

mimecast

Derrière les ÉCRANS :

L'évolution de la perception
du cyber-risque par les
conseils d'administration.



PARTIE I

La cybersécurité fait
son entrée au conseil
d'administration

- tout comme

**la volatilité
économique**



L'espace de travail moderne se caractérise par l'interconnexion : les modèles de travail hybrides ont transformé le fonctionnement des entreprises, en changeant les modes de communication, de partage des données et de collaboration.

Les collaborateurs peuvent télétravailler depuis pratiquement n'importe où, grâce aux e-mails et, plus récemment, aux outils collaboratifs tels que Microsoft Teams et Slack.

Les RSSI et autres responsables de la sécurité ont tiré la sonnette d'alarme sur le cyber-risque élevé découlant de l'espace de travail moderne, et grâce à la médiatisation des cyberattaques de plus en plus nombreuses et sophistiquées, les équipes de direction et le conseil d'administration en ont pris note. Alors que l'e-mail reste le vecteur d'attaque le plus ciblé par les attaquants, les outils collaboratifs représentent une nouvelle surface d'attaque pour les cybercriminels, augmentant encore les risques à gérer pour les responsables de la sécurité. Il est donc de plus en plus important de protéger les communications professionnelles, d'autant plus que le volume des menaces liées aux e-mails **a augmenté dans 82 % des entreprises au cours des 12 derniers mois.**¹ De nombreux chefs d'entreprise pensent à tort que l'utilisation de solutions de sécurité reconnues, mais disparates, est suffisante pour garantir la sécurité de leurs communications professionnelles. Cependant, il existe un risque de subir des cyberattaques à plusieurs niveaux et par plusieurs vecteurs, comme les ransomware et les attaques de type BEC (compromission des messageries d'entreprise), et de telles attaques peuvent avoir des effets dévastateurs sur le chiffre d'affaires et la réputation de l'entreprise dans le contexte latent de volatilité économique.

La cybersécurité et la reconnaissance du cyber-risque comme un risque commercial doivent influencer le comportement du personnel. La cybersécurité est la responsabilité de tous, et les RSSI se doivent de faire passer le message au conseil d'administration pour que des actions soient mises en œuvre.

Pour en savoir plus sur la perception actuelle des cyber-risques par les équipes de direction et le conseil d'administration, nous nous sommes entretenus avec **78 décideurs de 12 pays** pour découvrir les efforts déployés pour signaler ces risques et les recommandations destinées aux dirigeants afin de travailler en toute sécurité, malgré la prolifération des cyberattaques.



Les menaces liées aux e-mails ont augmenté dans 82 % des entreprises au cours des 12 derniers mois.

¹ La sécurité des e-mails en 2023 de Mimecast

PARTIE II

Le cyber-risque est
un risque économique



La cybersécurité le lien entre le cyber-risque et le risque commercial doivent devenir un enjeu prioritaire au niveau du conseil d'administration.

Bien qu'il puisse parfois sembler que la cybersécurité fonctionne en vase clos, le contexte économique plus large dans lequel elle se déroule peut provoquer des ondes de choc. Par exemple, le cyber-risque devrait continuer à augmenter à moyen et long terme, selon les rapports de la réunion annuelle du Forum économique mondial (FEM) à Davos. En effet, les cyber-risques figurent pour la première fois parmi les 10 principales préoccupations à long terme du rapport annuel sur les risques mondiaux du FEM en 2023. Ce nouveau classement annonce la longévité de la vague actuelle de cyberattaques.² « La cybercriminalité et la cyberinsécurité généralisées » figurent au huitième rang sur la liste des risques classés par gravité, derrière les problèmes mondiaux liés au changement climatique, aux catastrophes naturelles et aux migrations involontaires, mais devant les conflits géoéconomiques et les dommages environnementaux. Certains conseils d'administration abordent désormais régulièrement les risques posés par l'augmentation de la cybercriminalité, et c'est de bon augure. Ces défis macroéconomiques augmentent de jour en jour, générant une série de nouveaux enjeux pour les entreprises individuelles.

« Je crois que nous sommes en avance sur nos concurrents, car certains membres du conseil d'administration possèdent une solide expertise en matière de cybersécurité. Le principal avantage est que ces membres spécifiques peuvent informer les autres membres du conseil d'administration sur des questions liées à la cybersécurité. »

Directeur technique de l'informatique et des infrastructures, services financiers, plus de 1 000 employés, Émirats arabes unis

« Je pense que le conseil d'administration considère le cyber-risque comme un autre risque économique, mais dont l'impact potentiel est plus important. La principale difficulté, selon moi, est qu'il est très difficile de quantifier le cyber-risque avant qu'une faille majeure se produise et change la donne. »

DSI, secteur du conseil, plus de 1 500 employés, Asie-Pacifique

Par exemple, de nombreux RSSI reconnaissent qu'il existe un manque de connaissances au sein de leur conseil d'administration, ce qui les désavantage lorsqu'ils doivent documenter le retour sur investissement des initiatives de cybersécurité.³ Par ailleurs, face à la volatilité économique, la plupart des entreprises partout dans le monde se serrent la ceinture dans tous les domaines, y compris le marketing, les ventes et la technologie en général, ce qui peut entraîner une augmentation du cyber-risque en raison du shadow IT ou de l'externalisation à des tiers peu fiables. Le cyber-risque n'est pas simplement un problème informatique, c'est une vulnérabilité critique qui est directement assimilable au risque économique global. Avec des taux d'inflation record, des cyberattaques toujours plus complexes et des tensions géopolitiques, les entreprises ne peuvent tout simplement pas se permettre une architecture de sécurité fragile qui les rend vulnérables aux violations de données et met en péril leur stabilité organisationnelle.

