Delinea

L'impact de l'alignement du business sur l'efficacité de la stratégie en matière de cybersécurité

Enquête mondiale auprès de responsables de la cybersécurité

LIVRE BLANC

Synthèse

L'impact de la cybersécurité sur les entreprises est évident. Par exemple, en cas de cyber attaque massive, les activités d'une entreprise peuvent s'arrêter brutalement, à l'image d'un arrêt d'urgence qui fait dérailler un train lancé à pleine vitesse.

Au-delà de ce scénario catastrophe, le travail de l'équipe de cybersécurité a également un impact sur l'efficacité quotidienne de l'entreprise, la rapidité de la prestation des services, les coûts, la productivité des employés, l'expérience des utilisateurs et les ventes. Bien que ces impacts ne soient pas aussi dramatiques qu'un accident de train, ils peuvent ralentir les activités de l'entreprise et les faire dévier de leur trajectoire de telle sorte qu'il est difficile pour l'entreprise en question de s'en remettre.

L'importance de l'alignement entre la cybersécurité et le business enablement

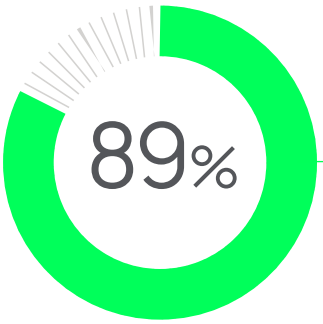
Alors que les entreprises continuent de naviguer dans un environnement informatique complexe et un climat économique incertain, l'alignement entre la cybersécurité et le business est essentiel pour réussir. On entend de plus en plus souvent dire que les équipes de cybersécurité ne devraient pas travailler en silo, en se concentrant uniquement sur la protection des technologies. Ces équipes s'entendent dire qu'elles ne peuvent pas être le « service qui dit toujours non » et qu'elles doivent au contraire devenir des « business enablers » concernant les activités.

Cependant, nombreuses sont les équipes qui ne savent pas comment faire de ces concepts à la mode une réalité. La plupart des responsables de la cybersécurité ont une formation technique et ont gravi les échelons des services techniques. Ils ont peut-être travaillé en silo pendant la majeure partie de leur carrière. Changer les mentalités pour permettre une nouvelle façon de travailler ne se fait pas du jour au lendemain. Pour y parvenir, la première étape consiste à acquérir une compréhension précise et partagée de la situation actuelle de notre secteur.

Dans ce contexte, nous avons interrogé plus de 2 000 décideurs en matière de cybersécurité travaillant dans des entreprises de plus de 500 employés dans 22 pays afin de comprendre leur situation actuelle en matière de business enablement. Plus précisément, nous voulions identifier, à l'aide de données, les éléments qui ont un impact significatif sur le business enablement, notamment l'alignement, les compétences et les structures organisationnelles.

Les résultats de l'enquête sont à la fois fascinants et troublants

Ils montrent que le secteur de la cybersécurité a encore un long chemin à parcourir pour devenir des moteurs efficaces du business enablement. Les données révèlent un manque d'alignement entre les équipes mais aussi au sein des équipes, ce qui peut avoir un impact négatif sur la sécurité et l'atteinte des objectifs du business.



En effet, 89% des personnes interrogées déclarent que leur entreprise a subi au moins un impact négatif au cours de l'année écoulée en raison d'un manque d'alignement entre le business et leur stratégie en matière de cybersécurité.

Une grande partie du problème réside dans l'incapacité de l'entreprise à aligner efficacement les objectifs et les indicateurs. Ce défi réside dans la lutte que mènent les entreprises pour parvenir à un accord commun sur un large éventail d'attentes.

Ce rapport vous donnera un aperçu de la situation actuelle et vous permettra de comprendre certains des facteurs qui déterminent non seulement la posture en matière de cybersécurité, mais aussi la réussite de l'entreprise.

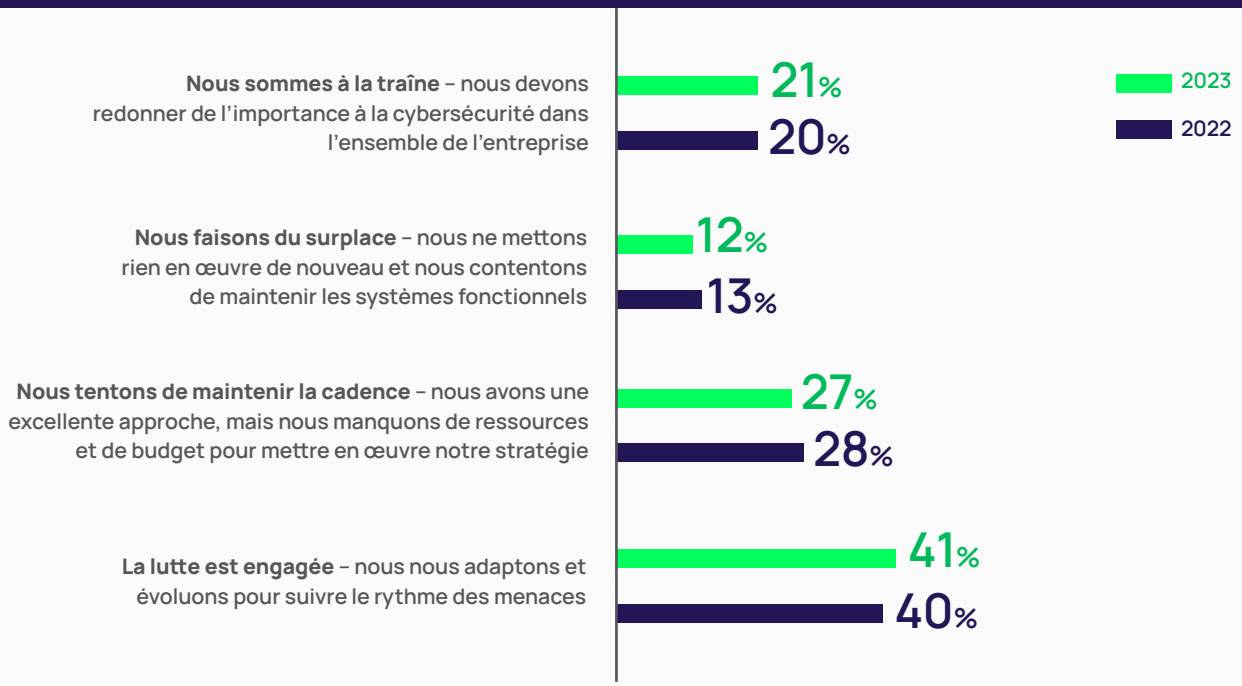
Résultat clé 1

Lorsque les responsables de la cybersécurité ne se sentent pas en sécurité, il est difficile de se concentrer sur autre chose.

Nous commençons ici à comprendre le contexte dans lequel opèrent les responsables de la cybersécurité.

Seuls 40 % des décideurs interrogés se disent prêts à s'engager dans la lutte pour la cybersécurité. La plupart des responsables de la sécurité affirment soit qu'ils tentent de maintenir la cadence, soit qu'ils font du surplace ou qu'ils sont à la traîne. Ces chiffres restent pratiquement inchangés par rapport à l'année dernière.

Figure 1 | Laquelle des affirmations suivantes décrit le mieux votre stratégie globale actuelle en matière de sécurité ?



Il est intéressant de noter que les membres d'une même équipe ne sont pas d'accord sur le niveau actuel de sécurité au sein de leur entreprise. Les personnes occupant des fonctions plus élevées sont plus positives sur ce point que celles qui assument des responsabilités quotidiennes en matière de gestion des technologies de l'information et de la sécurité.

Figure 2 | Laquelle des affirmations suivantes décrit le mieux votre stratégie globale actuelle en matière de sécurité ?

	PDG	RSSI/DSI/CSO	Directeur IT ou de la sécurité	Responsable IT ou de la sécurité
Nous sommes à la traîne – nous devons redonner de l'importance à la cybersécurité dans l'ensemble de l'entreprise	**39%**	16%	16%	22%
Nous faisons du surplace – nous ne mettons rien en œuvre de nouveau, nous nous contentons de maintenir les systèmes fonctionnels	6%	7%	12 %	15%
Nous tentons de maintenir la cadence – nous avons une excellente approche, mais nous manquons de ressources et de budget pour mettre en œuvre notre stratégie	17%	21%	28%	31%
La lutte est engagée – nous nous adaptons et évoluons pour suivre le rythme des menaces	38%	**56%**	**44%**	**32%**

Changer de mentalité

Si l'on considère la question du « business enablement » dans ce contexte, on comprend pourquoi il peut être difficile pour un responsable de la cybersécurité d'étendre ses attributions au-delà des principes fondamentaux de la sécurité. Nombre d'entre eux sont accaparés par la lutte quotidienne pour la protection de l'entreprise et la lutte contre les incidents au fur et à mesure qu'ils surviennent. Malheureusement, ce manque de confiance dans la sécurité signifie que de nombreux responsables de la cybersécurité n'ont pas la capacité de se concentrer également sur les objectifs du business.

Le véritable problème dans cette situation est le coût d'opportunité. La pression exercée pour atteindre un niveau de sécurité de base accapare l'énergie et les ressources nécessaires à la poursuite d'objectifs du business qui ne relèvent pas traditionnellement de la responsabilité de l'équipe chargée de la sécurité.

Pour un RSSI à la traîne ou en train de courir pour rester dans le coup, le conseil de se concentrer sur les objectifs du business peut sembler aller à l'encontre de sa vision du monde. Mais, comme vous le verrez dans ce rapport, le fait d'intégrer les objectifs du business peut également avoir un impact positif sur les objectifs de sécurité.

