Gagner en force pour affronter l'avenir

Conclusions du bilan IBM 2014 des directeurs de la sécurité informatique

IBM

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

On prétend que l'avenir n'a pas de limite. C'est une hypothèse bien inquiétante pour les responsables de la sécurité informatique. Déjà chargés de protéger l'entreprise contre une multitude de menaces en constante évolution, ils devraient aussi faire face à de nouveaux boulevards d'attaques plus sophistiquées.

Notre étude met en évidence les inquiétudes actuelles des responsables de la sécurité et les actions envisageables pour gérer les incertitudes à venir.

Etre le gardien du monde de l'informatique est de plus en plus difficile. L'innovation informatique avance à toute allure, produisant de nouvelles technologies remarquables et percutantes, qui élargissent souvent le périmètre des responsables de la sécurité en matière de défense. Face à l'enthousiasme généré par la puissance croissante des mobiles, du cloud et du big data, une diligence équivalente doit être consacrée à la sécurité. Sans parler des défis existants, tels que la gestion des risques informatiques, les réglementations, la conformité et la capacité à collaborer de façon efficace.

Le succès est loin d'être assuré... Combien de fois cette année uniquement, la presse a-t-elle relaté des atteintes aux données ou des atteintes à la sécurité des informations ? Alors que les responsables actuels de la sécurité des informations essaient de mettre en évidence diverses menaces dirigées contre leur entreprise, ils se retrouvent eux-mêmes sous le feu des projecteurs.

L'évaluation CISO 2012 de l'IBM Center for Applied Insights, la première évaluation de cette série, a créé trois archétypes pour les responsables de la sécurité – le Défenseur, le Protecteur et l'Influenceur- et a commencé à étudier leurs caractéristiques. Un an plus tard, l'évaluation CISO 2013 a fourni des étapes pratiques pour aider les responsables de la sécurité à atteindre la position d'Influenceur et a montré comment cette transition pourrait définir une nouvelle norme de leadership en matière de sécurité.

L'édition 2014 de l'évaluation CISO détermine l'état actuel du leadership en matière de sécurité et ce à quoi s'attendent les responsables pour les trois à cinq prochaines années. Les responsables de la sécurité sont au milieu d'une évolution. Devant faire face au spectre des attaques extérieures et aux besoins de leur propre organisation, ils évoluent vers un rôle de leadership dans l'entreprise qui met l'accent sur la gestion des risques et une approche plus intégrée et systémique.

Quelle est la prochaine étape dans l'évolution du leadership en matière de sécurité? Dotés d'un planning déjà bien chargé, que peuvent faire les responsables de la sécurité pour mieux se préparer et anticiper ?

Principaux thèmes

1. S'élever au-dessus d'un paysage transformé
2. Beaucoup d'inquiétudes par rapport aux menaces extérieures
3. L'attente de davantage de collaboration externe
4. Toujours axés sur la technologie d'aujourd'hui
5. Incertitudes quant à l'action du gouvernement

À propos de l'étude

Pour comprendre les conditions actuelles des responsables de la sécurité et obtenir un aperçu du paysage du futur, l'IBM Centre for Applied Insights, en collaboration avec IBM Security, a mené des entretiens approfondis avec 138 responsables de la sécurité – les dirigeants informatique et métier en charge de la sécurité des informations dans leur entreprise. Certains de ces responsables avaient le titre de Directeur de la sécurité informatique, mais compte tenu de la diversité des structures organisationnelles, certains ne portaient pas ce titre. Les autres personnes interrogées incluaient des responsables des technologies de l'information, des directeurs de la sécurité informatique et des directeurs de la sécurité. Soixante-trois pour cent des organisations interrogées avaient un Directeur de la sécurité informatique. La participation a couvert une large gamme de secteurs d'activité et cinq pays différents.

S'élever au-dessus d'un paysage transformé

Les responsables de la sécurité et leurs organisations observent des changements spectaculaires dans le paysage environnant : 82 % des répondants ont affirmé que la définition même de la sécurité avait changé au cours des trois dernières années. Les entreprises ne sont pas simplement en train de finaliser les détails de leur politique de sécurité, elles reconsidèrent l'ensemble de leurs stratégies pour tenir compte de l'expansion des données, des systèmes, des besoins utilisateurs et de l'importance générale de la sécurité à chaque point de liaison de l'entreprise.