² [Global Risks Report 2023](#), Forum économique mondial

³ [Cyber Chiefs Face Scrutiny and Challenges in 2023's Uncertain Economy](#), *Wall Street Journal*

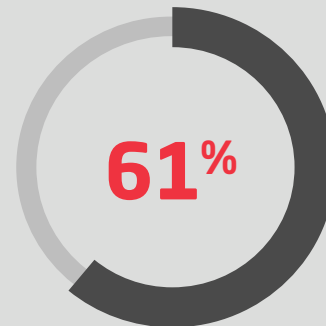
PARTIE II

Malgré la récession imminente et le manque de connaissances en matière de cybersécurité au niveau du conseil d'administration, la plupart des responsables de la sécurité interrogés dans le cadre de cette enquête estiment qu'ils ont besoin d'une augmentation de budget de **10 à 20 %** et qu'ils l'obtiendront probablement. En effet, dans les secteurs fréquemment attaqués, tels que les infrastructures critiques ou la finance, il est peu probable que les dépenses en matière de cybersécurité soient réduites.⁴ Mais pour améliorer ces chances, les responsables de la cybersécurité doivent informer clairement sur les risques et le rôle essentiel de la

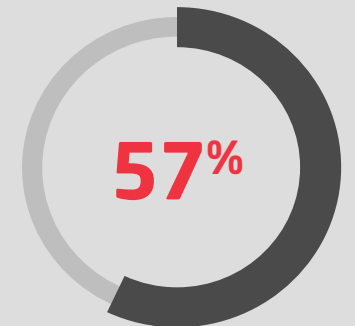
cybersécurité dans la protection de l'entreprise, et doivent également s'attendre à un examen plus approfondi de leurs dépenses. Le coût d'une violation sera souvent supérieur à toutes les mesures d'économie souhaitées par le conseil d'administration.

Contrairement aux interruptions de service entraînant des pertes économiques quantifiables, les dommages à la réputation d'une marque ayant subi une cyberattaque ne sont pas faciles à mesurer, mais ils ne doivent pas être sous-estimés. La confiance des clients se construit au fil des années et sa perte peut donc être dévastatrice.

Le rapport Brand Trust de Mimecast montre que **61 %** des consommateurs perdraient confiance dans leur marque préférée si celle-ci divulguait des informations personnelles sur une version usurpée de son site Web. La perte de confiance reflète directement une perte de revenus puisque plus de la moitié (**57 %**) des personnes interrogées cesseraient de consommer auprès de leur marque préférée si elles étaient victimes d'une attaque de phishing.



des consommateurs perdraient confiance dans leur marque préférée si celle-ci divulguait des informations personnelles sur une version usurpée de son site Web.



des personnes interrogées cesseraient de consommer auprès de leur marque préférée si elles étaient victimes d'une attaque de phishing

⁴ Cyber Chiefs Face Scrutiny and Challenges in 2023's Uncertain Economy, *Wall Street Journal*





« Parfois, ils ne comprennent pas le coût d'un type d'attaque en particulier. Je dois alors adopter une approche économique (en laissant de côté mon savoir-faire technique et en matière de sécurité) et essayer de leur faire comprendre l'ampleur de la perte et si nous sommes potentiellement menacés. »

*DT, secteur du divertissement,
<500 employés, Singapour.*

De plus, les menaces des cybercriminels deviennent de plus en plus sophistiquées et persistantes, tandis qu'un vivier de talents plus restreint oblige les employeurs à demander davantage aux analystes et ingénieurs en cybersécurité. Dans ce contexte, il est devenu beaucoup plus difficile de recruter et de fidéliser des professionnels de la cybersécurité. En moyenne, le temps de recrutement pour les postes dans le domaine de la cybersécurité est 21 % plus long que pour les autres postes informatiques, et des dizaines de milliers de postes restent vacants chaque année dans le domaine de la cybersécurité.⁵ Ces exigences croissantes entraînent davantage de stress, d'épuisement professionnel et de démissions

Les membres des conseils d'administration les plus avertis comprennent que l'investissement dans la cybersécurité ne consiste pas seulement à réduire les risques d'une cyberattaque aujourd'hui. Le maintien des investissements dans ce domaine permet aux entreprises de préserver la réputation de leur marque, de réduire les risques d'amendes réglementaires et de pertes de ventes en cas d'attaque réussie, mais aussi de réduire le stress auquel sont confrontés les professionnels de la cybersécurité, réduisant ainsi efficacement le taux de roulement d'employés hautement spécialisés et difficiles à recruter. En bref, investir dans la cybersécurité est synonyme de bonnes affaires.