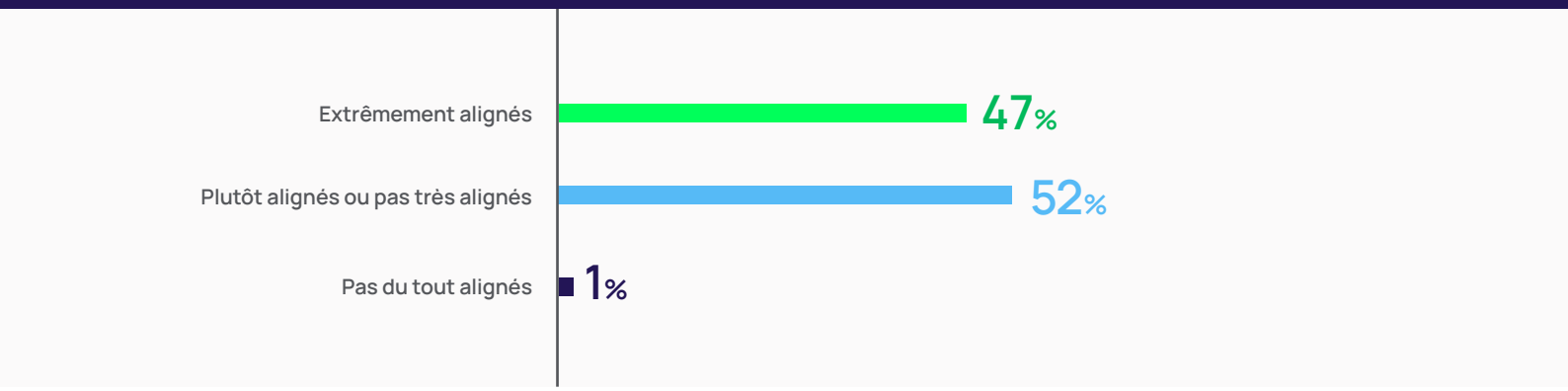
Résultat clé 2

Les décideurs en matière de cybersécurité déclarent que les objectifs du business sont importants mais admettent qu'ils ne les atteignent pas.

Les responsables de la cybersécurité admettent que les objectifs de sécurité et les objectifs du business sont mal alignés

Dans l'ensemble, moins de la moitié (47 %) des décideurs estiment que leurs objectifs en matière de cybersécurité sont parfaitement en phase avec les objectifs du business.

Figure 3 | Dans quelle mesure estimez-vous que vos objectifs en matière de cybersécurité sont alignés aux objectifs plus généraux du business ?



Il est intéressant de noter que la quasi-totalité des entreprises qui ont confiance dans leur dispositif de sécurité – celles qui disent que « la lutte est engagée » – se disent ***également*** très ou assez bien alignées sur les objectifs du business. Elles sont beaucoup plus susceptibles d'être alignées que leurs homologues qui déclarent faire du surplace ou de tenter de maintenir la cadence pour répondre aux besoins de sécurité.

À l'autre bout du spectre, les entreprises qui ont le moins confiance dans leur dispositif de sécurité pensent aussi qu'elles ont un bon alignement. Cela peut s'expliquer par une surestimation de l'alignement sécurité/business ou une sous-estimation de leur posture de cybersécurité.

Figure 4 | Dans quelle mesure estimez-vous que vos objectifs en matière de cybersécurité sont alignés sur les objectifs plus généraux du business ?

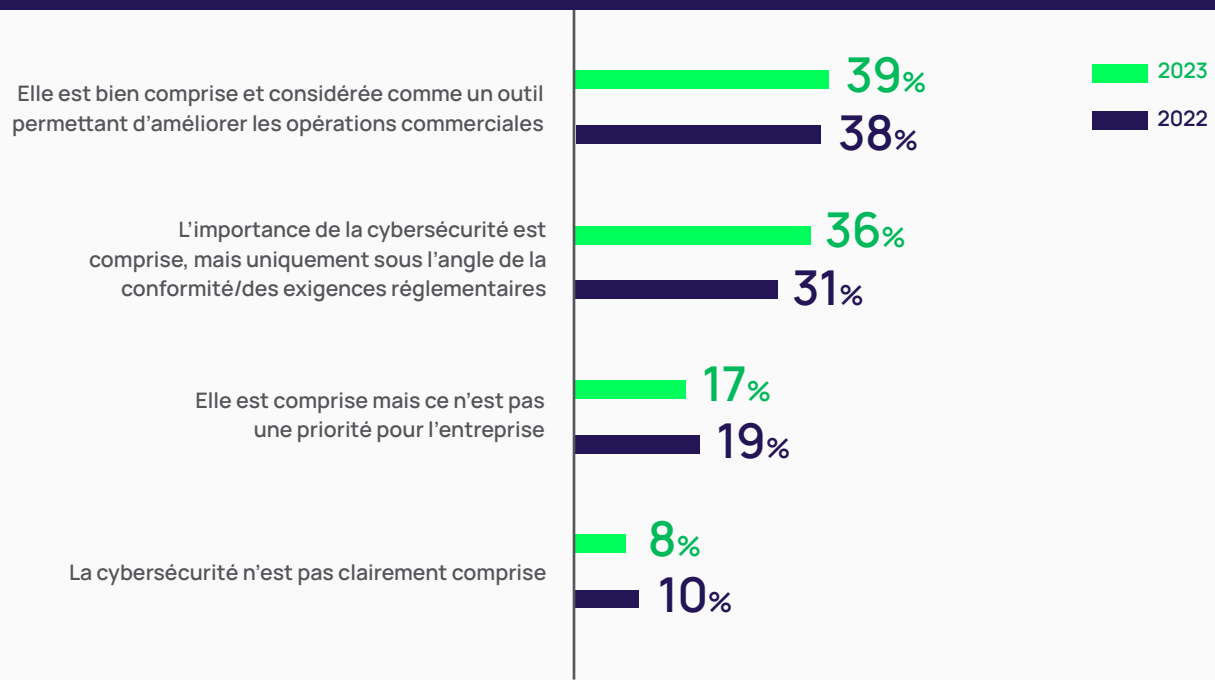
	Extrêmement alignés	Assez bien alignés	Peu alignés	Pas du tout alignés	Ne se prononce pas
Nous sommes à la traîne – nous devons redonner de l'importance à la cybersécurité dans l'ensemble de l'entreprise	59%	36%	4%	1%	1%
Nous faisons du surplace – nous ne mettons rien en œuvre de nouveau, nous nous contentons de maintenir les systèmes fonctionnels	29%	56%	13%	2%	0%
Nous tentons de maintenir la cadence – nous avons une excellente approche, mais nous manquons de ressources et de budget pour mettre en œuvre notre stratégie	31%	60%	7%	2%	0%
La lutte est engagée – nous nous adaptons et évoluons pour suivre le rythme des menaces	56%	43%	1%	0%	0%

Les plus hauts responsables d'une entreprise ne comprennent pas le lien entre business et sécurité.

La fonction de cybersécurité n'est pas encore reconnue par les plus hautes instances de l'entreprise comme un moteur de l'activité. Si la moitié des répondants (53 %) affirment que la cybersécurité est comprise par leur conseil d'administration et leur direction, ils pensent que ces dirigeants ne considèrent pas la sécurité comme un moteur de l'activité. Ce chiffre n'a pas beaucoup bougé au cours de l'année écoulée.

C'est un fait désolant mais qui montre à quel point la cybersécurité et les objectifs du business ne sont pas alignés au sein de l'entreprise.

Figure 5 | Laquelle des affirmations suivantes décrit le mieux la compréhension de la cybersécurité par le conseil d'administration ou la direction générale au sein de votre entreprise ?

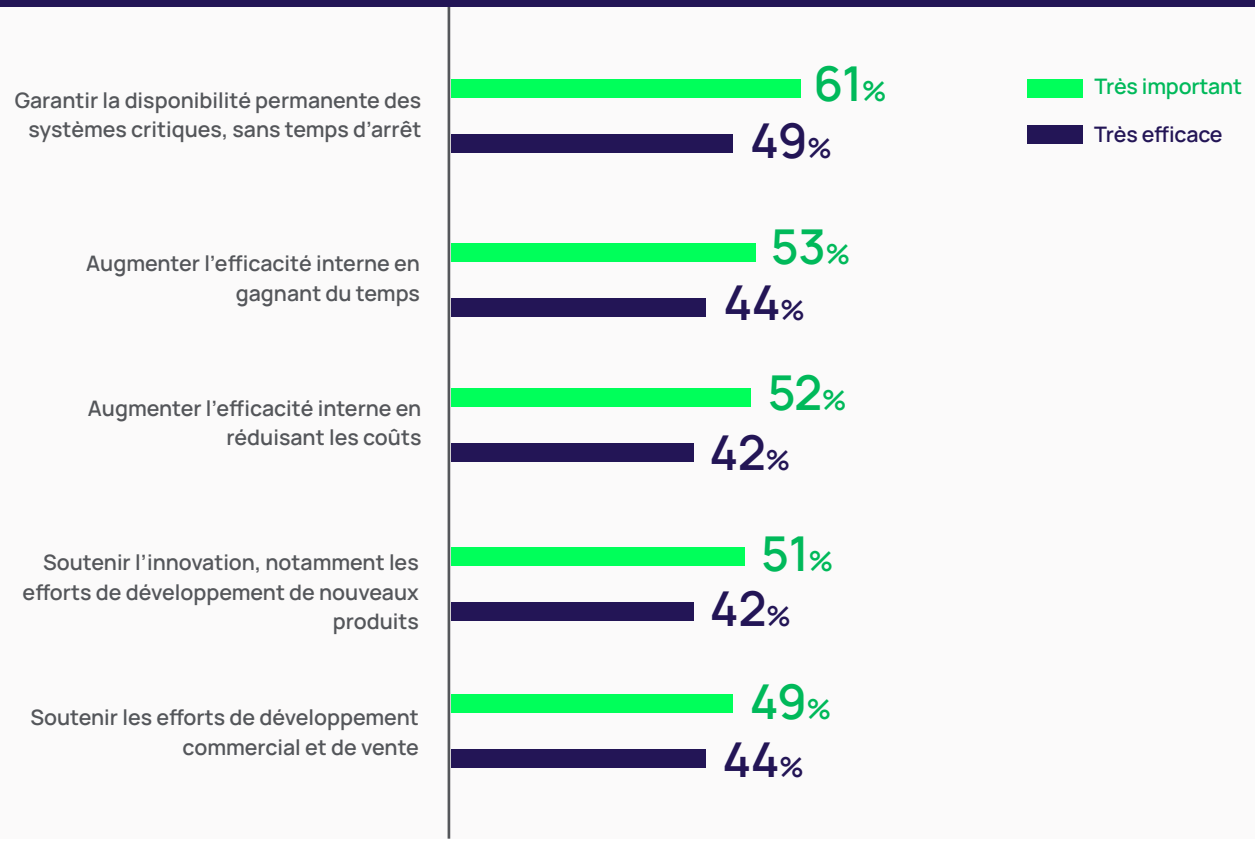


Les responsables de la cybersécurité ne pensent pas être efficaces dans la réalisation de leurs plus grandes priorités

Il s'avère que si l'objectif premier de la plupart des décideurs en matière de sécurité est ***technique*** — garantir la protection et la disponibilité des systèmes critiques — près de la moitié d'entre eux estiment également que leurs équipes doivent atteindre des objectifs ***du business*** tels que l'amélioration de l'efficacité, la réduction des coûts et le soutien à l'innovation et aux ventes.

