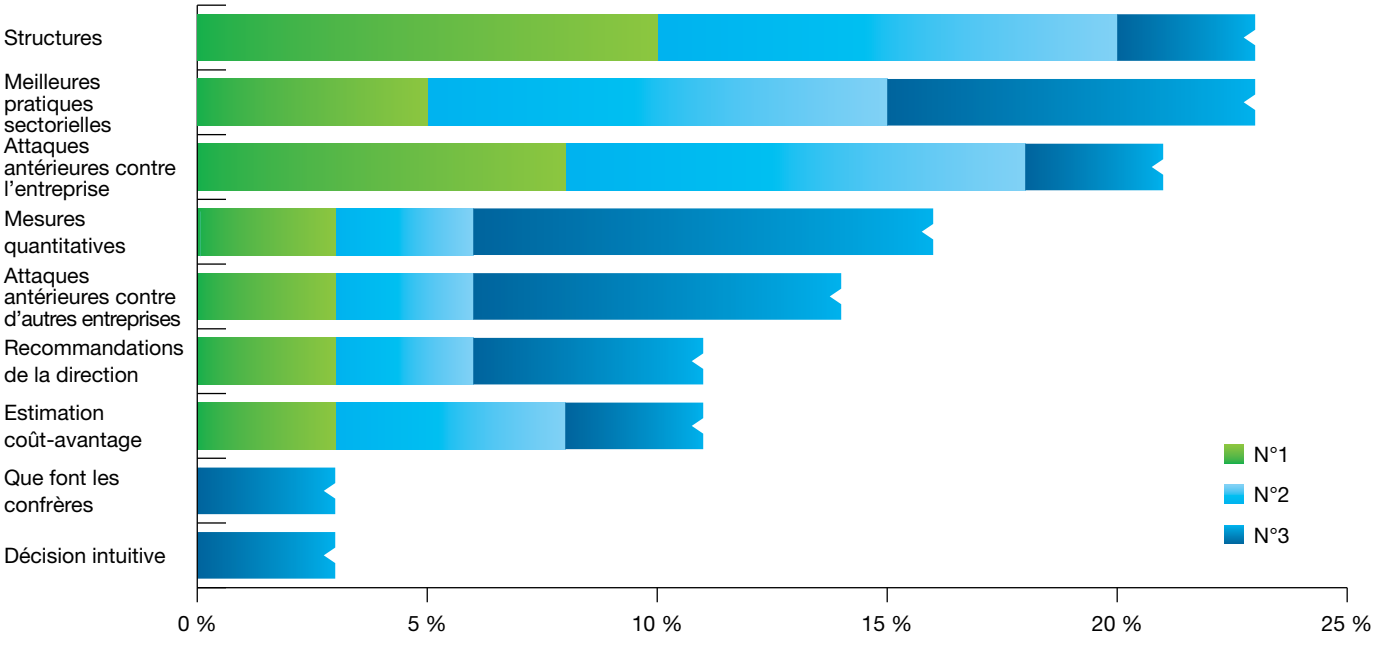
Les cadres de référence centrés sur le risque fournissent des normes, des meilleures pratiques et des directives visant à protéger les systèmes, les applications et les données. Les cadres de référence retenus englobent les normes les plus répandues, telles que NIST, ISO 2700 et COBIT, mais aussi des approches hybrides personnalisées en fonction des besoins de l'organisation. Ces cadres de référence sont en passe de devenir l'outil stratégique par excellence pour évaluer le risque, hiérarchiser les menaces, sécuriser les investissements et communiquer sur la progression des initiatives de sécurité les plus urgentes.

Créer des politiques efficaces

Le RSSI d'une société de services financiers travaille dans le cadre d'une stratégie claire dotée de « trois lignes de défense ». Sous la houlette du directeur d'exploitation, qui bénéficie d'une visibilité totale de toutes les opérations de l'organisation, le DSI élabore les politiques relatives au risque, autrement dit définit *ce qui est nécessaire,* tandis que le RSSI est chargé de réaliser la mise en œuvre concrète de ces politiques : il gère leur *mode d'application*. C'est la différence entre les politiques reposant sur des principes, qui gèrent la stratégie, et les politiques de réalisation, qui gèrent la mise en œuvre de la stratégie.

Cette approche permet au RSSI de créer des politiques de réalisation et d'investir dans les contrôles capables de répondre aux vraies menaces sous-jacentes qui visent l'organisation. Les investissements sont ainsi définis par les attentes des clients et non par la demande interne. Un déploiement graduel des contrôles de sécurité évite en outre les interruptions de l'activité et garantit un impact positif sur la sécurité globale.