« ...il peut s'avérer difficile de retenir des experts de cybersécurité talentueux. Les ressources dans ce domaine sont limitées et nous devons trouver un moyen de garder les personnes que nous avons embauchées et formées pour l'avenir. Nous manquons actuellement d'environ 30 % d'employés qualifiés, ce qui est problématique. Dans ce secteur, il n'est pas possible de trouver des profils compétents à un prix raisonnable. Le budget consacré à la cybersécurité est suffisant, mais il y a tellement de personnes non formées qu'il est difficile pour nous d'embaucher du personnel. »

*Directeur financier, services financiers,
plus de 1 000 employés, Afrique du Sud.*

⁵ CyberSeek

Pour mettre en évidence le lien entre le cyber-risque et le risque commercial, les cadres interrogés donnent les recommandations suivantes :

- 1** | Évitez le jargon et essayez de démystifier le risque posé par les cybermenaces à moyen et long terme.
- 2** | Lorsque vous présentez les bénéfices d'investir dans des solutions de pointe, faites le lien entre les cybermenaces et les résultats de l'entreprise. Certains dirigeants recommandent d'éviter de se concentrer sur la manière dont une attaque s'est produite mais plutôt sur les raisons pour lesquelles elle s'est produite, par exemple en s'appuyant fortement sur un fournisseur de sécurité monolithique.
- 3** | Concevez des mécanismes qui vous permettent d'aligner le cyber-risque sur le risque global de l'entreprise afin de créer une fonctionnalité de cybersécurité intégrée.
- 4** | Évitez de transformer chaque incident en crise. Soyez tactique lorsque vous présentez le cyber-risque au conseil d'administration afin qu'il puisse le quantifier avec précision sans attendre qu'une violation suscite l'urgence.



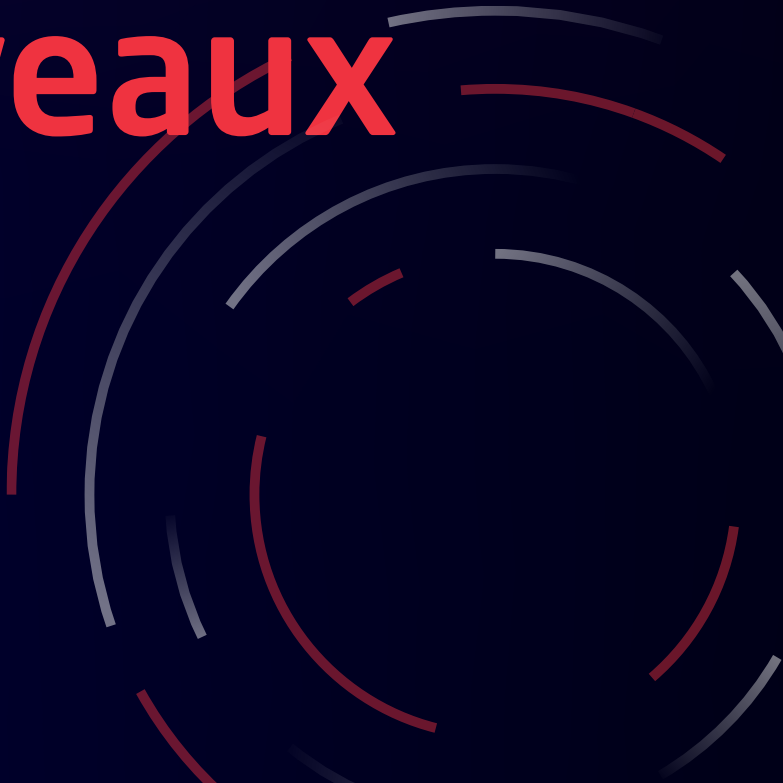


Je conseille aux RSSI de ne pas tout transformer en situation de crise. Choisissez de manière judicieuse les points que vous mettez en avant pour éviter tout effet de lassitude. Gardez des cartouches pour les incidents majeurs que vous souhaitez signaler et demandez au conseil d'administration et aux hauts dirigeants de promouvoir le changement. »

RSSI, secteur de la technologie, plus de 180 000 employés, États-Unis

PARTIE III

Valeur et efficacité
grâce à un **cadre de
cybersécurité à
plusieurs niveaux**



Mettez en œuvre des outils qui répondent aux besoins de votre entreprise, tout en tenant compte de sa taille, de sa complexité et de son secteur d'activité.

Les entreprises évoluent dans un environnement complexe et volatile, et sont confrontées à des menaces de plus en plus sophistiquées. Pour répondre à ces caractéristiques du marché, les RSSI sont contraints d'examiner les budgets et les technologies de cybersécurité à travers le prisme bien connu des « personnes, technologies et processus ».