Cette transformation s'accompagne d'un élargissement correspondant du rôle de Directeur de la sécurité informatique et des rôles similaires. Alors que ces dernières années, de nombreux professionnels de la sécurité aspiraient à devenir des influenceurs stratégiques, 61 pour cent des répondants de cette année se considèrent comme tels. En outre, 64 % considèrent leur stratégie de sécurité d'entreprise documentée comme très mature. Ce changement témoigne de la maturité croissante du rôle de responsable de la sécurité au sein d'entreprises de plus en plus conscientes des risques.

Cette autorité accrue n'est pas fondée sur un besoin spéculatif. Les responsables de la sécurité devront user de leur influence pour gérer un plus large éventail de menaces extérieures et des attentes plus élevées au sein de l'entreprise. Une application plus étendue de ce qui doit être protégé (p. ex., cloud, mobilité, etc.) et de nouvelles technologies de sécurité ont également contribué à cette tendance allant vers une complexité accrue. Les Directeurs de la sécurité informatique ne sont plus des organisateurs de la technologie de sécurité mais plutôt des décideurs qui doivent toujours prendre en compte les opérations métier. Les responsables de la sécurité obtiennent plus de pouvoir et l'utilisent pour contribuer aux objectifs plus vastes de l'entreprise tout en gérant les risques à chaque étape du chemin.

Obtenir davantage d'influence et de support

Influence

90 % Parfaitement d'accord sur le fait qu'ils ont une influence déterminante sur leur organisation

76 % Estiment que leur degré d'influence s'est accru de façon significative au cours des trois dernières années

Support organisationnel

71 % Parfaitement d'accord sur le fait qu'ils reçoivent le support organisationnel dont ils ont besoin

Collaboration interne

82 % Participent aux réunions de l'équipe dirigeante/stratégique chaque trimestre ou plus fréquemment

62 % Développent leur stratégie en matière de sécurité en conjonction avec d'autres stratégies (principalement, risque et opérations)

Figure 1. Cette maturité et cette influence croissantes sont nécessaires pour faire face à un paysage des menaces externes plus compliqué.

Perspective des directeurs de la sécurité informatique : un profil renforcé pour des défis plus ardus

par Jonathan Klein, Directeur de la sécurité informatique, Broadridge Financial Solutions

Mon profil en tant que Directeur de la sécurité informatique s'est développé au cours de ces dernières années. J'ai plus d'influence et je rencontre régulièrement les membres de l'équipe dirigeante et d'autres cadres supérieurs. Mais parce que la sécurité de l'information continue à devenir plus complexe, de nombreux défis restent à relever – je dois donc garder le rythme en termes de responsabilités et de capacités générales. Broadridge fournit toute une gamme de services technologiques et de traitement pour les établissements financiers. Dans ce rôle, nous devons traiter l'un des actifs les plus précieux de nos clients : leurs données.

L'un des plus grands défis des entreprises aujourd'hui est l'intégration des technologies de sécurité avec les processus métier appropriés. De nouvelles technologies promettent souvent de résoudre les dernières menaces de sécurité, mais elles sont inefficaces si elles ne sont pas correctement intégrées aux processus métier. J'amène les cadres de Broadridge à intégrer les considérations de sécurité et de risques dès les premiers stades de leurs décisions métier et à s'assurer que la technologie de sécurité protège non seulement notre organisation mais évolue également avec nos processus métier et nos stratégies.

Par exemple, il existe toute une variété de normes de données qui sont censées être totalement sécurisées. Les entreprises s'attendent trop souvent à ce que le respect de ces normes assure la sécurité des informations sensibles pour l'ensemble du cycle de vie des données, sans mesures complémentaires. Cette approche s'est avérée être une hypothèse dangereuse comme l'ont démontré des atteintes aux données de grande envergure. Chez Broadridge, nous nous concentrons sur la sécurisation des données que nous traitons. Nous ne nous contentons pas de cocher une case sur un formulaire de conformité.

La consumérisation de l'informatique crée également des complications. Il n'y a plus de distinction claire entre l'utilisation personnelle et professionnelle des systèmes et des applications. Cette situation conduit souvent à un accès public à des technologies conçues à l'origine pour être privées. Elle provoque également un retard de la sécurité par rapport aux nouvelles technologies rapidement adoptées par les consommateurs. L'accent est mis davantage sur les nouvelles fonctionnalités plutôt que sur la sécurité, ce qui rend difficile pour les entreprises d'adopter rapidement ces nouvelles technologies tout en évaluant également leur impact réel sur la sécurité.

