# Rapport pour les RSSI

La résilience numérique commence avec votre conseil d'administration.

splunk>
a CISCO company

Les RSSI font l'expérience du risque au quotidien. Nous luttons contre les logiciels malveillants, nous arrêtons les menaces internes et nous faisons respecter les règles de conformité.

Mais il y a un autre risque : être en décalage avec son conseil d'administration. Si nous ne parvenons pas à articuler l'impact potentiel des problèmes de sécurité, il y a toutes les chances pour qu'ils continuent de représenter une menace.

C'est le défi fondamental des RSSI et de leurs conseils d'administration : trouver la bonne façon de raconter la sécurité aux personnes qui peuvent soutenir notre vision. Dans le Rapport pour les RSSI de cette année, nous avons étudié cette relation à la loupe pour découvrir ce que chacun pensait de son autre moitié. L'étude a permis de confirmer une tendance observée ces dernières années : les RSSI interagissent davantage avec leur conseil d'administration.

Il reste toutefois de nombreux domaines où ils ne sont pas en phase : les compétences prioritaires des RSSI, mais aussi la manière dont ils doivent utiliser leur temps et les stratégies efficaces pour convaincre le conseil d'administration d'accorder des budgets supplémentaires.

Pour combler ce fossé, les RSSI devront parler le même langage que leur conseil d'administration. D'après mon expérience, cela veut dire qu'il faut passer beaucoup plus de temps avec les membres du conseil et d'autres décideurs pour mieux comprendre l'entreprise et faire de la sécurité un catalyseur. Les RSSI qui savent associer sécurité et revenus, et qui comprennent les inquiétudes du conseil d'administration pourront démontrer leur implication dans les enjeux et leur capacité à présenter des solutions, et pas seulement des problèmes qu'il appartiendra au conseil de résoudre.

Nous espérons que le Rapport pour les RSSI vous aidera à raconter votre histoire, à combler les manques de communication et à obtenir le soutien du conseil d'administration pour votre programme de sécurité.

Michael Fanning

RSSI, Splunk

# Sommaire

# Le début d’une belle amitié ?

L’eau et l’huile. Vénus et Mars. Quelle que soit la métaphore, une chose est claire : les RSSI et leur conseil d’administration sont fondamentalement différents et leurs parcours peuvent sembler très éloignés.

Les préoccupations financières des dirigeants d’entreprise entrent souvent en conflit avec les investissements vitaux que les RSSI réclament dans la cybersécurité. Les moindres malentendus dans la définition des priorités peuvent entraîner des conflits considérables en aval, et créer des situations totalement imprévues pour les RSSI et leur conseil d’administration.

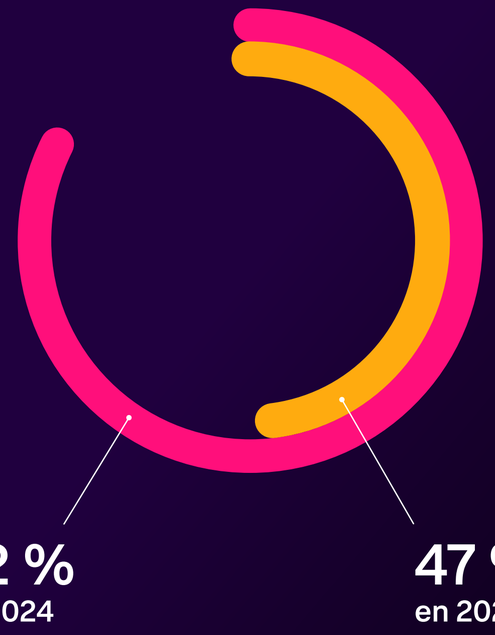
Les RSSI et les conseils d’administration ont plus souvent l’occasion de traiter ensemble des questions de cybersécurité et de risque métier, il n’est donc pas surprenant de voir leur relation se renforcer. Aujourd’hui, la plupart des RSSI (82 %) rendent directement compte au PDG, un chiffre considérable quand on pense qu’ils n’étaient que 47 % en 2023. Tels de nouveaux voisins, les RSSI et leur conseil d’administration apprennent à se connaître et découvrent leurs intérêts communs pour devenir au fil du temps des amis proches.

Malgré leurs différences, ils ont une mission commune : défendre l’entreprise. Le conseil d’administration protège la rentabilité et le cours de l’action ; le RSSI protège les données et les systèmes. C’est un excellent point de départ. Mais il faudra de la communication, de la compréhension et une bonne dose de patience pour parvenir à un résultat.

Pour réussir, chaque partie devra sortir de sa zone de confort et apprendre le langage de l’autre. Les RSSI devront comprendre en profondeur les rouages de l’entreprise et trouver de nouvelles façons de faire comprendre le retour sur investissement des initiatives de sécurité à leur conseil d’administration. Les membres du conseil d’administration, quant à eux, devront s’engager à promouvoir une culture axée sur la sécurité et consulter le RSSI lors de la prise de décisions affectant la gouvernance et les risques métiers.

Lorsque les RSSI et les membres du conseil prennent conscience qu’ils ont une mission commune, ils deviennent de puissants alliés capables de propulser l’entreprise sur la voie de la résilience numérique.

**De plus en plus de RSSI sont directement subordonnés au PDG**



# Les RSSI prennent leur place dans la haute direction

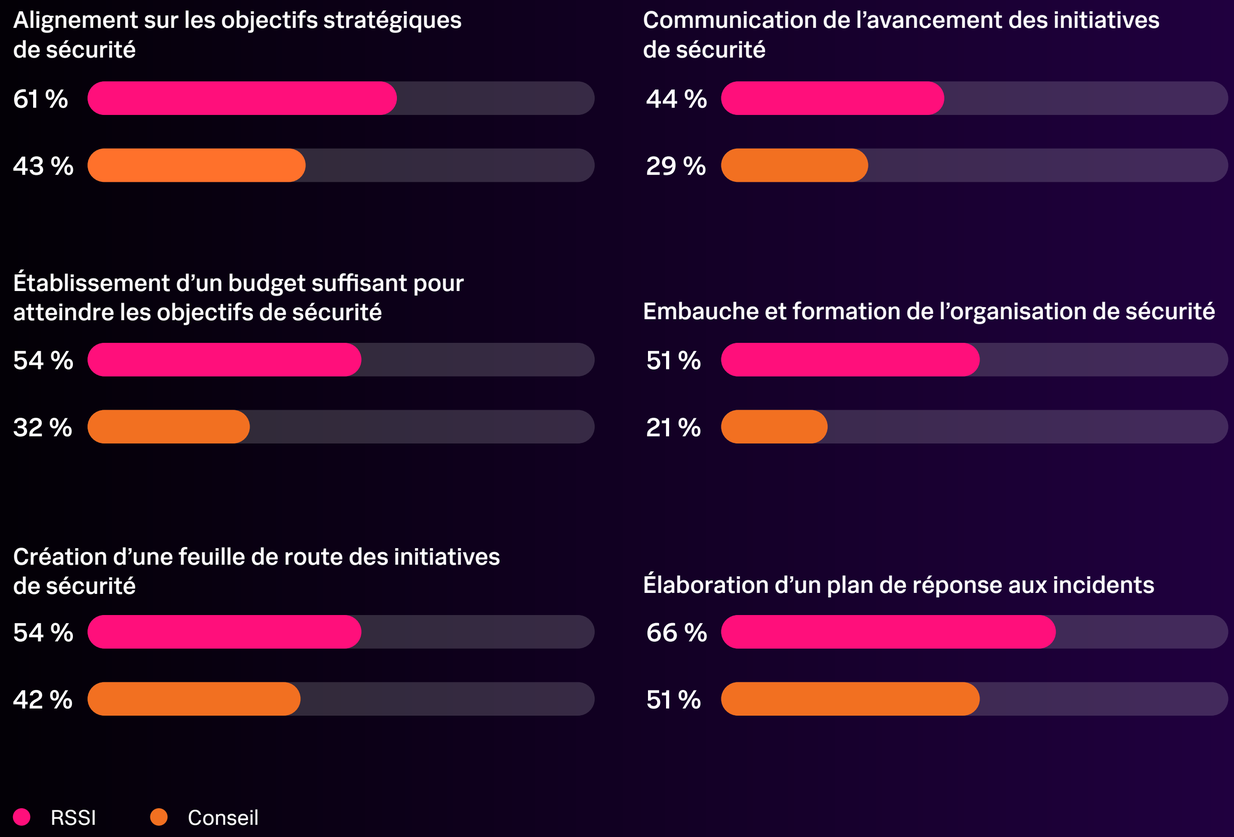
L'ascension des RSSI et, pour la plupart, leur relation directe avec le PDG leur permettent de consolider leur place au sein de la direction et d'avoir leur mot à dire dans les décisions stratégiques de l'organisation. Mais l'acquisition de ce statut ne s'est pas faite sans mal. Comme dans de nombreuses relations, l'un des partenaires a toujours une vision plus positive de la situation que l'autre.

Si l'on évalue la performance des RSSI en général, 84 % des membres de conseil d'administration interrogés affirment que le RSSI répond à leurs attentes. Cela semble positif à première vue. Mais face aux défis complexes auxquels sont confrontés les responsables de la sécurité, les normes d'excellence du conseil d'administration sont-elles des critères suffisants ? On pourrait penser que des RSSI aussi performants inspireraient confiance, mais seuls 8 % des membres du conseil d'administration interrogés considèrent qu'ils dépassent les attentes.

Si nous examinons cette relation en détail, les données de l'étude indiquent que les RSSI pensent qu'ils ont davantage la confiance du conseil en ce qui concerne leurs responsabilités de base. Par rapport aux autres membres du conseil d'administration, les RSSI ont le sentiment d'être sur une base plus solide sur tous les points : embauche et formation de l'organisation de sécurité, définition du budget et alignement sur les objectifs stratégiques de cybersécurité.