Plus de **90 % des cyberattaques** se font par le biais de la messagerie, ce qui nous rappelle que les cadres de tolérance et de gestion des risques doivent être fréquemment revus en identifiant la mission de l'entreprise et les ressources à protéger, et en communiquant régulièrement l'état des risques de cybersécurité aux parties prenantes. Les exercices de simulation menés par les RSSI sont un autre outil qui améliore la posture des entreprises en matière de cybersécurité et leurs plans de réponse aux incidents. Lorsqu'ils sont correctement communiqués, ils peuvent aider les employés à mieux comprendre les conséquences d'une mauvaise posture informatique.

Du point de vue technologique, les RSSI doivent rechercher des moyens plus cohérents, complets et automatisés de suivre l'activité, de se protéger contre l'exfiltration de données et d'agir plus rapidement pour limiter l'impact des attaques. Il ne suffit plus d'investir dans des outils de sécurité. En fait, de nombreuses entreprises ont connu des environnements de sécurité surchargés ou déconnectés au fil du temps.

« Nous avons une approche affinée de la gestion des risques qui met l'accent sur les processus technologiques et les cadres de cybercontrôle, et qui soutient financièrement l'équipe en investissant dans des systèmes, des infrastructures et de nouvelles technologies sur des plateformes sécurisées et stables afin d'atténuer les menaces émergentes. »

*Analyste du support informatique et des infrastructures (relevant directement du RSSI),
Australie, 1 000 employés*



Plus de 90 % des cyberattaques se font par la messagerie

PARTIE III

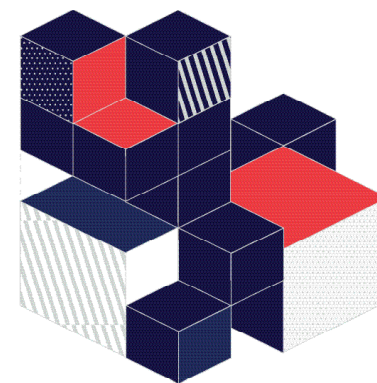
Au contraire, il est essentiel de faire place à des intégrations étroites et à des cadres de sécurité à plusieurs niveaux pour protéger les données dans l'ensemble de l'organisation et tout au long de leur cycle de vie, tout en évitant le piège d'une plateforme de sécurité monolithique hautement attaquée comme Microsoft 365. En effet, les fournisseurs de solutions de sécurité doivent répondre aux besoins des entreprises qui attendent des fonctionnalités plus nombreuses ou de meilleure qualité pour le même coût, ce qui met l'accent sur les solutions axées sur les intégrations visant à prévenir et à minimiser l'impact des attaques. Un moyen efficace d'y parvenir est de maximiser les partenariats que les entreprises entretiennent avec les fournisseurs existants, tels que les programmes ou les alliances d'API technologiques. En effet, **8 entreprises sur 10** sont plus susceptibles de travailler avec un fournisseur de cybersécurité doté d'une plateforme d'API ouverte.⁶

« **En tant que DSI, je dois m'assurer que l'entreprise dispose des systèmes et des technologies les plus récents qui constitueront une base solide pour atténuer les cyberattaques.** »