Les cadres de référence sont considérés comme l'approche de hiérarchisation la plus stratégique



Au-delà de la conformité : l'évolution vers une stratégie centrée sur le risque

Un grand nombre des RSSI interrogés ont reconnu que les solutions traditionnelles, centrées sur la conformité de la sécurité, leur permettaient d'être en règle, mais ne garantissaient pas une bonne préparation de l'entreprise face aux risques de violations de sécurité.

Les cadres de référence, en revanche, fournissent un meilleur modèle d'évaluation du risque, et permettent à l'organisation de réaliser une estimation plus rigoureuse et plus cohérente des problèmes de sécurité et de détecter les lacunes. La plupart des cadres de référence contiennent des éléments tels que les actifs métier, les processus, les vulnérabilités et les probabilités, mais les RSSI soulignent que la vraie valeur est qu'il est possible de les adapter en fonction de leur environnement. Cette personnalisation évite aux cadres de référence de se transformer en solutions de « cases à cocher » plus sophistiquées.

Les entreprises qui développement leur propres cadres de référence de cyber-risque comprennent en général plus en profondeur les risques réels de leur organisation. Dans la plupart des cas, des éléments de cadres de référence existants tels que NIST et COBIT sont utilisés comme base de départ pour créer des cadres de référence sur mesure servant de référence aux normes en vigueur dans toute l'entreprise.

Guides d'implémentation de la cybersécurité

Le Responsable de la conformité de la sécurité dans une société de gestion de données a choisi une approche différente, davantage centrée sur l'évaluation du risque de cybersécurité et moins sur la mise en œuvre à proprement parler de la stratégie de cybersécurité. Son équipe a mis au point un guide de projets qui définit les caractéristiques de chaque système à protéger. Ce guide définit une approche qui est ensuite appliquée par le responsable de la sécurité.

Ce dernier insiste sur l'intérêt des tests en continu : « Je ne crois pas à la sécurité de l'email, d'Internet ou de quoi que ce soit d'autre. C'est tout. » Fort de sa propre formation de PenTesteur, il teste constamment les applications externes de l'entreprise à partir d'un emplacement extérieur, préalablement doté de contrôles permettant de gérer les scénarios de type « zero-day ». L'agilité permet au dispositif de sécurité de réagir rapidement et de protéger l'entreprise.

« L'équipe de sécurité doit avoir une base de départ pour défendre son point de vue d'une façon convaincante et étayée par une réflexion. Elle ne peut pas se contenter d'argumenter qu'une solution doit être mise en place parce que c'est la dernière nouveauté à la mode. »

– Un RSSI du secteur de la distribution.

Les programmes de cybersécurité stratégiques comprennent cinq grands éléments

Une collaboration accrue avec la Direction

Les cadres de référence se sont aussi révélés être un outil de communication efficace. Ils fournissent aux RSSI un mécanisme de clarification qui leur permet de relayer la stratégie de cybersécurité auprès des équipes dirigeantes. 85 % des RSSI disent être davantage soutenus par la Direction dans le cadre de leurs projets de cybersécurité et 88 % précisent que leurs budgets de sécurité ont augmenté.

Néanmoins, plus de la moitié d'entre eux estiment insuffisantes les dépenses consacrées aux initiatives de sécurité dans leurs propres organisations et par leurs homologues dans d'autres sociétés. Fait digne d'intérêt, un quart des RSSI interrogés et qui jugeaient le niveau de dépenses bien adapté utilisaient aussi les cadres de référence comme outil stratégique.

85 %

des RSSI disent être davantage soutenus par la direction dans le cadre de leurs projets de cybersécurité

Orchestrer le cycle de vie de la cyberdéfense

Le RSSI d'une société de services financiers a choisi une approche ciblée des cadres de référence afin d'apporter une réponse aux priorités métier de l'entreprise. S'appuyant sur les standards NIST, ISO et SANS, il a mis au point un cadre de référence personnalisé capable de riposter aux attaques subies par l'entreprise.

Le cadre de référence privilégie les grands risques tels que la perte de données financières, la compromission de comptes financiers, la continuité opérationnelle et le risque réglementaire. Il identifie aussi les principaux acteurs des menaces, notamment les hacktivistes et les groupes de crime organisé.

Son équipe a élaboré un plan de déploiement graduel mettant en place une protection contre les risques les plus courants, à l'aide de divers outils orchestrés de manière à englober tout le cycle de vie de la cyberdéfense. Ce plan garantissait la continuité opérationnelle même en cas de défaillance d'un outil. Au lieu de consulter un réseau de confrères RSSI pour orienter ses décisions d'investissement, ce non-conformiste a choisi d'écouter la communauté des sociétés en capital-risque de la Silicon Valley pour se former aux nouveaux outils de rupture capables de l'aider à relever les enjeux de sécurité de son entreprise.