## Les RSSI surestiment leurs relations avec le conseil d'administration dans des domaines clés

Participants affirmant que la relation est *très bonne* ou *excellente*



**Les membres des conseils d'administration sont des dirigeants d'entreprise qui savent très bien gérer les résultats métiers et financiers. Mais ils ne comprennent pas concrètement qu'ils dépendent de la technologie et que la façon dont ils la gèrent a des implications en matière de sécurité.**

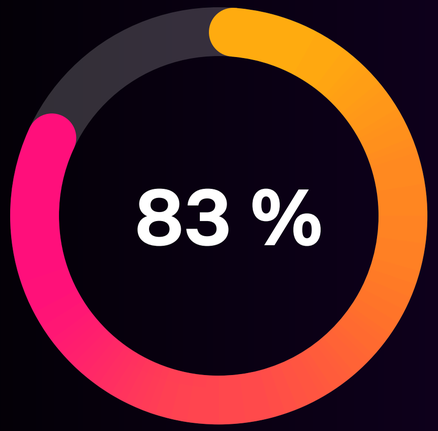
Christopher Kennedy, RSSI, Group 1001

Mais il y a un revers à cette médaille. Les RSSI n'accordent pas un grand crédit aux prouesses du conseil d'administration en matière de cybersécurité. Même si 60 % d'entre eux reconnaissent que les membres du conseil d'administration qui ont une expérience en cybersécurité influencent davantage les décisions dans ce domaine, les conseils d'administration n'ont pas tous un membre d'une telle autorité. Seuls 29 % des RSSI affirment que leur conseil d'administration comprend au moins un membre possédant une expertise en cybersécurité.

Ces relations fondamentales au sein du conseil d'administration sont le germe d'une grande part des divisions qui surviennent par la suite. Un léger déphasage en amont peut devenir considérable dans des domaines critiques en aval, comme la réponse aux incidents et la croissance de l'entreprise.

Mais ces perceptions pourraient évoluer, au moins en partie : 83 % des RSSI participent désormais *assez souvent* ou *la plupart du temps* aux réunions du conseil d'administration. Il est légitime de penser que cette évolution puisse façonner la manière dont les conseils d'administration abordent la politique de cybersécurité et la culture organisationnelle.

Heureusement, les écarts d'aujourd'hui ne sont pas insurmontables. La présence régulière des RSSI au sein du conseil d'administration et leurs conseils avisés en matière de risque métier renforceront la coordination et la confiance du conseil.




**des RSSI participent désormais *assez souvent* ou *la plupart du temps* aux réunions du conseil d'administration**

**Lorsque j'ai commencé en tant que RSSI, l'objectif était d'obtenir une place à la table du conseil d'administration. Les choses ont changé. Il n'y a plus de discussion ni de débat, on ne se demande plus si le RSSI doit directement rendre compte au conseil d'administration.**

Bruce Foreman, RSSI, UMass Memorial Health

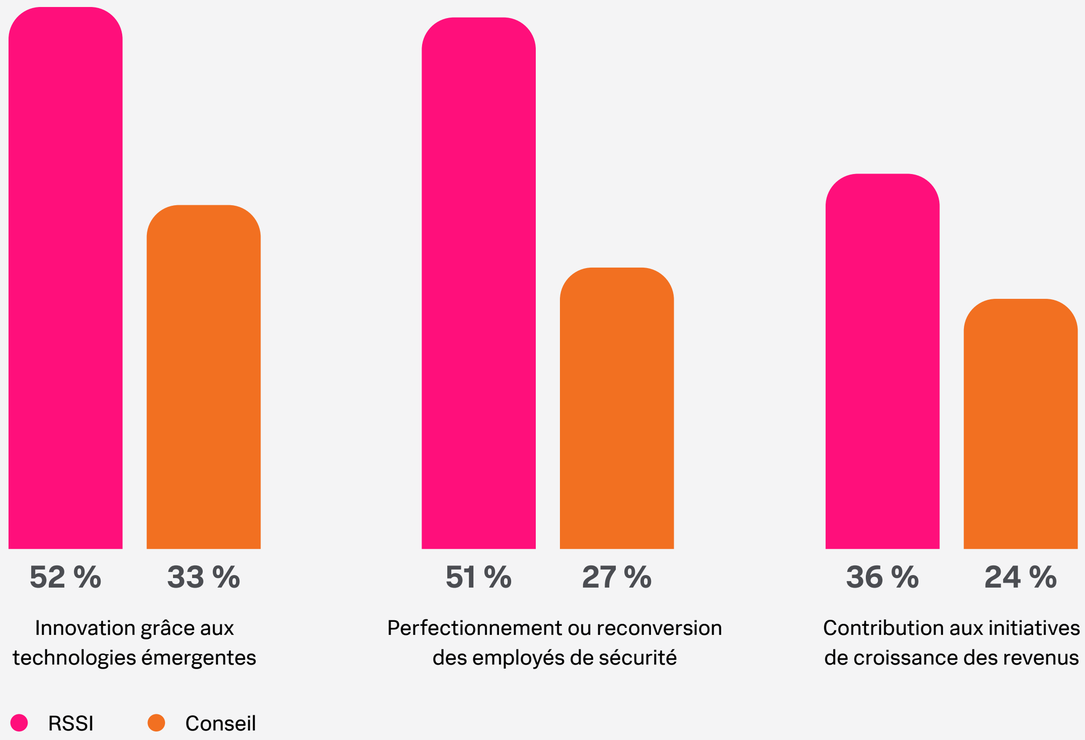
# RSSI et conseils d'administration cherchent la conciliation

Notre étude indique que l'écart qui sépare les deux parties pourrait se réduire sur certaines priorités de sécurité. Par exemple, on observe en effet un fort alignement sur la protection des informations sensibles de l'entreprise : 70 % des membres du conseil et 68 % des RSSI déclarent qu'elle est *très importante* ou *de la plus haute importance*.

Mais il reste de graves écarts. Les priorités du RSSI sont le reflet de son expertise technique, et celle-ci façonne la manière dont il exécute ces priorités et atteint ses objectifs à long et à court terme.

**Les plus grandes divergences de priorités entre les RSSI et les conseils d'administration**

Propositions classées comme *très importantes* ou *de la plus haute importance*



# Le conseil d’administration veut savoir : comment emploie-t-il son temps ?

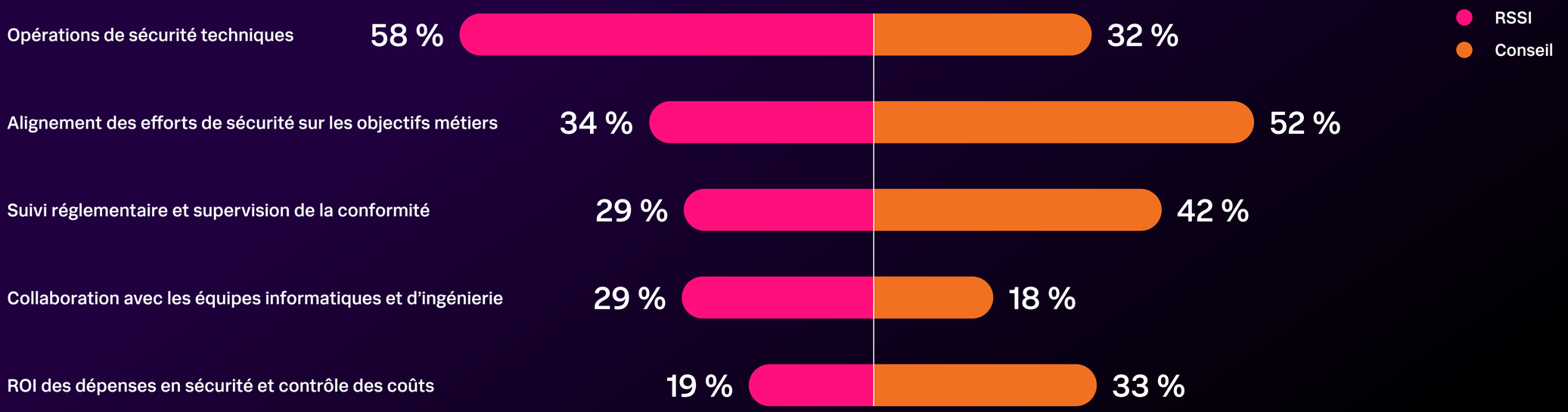
Outre certains désaccords concernant les priorités, les RSSI et les conseils d’administration divergent également sur la manière dont les RSSI et les équipes de sécurité devraient utiliser leur temps et leur énergie pour atteindre leurs objectifs.

Mais que font exactement les RSSI toute la journée ? Si 63 % des RSSI et des conseils d’administration s’accordent sur le fait que les RSSI consacrent la majeure partie de leur temps à renforcer la posture de sécurité et atténuer les risques, les perceptions divergent ensuite. Les membres du conseil estiment à 52 % que les RSSI passent l’essentiel de leur temps à soutenir l’entreprise en alignant les efforts de sécurité sur les objectifs métiers, mais seulement 34 % des RSSI partagent cet avis. En réalité, les aspects techniques de la cybersécurité occupent une part bien plus grande de la journée du RSSI que ce qu’imagine le conseil d’administration. Selon 58 % des RSSI, leur équipe et eux consacrent l’essentiel de leur temps au choix, à l’installation et à l’exploitation des technologies.

> **« Si une entreprise n’est pas familiarisée avec le coût de la cybersécurité, le RSSI doit expliquer l’intégralité des tâches de l’équipe de sécurité au conseil d’administration et la façon dont ces responsabilités s’intègrent à l’ensemble de l’entreprise.**
>
> Christopher Kennedy, RSSI, Group 1001

# Perceptions et réalité

À quoi les RSSI et leurs équipes consacrent-ils la majeure partie de leur temps ?



# Les compétences métiers aident les RSSI à se diversifier

Les conseils d'administration fondent de grands espoirs sur les RSSI, en particulier concernant leurs compétences de dirigeants d'entreprise. Cependant, les RSSI pourraient avoir une autre image de cette ambition ou emprunter d'autres chemins pour y parvenir.