Cependant, moins de la moitié d'entre eux estiment qu'ils sont très efficaces pour atteindre leurs objectifs prioritaires, qu'il s'agisse d'objectifs techniques ou commerciaux.

Figure 6 | Quel est le degré d'importance des objectifs suivants pour votre équipe de cybersécurité ? Dans quelle mesure pensez-vous que votre équipe de cybersécurité est efficace pour atteindre ces objectifs ?



De la même manière, les entreprises les plus confiantes dans leur dispositif de sécurité sont plus susceptibles d'être très ***efficaces*** pour atteindre leurs objectifs du business. Une fois de plus, les équipes de sécurité les moins confiantes affirment qu'elles sont efficaces, comme le montre le tableau ci-dessous.

Figure 7 | Dans quelle mesure pensez-vous que votre équipe de cybersécurité est efficace pour atteindre ces objectifs ?

	Garantir la disponibilité permanente des systèmes critiques, sans temps d'arrêt	Soutenir les efforts de développement commercial et de vente	Augmenter l'efficacité interne en gagnant du temps	Soutenir l'innovation, notamment les efforts de développement de nouveaux produits	Augmenter l'efficacité interne en réduisant les coûts
Nous sommes à la traîne – nous devons redonner de l'importance à la cybersécurité dans l'ensemble de l'entreprise	62%	60%	65%	58%	61%
Nous faisons du surplace – nous ne mettons rien en œuvre de nouveau, nous nous contentons de maintenir les systèmes fonctionnels	51%	49%	44%	40%	43%
Nous tentons de maintenir la cadence – nous avons une excellente approche, mais nous manquons de ressources et de budget pour mettre en œuvre notre stratégie	53%	48%	42%	40%	48%
La lutte est engagée – nous nous adaptons et évoluons pour suivre le rythme des menaces	62%	53%	55%	55%	48%

Changer de mentalité

Plusieurs raisons peuvent expliquer ce manque d'alignement. Voici quelques-unes des raisons possibles :

1. **Désalignement des objectifs de sécurité et des objectifs du business :** les responsables de la sécurité peuvent trop se concentrer sur l'atténuation des risques et la protection des actifs, sans comprendre les objectifs plus larges de l'entreprise.

2. **Manque de communication et de collaboration :** les responsables de la sécurité peuvent ne pas communiquer efficacement leurs objectifs aux autres unités opérationnelles ou parties prenantes, ou ne pas collaborer avec elles pour élaborer des stratégies de sécurité qui soutiennent les objectifs du business. Les mesures de sécurité peuvent ainsi être considérées comme des obstacles aux objectifs du business plutôt que comme des éléments facilitateurs.

3. **Ressources insuffisantes :** les responsables de la sécurité peuvent ne pas disposer des ressources adéquates, telles que le budget, le personnel ou la technologie, pour mettre en œuvre des mesures de sécurité qui répondent aux objectifs du business. Il peut en résulter des mesures inadéquates ou inefficaces, ou qui imposent des charges de travail excessives à d'autres unités opérationnelles.

4. **Des indicateurs inadéquats :** les responsables de la sécurité peuvent ne pas disposer des indicateurs appropriés pour déterminer l'efficacité de leurs mesures de sécurité par rapport aux objectifs du business. Cela peut donner l'impression que les mesures de sécurité ne sont pas efficaces, même si elles le sont.

5. **Manque de compréhension des objectifs du business :** les responsables de la sécurité peuvent ne pas avoir une compréhension claire des objectifs, des priorités et des défis de l'entreprise. Il peut en résulter des mesures de sécurité qui ne tiennent pas compte des besoins spécifiques de l'entreprise.

Nous examinerons chacune de ces raisons potentielles dans la suite du rapport.

Résultat clé 3

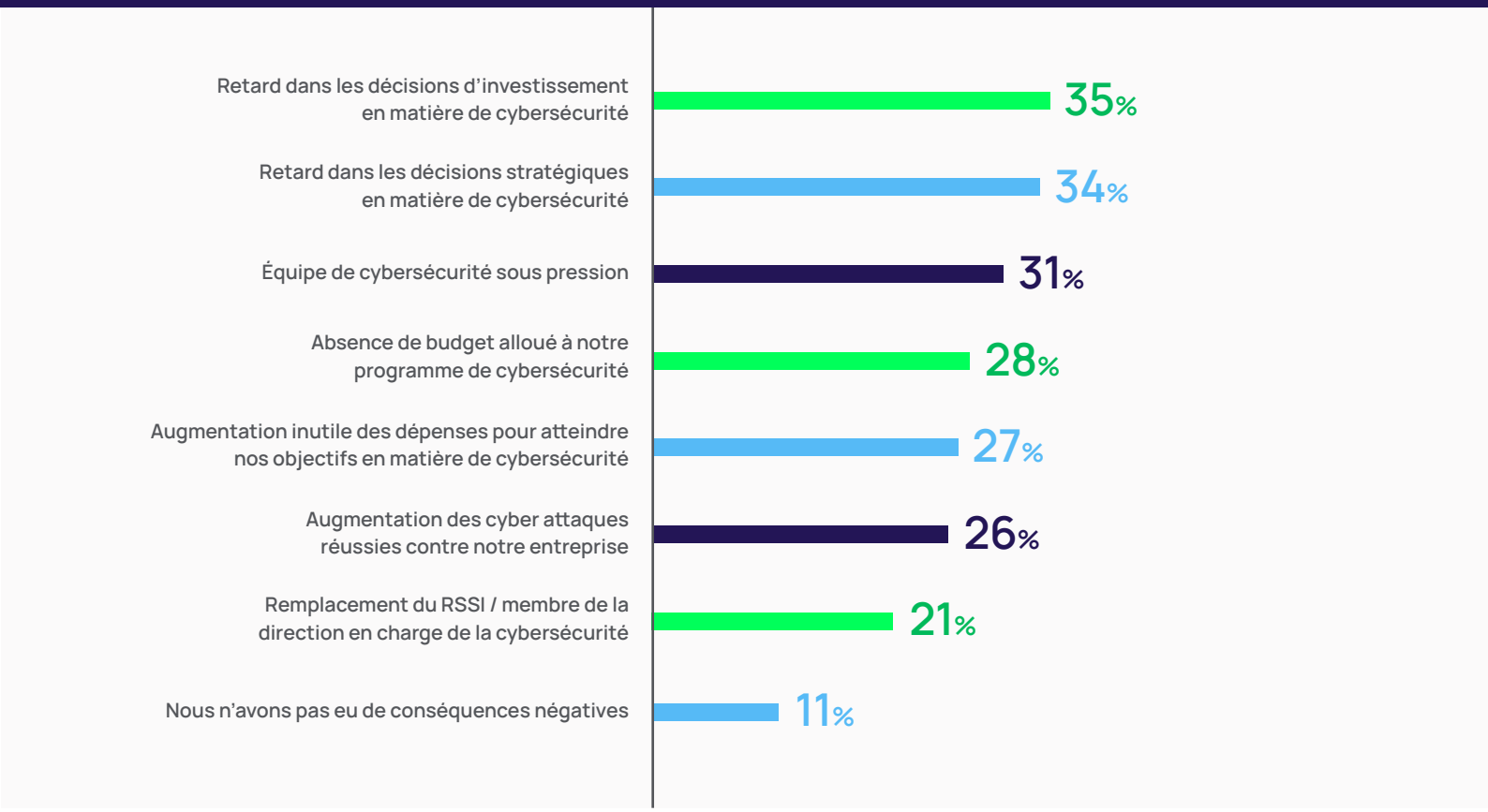
Le désalignement a un impact négatif **à la fois** sur les objectifs du business **et** sur les objectifs de sécurité.

Une cyber attaque réussie peut entraîner des violations de données, des pannes de système, des pertes financières et une atteinte à la réputation de l'entreprise, ce qui peut nuire à ses objectifs du business. Les résultats de la recherche confirment cette affirmation.

Les impacts négatifs sont multiples

Près de neuf entreprises sur dix ont subi au moins un impact négatif au cours de l'année écoulée en raison d'un manque d'alignement entre la cybersécurité et le business.

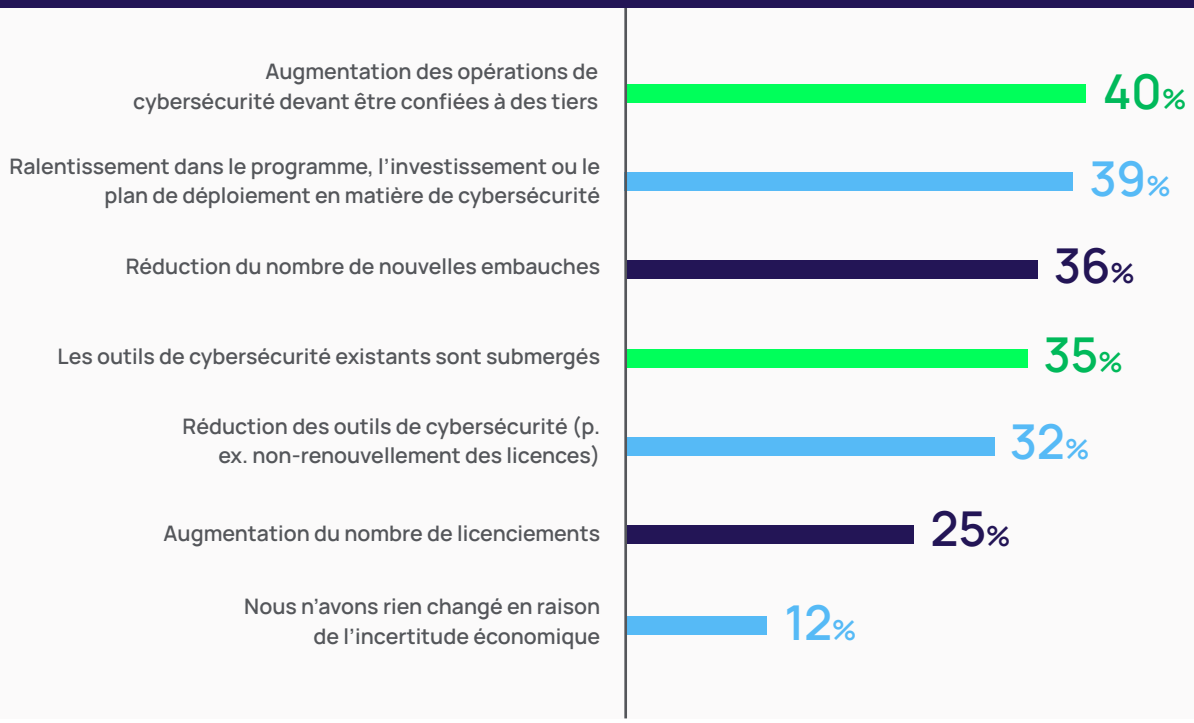
Figure 8 | Quelles sont, le cas échéant, les conséquences négatives que vous avez subies en raison d'un mauvais alignement entre les objectifs de cybersécurité et les objectifs du business ? (Sélectionnez jusqu'à trois éléments.)