« Il semble que nous soyons tous engagés dans une course aux cyberarmements dont il est impossible de se retirer et qui n'admet aucun traité. Nous n'avons pas d'autre choix que de répondre à cette menace. »

– Un RSSI dans les services financiers.

Mise en application des connaissances sur les cadres de référence cybersécurité

Forts de connaissances obtenues grâce aux nouveaux cadres de référence stratégiques, quels facteurs les RSSI considèrent-ils comme des priorités d'investissement ? « La réduction du risque perçu » et la « conformité » arrivent toujours en tête de liste. Ils sont les critères de référence permettant de mesurer si les objectifs de sécurité élémentaires sont atteints. Les obligations de conformité phagocytent toujours une part considérable du budget de sécurité. Toutefois, la réduction du risque perçu, évaluée à l'aide d'une approche « cadre de référence », impulse l'investissement dans d'autres projets de sécurité.

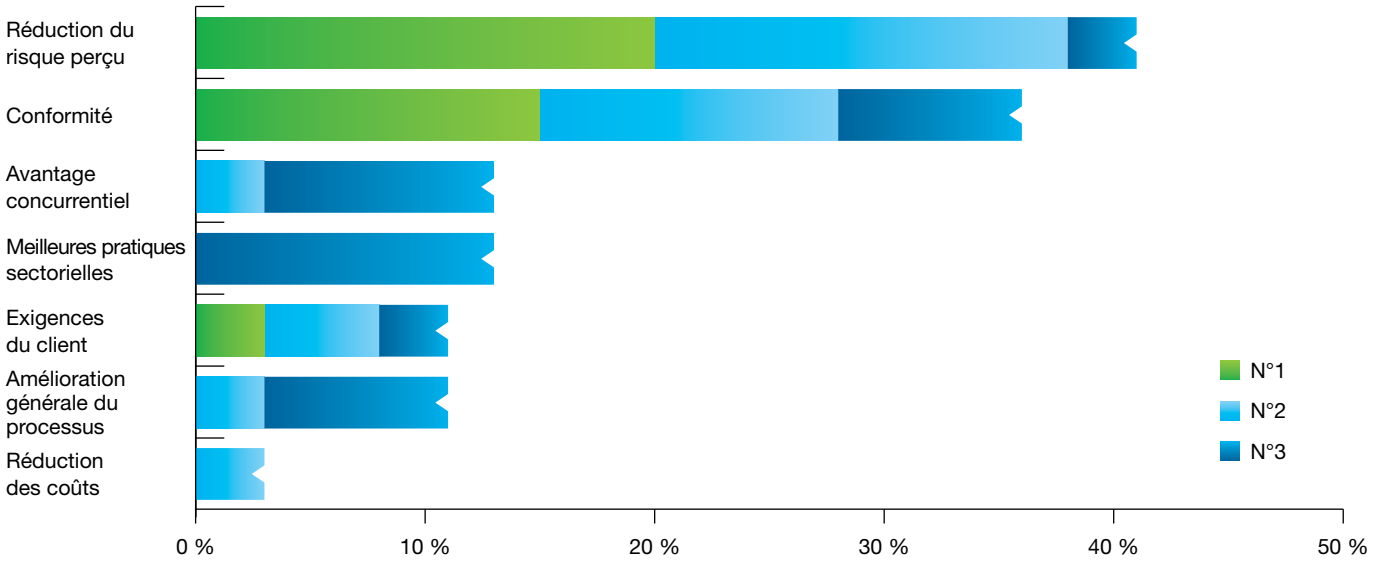
Mais même en cas de financement adapté des projets de sécurité, de nombreux RSSI se heurtent à des obstacles de mise en œuvre, surtout à l'heure de trouver les compétences nécessaires. Certains RSSI, se voyant refuser leurs demandes de budgets par la Direction, ont découvert que cette dernière estimait que l'équipe de sécurité ne pourrait pas absorber les dépenses de sécurité approuvées et les mettre en œuvre correctement. Cette pénurie de talents a conduit de nombreux RSSI à se tourner vers des sous-traitants pour pallier les lacunes et parfois à leur confier le rôle de formateurs des équipes internes.

Une récente étude de l'IBM Center for Applied Insights, intitulée « Shaping security problem solvers: Academic insights to fortify for the future » souligne également la nécessité de cultiver les compétences requises en sécurité pour répondre aux besoins croissants des entreprises.[2] Les cursus en sécurité actuels forment des spécialistes polyvalents, compétents tant les domaines techniques qu'économiques. Ils peuvent jouer le rôle d'intermédiaires entre le service informatique et l'entreprise, et apportent des compétences en analyse prédictive et comportementale qui sont essentielles pour gérer les programmes de cybersécurité.