Plus que les RSSI, les membres du conseil d'administration mentionnent le sens des affaires et les compétences transversales telles que l'empathie et la communication comme compétences à développer en priorité. Mais les RSSI s'intéressent davantage à faire progresser la collaboration avec les équipes informatiques et d'ingénierie, et à approfondir leurs connaissances en conformité.

« L'acquisition et l'approfondissement de nouvelles compétences ne font qu'ajouter à la complexité et à la difficulté du travail du RSSI », affirme Marcus LaFerrera, Directeur de l'équipe de recherche en sécurité SURGe.

C'est sans doute ce qui explique que 53 % des RSSI déclarent que leurs responsabilités et les attentes vis-à-vis de leur rôle se sont alourdies depuis leur prise de fonction.

Même si les RSSI font partie des cadres dirigeants, et malgré le désir des autres membres du conseil de les voir développer leurs compétences métiers, ces derniers ne voient toujours pas au-delà de leurs qualifications techniques. Les RSSI ont toutefois le pouvoir de changer cette perception. « À moins que le RSSI n'ait la sagesse et les moyens de défendre une place plus adéquate dans l'ordre hiérarchique, je pense qu'il sera toujours considéré comme le petit génie capable de résoudre tous les problèmes par la technologie, sans que les autres membres ne comprennent concrètement le rôle de la technologie dans l'entreprise », a déclaré Christopher Kennedy, RSSI de Group 1001.

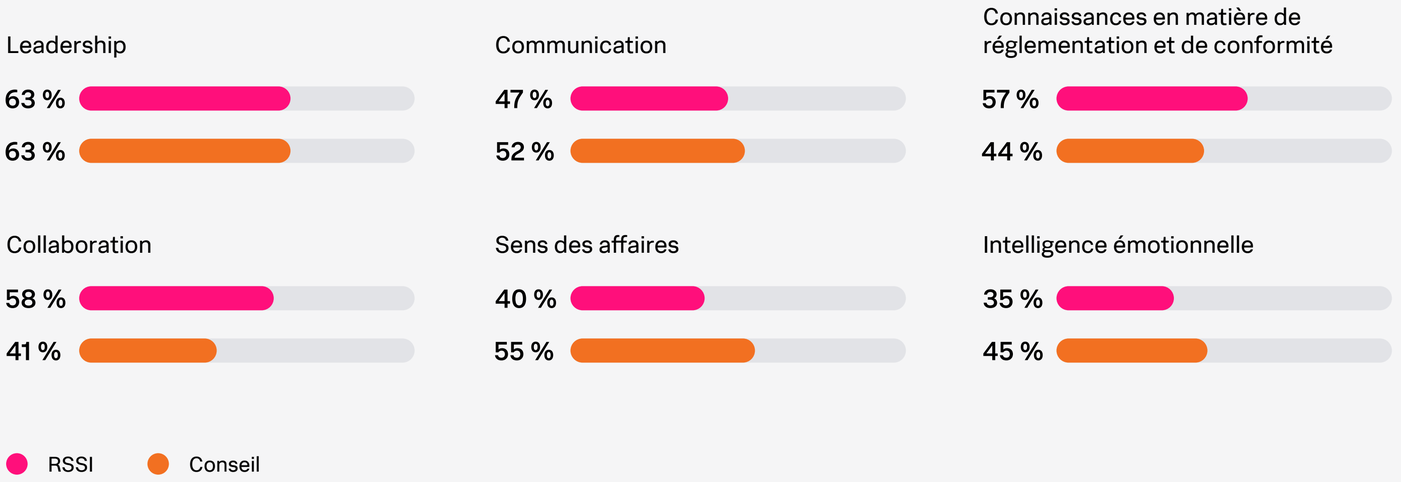
Ce sera au RSSI d'acquérir une connaissance approfondie des priorités de l'entreprise et du conseil d'administration, puis de les relier aux objectifs de revenus et de croissance. Il pourra jeter des ponts en misant sur une communication ascendante, proactive et efficace et sur une compréhension détaillée de la stratégie de l'organisation. Armé de cette vue d'ensemble, il déterminera de quelle manière y intégrer la stratégie de sécurité.

« Le RSSI doit collaborer et s'associer avec d'autres fonctions de l'entreprise. La sécurité ne doit pas être un service isolé. Nous devons travailler avec le service juridique, avec la gestion des risques, avec les décideurs métiers. Le RSSI doit donc savoir communiquer », déclare Chenxi Wang, Associée générale chez Rain Capital et membre du conseil d'administration de MDU Resources.

**53 %**

**des RSSI déclarent que leurs responsabilités et les attentes vis-à-vis de leur rôle se sont alourdies**

## Les compétences à développer en priorité pour les RSSI



# Le RSSI et le conseil d'administration n'ont pas la même vision du succès

En général, les conseils d'administration et les RSSI conviennent de l'importance des principaux KPI de cybersécurité, comme le nombre d'incidents de sécurité matériels et la rapidité de la gestion des vulnérabilités. Mais ils sont aussi très nombreux (79 %) à affirmer que les KPI de leurs équipes de sécurité ont considérablement changé au cours des dernières années.

« L'entreprise évolue. Nous avons pour ambition d'étudier de nouveaux modèles métiers et de nouveaux domaines d'activité, et nous allons être amenés à traiter des informations sur les consommateurs et des données personnelles. Ma position a changé parce que je considère désormais la sécurité comme un risque plus important qu'il y a deux ans », explique Prasanna Ramakrishnan, RSSI monde chez Clarios.

Les conseils d'administration disposent également de normes spécifiques pour évaluer les performances du RSSI, à commencer par la rentabilité des investissements en sécurité. C'est probablement l'une des raisons pour lesquelles les conseils d'administration attendent des RSSI qu'ils adoptent une approche stratégique plutôt que tactique, et qu'ils communiquent de manière plus globale sur l'impact que leurs initiatives exercent sur l'entreprise.

« Nous ne validons pas un investissement de sécurité à moins que le retour sur investissement ne soit d'au moins 15 %. Autrement, ce sera difficile à justifier », affirme un membre du conseil d'administration d'un groupe bancaire multinational basé au Royaume-Uni.

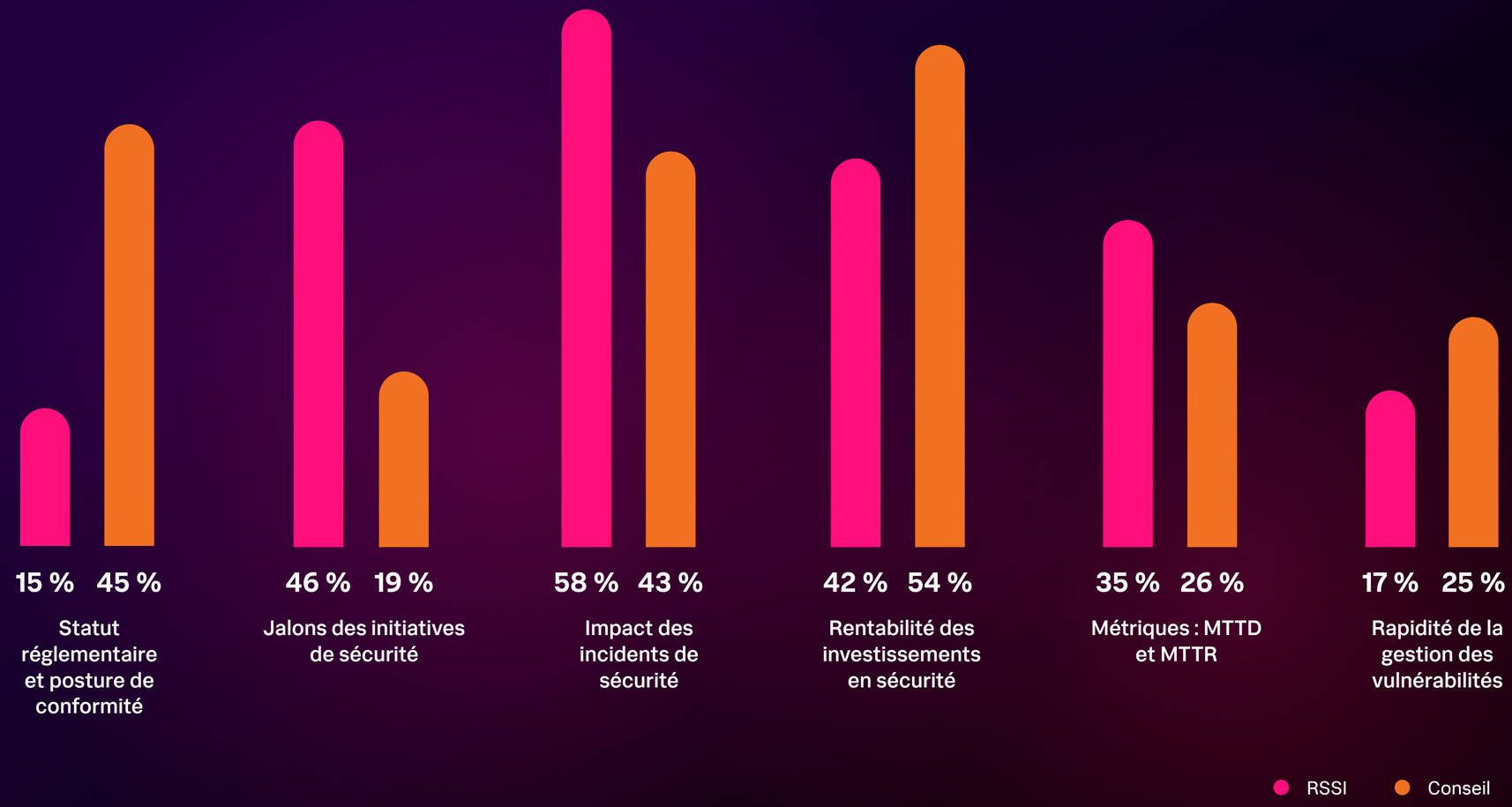
La véritable conclusion ? D'une part, les conseils d'administration n'attendent pas des RSSI qu'ils soient des pompiers héroïques. Au-delà de la prise en charge des incidents qui ne manqueront pas de se produire, ils recherchent un leadership mature, stratégique et proactif, doublé d'une capacité d'intervention opérationnelle. Les RSSI réussiront en apprenant à expliquer au conseil d'administration l'impact positif de leurs KPI de sécurité sur l'entreprise.