S'assurer que la sécurité est la pièce maîtresse et non la touche finale, sera un impératif clé pour le Directeur de la sécurité informatique dans le cadre de l'influence croissante de son rôle.

Beaucoup d'inquiétudes par rapport aux menaces extérieures

Une maturité et une influence accrues sont essentielles à la lumière des défis posés par les menaces persistantes, les entreprises criminelles, les hackers parrainés par des gouvernements, les hacktivistes et autres cyber-criminels. Cette menace est considérée *si* importante à la fois par les responsables de la sécurité et par leur organisation que beaucoup estiment être en train de perdre le combat. Près de 60 % des responsables de la sécurité interrogés ont déclaré que la sophistication des assaillants dépassait celle de leur défense. Plus de 80 % des responsables de la sécurité ont vu la menace extérieure augmenter au cours des trois dernières années et celle-ci est considérée comme le défi actuel le plus important. En outre, l'accent mis sur la menace extérieure ne va pas diminuer dans le futur, car la moitié des dirigeants interrogés estiment que cette menace exigera les plus gros efforts organisationnels au cours des trois à cinq prochaines années.

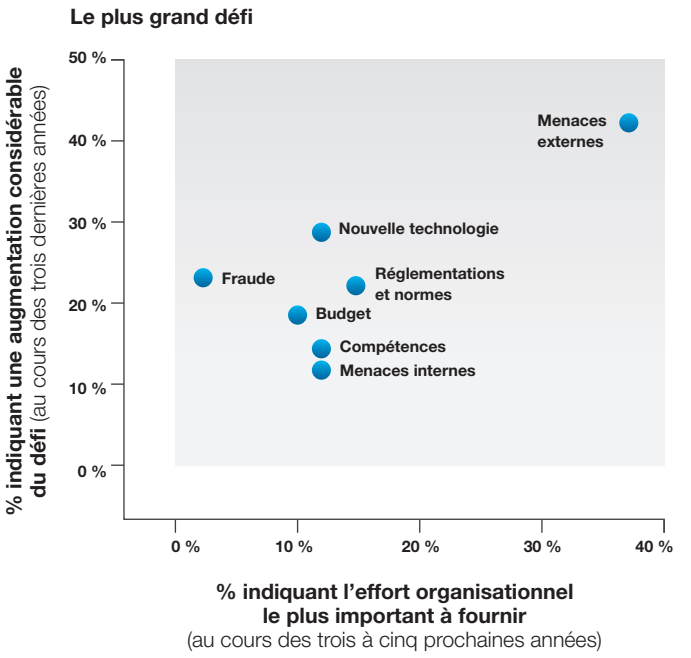


Figure 2. Les responsables de la sécurité vont continuer à se concentrer sur les menaces externes dans le futur proche et travailler à réduire le risque.

Perspective des directeurs de la sécurité informatique : améliorer les stratégies de sécurité grâce à la collaboration

Par John Taylor
Ancien responsable mondial de la sécurité informatique, British American Tobacco

La collaboration externe permet aux responsables de la sécurité d'observer les pratiques du secteur et d'évoluer avec leurs pairs – pour mieux comprendre où se passent les « bonnes choses ». En outre, elle permet la formulation d'idées qui peuvent être utilisées dans votre propre environnement. Chez British American Tobacco, nous avons mis en place toute une variété de mesures collaboratives – formelles et informelles – pour nous assurer de pratiquer un partage suffisant avec nos homologues.

Nos relations les plus approfondies concernent les collègues de notre secteur d'activité, suivis par les fournisseurs et les partenaires, puis les gouvernements. J'avais pour habitude d'envoyer des membres de l'équipe assister aux conseils consultatifs mondiaux et j'invitais des experts pour diriger des discussions mais j'ai également obtenu des informations au cours de dîners informels ou de discussions autour d'un café. L'objectif était de recueillir des idées et de savoir ce que les gens observaient en termes de nouveaux défis et de nouvelles menaces. Cela peut sembler un peu paradoxal, mais à mesure que la protection de la vie privée et la rétention des données deviennent plus difficiles, la clé pour être plus sécurisé consiste à être plus ouvert.

Toutefois, il faut se réserver une bonne dose de cynisme quant aux groupes à créer ou à rejoindre, car en avoir un trop grand nombre dilue le but et réduit la valeur. Nous devons supporter uniquement les groupes les plus efficaces et nous devons nous assurer qu'ils ont une vue à 360 degrés des risques potentiels.