DSI, services financiers, Allemagne, < 1 000 employés

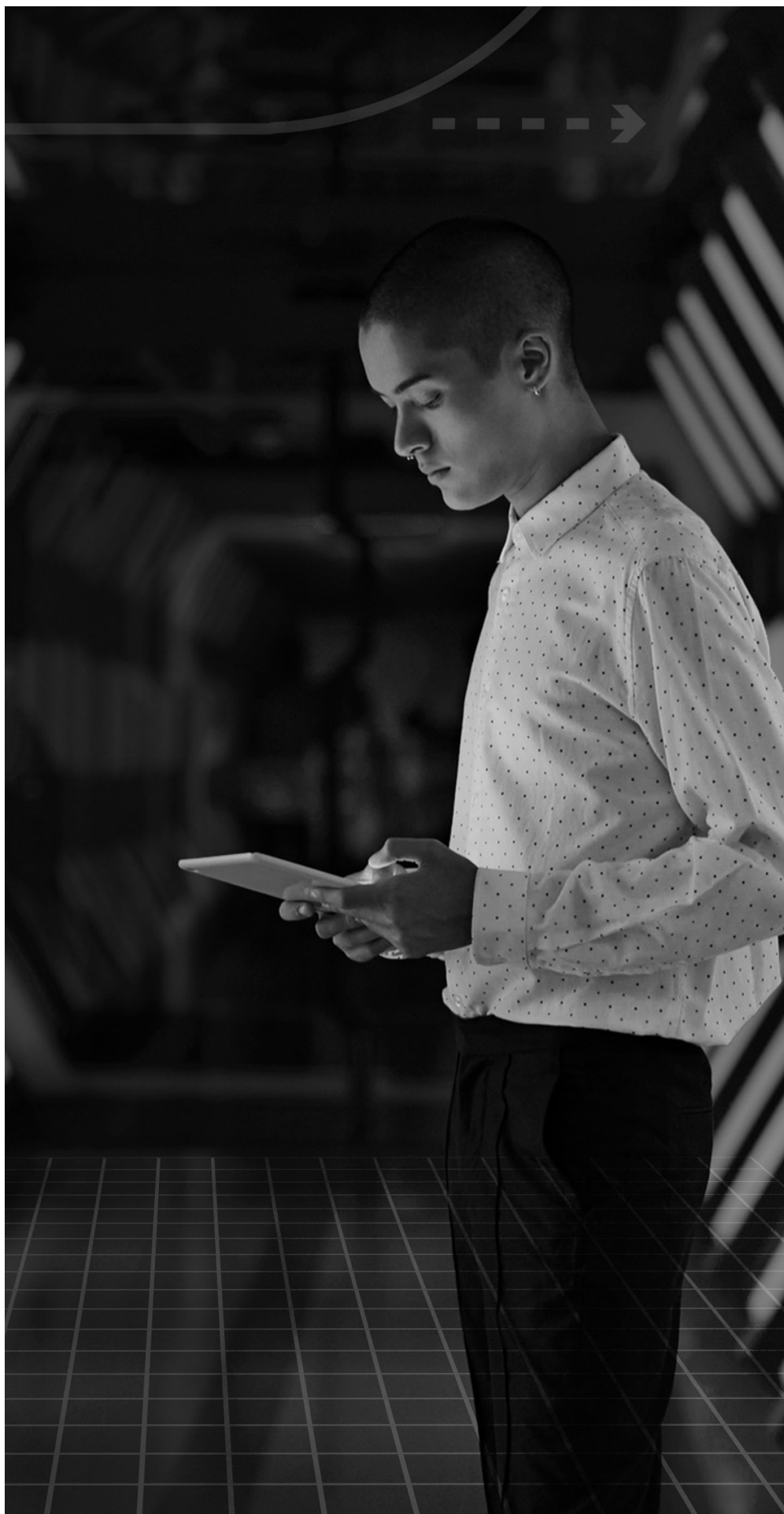
L'objectif est de créer un modèle de défense en profondeur qui permette aux équipes de cybersécurité de détecter les cybermenaces et d'y remédier rapidement à l'aide d'un ensemble de produits de sécurité de pointe qui partagent des données et des informations analytiques. Avec un tel cadre de sécurité multicouche, les équipes du SOC peuvent lier la prévention, la détection, l'investigation et la réponse sur l'ensemble des outils et activités. Ce type de modèle s'éloigne des solutions de fournisseur unique qui, malgré leur qualité, peuvent permettre aux attaquants de s'infiltrer dans les environnements de sécurité sans être détectés.

De plus, pour renforcer cette approche et fidéliser les talents en réduisant les faiblesses du SOC, de nombreuses entreprises investissent davantage dans des outils d'automatisation. Cependant, des employés qualifiés sont toujours nécessaires pour mettre en œuvre et gérer ces outils automatisés à plusieurs niveaux.



8 entreprises sur 10 sont plus susceptibles de travailler avec un fournisseur de cybersécurité doté d'une plateforme d'API ouverte.

⁶ La sécurité des e-mails en 2023 de Mimecast



Il faut tout d'abord discuter de l'approche de la défense en profondeur, du plus haut niveau jusqu'au bas de la pyramide organisationnelle. Il est nécessaire de connaître la cybersécurité à tous les niveaux. Et ce que fait notre organisation pour assurer notre sécurité. »

DT, Singapour, secteur du divertissement, moins de 500

Pour renforcer la posture de sécurité via des cadres de cybersécurité à plusieurs niveaux, les cadres interrogés formulent les recommandations suivantes:

- 1** Identifiez les principales menaces qui pèsent sur l'entreprise et établissez un profil de risque de l'organisation. Les attaques par e-mail telles que le phishing et le piratage de compte sont extrêmement préoccupantes, il est donc essentiel de choisir une solution qui tient compte du secteur d'activité, de la complexité de l'environnement de sécurité et de l'environnement réglementaire.
- 2** Optimisez les relations avec les fournisseurs pour produire un modèle de défense en profondeur aussi fluide que possible.
- 3** Une fois le profil de risque établi, élaborer un cadre de cybersécurité répondant à toutes les principales préoccupations et mettez en place les couches de cybersécurité nécessaires pour lutter contre les menaces identifiées. Mettez en place des indicateurs clés de performance, puis contrôlez et ajustez le cadre en conséquence avec l'aide et la participation du conseil d'administration de l'entreprise.
- 4** Dans des environnements plus complexes, les responsables de la sécurité peuvent prévenir les pertes de données avec moins de ressources en utilisant plus d'intelligence grâce aux technologies d'apprentissage automatique et aux analyses traditionnelles. Ils peuvent également automatiser davantage et se décharger des tâches manuelles répétitives qui épuisent les professionnels de la cybersécurité et aggravent la pénurie de compétences.



Lors des réunions du conseil d'administration, nous insistons sur la mise en place d'une infrastructure informatique robuste et d'un personnel ayant de solides connaissances en matière de cybersécurité. La discussion porte sur tous les paramètres de l'infrastructure informatique, la surveillance de la sécurité, la virtualisation des centres de données, les migrations de pare-feu et les nouveaux processus qui peuvent être ajoutés à notre configuration actuelle pour protéger notre entreprise de toute violation de données.