Lorsqu'ils présentent des initiatives et des estimations, les RSSI peuvent convaincre leur conseil en rappelant que le coût des pertes de revenus et des dommages à la réputation sera probablement inférieur au coût des temps d'arrêt causés par un incident de sécurité.

**Les RSSI doivent aussi changer de tactique pour se faire entendre ; il faut qu'ils profitent du précieux temps qu'ils passent au conseil d'administration pour justifier la rentabilité de leurs investissements en sécurité et présenter la sécurité comme un catalyseur, et non plus seulement un centre de coûts.**

Kirsty Paine, Directrice technique de terrain et conseillère stratégique, Splunk

# Les RSSI et les conseils d’administration ne mesurent pas la réussite de la même façon

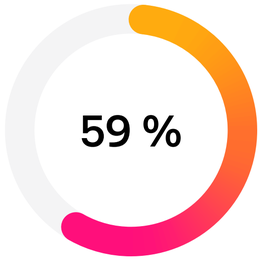


# Les RSSI font de la conformité une affaire personnelle

Les environnements réglementaires sont devenus plus complexes, ramifiés et punitifs. Ils exigent un signalement plus rapide des incidents et font peser davantage de responsabilités sur les épaules des RSSI. Ceux-ci tendent donc à adopter une approche plus rigoureuse et personnelle de la conformité.

## Le dilemme : signaler ou non les défauts de conformité

Il n'est guère surprenant que les RSSI attachent la plus grande importance à la conformité de leur entreprise : beaucoup de choses dépendent de leurs décisions. En effet, c'est le RSSI, et non le conseil d'administration, qui sera tenu pour responsable en cas d'incident de sécurité. Les RSSI sont soumis à une supervision réglementaire intense ; ils sont responsables juridiquement et exposés à de lourdes sanctions financières. Enfin, ils peuvent perdre leur emploi s'ils sont reconnus coupables d'infraction.




**des RSSI n'hésiteraient pas à lancer l'alerte si leur entreprise ne respectait pas ses obligations de conformité**

Plus choquant encore, 21 % des RSSI avouent avoir subi des pressions visant à les empêcher de signaler un problème de conformité. Heureusement, la majorité des RSSI interrogés sont prêts à agir dans le bon sens : 59 % d'entre eux expliquent qu'ils lanceraient l'alerte si leur entreprise ne respectait pas ses exigences de conformité.

« En faisant pression sur les RSSI pour qu'ils ne signalent pas les problèmes, plutôt que de faire preuve de transparence face aux échecs et aux enseignements, on s'interdit de prendre des décisions basées sur le risque et on prive les bonnes personnes d'informations réelles. Cela peut être vraiment dangereux », affirme Kirsty Paine, Directrice technique et conseillère stratégique pour Splunk, une filiale de Cisco.

Bien entendu, lorsqu'un incident est considéré comme « matériel » (et cette définition est vague), les entreprises doivent le signaler aux autorités dans un délai de quelques heures à quelques jours, selon la région où elles sont implantées. Les mandats récents, notamment la décision de la SEC en matière de cybersécurité aux États-Unis, et la directive NIS2 et le règlement DORA en Europe, imposent des fenêtres de signalement beaucoup plus réduites (24 heures seulement pour NIS2) pour la divulgation des incidents de cybersécurité. De même, la loi australienne sur la sécurité des infrastructures critiques (SOCI) exige un signalement dans les 12 heures suivant la découverte d'un incident.

En ce qui concerne le signalement des incidents et les autres protocoles de conformité, les RSSI doivent travailler sur la gestion de crise bien avant qu'un incident ne se produise. Un plan proactif permettra de tenir compte des attentes du conseil d'administration et de définir une réponse pour l'ensemble de l'entreprise.

**« Je pense que tous ceux qui travaillent comme responsable de la sécurité ou qui siègent au conseil d'administration d'une entreprise cotée devraient s'inquiéter de leur responsabilité personnelle en cas de défaillance de leur part.**

Chenxi Wang, Associée générale de Rain Capital et membre du conseil d'administration de MDU Resources

**21 %**

**des RSSI ont subi des pressions visant à les empêcher de signaler un problème de conformité**

# Les RSSI se soumettent aux obligations de conformité… jusqu'à un certain point

Dans l'environnement réglementaire rigoureux actuel, la conformité devient une part importante du travail d'un RSSI. Cela pourrait expliquer pourquoi 57 % des personnes interrogées considèrent « l'approfondissement des connaissances en matière de réglementation et de conformité » comme un axe de développement prioritaire.

Et même si le maintien de la conformité est essentiel pour l'entreprise, les RSSI n'y voient pas nécessairement le meilleur moyen de mesurer leur performance en matière de supervision de la sécurité. Seuls 15 % des RSSI classent l'état de conformité parmi les principaux KPI, contre 45 % des membres du conseil : l'écart est considérable. Traditionnellement, les RSSI ne la perçoivent pas comme une activité de sécurité stratégique.

Cette déconnexion peut indiquer que la conformité ne recouvre pas du tout la même réalité pour les conseils d'administration et les RSSI. « Les membres du conseil savent que la conformité est essentielle, mais ils ont rarement une vision complète du travail que cela implique. En l'absence d'informations quotidiennes, il ne faut pas être surpris que les membres du conseil imaginent que c'est une mission facile ou qu'ils ne comprennent pas pourquoi les RSSI et leurs équipes prennent autant de temps pour atteindre et préserver une posture de conformité robuste », affirme Kirsty Paine.

> **« Que ce soit HIPAA ou un autre règlement, ce sont toujours des cases à cocher. "Vous avez fait ça, vous êtes en conformité." Mais cela ne veut pas dire pour autant que vous êtes en sécurité. C'est un seuil de référence, mais selon moi ce seuil est très bas.**
>
> Bruce Foreman, RSSI, UMass Memorial Health

# Des preuves plus solides pour alimenter le débat budgétaire

Les budgets de cybersécurité traduisent des incohérences et un manque d'alignement qui refroidissent l'enthousiasme des RSSI, frustrent les conseils d'administration et élargissent le fossé qui les sépare.

Seuls 29 % des RSSI déclarent recevoir un budget adapté à leurs initiatives de cybersécurité et à leurs objectifs, alors que 41 % des membres du conseil pensent que les budgets de cybersécurité répondent aux besoins. Les RSSI s'inquiètent à juste titre de l'impact de ce manque de soutien sur la posture de sécurité de leur entreprise, et 64 % d'entre eux craignent de ne pas en faire assez dans le contexte réglementaire et le paysage des menaces d'aujourd'hui.

**Quand on se présente au conseil d'administration pour expliquer que nous sommes exposés à une cybermenace potentielle, l'investissement est difficile à justifier. Je suis régulièrement confronté au même problème : il y a la certitude d'un investissement d'une part, et d'autre part la probabilité d'une menace qui pourrait ne pas se concrétiser.**

Membre du conseil d'administration d'un groupe bancaire multinational basé au Royaume-Uni

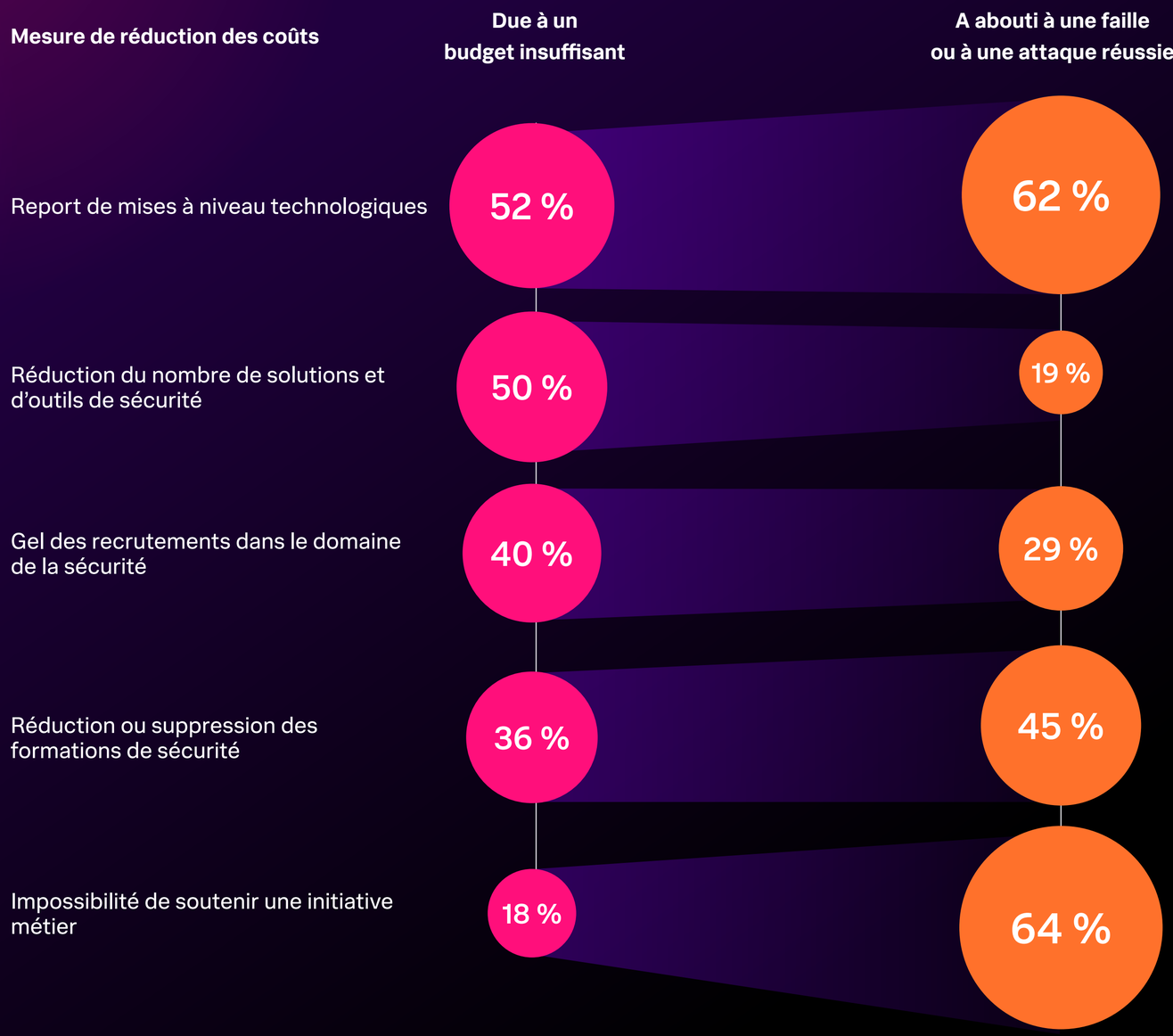
# De petites réductions lourdes de conséquences