Pour que la collaboration évolue, certains groupes doivent être exclusivement des professionnels de la sécurité, mais d'autres doivent être supportés par les organisations membres, les fournisseurs et les partenaires. Les DSI doivent également être inclus dans les groupes plus larges et non pas limités au groupe des responsables de la sécurité. Lorsqu'il s'agit de collaboration, nous, dans la fabrication, pouvons observer des secteurs d'activité plus expérimentés pour nous orienter. Le secteur bancaire a toujours fait beaucoup pour partager l'information (en particulier sur les menaces) pour aider à protéger ses grands volumes d'informations privées et ses actifs financiers, créant un modèle auquel les autres industries devraient aspirer.

La réalité, sur le plan des menaces actuelles, qui sont en permanente évolution, c'est que nous ne pouvons pas tout protéger entièrement. D'autres entreprises font face aux mêmes difficultés, donc avoir le point de vue de mes pairs me permet d'améliorer nos stratégies autour de nos informations les plus sensibles.

Le besoin de plus de collaboration externe

À mesure que les frontières de la sécurité de l'information des entreprises se développent, fusionnent et disparaissent, les responsables de la sécurité doivent de plus en plus sécuriser des écosystèmes entiers et non pas simplement leur propre organisation. La protection au moyen de l'isolement est de moins en moins réaliste dans le monde d'aujourd'hui : 62 % des responsables de la sécurité ont reconnu que le niveau de risque de leur organisation augmentait en raison du nombre d'interactions et de connexions avec les clients, les fournisseurs et les partenaires. Mais malgré l'interconnectivité généralisée qui régit les entreprises actuelles, les responsables de la sécurité eux-mêmes ne collaborent pas suffisamment. Actuellement, seulement 42 % des organisations interrogées font partie d'un groupe de sécurité officiel associé à leur secteur d'activité. Toutefois, 86 % pensent que ces groupes vont devenir de plus en plus nécessaires dans les trois à cinq prochaines années.

Partage des informations sur les menaces

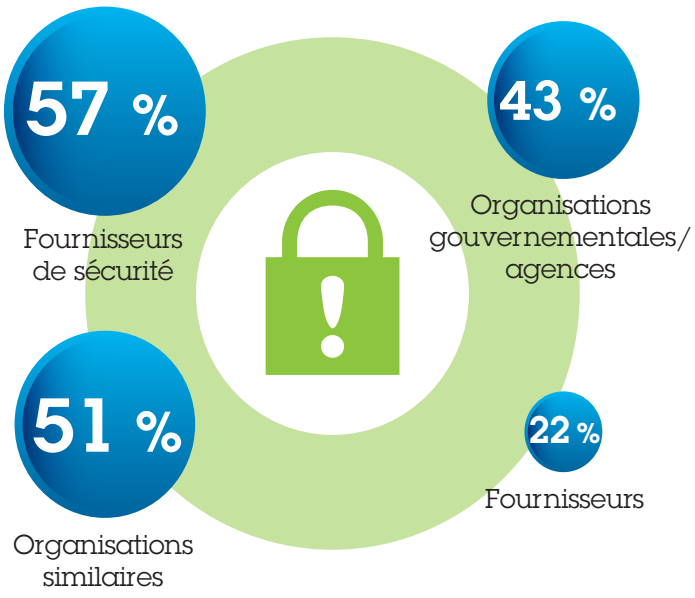


Figure 3. Pour réduire le risque issu de relations plus étroites avec clients, fournisseurs et partenaires, une approche de type « sécuriser l'écosystème » est justifiée.

Toujours axés sur la technologie d'aujourd'hui

Près de la moitié des répondants ont placé le déploiement de nouvelles technologies de sécurité parmi leurs trois principales initiatives, ce qui en fait l'objectif le plus important pour les responsables de la sécurité. Ils ont indiqué qu'ils étaient compétents au niveau des technologies de sécurité établies. Plus de 70 % se considèrent comme très matures en ce qui concerne la prévention des intrusions réseau, la détection avancée des programmes malveillants et l'analyse de la vulnérabilité du réseau.

Cependant, les domaines plus récents, tels que la prévention des fuites de données, la sécurité du cloud et des mobiles, s'avèrent plus problématiques : chacun de ces domaines a été identifié par 28 % des répondants, comme nécessitant une transformation ou une amélioration considérable et figure en tête de liste des domaines nécessitant une remise à plat ou une approche différente.