Pourquoi maintenant ? Le climat économique actuel est en partie responsable

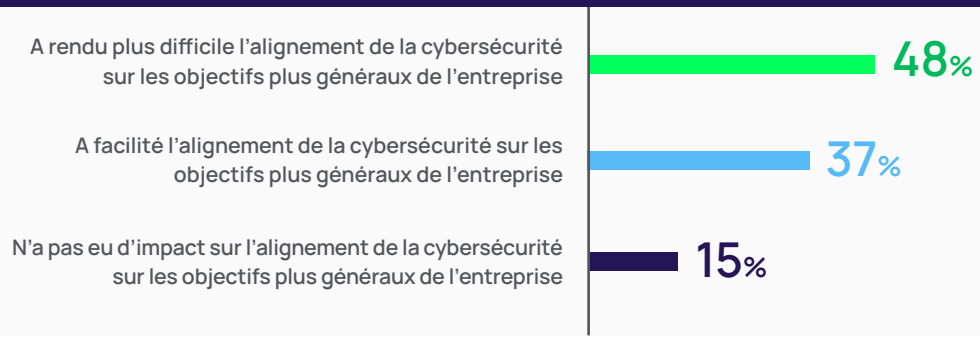
88 % des entreprises ont connu des changements dus à l'incertitude économique. Nombre de ces changements ont des répercussions négatives sur la sécurité, comme un ralentissement du programme et des investissements dans la technologie, ainsi qu'un manque de ressources, comme le montre le graphique ci-dessous.

Figure 9 | Comment l'incertitude économique récente a-t-elle affecté votre équipe de cybersécurité au cours des 6 derniers mois ?



Dans un environnement en mutation, l'alignement peut s'avérer difficile. Environ la moitié des personnes interrogées reconnaissent que l'incertitude économique a rendu plus difficile l'alignement de la cybersécurité et des activités business.

Figure 10 | Comment l'incertitude économique récente a-t-elle affecté l'alignement des objectifs de cybersécurité et des objectifs plus larges du business ?



Changer de mentalité

Avec de tels enjeux, la vraie question concernant l'alignement de la sécurité et du business n'est pas « Comment pouvons-nous y arriver ? » mais « Comment pouvons-nous nous permettre de ne pas le faire ? ».

En intégrant la cybersécurité dans la stratégie globale de l'entreprise, vous pouvez développer une approche proactive de la sécurité qui peut réduire le risque de cyber attaques et contribuer à préserver les opérations critiques de l'entreprise.

Ressource clé :

Lire l'enquête mondiale auprès de responsables de la cybersécurité Benchmarking des failles de sécurité et des accès à privilèges.

Résultat clé 4

L'inadéquation des indicateurs reflète l'absence d'alignement entre la cybersécurité et le business

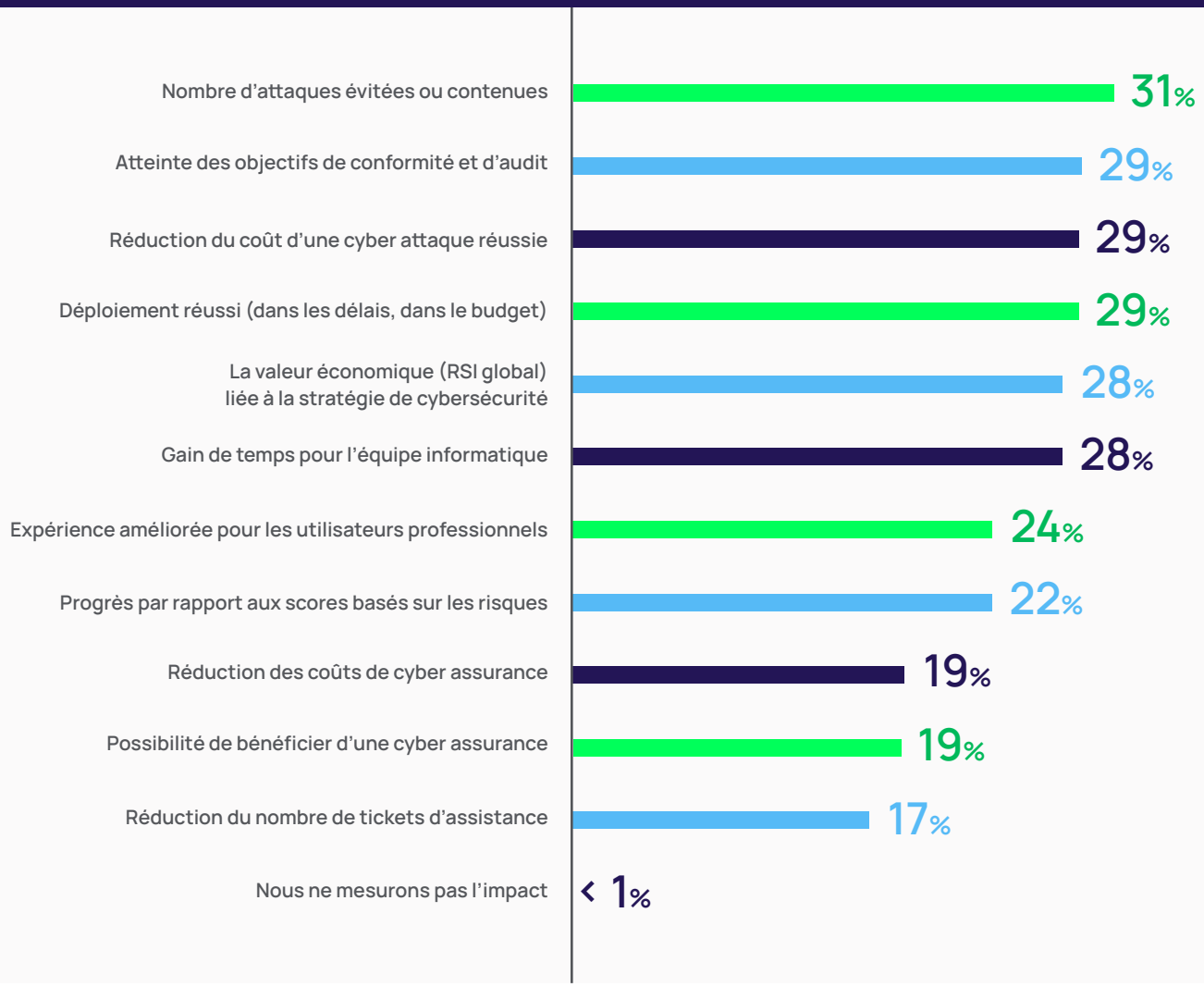
Pour pouvoir gérer quelque chose, il faut pouvoir le mesurer. Pour atteindre les objectifs de business enablement, les objectifs de l'équipe et les MBO (Management by Objectives) ou OKR (Objective and Key Results) individuels doivent être liés et suivis en permanence.

Malheureusement, à quelques exceptions près, cela ne semble pas être le cas. Ce que les dirigeants veulent faire n'est pas la même chose que ce qu'ils mesurent et rapportent réellement.

La différence entre les indicateurs techniques et business

Les données montrent que les performances des programmes de cybersécurité sont encore principalement jugées sur la base d'indicateurs techniques ou d'activité, tels que le nombre d'attaques évitées ou contenues, plutôt que sur la base d'indicateurs business, tels que la valeur économique, l'expérience des utilisateurs, les coûts d'assurance ou l'impact sur d'autres équipes.

Figure 11 | Parmi les éléments suivants, lesquels sont les plus importants pour mesurer le succès de vos programmes de cybersécurité ? (Sélectionnez jusqu'à trois éléments.)



Cela dit, le RSI global et la valeur économique sont plus importants pour les petites entreprises comptant moins d'employés.

Figure 12 | Parmi les éléments suivants, lesquels sont les plus importants pour mesurer le succès de vos programmes de cybersécurité ? (Sélectionnez jusqu'à trois éléments.)

	1er	2e	3e
500-999 employés	La valeur économique (RSI global, **29%**)	Nombre d'attaques évitées / Réduction des coûts / Gain de temps (tout **28%**)	
1 000-4 999 employés	Nombre d'attaques évitées / contenues (**32%**)	Déploiement réussi / Gain de temps pour l'équipe informatique (les deux **31%**)	
+ de 5 000 employés	Nombre d'attaques évitées et contenues / Atteinte des objectifs d'audit et de conformité (les deux **31%**)		Réduction du coût des cyber attaques réussies (**30%**)

Il n'est pas surprenant que les dirigeants ayant des responsabilités étendues, tels que les PDG, soient plus préoccupés par la mesure de l'expérience utilisateur et la réduction des frictions que les RSSI. Il est toutefois intéressant de noter que les directeurs et les chefs de service mettent également l'accent sur des indicateurs business tels que la valeur économique ou le RSI.

Figure 13 | Parmi les éléments suivants, lesquels sont les plus importants pour mesurer le succès de vos programmes de cybersécurité ? (Sélectionnez jusqu'à trois éléments.)

	1er	2e	3e
PDG / Propriétaire d'entreprise	Amélioration de l'expérience des utilisateurs professionnels (**31%**)	Déploiement réussi (dans les délais, dans le budget, **30%**)	Atteinte des objectifs de conformité et d'audit (**29%**)
RSSI/DSI/CSO	Nombre d'attaques évitées / contenues (**32%**)	Déploiement réussi (dans les délais, dans le budget, **31%**)	Valeur économique / Réduction des coûts / Atteinte des objectifs de conformité (tous **28%**)
Chef du service informatique	La valeur économique (RSI global, **34%**)	Nombre d'attaques évitées / contenues (**32%**)	Réduction des coûts / Atteinte des objectifs de conformité (les deux **30%**)
Directeur IT	La valeur économique (RSI global, **32%**)	Nombre d'attaques évitées / contenues / Gain de temps pour les équipes informatiques (les deux **30%**)	
Responsable informatique	Nombre d'attaques évitées / contenues (**33%**)	Réduction des coûts / Atteinte des objectifs de conformité / Déploiement réussi (tous **30%**)	
Responsable de la sécurité	Réduction du coût des cyber attaques réussies (**36%**)	Déploiement réussi (dans les délais, dans le budget, **29%**)	Atteinte des objectifs de conformité et d'audit (**27%**)

Changer de mentalité

Les équipes de cybersécurité se concentrent souvent sur les indicateurs techniques parce qu'ils fournissent des données qui peuvent être utilisées pour évaluer le niveau de sécurité d'une entreprise. Les indicateurs techniques tels que le nombre de vulnérabilités détectées et corrigées, le temps nécessaire pour détecter les incidents de sécurité et y répondre, et le pourcentage de systèmes dotés d'un logiciel de sécurité mis à jour donnent une idée de l'efficacité des contrôles de sécurité et permettent aux équipes d'identifier les domaines à améliorer.