De nombreux RSSI ont mis en place des mesures d'économie pour faire face à l'insuffisance des budgets. Parmi les mesures les plus importantes, ils évoquent le report d'une mise à jour de sécurité, la baisse du nombre de solutions pour réduire les coûts de licence, ainsi que le gel des promotions, des augmentations et des embauches. Mais ces coupes dans la sécurité ne passent pas inaperçues : elles ont souvent de graves conséquences, en permettant à des attaques de réussir ou en facilitant les failles de données.

Pendant ce temps, les cyberattaques ne montrent aucun signe de ralentissement. Pas moins de 94 % des RSSI déclarent avoir subi une cyberattaque perturbatrice. La majorité d'entre eux (55 %) disent en avoir fait l'expérience au moins *quelques fois*, et 27 % de plus confient que cela s'est produit *plusieurs fois*.

Il faudra impérativement un financement adéquat pour établir des cyberdéfenses à la hauteur des enjeux. Pour 64 % des RSSI, la gestion des cyber-risques sera le domaine d'investissement le plus important à l'avenir. Mais il faudra aussi investir dans les infrastructures, les outils, les solutions et les services pour aider les RSSI et leurs équipes à protéger les données et les systèmes de leur organisation.

# Les budgets de sécurité insuffisants ont des conséquences



# Les RSSI défendent la sécurité en parlant le langage du conseil d'administration

Mais comment convaincre le conseil d'administration de desserrer les cordons de la bourse ? De nombreux dirigeants privilégient la croissance de l'entreprise (44 %) face au renforcement du programme de cybersécurité (24 %). Ils sont donc plus enclins à soutenir les initiatives de cybersécurité qui génèrent le plus de valeur pour les actionnaires et l'entreprise. Présenter la sécurité comme un catalyseur métier est de loin l'argument le plus puissant, comme en témoignent 64 % des membres du conseil. Mais les RSSI ne sont que 43 % à avoir recours à cette pratique.

Pour obtenir ce qu'ils veulent, ils doivent apprendre à présenter leurs besoins d'une manière convaincante pour le conseil d'administration. En bref, ils doivent apprendre à parler sa langue.

Pour obtenir l'attention de leur conseil d'administration et obtenir les budgets dont ils ont besoin, les RSSI ont tout intérêt à présenter des chiffres concrets sur les coûts directs et secondaires des temps d'arrêt, en incluant la perte de revenus, les pénalités liées aux SLA et les facteurs qui auront un impact sur les actionnaires. Les temps d'arrêt coûtent 400 milliards de dollars par an aux entreprises du Global 2000 : cela fait une moyenne de 200 millions de dollars par entreprise, soit environ 9 % des bénéfices.

Pour 46 % des membres des conseils d'administration, ces types de coûts représentent un argument convaincant dans les discussions budgétaires. 39 % des RSSI misent déjà sur ces approches, mais ils disposent encore d'une grande marge pour affûter leur pouvoir de persuasion. Ils peuvent notamment présenter des mesures de cyber-risque et des recommandations pour orienter les décisions de gestion, et informer le conseil d'administration sur l'impact des cyberattaques.

L'argent reste le nerf de la guerre. Correctement employé, il peut empêcher des failles coûteuses et des infractions réglementaires, et ainsi sauver la réputation de votre entreprise et lui faire économiser des millions de dollars. La stratégie de communication gagnante consiste à expliquer comment la sécurité génère un retour sur investissement, aide l'entreprise à se développer et protège le cours des actions. Avec un tel discours, vous susciterez toujours l'intérêt de votre conseil d'administration.

CHAPITRE 5

# L’IA renforce les défenseurs autant que leurs adversaires

Pour les RSSI comme pour les conseils d’administration, l’IA est à la fois source d’incertitudes et de promesses. Ils s’accordent sur le fait que cette technologie mérite des investissements, aujourd’hui et demain. Pourtant, les RSSI restent nombreux à penser qu’ils n’évoluent pas assez vite pour rester compétitifs et suivre le rythme de l’innovation.

Dans le domaine de la sécurité, l’IA peut être un puissant levier pour l’analyse des logiciels malveillants, la détection des menaces, l’application des normes de configuration et d’autres fonctions, mais il faut pour cela que les RSSI aident leur conseil d’administration à en comprendre les possibilités et le motivent à investir davantage dans l’infrastructure, la formation et la gouvernance.

# L’IA avantage les pirates

L’IA représente toujours une menace dans le monde cyber : 53 % des RSSI estiment en effet qu’elle donnera un avantage (léger ou significatif) à leurs adversaires. Notons toutefois que ce groupe est en net recul par rapport à 2023, où ils étaient 70 %.

Les menaces IA qui suscitent le plus d’inquiétude sont les attaques de phishing, toujours plus réalistes, et les deepfakes (57 %), suivies des nouvelles souches de malwares (44 %), des attaques d’ingénierie sociale adaptative (40 %) et de l’exploitation de solutions d’IA générative existantes (40 %). Et ces inquiétudes sont loin d’être infondées, notamment lorsqu’on parle des deepfakes. L’ingénierie sociale est déjà le vecteur d’attaque le plus couramment employé au cours de l’année écoulée, avec une prévalence de 67 %. Il est fort probable que ce type d’attaque poursuive son développement grâce à l’IA qui imite le comportement et le discours humains de façon toujours plus convaincante.

## Les menaces les plus inquiétantes de l’IA générative pour les RSSI

- **57 %** Réalisme extrême des e-mails de phishing
- **44 %** Apparition d’un nouveau malware capable d’échapper à la cybersécurité
- **40 %** Tactiques d’ingénierie sociale adaptatives
- **40 %** Exploitation des outils d’IA générative utilisés par l’entreprise
- **38 %** Automatisation et hausse de l’efficacité des attaques
- **33 %** Accélération des attaques par force brute
- **30 %** Deepfakes audio et vidéo réalistes

# Les possibilités infinies de l'IA

Malgré leurs inquiétudes concernant l'usage que des acteurs malveillants peuvent faire de l'IA, la majorité des RSSI reconnaissent ses promesses. Pour eux, l'engouement médiatique autour de l'IA est *proportionné* (70 %), voire *trop modeste* (21 %).

Bien souvent, les RSSI et leurs équipes sont tellement occupés à jouer au chat et à la souris avec leurs adversaires que rêver d'investissements futurs devient presque un luxe. Le hasard a voulu que l'essor de l'IA comme outil de cyberdéfense leur permette de se tourner davantage vers l'avenir.

Pour 22 % des RSSI, l'IA donnera aux cyberdéfenseurs un léger avantage sur leurs adversaires. Ils sont également une majorité (53 %) à estimer qu'ils adoptent l'IA au bon rythme, même si plus d'un tiers (38 %) pensent qu'ils n'avancent pas assez vite. Les autres dirigeants affirment, eux aussi, que leur entreprise utilise actuellement l'IA pour la cybersécurité (24 %), a déjà fait des projets pour l'utiliser l'année prochaine (41 %) ou s'intéresse à ce type d'initiative (33 %).

De nombreux RSSI posent les bases de nouvelles cyberdéfenses reposant sur l'IA. Près des deux tiers (65 %) d'entre eux forment activement les équipes de sécurité à l'ingénierie de prompt. En outre, ils sont une majorité (56 %) à établir des protocoles pour déterminer quelles tâches peuvent être confiées à l'IA et lesquelles sont mieux adaptées aux humains.

Si l'on considère tout l'éventail des scénarios d'utilisation à venir, l'IA sera un domaine d'investissement essentiel pour les RSSI et leur conseil d'administration. Les RSSI auront ainsi de nombreuses occasions de mettre en avant le ROI de cet outil en tant que catalyseur métier. C'est en démontrant l'impact positif de l'IA sur la compétitivité et les délais de mise sur le marché qu'ils obtiendront l'adhésion du conseil d'administration. Ils pourraient même voir leurs budgets augmenter.