- **Données** – 72 % des responsables de la sécurité ont indiqué que les renseignements de sécurité en temps réel étaient de plus en plus importants pour leur organisation. Et pourtant, des domaines tels que la classification et la découverte des données et l'analyse des renseignements de sécurité ont relativement peu de maturité et nécessitent davantage d'amélioration ou de transformation.
- **Cloud** – Il existe toujours de fortes préoccupations quant à la sécurité du cloud, mais la consommation du cloud est néanmoins largement répandue et va continuer à augmenter. 86 % des répondants ont adopté le cloud ou le planifient. Au cours des trois à cinq prochaines années, les trois quarts des responsables de la sécurité s'attendent à ce que leur budget de sécurité pour le cloud augmente et parfois de façon spectaculaire.
- **Mobile** – La majorité des responsables de la sécurité ont indiqué ne pas avoir une approche efficace de la gestion des terminaux mobiles. En termes de maturité, la sécurité des mobiles se classait au tout dernier rang des technologies.

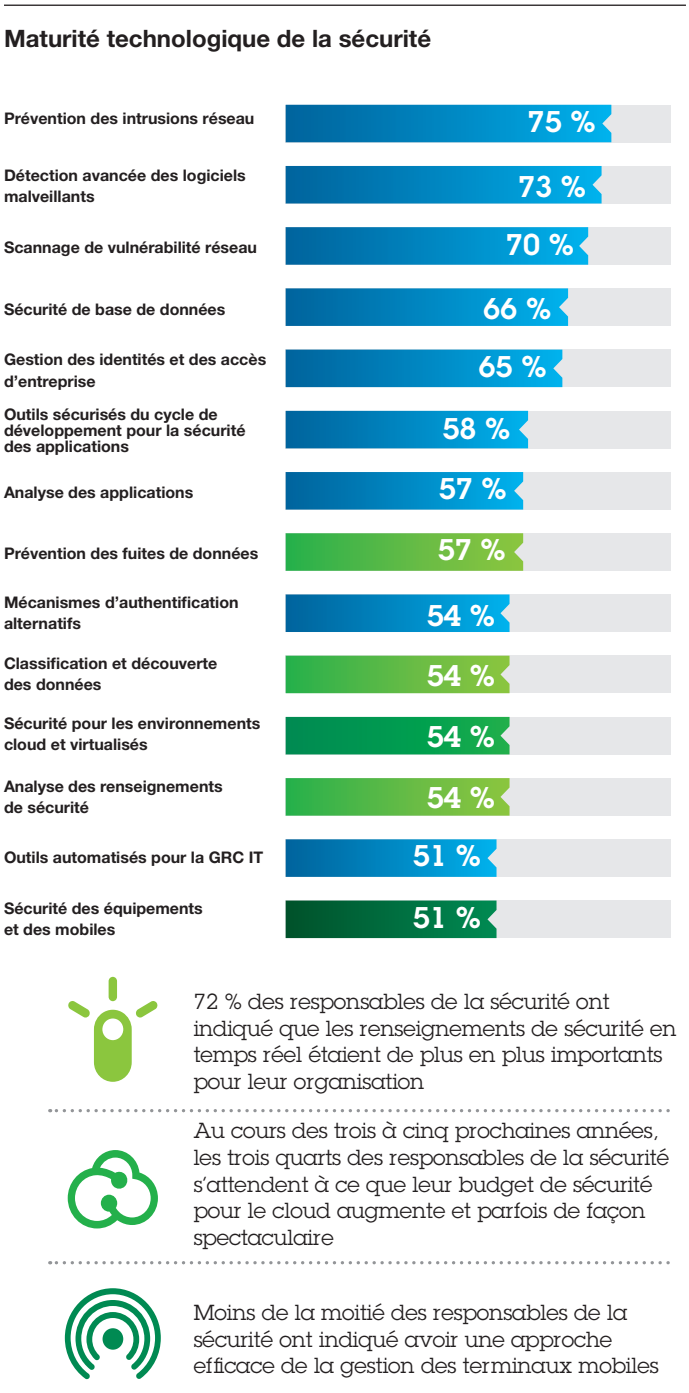


Figure 4. Les responsables de la sécurité se considèrent comme très matures dans des domaines plus traditionnels mais leur confiance n'est pas aussi élevée dans les domaines émergents, tels que l'analytique, le cloud et les mobiles.