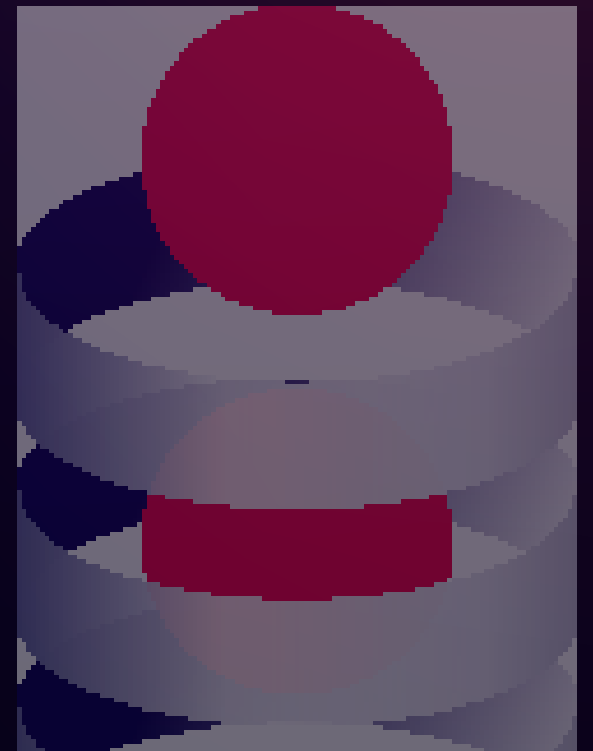
DT, secteur pharmaceutique, plus de 1 500 employés, Canada



PARTIE IV

La Protection contre le phishing

est un est un
travail d'équipe



Sécurisez votre organisation en vous protégeant contre le phishing et en investissant dans des formations de sensibilisation à la sécurité pour les collaborateurs.

Les attaques par e-mail sont en hausse dans trois entreprises sur quatre, et autant d'entre elles se préparent à de graves conséquences d'une telle attaque au cours l'année prochaine.⁷ Par conséquent, les dirigeants se sont tournés vers la création d'une culture de la sécurité à l'échelle de l'entreprise,⁸ notamment en investissant dans des formations de sensibilisation en tandem avec des cadres de cybersécurité à plusieurs niveaux pour minimiser la probabilité d'une attaque réussie.

« Notre conseil d'administration est conscient que le courrier électronique reste l'un des principaux vecteurs d'attaque. C'est pourquoi nous avons investi de manière significative dans la sécurité de la messagerie. »

RSSI, secteur de la vente au détail, plus de 1 000 employés, Royaume-Uni

Le courrier électronique est un vecteur d'attaque attrayant pour les cybercriminels en raison de son omniprésence et de son volume sur le lieu de travail et à l'extérieur. Et même avec les meilleures solutions de cybersécurité, les erreurs humaines laissent toujours une porte ouverte aux attaquants.

« Les e-mails constituent actuellement la plus grande menace, et les e-mails de phishing constituent le moyen le plus courant de voler des informations au sein d'une organisation. C'est l'une des zones les plus à risque et la plus préoccupante pour moi. Nous avons déjà subi une attaque par e-mail de phishing qui a entraîné le piratage des boîtes des boîtes mail de nos collaborateurs, et nous signalons ces scénarios au Bureau du commissaire à l'information (ICO). »

Directeur de la technologie, services publics, plus de 1 000 employés, Royaume-Uni

Le phishing est l'une des cybermenaces les plus anciennes, et il continue d'exister car les attaquants les utilisent continuellement. De plus, les outils d'automatisation et les kits de phishing permettent aux cybercriminels les moins compétents de ratisser plus large, ce qui peut causer des dommages plus importants aux entreprises. Dans le contexte de la pandémie mondiale, le récent rapport sur la sécurité des e-mails a révélé que **97 % des entreprises** ont subi des attaques de phishing, et **59 %** d'entre elles ont signalé une augmentation significative des menaces de phishing auxquelles elles sont confrontées.

⁷ Le cyber-risque et les équipes de direction dans le rapport La sécurité des e-mails de Mimecast

⁸ Le cyber-risque et le conseil d'administration : son soutien permet de former le personnel à la cybersécurité, Mimecast

PARTIE IV

« C'est une erreur humaine, et vous ne pouvez pas analyser ce qui se passe dans l'esprit d'une personne. Nous ne pouvons que former les employés à ne pas cliquer sur des liens inutiles, mais c'est à eux de prendre leurs responsabilités.. Ainsi, tant que la compromission des e-mails et le phishing existeront et continueront de fonctionner, il y aura toujours une faille dans la cybersécurité. »

*RSSI, secteur commerce de détail,
plus de 1 000 employés, Australie*

Pour atténuer ces menaces persistantes et adaptables, les RSSI cherchent à développer une culture axée sur la sécurité à travers l'entreprise, y compris au sein du conseil d'administration. Mais changer le comportement humain est loin d'être simple et demande du temps. Les efforts de sensibilisation à la cybersécurité et de résolution des menaces mettent donc du temps à porter leurs fruits par rapport à la mise en œuvre de la sécurité des e-mails ou d'autres outils technologiques. Ainsi, de plus en plus de dirigeants comprennent qu'une culture qui donne la priorité à la cybersécurité est essentielle pour favoriser la sécurité à long terme. Mais le développement d'une telle culture demande de la persévérance, de la créativité et un fort engagement de la part des dirigeants.