Toutefois, si les indicateurs techniques sont importants, ils ne sont pas les seuls facteurs qui déterminent le succès d'un programme de cybersécurité. La cybersécurité a pour but ultime de servir les objectifs du business, c'est-à-dire les résultats stratégiques rendus possibles par une sécurité efficace.

Les responsables de la cybersécurité peuvent améliorer l'alignement en établissant des objectifs clairs et mesurables liés aux objectifs stratégiques de leur entreprise. Il pourrait s'agir d'identifier les actifs les plus critiques pour l'entreprise, l'impact potentiel sur l'entreprise si ces actifs étaient attaqués et la manière dont des contrôles de sécurité efficaces améliorent la disponibilité, la confidentialité et l'intégrité de ces actifs. Par exemple, lorsque le service est en panne, le coût financier et opérationnel est évident. Les résultats en matière de cybersécurité peuvent être mesurés en fonction du coût de l'inaction par rapport au coût de l'action.

Les équipes chargées de la cybersécurité pourraient également s'efforcer d'améliorer leur communication et leur collaboration avec d'autres services de l'entreprise, tels que la gestion des risques, la conformité et les opérations commerciales. En travaillant en étroite collaboration avec ces parties prenantes, les équipes de cybersécurité peuvent mieux comprendre le contexte et les priorités de l'entreprise et aligner leurs activités en conséquence.

Enfin, les équipes de cybersécurité pourraient envisager d'adopter une approche de la sécurité davantage axée sur les risques, dans laquelle les indicateurs techniques sont utilisés en conjonction avec les résultats de l'entreprise pour prendre des décisions plus éclairées. Il s'agirait d'identifier les risques les plus importants pour l'entreprise et de concentrer les ressources sur l'atténuation de ces risques plutôt que de rechercher des indicateurs techniques pour eux-mêmes.

Pour mesurer l'alignement de la cybersécurité et des objectifs du business, il convient de prendre en compte les éléments suivants :

1. **Indicateurs de gestion des risques :** pour mesurer l'efficacité d'une entreprise dans l'identification et l'atténuation des risques de cybersécurité, y compris la fréquence des incidents et les délais de réponse.

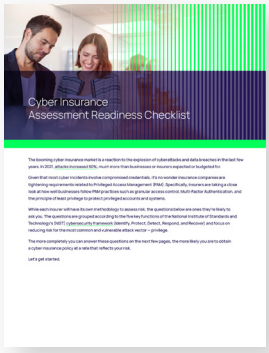
2. **Indicateurs de conformité :** pour savoir dans quelle mesure une entreprise respecte les normes de conformité réglementaires et sectorielles en matière de cybersécurité.

3. **Indicateurs de continuité des activités :** pour mesurer la capacité d'une entreprise à maintenir ses activités pendant un incident de cybersécurité, y compris la durée du temps d'arrêt et le délai de récupération.

4. **Indicateurs de coût :** pour suivre le coût de la mise en œuvre et du maintien des mesures de cybersécurité par rapport au budget global.

5. **Indicateurs de productivité :** pour mesurer la rapidité avec laquelle un nouvel employé ou un nouveau fournisseur peut être intégré, recevoir les ressources et l'accès nécessaires pour faire son travail.

En utilisant ce type d'indicateurs, vous pouvez évaluer l'efficacité de votre stratégie de cybersécurité pour ce qui est de permettre à l'entreprise d'atteindre ses objectifs et de prendre des décisions éclairées concernant les investissements dans les ressources de cybersécurité.



Ressources clés :

- Liste de contrôle de la cyber assurance : pour répondre aux questions que les fournisseurs de cyber assurance ne manqueront pas de poser
- S'aligner sur les cadres réglementaires et les exigences de conformité

Résultat clé 5

En l'absence de changements structurels, l'alignement entre la cybersécurité et le business s'annonce difficile.

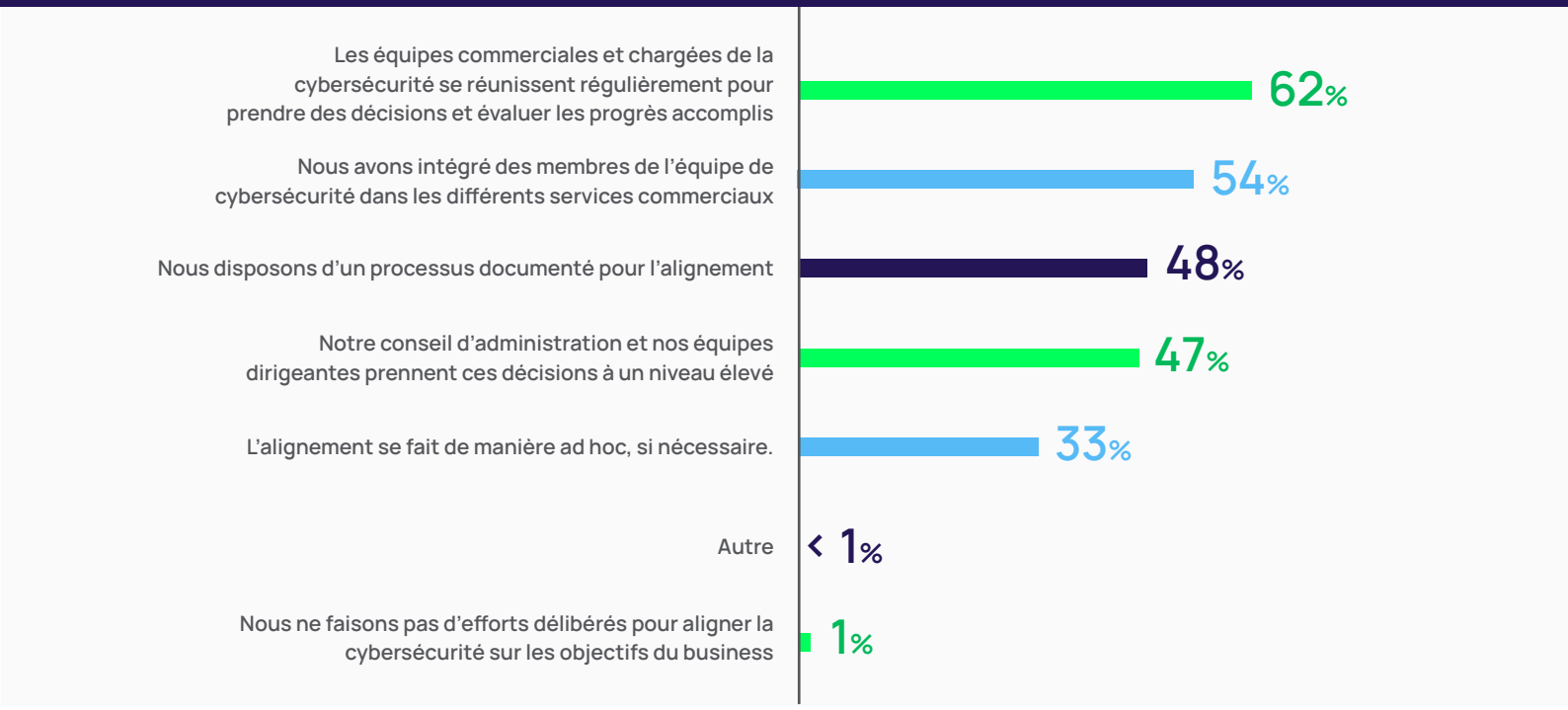
Pour aligner le business et la cybersécurité, il est essentiel de tenir compte de la structure organisationnelle. C'est donc sur cela que nous allons nous pencher.

Passer de la parole aux actes

La bonne nouvelle, c'est que les différents services échangent au sein de l'entreprise. La plupart des équipes de cybersécurité rencontrent régulièrement leurs homologues à des niveaux élevés ou ont même intégré des membres de l'équipe de sécurité à des postes commerciaux.

Cependant, moins de la moitié des entreprises documentent les politiques et les procédures pour les aider à s'aligner.

Figure 14 | Comment votre entreprise s'assure-t-elle que les objectifs de cybersécurité sont alignés sur les objectifs plus larges du business ? (Sélectionnez toutes les réponses qui s'appliquent.)



Les sondés qui se considèrent comme « **très alignés** » sont les plus susceptibles de dire que :