## Principales applications de l'IA générative pour la sécurité selon les RSSI

**47 %**
Analyse des logiciels malveillants, détection des menaces et enrichissement des alertes

**39 %**
Création de normes de configuration logicielle sécurisées

**32 %**
Création de règles de détection des menaces

**30 %**
Analyse des sources de données pour réduire le bruit des alertes

**30 %**
Recherche proactive des menaces

**28 %**
Création de rapports de sécurité pour la communication interne

**25 %**
Élaboration de politiques de cybersécurité

# L’alignement du RSSI et du conseil, une synergie puissante

À l’heure où la cybersécurité trouve systématiquement sa place dans les décisions d’entreprise, il devient très utile que le conseil d’administration compte au moins un membre avec une expertise en matière de sécurité. Pour des questions de proximité, la présence du RSSI ou d’un expert en cybersécurité au sein du conseil d’administration peut renforcer la relation entre le RSSI et le reste du conseil. Du fait de leurs connaissances approfondies en sécurité, les dirigeants avec une expérience de RSSI peuvent avoir davantage confiance dans la posture de sécurité de l’organisation. Ils s’inquiètent beaucoup moins que les autres membres du conseil que l’entreprise n’en fasse pas assez pour se protéger (37 % contre 62 % en moyenne selon l’étude).

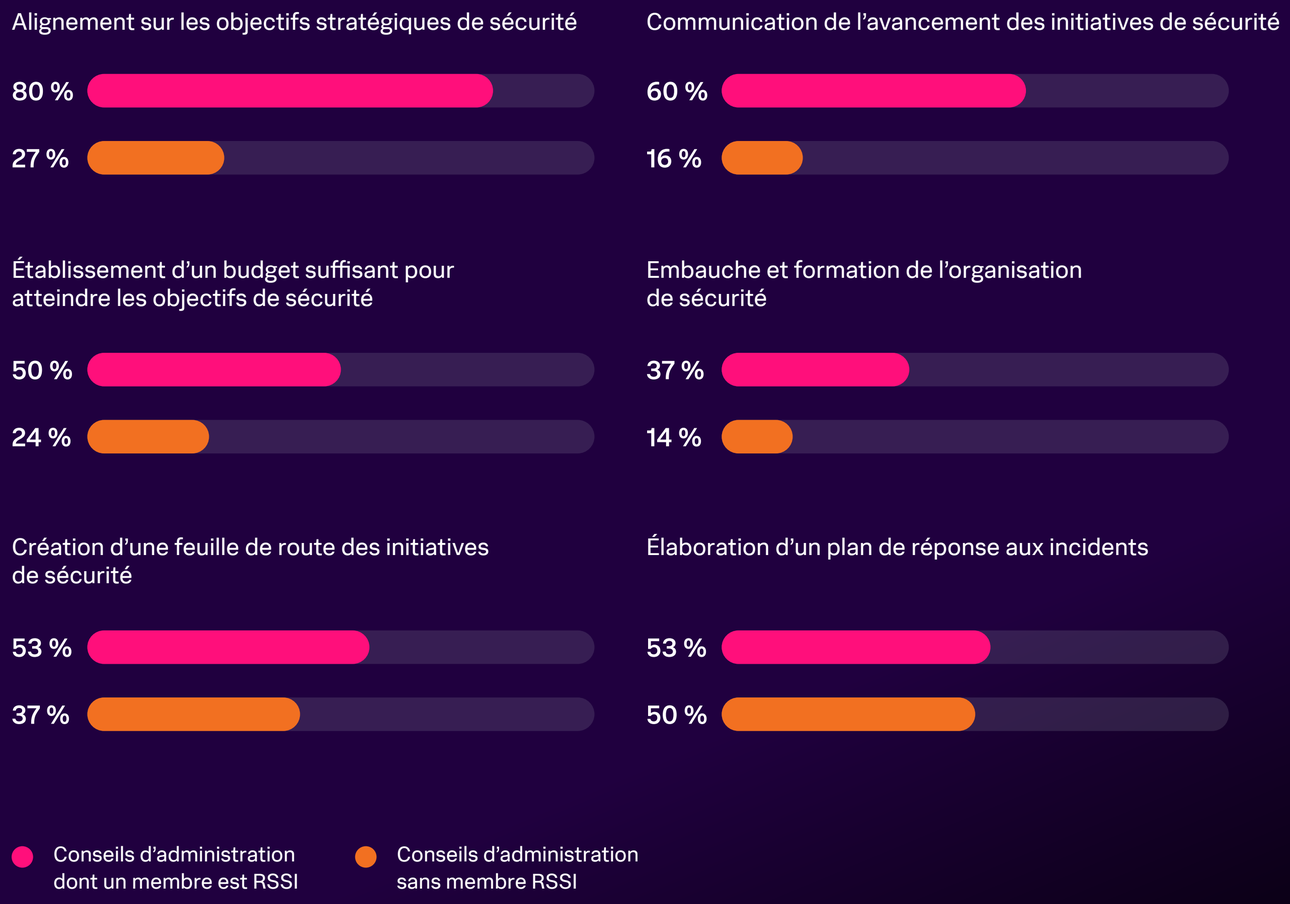
Avoir un pied dans chaque monde leur permet de dresser un tableau précis de la posture de sécurité de l’entreprise, de mieux justifier les investissements futurs et de démontrer comment la cybersécurité fait avancer l’entreprise.

Mais il ne suffit pas d’intégrer un RSSI au conseil pour résoudre tous les problèmes de sécurité. Bien sûr, une entreprise qui prend la sécurité au sérieux comptera un RSSI ou un expert en sécurité au sein de son conseil d’administration, et cela témoigne de son engagement envers la culture de la sécurité et de sa volonté d’adopter des initiatives dans le domaine.

Mais qu’ils siègent ou non au conseil, les RSSI qui entretiennent de bonnes relations avec les autres dirigeants parviendront à faire beaucoup plus.

**La présence d’un membre possédant une expérience de RSSI au sein du conseil est un avantage pour les relations**

Domaines dans lesquels les relations ont été qualifiées de *très bonnes* ou d’*excellentes*



# La communication favorise la collaboration… et les budgets

Des interactions régulières entre le RSSI et le conseil ne sont pas seulement bénéfiques pour l'harmonie des relations, aussi fructueuses soient-elle. Les RSSI qui entretiennent des relations saines avec leur conseil d'administration peuvent compter sur une meilleure collaboration avec toute l'organisation. Ils font état de partenariats particulièrement solides avec les opérations informatiques (82 % contre 69 % des autres RSSI) et l'ingénierie (74 % contre 63 %). Cela peut être dû au fait qu'ils communiquent efficacement les besoins et les stratégies métiers du conseil d'administration à des départements plus techniques, en faisant le lien avec le reste de l'entreprise.

Les RSSI entretenant des relations harmonieuses avec le conseil d'administration jouissent également d'une plus grande liberté pour tester et tenter de nouveaux investissements technologiques. Ils ont plus souvent la possibilité d'étudier des applications de l'IA générative, notamment pour créer des règles de détection des menaces (43 % contre 31 % des autres RSSI), analyser des sources de données (45 % contre 28 %), répondre aux incidents et investiguer (42 % contre 29 %), et rechercher proactivement les menaces (46 % contre 28 %).

Les RSSI sont des agents de liaison essentiels, capables de traduire le langage des départements technologiques et de défendre la sécurité dans des termes intelligibles par le conseil d'administration, et inversement. À l'avenir, les occasions de développer et de renforcer ces relations seront même amenées à se multiplier. Les conseils d'administration ont montré qu'ils étaient prêts à apprendre, tout simplement parce que c'est utile à leur stratégie métier, à leurs pratiques et à leurs investissements. Autrement dit, les RSSI peuvent contribuer à façonner l'entreprise par le biais de la cybersécurité.

CHAPITRE 7

# Tendez la main au conseil d'administration

Le voyage se poursuit pour les RSSI et les conseils d'administration. Ils ont réalisé de grands progrès pour s'accorder sur les objectifs, les priorités et les stratégies métiers. Mais il y a de nombreuses occasions de combler l'écart.

En prenant quelques mesures essentielles, les RSSI peuvent favoriser cet alignement et cultiver des relations plus solides, plus saines et plus productives au sein du conseil d'administration.

1

## Expliquez ce que vous faites (et pourquoi) à votre conseil d'administration

Il est toujours possible pour les conseils d'administration d'affiner leur expertise en matière de sécurité. Les discussions autour de la stratégie de réponse aux incidents constituent une excellente opportunité : non seulement elles leur donneront un aperçu des procédures standards en vigueur, mais elles mettront également en lumière la valeur de ces procédures face aux auditeurs ou pendant une crise.

N'hésitez pas à proposer des simulations pour donner corps aux concepts. Utilisez des éléments visuels et narratifs pour faire passer votre message. Développez ensuite une stratégie et un rythme de suivi, puis ponctuez la mise en œuvre de votre plan de sessions itératives.

2

## Inspirez confiance (et obtenez des budgets)

Vous avez tout intérêt à parler le langage du conseil. Votre expertise en cybersécurité est bénéfique pour le conseil d'administration, mais c'est à vous de lui faire comprendre vos besoins et vos priorités. Mettez l'accent sur le ROI plutôt que sur le MTTD et apprenez à communiquer efficacement la valeur de vos investissements et l'importance d'une répartition efficace des ressources. (C'est peut-être plus difficile, mais la sécurité n'a jamais été un métier facile.)

Pensez également à approfondir des sujets comme la protection des revenus et de la valeur pour les actionnaires et l'atténuation des perturbations métiers. Votre objectif est de renforcer la confiance dans la marque et de fournir des expériences clients sécurisées et fluides. Le conseil d'administration se soucie de la croissance de l'entreprise ? Utilisez ses propres KPI.

3

## Assumez pleinement la question de la conformité et connaissez l'étendue de votre responsabilité personnelle.

Les RSSI sont confrontés à un environnement réglementaire plus rigoureux et punitif que jamais, et ils doivent y être préparés. Vous devez connaître votre responsabilité personnelle, faire éventuellement appel à un avocat en cas d'incident et adopter une approche stratégique et bien documentée. Présentez les risques au conseil d'administration et expliquez pourquoi les événements importants doivent impérativement être signalés.

Vous devez également savoir ce que le conseil attend de vous en cas de crise, formaliser ces attentes par écrit et veiller à ce que toutes les parties soient d'accord avant qu'un incident ne se produise. Relisez votre contrat de travail ; si vous voyez des lacunes, comblez-les.