Les vulnérabilités de la chaîne logistique, l'essor de la collaboration en ligne et la croissance des réseaux numériques comptent parmi les principales raisons pour lesquelles le paysage électronique devient plus périlleux. L'explication est simple : la rencontre des communications, des personnes et des données comporte un risque énorme, car les acteurs malveillants exploitent l'espace de travail moderne. Les efforts de transformation numérique que les entreprises mettaient en œuvre avant la pandémie faisaient déjà l'objet d'un nombre record de violations de données. Mais avec l'expansion rapide de leurs canaux de communication numérique dans le sillage de la pandémie, les entreprises ont également élargi sans le vouloir la surface d'attaque des acteurs malveillants.



PARTIE IV

« Au niveau du conseil d'administration, j'aimerais que l'on parle davantage de la psychologie de la gestion des cyberattaques telles que les attaques par ransomware. Il serait bénéfique d'envisager ces événements d'un point de vue non technologique. Nous devons également discuter de la manière dont nous pouvons faire de la cybersécurité le problème de tous, et pas seulement du responsable informatique. »

*Directeur général de l'informatique,
Infrastructure, plus de 2 500 employés, Australie*

Le simple fait de savoir à quoi peut ressembler un e-mail indésirable ou un e-mail de phishing ne suffit pas. C'est pourquoi les connaissances contextuelles et l'engagement de l'entreprise à faire de la sécurité la responsabilité de tous peuvent contribuer à maximiser les avantages de la formation de sensibilisation.

Les organisations de tous bords vivent une période charnière et des changements de grande ampleur semblent inévitables. Cependant, définir une stratégie qui réponde aux problèmes critiques de cybersécurité, qu'il s'agisse de garantir la sécurité des systèmes internes et des clients ou d'alléger la pression sur les professionnels de la cybersécurité, ne sera pas une tâche facile. Cela nécessitera la participation active non seulement du conseil d'administration, mais aussi de chaque collaborateur de l'entreprise.





Pour se protéger contre les menaces transmises par e-mail et développer une culture axée sur la sécurité, les cadres interrogés donnent les recommandations suivantes :

- 1** Le phishing est un problème qui ne disparaîtra pas, quel que soit le secteur d'activité, la taille ou la situation géographique de votre entreprise. Veillez à ce que chacun adopte de meilleures habitudes en matière de cybersécurité et se sente libre de communiquer sur les cybermenaces potentielles. Ces pratiques constituent un aspect essentiel de la capacité de toute entreprise à atténuer les cyber-risques.
- 2** La création d'une culture de la sécurité au sein du conseil d'administration, des équipes de direction et de tous les départements de l'entreprise est une pratique fondamentale pour réduire les cyber-risques. Pour que ces bases soient efficaces, il est impératif de faire de la cybersécurité la responsabilité de tous les employés.