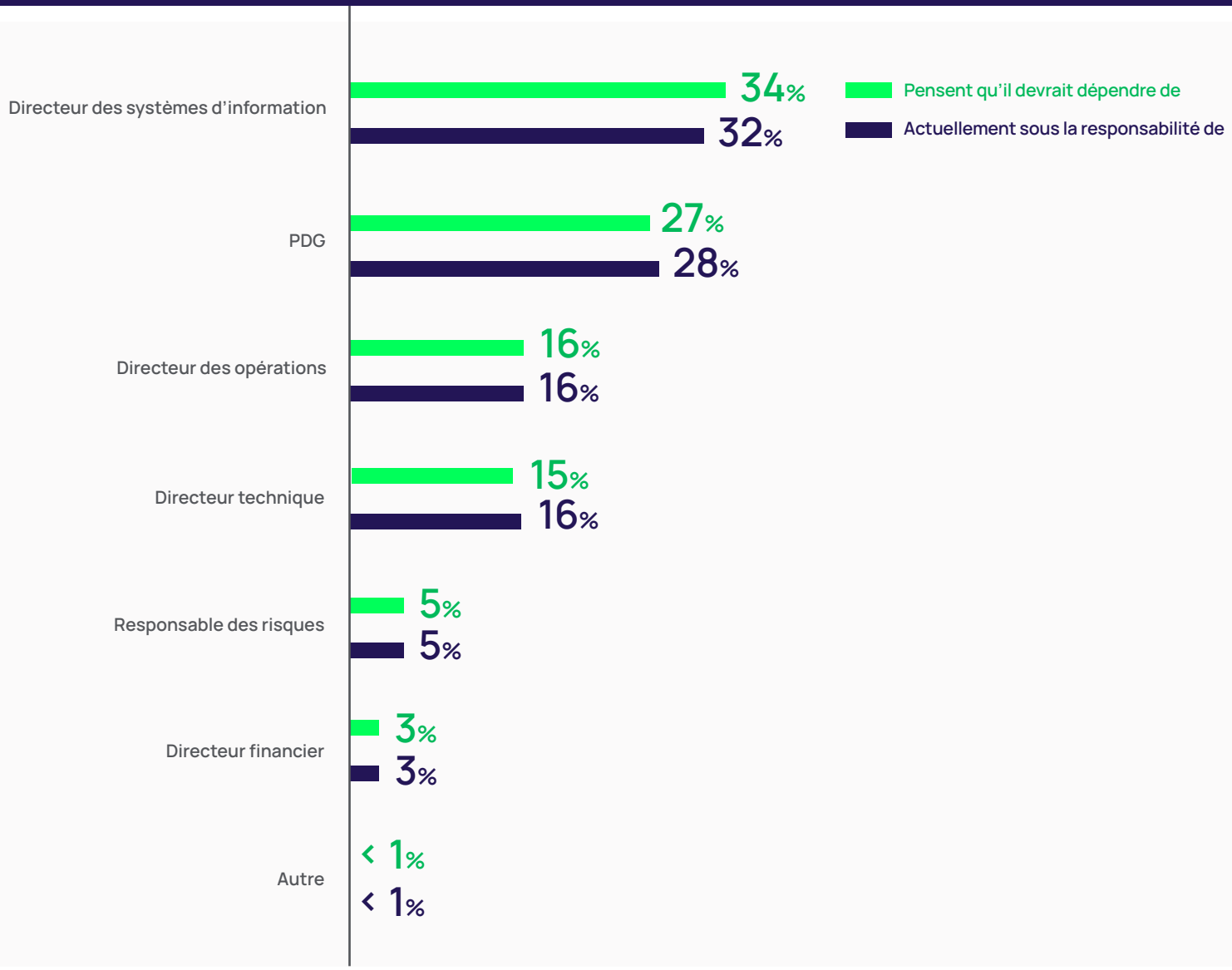
- Les équipes commerciales et de cybersécurité se réunissent régulièrement pour prendre des décisions et évaluer les progrès (68 %)
- Nous avons intégré des membres de l'équipe de cybersécurité dans les différents services commerciaux (61 %)
- Notre conseil d'administration et nos équipes dirigeantes prennent ces décisions à un niveau élevé (56 %)

La structure hiérarchique peut nuire à la mise en œuvre des activités de l'entreprise au lieu de la favoriser

Plus d'un tiers (34 %) des personnes interrogées pensent que la bonne personne à qui un RSSI doit rendre compte est le DSI. Dans la plupart des entreprises, c'est le cas.

Il est intéressant de noter que les préférences en matière de hiérarchie varient en fonction du poste occupé. Par exemple, les PDG sont plus enclins à préférer que les RSSI leur soient rattachés, tandis que les directeurs informatiques sont plus enclins à dire que les RSSI devraient être rattachés à leur patron, le DSI.

Figure 15 | Selon vous, à qui le RSSI ou le plus haut responsable de la cybersécurité devrait-il rendre compte, afin d'aligner au mieux la cybersécurité sur les objectifs globaux de l'entreprise ?
Actuellement, de qui dépend le RSSI ou le responsable le plus haut placé en matière de cybersécurité dans votre entreprise ?



Les compétences actuelles reflètent la nécessité que les responsables de la cybersécurité se concentrent plus sur les activités commerciales.

Dans l'ensemble, les personnes interrogées estiment que le savoir-faire technique est la compétence la plus essentielle pour un responsable de la cybersécurité tel qu'un RSSI. Elles placent cette compétence bien plus haut dans l'échelle d'importance que les compétences liées à l'entreprise telles que la communication, la collaboration, l'élaboration d'un dossier commercial et le sens des affaires.

Figure 16 | Quelle est l'importance de chacune de ces compétences pour un RSSI / responsable de la cybersécurité ? Sélectionnez un élément par ligne

Comme le montre le graphique ci-dessous, les compétences dont les répondants estiment manquer le plus sont la capacité à gérer ou à désamorcer des situations stressantes, suivies par des compétences telles que l'élaboration d'un dossier commercial et la communication. Sans ces compétences, les responsables de la cybersécurité auront beaucoup de mal à s'aligner sur leurs collègues commerciaux.

Figure 17 | Quelles sont, d'après vous, vos lacunes en matière de compétences ? Sélectionnez toutes les réponses qui s'appliquent

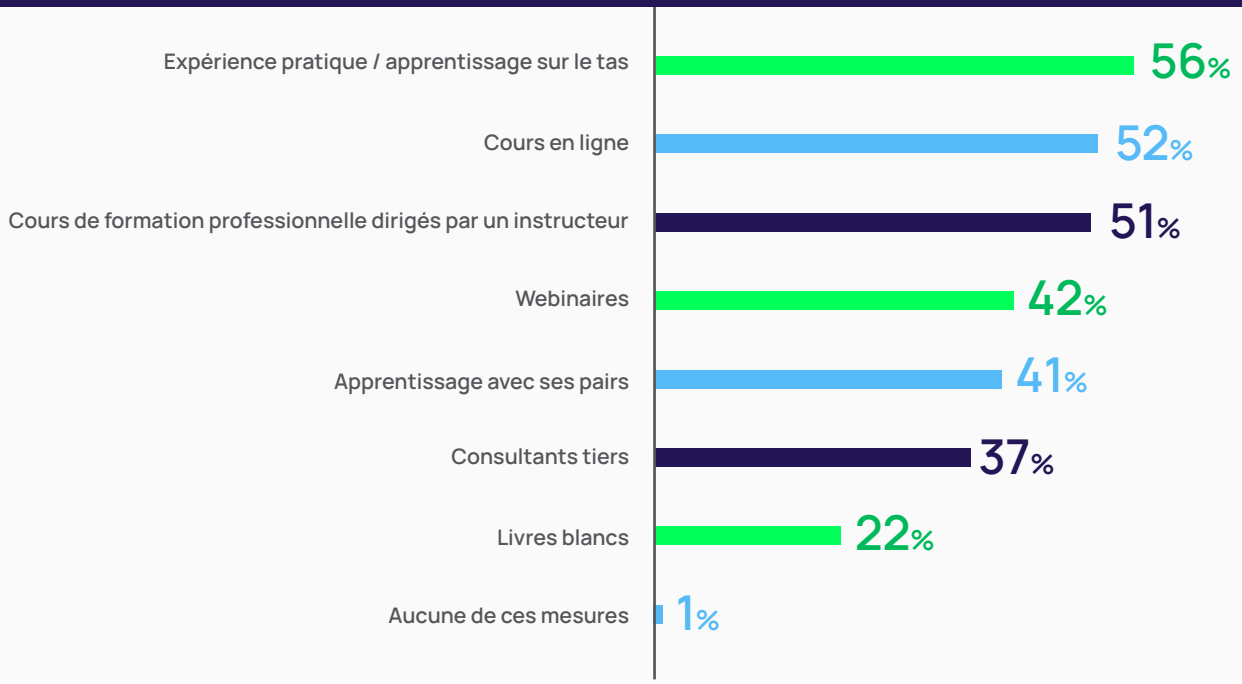
Figure 18 | Quelles sont, d'après vous, vos lacunes en matière de compétences ?

	1er	2e	3e
PDG / Propriétaire d'entreprise	Gestion des situations stressantes / Communication (partager des informations, expliquer, éduquer, les deux **38%**)		Capacité à présenter un dossier convaincant à la direction et au conseil d'administration (**36%**)
RSSI/DSI/CSO	Compréhension des exigences légales / savoir-faire technique (**32%**)	Gestion des situations stressantes / Capacité à présenter efficacement un dossier à la direction générale / Communication / Compréhension des exigences réglementaires et de conformité (tout **31%**)	
Chef du service informatique	Gestion des situations stressantes (**31%**)	Compréhension des exigences légales / Communication / Management du personnel (tout **29%**)	
Directeur IT	Gestion des situations stressantes (**32%**)	Compréhension des exigences légales (**31%**)	Compréhension des exigences de conformité et de réglementation (**30%**)
Responsable informatique	Capacité à présenter un dossier convaincant à la direction et au conseil d'administration (**34%**)	Réduction des coûts / Atteinte des objectifs de conformité / Déploiement réussi (tous **30%**)	
Responsable de la sécurité	Management du personnel (**37%**)	Sens des affaires (**29%**)	Capacité à présenter un dossier convaincant à la direction et au conseil d'administration (les deux **28%**)

La formation réactive ne comble pas le déficit de compétences

L'expérience pratique et l'apprentissage sur le tas sont les moyens les plus populaires pour les personnes sondées d'améliorer leurs compétences. Il semble que les individus se disent « nous nous occuperons de ce problème quand il le faudra ». Cela n'augure rien de bon pour le développement des compétences nécessaires au business enablement proactif et intentionnel.

Figure 19 | Comment améliorez-vous vos propres compétences et vous formez-vous pour vous aligner sur les objectifs du business et améliorer les performances commerciales globales de l'entreprise ?



Cela dit, et cela devrait maintenant être évident, le business enablement n'est pas seulement dépendant des compétences. La bonne volonté est également cruciale.

Changer de mentalité

Pour mieux s'aligner sur l'objectif de « business enablement » et l'atteindre, les responsables de la cybersécurité devraient envisager les mesures suivantes :

Organiser des réunions efficaces

On pourrait naturellement penser que la meilleure façon d'assurer l'alignement est de réunir tout le monde en premier lieu. Mais le fait de se rencontrer ne garantit pas toujours l'alignement. En effet, ce type de réunion n'est peut-être même pas nécessaire. L'alignement consiste à faire en sorte que les équipes interagissent les unes avec les autres d'une manière très spécifique, qu'elles se rencontrent ou non.

En fin de compte, l'alignement peut être synchrone ou asynchrone. Localisé au même endroit ou distribué. En personne ou par le biais d'un appel Zoom. Tant qu'il aide les équipes à se comprendre, à partager des objectifs et à mesurer collectivement les succès.

Développer les compétences

Il est fort probable que les entreprises ne trouveront pas en une seule personne la combinaison parfaite de compétences commerciales et de sécurité. Pour trouver la bonne combinaison, les responsables de la cybersécurité devront regarder au-delà des experts techniques et faire appel à des personnes ayant des parcours non traditionnels pour travailler avec leurs équipes.

Réorganiser la structure hiérarchique

Si le fait que le RSSI soit rattaché au DSI peut présenter des avantages, cela peut aussi poser des problèmes.