Un peu plus de la moitié des répondants ont indiqué que le rythme croissant de l'innovation en matière de sécurité met à l'épreuve la capacité de leur organisation à répondre correctement aux besoins en matière de sécurité. Contraints de déployer, d'intégrer et d'améliorer les systèmes actuels, les responsables de la sécurité n'ont que peu de capacités disponibles pour examiner les technologies en développement. C'est pourquoi, en ce qui concerne l'avenir, plus de la moitié des répondants ne pouvaient imaginer une autre capacité de sécurité au-delà de ce qui existe actuellement. Les responsables se concentrent sur les technologies de sécurité actuelles.

Incertitudes quant à l'action du gouvernement

Les règlements, les normes et la conformité sont des paramètres que tous les responsables des risques et de la sécurité doivent traiter régulièrement. Les répondants ont indiqué que ce domaine va continuer à être déterminant dans le futur mais il existe une forte incertitude quant à savoir comment les choses vont évoluer.

Une grande part des perspectives de l'entreprise dans ce domaine dépend de sa position géographique, dans la mesure où les réglementations et les normes diffèrent d'un pays à l'autre et évoluent sans cesse. Pour les entreprises opérant à l'échelle mondiale, une telle variété de réglementations génère encore plus de complications.

Perspective des directeurs de la sécurité informatique : Résoudre les difficultés juridiques et de protection de la vie privée en réduisant la complexité

Par Jamie Giroux
Responsable de la Sécurité et des Audits, MAXIMUS

La complexité de la sécurité va continuer à croître, ce qui signifie que les futurs responsables de la sécurité devront promouvoir la simplification de leurs processus. Il est impératif d'assurer une communication renforcée, voire une intégration complète entre l'aspect technologique de la sécurité et les aspects juridique et de protection de la vie privée. Vous ne pourrez pas sécuriser un système correctement sans savoir tout ce qui s'y passe : juridique, protection de la vie privée, contrats, négociations, et en coordonnant tous ces éléments disparates.

Plusieurs développements potentiels sur le marché et sur le front juridique peuvent aider les responsables de la sécurité de demain. Davantage de compatibilité entre les produits et les services des fournisseurs autorise une vision panoramique de la sécurité qui montre où se situe le vrai risque du niveau le plus haut au niveau le plus bas. Si le fait de connaître l'emplacement d'une attaque en frontal est précieux, il est plus utile encore de pister cette attaque tout du long jusqu'à un serveur ou un poste de travail. C'est une entreprise difficile, si vous avez des dizaines de tableaux de bord et d'outils qui ne fonctionnent pas à l'unisson.

Cependant, une grande part des opportunités réside entre les mains des législateurs. Aux États-Unis, et c'est l'une de nos plus grandes lacunes, nous n'avons pas de norme nationale, de plus petit dénominateur commun pour l'ensemble du pays qui établit un groupe de critères de sécurité. Dans une société telle que MAXIMUS qui intervient dans de multiples secteurs d'activité dans chacun des états, toutes ces réglementations différentes entrent souvent en conflit.

Si une part de la sécurité de l'information du futur repose entre nos mains, une part de celle-ci est subordonnée à la réalisation d'une législation appropriée. Quelles que soient les exigences métier et juridiques, les responsables de la sécurité doivent façonner leur technologie pour y répondre de la façon la moins compliquée possible.

Indépendamment de l'emplacement géographique, des questions très générales apparaissent : le gouvernement sera-t-il un obstacle ou une aide ? Y aura-t-il plus ou moins de collaboration et de transparence dans le futur ? Comment vie privée et besoins croissants de sécurité vont-ils s'équilibrer ?

- Plus de trois quarts des répondants (79 %) estiment que les difficultés liées aux réglementations gouvernementales et aux normes de l'industrie ont augmenté au cours des trois dernières années.
- Les réglementations et les normes ont été l'un des domaines nécessitant le plus d'efforts d'organisation et arrivent en deuxième position après les menaces extérieures.
- 60 % sont dans l'incertitude quant à savoir si les gouvernements vont gérer la gouvernance de la sécurité à un niveau national ou mondial et quel en sera le degré de transparence.
- 22 % uniquement estiment qu'une approche globale de la lutte contre la cybercriminalité sera établie d'ici trois à cinq ans.

Gagner en force pour affronter l'avenir

Que peuvent faire les responsables de la sécurité pour résoudre ces difficultés ? Comment les dirigeants peuvent-ils éviter les actions qui risqueraient de freiner l'activité ?