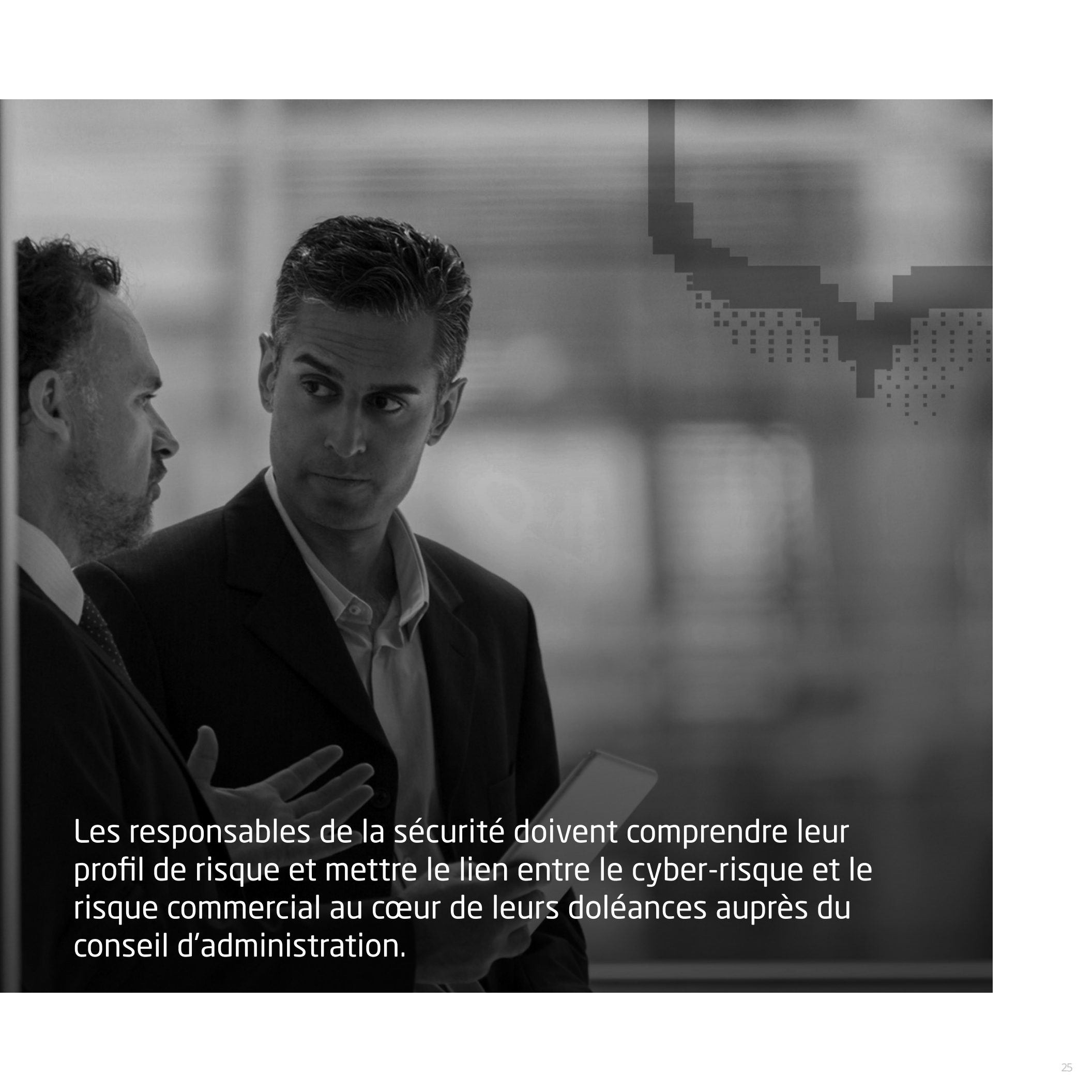
PARTIE V

Le mot de la fin :

Être responsable de la cybersécurité n'a jamais été aussi difficile :

Des attaques de plus en plus sophistiquées et de plus en plus nombreuses s'infiltrent dans les entreprises en raison de l'espace de travail moderne, tandis que le recrutement de professionnels de la cybersécurité continue de poser problème. Pourtant, **les RSSI n'ont jamais eu une telle opportunité de protéger leur organisation**: gardez le lien entre le cyber-risque et le risque commercial au cœur de vos interventions auprès du conseil d'administration ; évitez le piège d'un fournisseur de sécurité monolithique en mettant en œuvre des outils de cybersécurité à plusieurs niveaux et de pointe ; et protégez-vous contre les menaces primaires comme le phishing grâce à la protection de la messagerie électronique et à la sensibilisation des collaborateurs. Les responsables de la sécurité doivent comprendre leurs profils de risque et bien les présenter, tout en réduisant la surface d'attaque et en augmentant les contrôles.

Les conseils d'administration s'intéressent enfin à la cybersécurité, mais ils ont encore beaucoup d'autres priorités, notamment le risque de récession, le changement climatique et l'incertitude géopolitique. Ainsi, une plus grande attention ne se traduit pas automatiquement par davantage d'argent ou d'avantages pour la cyberdéfense, **mais plutôt par une surveillance accrue**. Cependant, l'opportunité de mettre en évidence le cyber-risque en tant que risque économique existe bel et bien.



Les responsables de la sécurité doivent comprendre leur profil de risque et mettre le lien entre le cyber-risque et le risque commercial au cœur de leurs doléances auprès du conseil d'administration.

PARTIE VI

Méthodologie

À propos des résultats inclus dans ce rapport

Les participants à l'enquête travaillent dans des organisations de moins de 500 employés (35 %), de 501 à 1 000 employés (33 %) et de plus de 1 000 employés (32 %).

Ces entreprises sont réparties dans **cinq secteurs** : les services financiers (29 %), le secteur de la santé (21 %), le secteur public (15 %), le commerce de détail (15 %) et le divertissement (19 %).

78 personnes **travaillant dans des entreprises** en Australie, à Singapour, en France, en Allemagne, aux Pays-Bas, entreprises situées en Australie, en Suède, au Danemark, aux Émirats arabes unis, en Arabie saoudite, au Canada, aux États-Unis et au Royaume-Uni ont répondu à l'enquête.





Work Protected.

Advanced Email & Collaboration Security

The Mimecast logo consists of a red rounded rectangle with the word "mimecast" in white lowercase letters.

www.mimecast.com | ©2024 mimecast | Tous droits réservés | GL-4485

Mimecast : Work Protected™ Depuis 2003, Mimecast permet aux entreprises d'éviter les incidents en travaillant en toute sécurité. Nous donnons à plus de 40 000 clients les moyens d'atténuer les risques et de gérer les complexités dans un paysage de menaces dominé par les cyberattaques malveillantes, les erreurs humaines et les failles technologiques. Nos solutions avancées offrent les capacités proactives de détection des menaces, de protection de la marque, de sensibilisation et de conservation des données dont les lieux de travail en constante évolution ont besoin aujourd'hui. Grâce aux solutions Mimecast, la sécurité de la messagerie électronique et des outils collaboratifs d'entreprise devient les yeux et les oreilles des entreprises du monde entier.