« Le secret est de créer un nouvel ensemble de compétences qui permettra aux individus de s'adapter à des environnements en constante évolution, au lieu de se contenter de les former aux techniques de pointe en cybersécurité. »

– Un maître de conférences en Sécurité des Données, Etats-Unis.

Les cadres de référence sont considérés comme l'approche de hiérarchisation la plus stratégique



Quelles que soient leurs missions – évaluation du risque, identification des menaces ou choix des outils à inclure dans leur stratégie de cybersécurité – les RSSI font en majorité appel à des réseaux de confrères et à des informations extérieures pour prendre leurs décisions. Certains RSSI apprécient d'utiliser des flux de données externes de renseignements sur les menaces afin d'améliorer la visibilité des menaces de sécurité. D'autres font le choix de la technologie de prévention des pertes de données (DLP). Au vu de ces sources, 85 % des RSSI estiment disposer de l'information suffisante pour sélectionner les offres de sécurité adaptées à leur entreprise.

85 %

des RSSI estiment disposer de l'information suffisante pour sélectionner des solutions de sécurité pour leur entreprise.

Elever le niveau de la stratégie de cybersécurité

Il reste certes toujours des inconnues et tous les RSSI craignent l'effet de l'angle mort. Néanmoins, l'utilisation d'un cadre de référence offre une meilleure préparation, veille à la mise en place des contrôles adéquats et garantit la protection de l'entreprise. En personnalisant des cadres de référence conformes aux normes de l'industrie, en leur intégrant des renseignements extérieurs et des informations en provenance de leurs réseaux professionnels, les spécialistes de la cybersécurité font face aux risques réels qui menacent leurs entreprises. Par ailleurs, les cadres de référence eux-mêmes sont devenus un prisme d'une importance capitale : par leur intermédiaire, la direction définit la perception du risque et décide des priorités des investissements de sécurité.

Faites évoluer votre programme de cybersécurité

Au-delà de la conformité : passez à une stratégie centrée sur le risque
Personnalisez les cadres de référence pour faire une évaluation stratégique des risques réels courus par l'entreprise. Mettez en avant les priorités de la cybersécurité.

Améliorez la collaboration avec les dirigeants
Utilisez les cadres de référence comme un outil de communication. Relayez la stratégie de cybersécurité d'une façon plus claire et convaincante auprès des décideurs.

Mettez en œuvre les connaissances en cybersécurité définies par les cadres de référence
Faites appel aux bons profils, à des renseignements externes et aux meilleures pratiques sectorielles pour mettre en œuvre les directives des cadres de référence.

A propos des auteurs

Bob Kalka est Vice-président d'IBM Security, en charge des avant-ventes au niveau International, des Comptes Stratégiques et des programmes de formation des forces de vente et d'avant-vente en Sécurité. Il a occupé différentes fonctions de direction dans plusieurs secteurs : gestion de produits, ventes, développement d'activité, gestion du marketing et développement de produit. Il détient la certification CRISC (Certified in Risk and Information Systems Control) d'ISACA ainsi qu'une certification ITIL. Il a également déposé un brevet concernant un logiciel distribué sécurisé aux Etats-Unis. Pour le contacter, écrivez-lui à l'adresse bkalka@us.ibm.com.

Cynthya Peranandam est Consultante Principale auprès de l'IBM Center for Applied Insights, où elle anime des débats stratégiques. Elle a auparavant supervisé la stratégie marketing des solutions IBM Social Business et de la plateforme de cloud privé d'IBM. Elle a collaboré avec des clients dans toutes les dimensions de l'univers numérique et a impulsé l'adoption et la commercialisation de technologies émergentes par le biais du programme IBM destiné aux premiers utilisateurs. Pour la contacter, écrivez-lui à l'adresse cynthya@us.ibm.com ou sur Twitter @cperanandam. Vous pouvez également consulter ses articles sur le blog de Center.

Contributeurs

David Jarvis
Caleb Barlow
Sue Ann Wright
Ellen Cornillon
Laura DeLallo
Angie Casey
Walker Harrison

Compagnie IBM France
17 Avenue de l'Europe
92 275 Bois-Colombes Cedex

La page d'accueil d'IBM est accessible à l'adresse suivante :
ibm.com

[1] « Identifying How Firms Manage Cybersecurity Investment, » Southern Methodist University, octobre 2015, http://bit.ly/CISO-cybersecurity-investment

[2] Jarvis, David. *Shaping security problem solvers: Academic insights to fortify for the future*, IBM Center for Applied Insights, 2015, http://bit.ly/academic-insights-on-cybersecurity

Les conclusions du présent rapport ne sont pas censées être validées par le Darwin Deason Institute for Cyber Security de la SMU. Le Darwin Deason Institute for Cyber Security n'exprime aucun accord ou désaccord avec les opinions présentées dans ce rapport.

Pensez à recycler ce document

WGL03092-FRFR-01