Que peuvent-ils faire pour préparer leur entreprise à l'avenir ? Les responsables de la sécurité peuvent agir dans quatre domaines :

Consolider la sécurité du cloud, des mobiles et des données

Un écart de maturité existe entre les sociétés qui utilisent des technologies de sécurité plus traditionnelles et celles qui progressent vers de nouveaux domaines. Pour libérer des ressources qui pourront se concentrer sur de nouveaux domaines, réfléchissez à vos capacités suffisamment matures pour vous permettre de déléguer, d'automatiser ou de sous-traiter.

- Les entreprises adoptent largement le cloud et consacrent d'importantes ressources à sa sécurisation. Il peut exister des préoccupations par rapport au cloud mais il fait désormais partie de l'entreprise. Assurez-vous que votre organisation tire le meilleur parti de l'opportunité du cloud avec le moins de risques.
- La sécurité des terminaux mobiles a généralement du retard. À mesure que davantage de terminaux sont connectés et que la promesse de « l'Internet des objets » se réalise, ces problèmes vont tout simplement s'aggraver. Concentrez vos efforts sur le renforcement des capacités de sécurité pour les mobiles.
- Avec les quantités croissantes de données générées par les entreprises, ne vous laissez pas submerger – concentrez-vous sur vos ressources les plus critiques. Pour vous aider à gérer l'augmentation des menaces extérieures, faites progresser votre approche vis-à-vis des renseignements de sécurité et des analyses en temps réel.

Améliorez la formation et les compétences de leadership

Interrogés sur les compétences qu'ils estimaient nécessaires pour les trois à cinq prochaines années à venir, les responsables de la sécurité ont mentionné la formation et l'éducation de leur organisation et le fait de se préparer à assumer davantage de leadership, comme étant les compétences les plus importantes. N'oubliez pas de compléter les connaissances technologiques par des compétences de gestion de base, car ces compétences vont jouer un rôle proportionnel à l'influence croissante des responsables de la sécurité.

Engagement en dehors de votre organisation

Face à la conviction généralisée selon laquelle les connexions avec les clients, fournisseurs et partenaires vont augmenter les niveaux de risque, les responsables de la sécurité doivent trouver la meilleure façon de protéger l'ensemble de leur écosystème et non pas uniquement leur organisation. Faites un effort concerté pour déterminer comment évaluer clairement vos sécurités réciproques – comment pouvez-vous mieux bâtir la confiance réciproque et la confiance en des écosystèmes plus vastes ? Cette exigence est particulièrement importante étant donné que 14 % pensent qu'une façon standardisée d'évaluer et de quantifier les informations sur les risques de sécurité sera largement utilisée dans les trois à cinq prochaines années. Utilisez les groupes sectoriels comme des voies de communication critiques pour les bonnes idées.

Plan pour plusieurs scénarios gouvernementaux

En raison de l'incertitude quant à ce que les gouvernements pourraient faire ou ne pas faire à l'égard de la cybersécurité, planifiez pour de multiples possibilités. Même s'il est concevable que les gouvernements adopteront des normes de sécurité plus élevées et des lignes directrices qui aideront directement les entreprises, vous ne pouvez pas compter sur de telles circonstances.

Entretenez-vous régulièrement avec le responsable de la protection de la vie privée et le conseiller juridique pour mieux comprendre quelles exigences pourraient survenir. 72 % des répondants ont indiqué que la protection de la vie privée des clients est de plus en plus un sujet de discussion avec les responsables de l'entreprise, pourtant seuls 9 % des responsables de la sécurité placent le responsable de la protection de la vie privée parmi leurs trois principaux partenaires stratégiques dans l'entreprise. Seulement 14 % considèrent le conseiller juridique comme l'un de leurs trois principaux partenaires. Adoptez une approche globale qui s'appuie sur le point de vue de rôles situés en dehors de la fonction de sécurité.

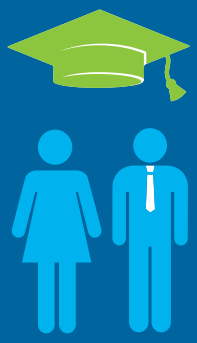
Un rôle plus influent dans le futur

Il ne fait aucun doute que les périls grandissants de la sécurité de l'information s'avéreront difficiles pour tous ceux qui sont affectés à la protection de l'entreprise. Mais les responsables de la sécurité informatique doivent considérer le futur non pas comme un défi insurmontable mais plutôt comme une occasion d'accroître leur niveau de contribution. La montée des menaces au cours de la dernière décennie a déjà forgé une classe supérieure de leaders dans le secteur de la sécurité, des leaders capables de diriger leur entreprise à travers une tempête persistante de risques d'envergure. En comprenant les dangers pour les entreprises et en mettant en place des mesures spécifiques pour y remédier, nous pourrons continuer à fournir l'environnement nécessaire pour permettre aux entreprises de prospérer.