4

## Élargissez votre périmètre d'action pour inclure la stratégie métier

Nous savons qu'il n'est pas facile de sortir de sa zone de confort. Mais en assumant le rôle de stratège d'entreprise, vous apprendrez à équilibrer les besoins métiers et la protection de l'entreprise. En effet, si vous voulez renforcer la sécurité, vous devez montrer comment la sécurité renforce l'entreprise.

Il ne s'agit pas seulement d'acquérir une perspective métier, même si vous en aurez grandement besoin. Développez vos compétences transversales. Perfectionnez votre communication pour être plus efficace et déterminez comment votre conseil d'administration préfère recevoir les informations. Miser sur l'intelligence émotionnelle peut aussi considérablement améliorer la situation.

5

## Développez votre leadership à l'échelle de l'entreprise, sans vous restreindre au domaine de la sécurité

Les RSSI et les membres du conseil d'administration s'accordent sur l'importance des compétences en leadership. Le but est d'adopter une approche de gestion reposant sur la compréhension des priorités et des motivations du conseil. Cela implique également une communication efficace avec les RH, le service juridique et les dirigeants, car tous jouent un rôle essentiel quand il faut faire avancer vos priorités et obtenir des investissements technologiques plus importants.

Pour établir des relations solides, identifiez les acteurs clés, passez du temps avec eux et témoignez un réel intérêt pour leur travail et leurs défis. Participez aux grandes initiatives : de cette manière, si une crise survient, vos collègues vous verront déjà comme un membre de l'équipe et seront motivés à soutenir vos efforts.

# Devenez un leader de la sécurité avec Splunk


**Les Résilients :**
**le podcast des super-héros du numérique**

Notre podcast met en scène des super-héros du numérique qui œuvrent au quotidien pour protéger leurs organisations. Qu'ils soient RSSI, DSI ou CTO, leur valeur commune est la résilience d'entreprise.

Écouter le podcast


**État de la cybersécurité en 2024 :**
**la course à l'exploitation de l'IA**

Découvrez comment les dirigeants et les professionnels de la sécurité gèrent les opportunités et les défis que représentent les mandats de conformité, la pénurie de talents et l'essor de l'IA générative.

Lire le rapport

# Annexe – Résultats par secteur d'activité

## Fabrication

Par rapport à leurs homologues d'autres industries, les RSSI du secteur manufacturier se sentent moins soutenus par leur direction et expriment globalement moins d'optimisme quant aux possibilités de collaboration et aux budgets de cybersécurité. Ce manque de soutien pourrait expliquer pourquoi le secteur manufacturier subit davantage de cyberattaques que les autres.

Les RSSI sont moins nombreux à affirmer que leur direction soutient la stratégie de l'équipe de cybersécurité et défend ses politiques (41 % contre 57 % en moyenne tous secteurs confondus). Ils ont moins souvent le sentiment que leurs collègues que les KPI de leur équipe sont importants pour leur conseil d'administration (52 % contre 64 % en moyenne).

Interrogés sur le financement de la cybersécurité, seuls 20 % des participants du secteur manufacturier déclarent que leur entreprise prévoit des budgets de cybersécurité adéquats, et ils ne sont que 50 % à penser pouvoir convaincre leur conseil d'augmenter les budgets de leurs équipes en cas de besoin. Les dépenses du secteur manufacturier sont inférieures à la moyenne mondiale, avec 65 millions de dollars de dépenses annuelles prévues contre 75 millions de dollars en moyenne.

Avec un soutien limité et un faible intérêt stratégique pour la cybersécurité, les entreprises du secteur de la fabrication peuvent être de plus en plus vulnérables au vol d'identifiants (signalé par 58 % des RSSI du secteur) ; de plus, l'absence fréquente de processus formalisé de réponse aux incidents (44 %) a facilité la réussite des attaques. 95 % des entreprises du secteur déclarent avoir été touchées par des cyberattaques à plusieurs reprises au cours des 12 derniers mois (contre 82 % en moyenne tous secteurs confondus). Malgré ces attaques, seulement 9 % des conseils d'administration de l'industrie mentionnent le renforcement du programme de cybersécurité comme le prochain investissement prioritaire.

Il est possible qu'ils s'inquiètent davantage du paysage géopolitique. En effet, ils sont 36 % (contre 25 % en moyenne) à percevoir l'instabilité géopolitique comme le plus grand risque pour leur entreprise. Cela s'explique sans doute par le fait que la fabrication est distribuée à l'échelle mondiale et affectée par les perturbations de la chaîne d'approvisionnement.

Pour mieux s'entendre avec leur conseil d'administration, les RSSI du secteur manufacturier peuvent miser sur la conformité réglementaire. Pour 64 % des membres du conseil, la conformité est l'un des principaux indicateurs de réussite des RSSI, mais ceux-ci sont 26 % seulement à dire que leur équipe consacre beaucoup de temps et d'efforts aux questions juridiques et réglementaires.

## Services financiers

Dans le secteur des services financiers, les RSSI ont tendance à entretenir des relations plus harmonieuses avec leur conseil d'administration que dans les autres industries. Ils comprennent qu'on mesure leur réussite à la rentabilité des investissements en sécurité : 60 % en conviennent. Et cette métrique est essentielle pour 64 % des membres de conseils d'administration.

Mais ce secteur a ses propres défis. Les institutions financières sont des cibles privilégiées pour les attaques de ransomware : 65 % d'entre elles en ont subi au moins une au cours de l'année écoulée, contre 48 % en moyenne, tous secteurs confondus. Les pirates qui utilisent les ransomwares ont des objectifs très lucratifs, et les conseils d'administration du secteur financier font du renforcement de leurs cyberdéfenses une priorité. Les membres de ces conseils mentionnent en effet à 55 % la cybersécurité comme priorité d'investissement, contre 24 % en moyenne, tous secteurs confondus. Les écarts les plus importants concernent la sécurité des tierces parties et de la chaîne d'approvisionnement (68 %) et l'infrastructure cloud (56 %).

Les RSSI ont souvent leur place à la table des discussions, puisque 42 % d'entre eux participent la plupart du temps aux réunions du conseil d'administration (contre 20 % en moyenne). Et lorsqu'ils collaborent à l'élaboration du budget de cybersécurité, le conseil fait plus souvent une évaluation positive de cet aspect de leur relation de travail. Leurs membres sont 73 % à penser que le partenariat entre le conseil et le RSSI est efficace, contre seulement 32 % en moyenne, tous secteurs confondus. La vitalité de ce partenariat pourrait expliquer en partie les investissements plus importants consentis dans la cybersécurité. Les institutions financières dépensent en moyenne 105 millions de dollars par an dans ce domaine, un chiffre bien supérieur à la moyenne globale de 75 millions de dollars.

Et ce n'est pas le seul domaine dans lequel les services financiers sont en tête : ils sont aussi des pionniers de l'IA générative. Les participants du secteur des services financiers étaient plus nombreux à penser que les équipes de cyberdéfense pourraient prendre l'avantage sur leurs adversaires en utilisant cette nouvelle technologie (44 %, contre 25 % de l'ensemble des participants). Cet optimisme se traduit par une adoption plus rapide de l'IA générative : 46 % des conseils d'administration des services financiers affirment que leur équipe de cybersécurité l'utilise, alors que la moyenne tous secteurs confondus ne dépasse pas 24 %.

## Communication et médias

La relation entre le RSSI et le conseil d'administration est complexe dans le secteur des communications et des médias. Malgré des contacts directs, les RSSI ne participent que rarement aux réunions du conseil d'administration. Et même si les équipes de cybersécurité semblent bénéficier d'un financement adapté, de nombreuses entreprises du secteur n'ont pas investi dans des mesures de cybersécurité suffisantes pour empêcher les attaques de réussir.

Si la plupart des RSSI du secteur des communications et des médias répondent aux attentes de leur conseil d'administration, ils sont tout de même 9 % à afficher des « performances très insuffisantes », un chiffre plus inquiétant encore si on le compare à la moyenne globale de 1 %. Cela peut être dû au fait que les RSSI du secteur des communications et des médias sont moins susceptibles d'aligner les priorités de leur équipe sur celles du conseil d'administration (ils sont 51 % à le faire, alors que la moyenne tous secteurs confondus est à 62 %).

Les RSSI ont également du mal à communiquer à leur conseil l'avancement de leurs objectifs de sécurité. 35 % des RSSI qualifient de très bon ou d'excellent ce domaine de leurs relations de travail, mais cet avis n'est partagé que par 27 % des membres du conseil. Ce décalage pourrait être corrigé en donnant plus de temps aux RSSI lors des réunions du conseil d'administration : cela leur permettrait de présenter les initiatives de cybersécurité avec une plus grande transparence et de veiller à ce qu'elles s'alignent sur les priorités du conseil. Si 78 % des RSSI ont « au moins quelques contacts directs » avec leur conseil d'administration, ils ne sont que 7 % dans le secteur de la communication et des médias à participer la plupart du temps ou systématiquement aux réunions.

Malgré les difficultés de leurs relations avec les RSSI, les conseils d'administration du secteur des communications et des médias sont prêts à renforcer les investissements dans la cybersécurité : tous sans exception (100 %) affirment qu'ils augmenteront probablement le financement de la cybersécurité au cours des trois prochaines années (contre 89 % en moyenne tous secteurs confondus).

Le soutien financier constant du conseil d'administration va devenir crucial ces prochaines années. Au cours des 12 derniers mois, 49 % des entreprises du secteur des communications et des médias ont été victimes de cyberattaques perturbatrices à plusieurs reprises, contre 27 % en moyenne tous secteurs confondus. Les attaques les plus courantes utilisent l'ingénierie sociale (69 %), le DDoS (44 %) et la prise de contrôle de compte (40 %). Pour faire face à ces menaces, les RSSI et les conseils d'administration ont tout intérêt, dans un premier temps, à améliorer la formation en sécurité pour améliorer les pratiques relatives aux mots de passe et apprendre aux employés à reconnaître les escroqueries par phishing et autres attaques d'ingénierie sociale.