Le RSSI doit-il rendre compte au DSI ?

AVANTAGES

- **Alignement avec la stratégie informatique :** le RSSI et le DSI travaillent en étroite collaboration pour aligner la stratégie de sécurité informatique de l'entreprise sur sa stratégie commerciale globale. Cette approche garantit que la sécurité est intégrée dans tous les aspects de l'informatique, y compris le développement et la mise en œuvre de nouvelles technologies, applications et infrastructures.

- **Responsabilité claire :** en rendant compte au DSI, le RSSI est clairement responsable de la sécurité des systèmes informatiques de l'entreprise. Cette responsabilité permet de s'assurer que les risques de sécurité sont identifiés, évalués et traités rapidement et efficacement.

- **Affectation des ressources :** le DSI est responsable de l'affectation des ressources aux projets informatiques et le fait que le RSSI relève du DSI garantit que la sécurité est prise en compte dans l'affectation des ressources. Le RSSI peut aider le DSI à identifier les domaines dans lesquels des ressources supplémentaires sont nécessaires pour renforcer le dispositif de sécurité de l'entreprise.

- **Meilleure communication :** le RSSI et le DSI comprennent mieux les défis auxquels ils sont mutuellement confrontés et peuvent travailler ensemble pour les relever. En rendant compte au DSI, le RSSI a un meilleur accès aux décideurs informatiques et peut communiquer plus efficacement avec eux.

INCONVÉNIENTS

- **Conflit d'intérêts :** le DSI est responsable de la fourniture de services et de projets informatiques dans les délais et le budget impartis. Cette priorité accordée à la prestation de services peut parfois entrer en conflit avec la responsabilité du RSSI de garantir la sécurité des systèmes informatiques. Ce conflit peut conduire le RSSI à être contraint de donner la priorité à la prestation de services informatiques plutôt qu'à la sécurité.

- **Manque d'autonomie :** cela peut limiter l'autonomie du RSSI et sa capacité à travailler de manière indépendante. Si le DSI ne soutient pas la question de la sécurité ou n'y consacre pas suffisamment de ressources, le RSSI peut avoir du mal à mettre en œuvre les contrôles de sécurité de manière efficace.

- **Obstacles à la communication :** cela peut limiter leur capacité à communiquer avec le PDG et le conseil d'administration pour comprendre la position de l'entreprise en matière de sécurité.

- **Attention limitée portée à la sécurité :** cela peut renforcer la perception que la sécurité est une préoccupation secondaire et qu'elle ne reçoit pas l'attention et les ressources qu'elle mérite.

- **Gestion des risques et de la conformité :** l'accent mis par le DSI sur la prestation de services informatiques peut parfois conduire à une approche de la sécurité axée sur la conformité, où l'accent est mis sur le respect des exigences réglementaires plutôt que sur la gestion des risques de sécurité.

Dans l'ensemble, si le fait que le RSSI relève du DSI peut être bénéfique, il est important de résoudre ces problèmes potentiels pour que la sécurité reçoive l'attention qu'elle mérite et que le RSSI puisse travailler en toute indépendance et fournir une évaluation objective de la situation de l'entreprise en matière de sécurité.

Que faire maintenant ?

Il est essentiel que la cybersécurité s'aligne sur les objectifs du business, car les risques peuvent avoir une incidence directe sur la capacité d'une entreprise à atteindre ses objectifs stratégiques. Plus la cybersécurité est en phase avec les activités de l'entreprise, plus cette dernière est résiliente ET plus elle peut prospérer.

Passer du « moi » au « nous »

La mise en place d'un alignement efficace entre la sécurité et le business de l'entreprise nécessite un ensemble de compétences. Elle exige des indicateurs communs. Mais surtout, elle nécessite une application large et cohérente dans l'ensemble de l'entreprise. Les responsables de la cybersécurité doivent travailler en étroite collaboration avec d'autres services pour allouer les ressources adéquates et prendre les bonnes décisions.

En outre, à mesure que les entreprises avancent dans leur parcours du « moi » au « nous », elles devront envisager très différemment la manière dont elles conçoivent l'objectif de la cybersécurité. Plutôt que de considérer la responsabilité de l'équipe de cybersécurité uniquement en termes de protection des ressources, elles doivent élargir leur perspective pour inclure leurs objectifs stratégiques. Cette perspective doit transparaître dans chaque évaluation, chaque rapport du conseil d'administration et chaque communication de l'équipe de sécurité avec l'ensemble de l'entreprise.

Ce n'est qu'à cette condition que les entreprises pourront assurer leur cyberrésilience et parvenir à une croissance durable de leurs activités.

Méthodologie

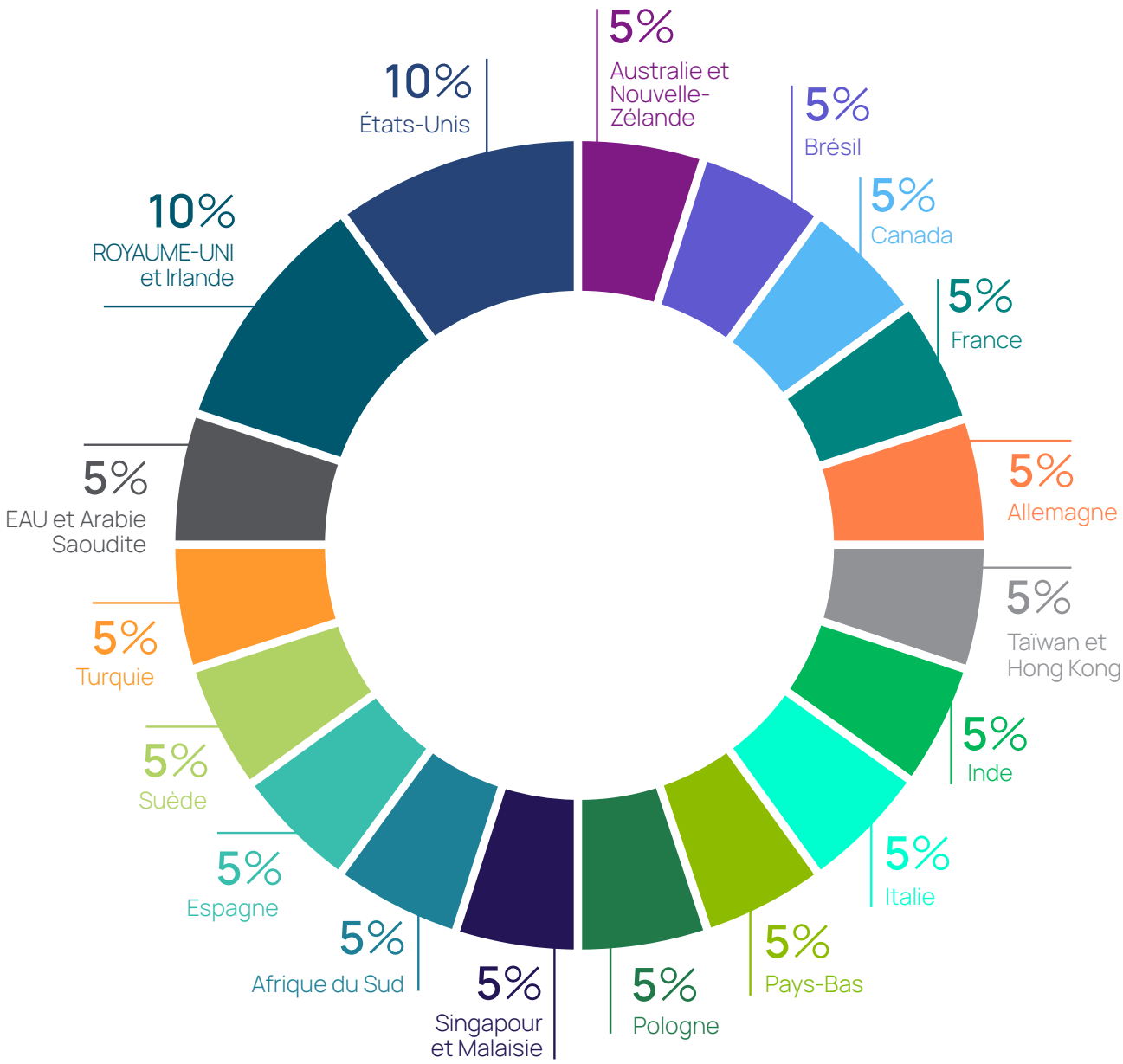
L'enquête a recueilli les réponses de 2 007 personnes au cours du mois de mars 2023.

Elle comprend des réponses provenant de membres de la direction générale et de la direction des services et de managers. Les personnes interrogées sont originaires de 23 pays et travaillent dans des entreprises comptant 500 employés ou plus dans 22 secteurs d'activité.

Tous les participants ont déclaré avoir pris part à la prise de décision en matière de sécurité en tant que décideur ultime, membre d'une équipe ou personne influente.

Les résultats ne sont pas pondérés.

Pays : Dans quel pays vivez-vous ?

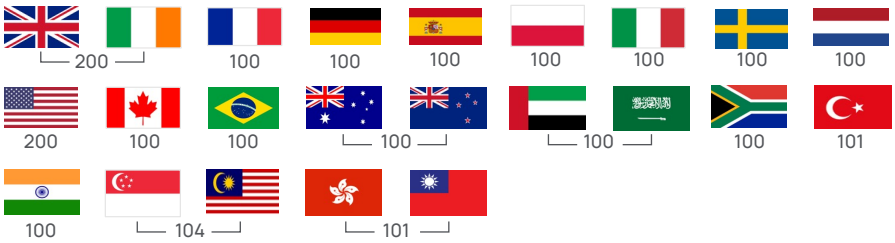


Résumé des données démographiques des sondés

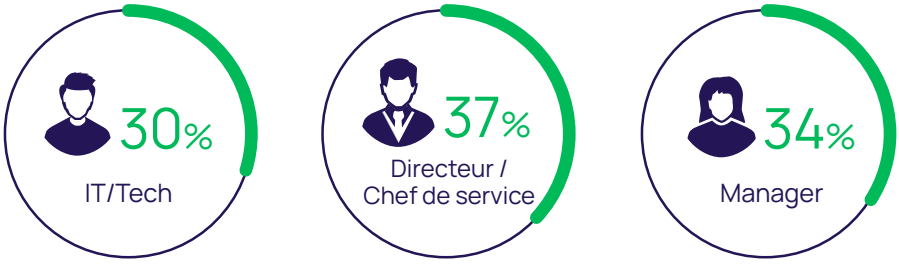
Données démographiques

Total des sondés : **2007**

Pays de résidence



Type de poste



Taille de l'entreprise

Nombre d'employés	500-999	1000-4999	+ de 5 000
% de sondés	35 %	40 %	26 %

Secteur d'activité

Sexe et âge

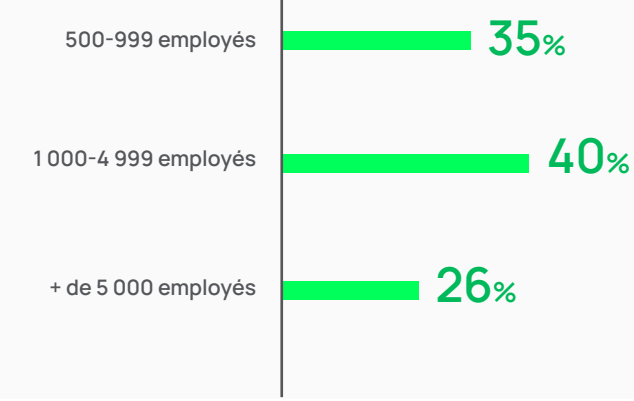
66 % des sondés étaient de sexe masculin et 34 % de sexe féminin