Il existe un certain nombre de mesures de sécurité que les responsables peuvent mettre en place dès aujourd'hui pour renforcer leur organisation en vue d'affronter l'avenir.

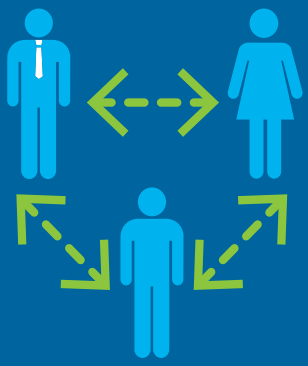
Consolider la sécurité du cloud, des terminaux mobiles et des données

Les responsables n'attendent pas que les capacités des technologies futures résolvent leurs problèmes, ils s'efforcent de déployer les technologies de sécurité d'aujourd'hui pour réduire les écarts.



Améliorez la formation et les compétences de leadership

Les compétences technologiques restent importantes mais les compétences de gestion pures vont prendre de plus en plus d'importance avec l'influence croissante des responsables de la sécurité.



Engagement dans davantage de collaboration externe

Les leaders devraient faire un effort concerté pour déterminer comment construire et évaluer clairement la sécurité de leur écosystème.

Plan pour plusieurs scénarios gouvernementaux

Un dialogue régulier avec le responsable de la protection de la vie privée et le conseiller juridique est essentiel pour permettre au responsable de la sécurité informatique de comprendre quelles exigences risquent de survenir.

A propos des auteurs

Marc van Zadelhoff est le vice-président en charge de la stratégie mondiale, du marketing et de la gestion des produits pour IBM Security. Il a plus de 20 ans d'expérience dans le domaine de la stratégie, du capital risque, du développement des entreprises et du marketing dans le domaine de l'informatique et de la sécurité. Marc travaille avec des clients du monde entier pour les conseiller en matière de stratégies de sécurité et de développement de nouvelles technologies répondant à leurs besoins. Il dirige également l'IBM Security Board of Advisors, composé de 25 responsables de haut niveau de la sécurité informatique qui conseillent IBM sur son portefeuille de solutions de sécurité. Marc a été membre de l'équipe de direction de la société Consul des Pays-Bas avant son acquisition par IBM en 2007. Vous pouvez contacter Marc sur LinkedIn et sur marc.vanzadelhoff@us.ibm.com

Kristin Lovejoy est la Directrice générale de la Division des Services de sécurité d'IBM, chargée du développement et du déploiement de services professionnels et managés de sécurité pour les clients IBM dans le monde entier. Précédemment, Kris était Vice-Présidente IBM en charge des risques de la technologie de l'information et responsable mondiale de la sécurité informatique, en charge de la gestion, du suivi et des tests des fonctions de sécurité et de résilience d'entreprise IBM au niveau mondial. Aujourd'hui, Kris fait partie d'un grand nombre de conseils et de comités consultatifs externes. Elle est un expert reconnu dans le domaine de la sécurité, du risque, de la conformité et de la gouvernance, et apparaît régulièrement sur CNBC, NPR et WTOP. Vous pouvez contacter Kris sur LinkedIn et sur klovejoy@us.ibm.com

David Jarvis est le directeur de l'équipe de recherche et du programme de l'IBM Centre for Applied Insights. Il s'est spécialisé sur des sujets technologiques et d'entreprise émergents et stratégiques. Il est le co-auteur d'un certain nombre d'études IBM notamment les évaluations 2012 – 2014 IBM CISO. Outre ses responsabilités en matière de recherche, David enseigne dans le domaine de la prévoyance d'entreprise et de la résolution créative des problèmes. Vous pouvez contacter David sur LinkedIn et sur djarvis@us.ibm.com

Contributeurs

Walker Harrison
Tanya Dhamija
Yana Krasnitskaya
Ellen Cornillon
Sue Ann Wright

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

Pensez à recycler ce document

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.

WGL03061-FRFR-00