des sondés étaient âgés entre

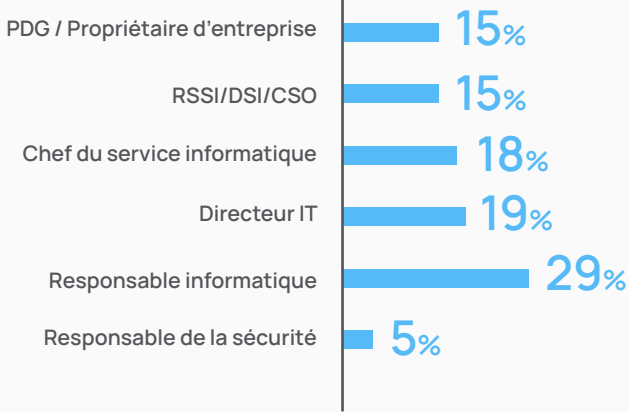
25-44 ans

Taille de l'entreprise et poste : Combien d'employés compte l'entreprise pour laquelle vous travaillez ? Lequel des énoncés suivants décrit le mieux votre poste ?

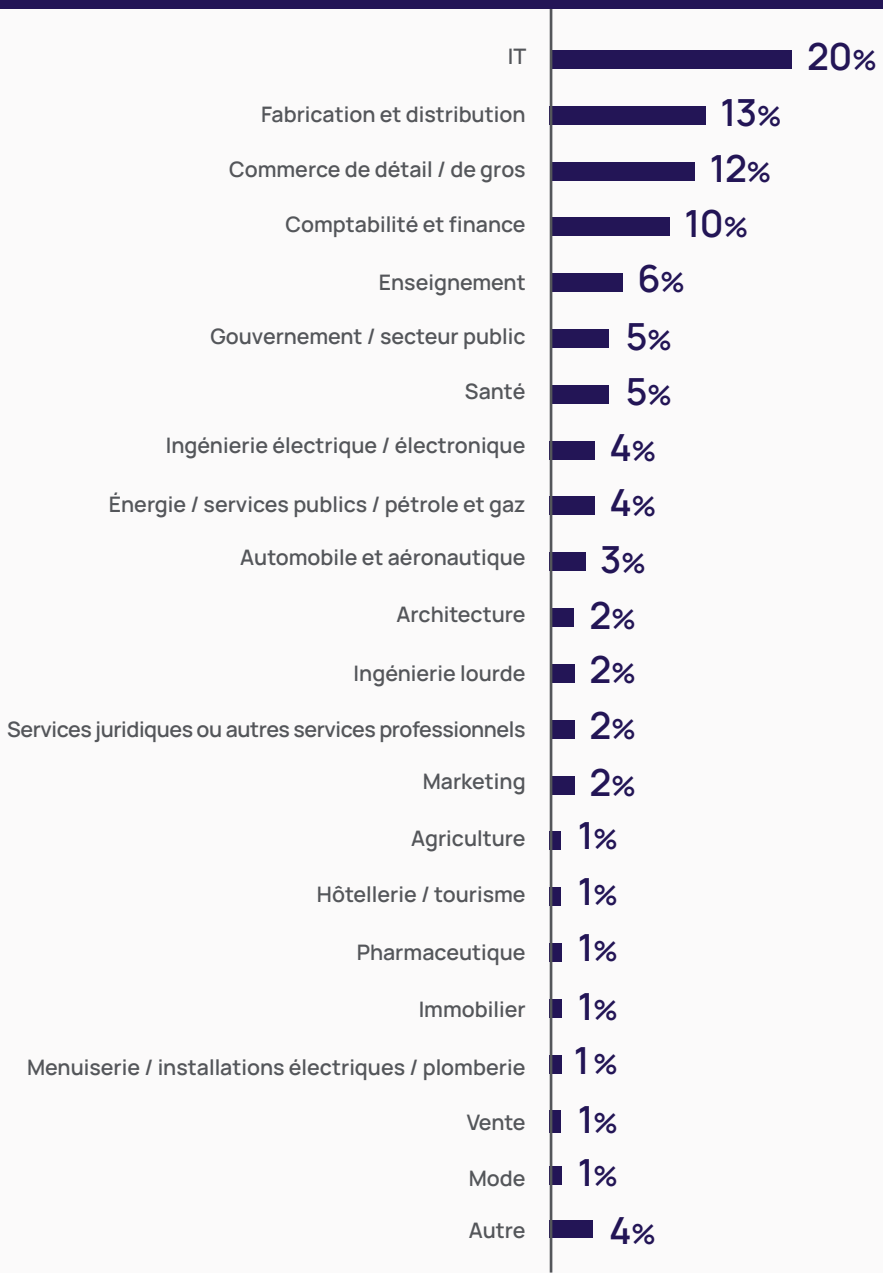
Taille de l'entreprise



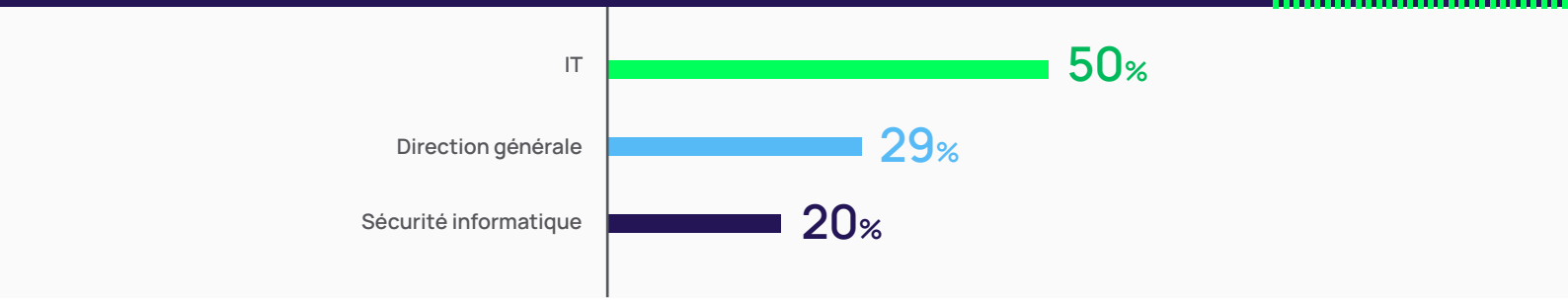
Intitulé du poste



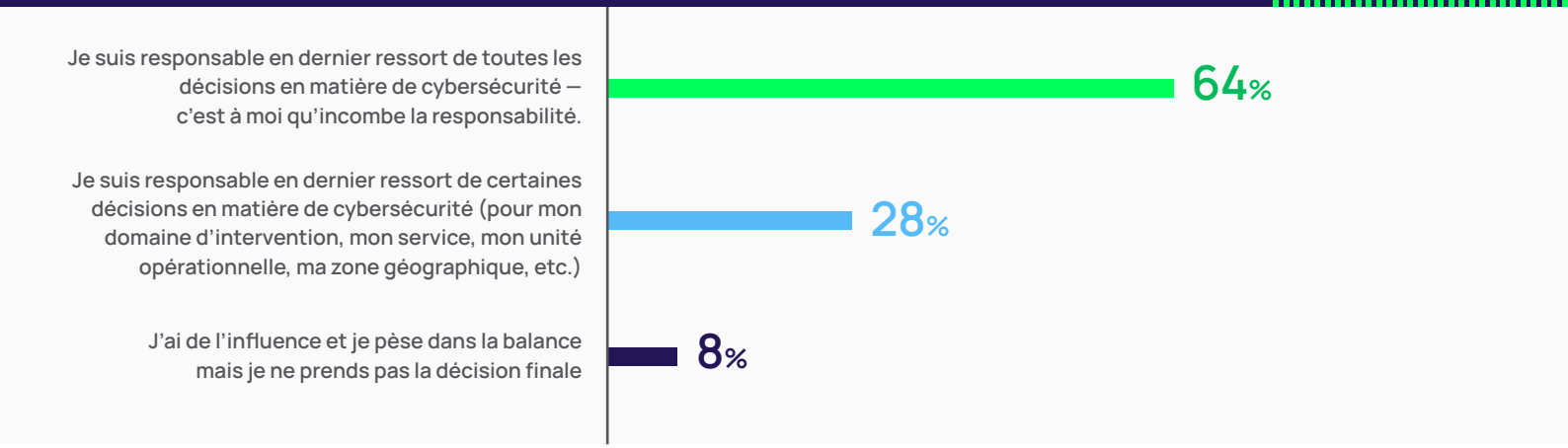
Secteur : Lequel de ces énoncés décrit le mieux votre secteur d'activité ?



Services : Au sein de quel service travaillez-vous ?



Responsabilité : Dans quelle mesure êtes-vous responsable de la prise de décisions en matière de cybersécurité au sein de votre entreprise ?



Delinea

Defining the boundaries of access

Delinea est un fournisseur majeur de solutions de gestion des accès à privilèges (PAM) pour les entreprises modernes et hybrides. Delinea Platform étend de manière intuitive les solutions PAM en fournissant des autorisations pour toutes les identités, en contrôlant l'accès à l'infrastructure cloud hybride la plus critique et aux données sensibles d'une entreprise pour aider à réduire les risques, à garantir la conformité et à simplifier la sécurité. Delinea supprime la complexité et définit les limites de l'accès pour des milliers de clients dans le monde. Nos clients s'étendent des PME aux plus grandes institutions financières au monde, agences de renseignement et sociétés spécialisées dans les infrastructures critiques. **delinea.com/fr/**