## Secteur public

À bien des égards, les RSSI du secteur public ne sont pas en phase avec leur conseil d'administration en matière de cybersécurité. Alors que 80 % des membres de ces conseils pensent que leur RSSI consacre l'essentiel de son temps à soutenir l'activité, ce n'est une réalité que pour 26 % des responsables. Et même si 51 % des RSSI pensent être capables de formaliser une feuille de route avec leur conseil d'administration, seuls 20 % des membres du conseil partagent cet avis.

Pour favoriser le consensus et l'alignement, les RSSI du secteur public doivent comprendre toute l'importance que leur conseil d'administration accorde à l'efficacité opérationnelle. Cette question est en effet *très importante* ou *de la plus haute importance* pour 80 % d'entre eux, très loin devant la moyenne globale de 29 %. Et on comprend tout à fait qu'ils donnent la priorité à l'efficacité opérationnelle, dans un secteur souvent confronté à des budgets limités et au manque de personnel. Les dépenses du secteur public en matière de cybersécurité ont atteint en moyenne 55 millions de dollars en 2024, contre 75 millions de dollars de moyenne, tous secteurs confondus.

Pour évaluer les performances des RSSI, les conseils d'administration mettent l'accent sur la rentabilité des investissements en sécurité (80 % dans le secteur public, contre 54 % en moyenne). À l'avenir, les RSSI doivent apprendre à communiquer plus clairement la valeur de ces investissements. Ce changement d'approche les rendra plus convaincants auprès de leur conseil d'administration lorsqu'ils présenteront leurs KPI, plaideront pour de nouveaux investissements et établiront des feuilles de route de sécurité. En adaptant leur discours lors des discussions budgétaires, les RSSI et leurs équipes seront mieux armés pour faire face au déluge d'attaques d'ingénierie sociale, véritable épidémie qui touche 72 % des organisations du secteur public.

Les prochaines stratégies de cyberdéfense pourraient également miser sur l'IA. Dans le secteur public, RSSI et conseils d'administration s'accordent parfaitement quand il s'agit d'investir dans cette technologie et d'accélérer son adoption. Aucun conseil n'utilise encore l'IA générative dans des applications de cybersécurité, mais tous, sans exception, affirment qu'ils prévoient de le faire ou d'étudier le sujet au cours des douze prochains mois.

# Annexe – Résultats par région

## Amérique du Nord

Les RSSI d'Amérique du Nord entretiennent généralement de très bonnes relations de travail avec leur conseil d'administration. Affichant un meilleur alignement en termes d'objectifs et de budget que dans les autres régions, 71 % des RSSI nord-américains se disent directement en phase avec les priorités de leur conseil d'administration, contre 62 % en moyenne à l'échelle mondiale. Les conseils d'administration nord-américains sont également plus sensibles que leurs homologues aux défis propres au travail de leur RSSI : 67 % des membres du conseil relèvent que les responsabilités des RSSI et les attentes vis-à-vis de leur rôle se sont alourdies.

Lorsque le conseil d'administration comprend le rôle du RSSI et que celui-ci comprend de son côté les priorités du conseil d'administration, leur relation de travail s'améliore, et cela se voit dans les budgets. Les entreprises nord-américaines sont plus nombreuses à considérer que leurs budgets de cybersécurité sont adaptés (44 % contre 31 % à l'échelle mondiale). Les RSSI affirment également qu'ils peuvent convaincre le conseil d'augmenter le budget en cas de besoin (68 % contre 59 % en moyenne). Les chiffres sont là : les entreprises nord-américaines disposent de budgets plus conséquents, avec des dépenses annuelles de cybersécurité évaluées à 110 millions de dollars en moyenne, contre 75 millions de dollars à l'échelle mondiale.

Il semble que les RSSI d'Amérique du Nord comprennent les centres d'intérêt de leur conseil d'administration et soient ainsi plus à même de répondre à leurs besoins. 15 % des conseils d'administration d'Amérique du Nord estiment que les performances de leur RSSI dépassent les attentes, contre 8 % de moyenne mondiale. Naturellement, il reste toujours une marge de progression. Les RSSI d'Amérique du Nord devraient mettre l'accent sur la rentabilisation de leurs investissements en sécurité dans leurs échanges avec les membres du conseil d'administration. Ceux-ci sont en effet 55 % à utiliser cet indicateur pour évaluer la réussite des RSSI qui, de leur côté, ne sont que 35 % à le considérer comme un indicateur de performance de premier plan.

Pour rester compétitives sur la scène internationale, les entreprises nord-américaines devront accélérer l'adoption de l'IA générative. Seuls 15 % des conseils d'administration de la région disent utiliser cette technologie pour la cybersécurité, contre 24 % dans le monde. Ce résultat contraste avec le fait que plus de la moitié (54 %) des personnes interrogées dans la région estiment que l'IA générative donnera un avantage à leurs adversaires. À l'avenir, les RSSI nord-américains auront sans doute intérêt à miser sur l'adoption de l'IA pour suivre le rythme de leurs concurrents et devancer les acteurs malveillants.

## Europe

Si on les compare à la moyenne mondiale, les RSSI européens sont en meilleure position pour défendre leur fonction de cybersécurité et investir dans des technologies avancées comme l'IA générative. Les conseils d'administration européens sont plus nombreux que les autres à s'être dotés d'un sous-comité axé sur la cybersécurité (55 %). Les RSSI européens sont également plus présents aux réunions du conseil : 87 % d'entre eux disent y assister assez souvent ou plus.

Malgré ces tendances positives, les RSSI européens ont encore des progrès à faire pour promouvoir leurs initiatives de cybersécurité et augmenter leurs financements. Ils sont moins nombreux (49 %) à déclarer que leur relation de travail avec le conseil d'administration se passe bien, un chiffre inférieur à la moyenne mondiale. Pour la plupart d'entre eux, la meilleure façon de défendre les investissements est de discuter des indicateurs et des recommandations en matière de cyber-risque (55 %), et des obligations de conformité (49 %). Mais les conseils d'administration approuvent plus facilement les augmentations budgétaires lorsque les RSSI démontrent que la sécurité est un catalyseur de l'activité (58 %) et décrivent le coût des temps d'arrêt (56 %).

Une part de ces augmentations de budget pourrait être consacrée à l'adoption de l'IA générative pour la cybersécurité, un domaine dans lequel l'Europe a pris de l'avance. Les entreprises européennes sont en effet 39 % à avoir intégré l'IA à leurs initiatives de cybersécurité, contre 24 % en moyenne dans le monde. Les RSSI européens sont également en tête lorsqu'il s'agit d'établir des protocoles pour déterminer quelles tâches seront mieux gérées par l'IA et lesquelles doivent être confiées aux membres de l'équipe de sécurité.

Face aux attaques de ransomware, les entreprises européennes sont également mieux protégées. Les victimes d'attaques de ransomware ne sont que 3 % à avoir directement versé la rançon, un chiffre inférieur à la moyenne mondiale. Et dans 23 % des cas (soit plus que dans toutes les autres régions), leur cyberassurance les couvre en cas d'attaque.

## APAC

Les RSSI de la région Asie-Pacifique ont tendance à entretenir des relations moins étroites avec leur conseil d'administration que leurs homologues internationaux, et ils ont plus de mal à convaincre lorsqu'ils défendent la cybersécurité et demandent des augmentations budgétaires. Rares sont ceux qui affirment que leur conseil pourrait soutenir l'augmentation des investissements dans la cybersécurité au cours des trois prochaines années (18 % des RSSI de la région APAC contre 27 % à l'échelle mondiale).

Dans le même temps, les membres des conseils d'administration de la région Asie-Pacifique sont moins nombreux à voir dans le renforcement de leur programme de cybersécurité une priorité d'investissement majeure pour les 12 prochains mois (9 % d'entre eux contre 24 % des conseils à l'échelle mondiale). Il apparaît que les équipes dirigeantes de la région Asie-Pacifique se concentrent davantage sur la croissance de l'entreprise : 38 % l'évoquent comme la priorité numéro un.

En revanche, les RSSI de la région APAC participent plus fréquemment aux réunions du conseil d'administration : 22 % d'entre eux sont même présents à la plupart ou à toutes les réunions.

S'ils recadrent leur discours pour sensibiliser leur conseil d'administration aux cybermenaces, ils obtiendront peut-être davantage de soutien lorsqu'ils demanderont des augmentations budgétaires ou un appui pour une nouvelle initiative de cybersécurité.

La conformité est l'autre grand défi des entreprises de la région APAC. 28 % des RSSI disent en effet avoir subi des pressions visant à les empêcher de signaler un incident ou un problème de conformité, soit le taux le plus élevé parmi toutes les régions. Cela peut s'expliquer en partie par le fait que la région APAC tarde à établir une gouvernance claire pour le signalement des incidents de cybersécurité ; 40 % seulement des entreprises de la région ont défini des protocoles clairs de signalement, un chiffre inférieur aux deux autres régions.

Lorsqu'on leur demande dans quelle mesure leur entreprise utilise aujourd'hui l'IA générative pour la cybersécurité, 18 % des conseils d'administration de la région Asie-Pacifique déclarent en faire un usage modéré, ce qui est inférieur à la moyenne mondiale. Mais cela pourrait changer très bientôt. En effet, 44 % des conseils d'administration prévoient de mettre l'IA générative au service de la cyberdéfense au cours des 12 prochains mois, et ils sont 35 % de plus à exprimer un intérêt pour ce projet.

# Méthodologie

Les chercheurs d'Oxford Economics ont interrogé 600 personnes (500 RSSI, DSI ou autre type équivalent de responsable de la sécurité et 100 membres de conseils d'administration) en juin et juillet 2024. Les catégories de participants comprenaient des RSSI qui étaient également membres du conseil d'administration. Les participants se trouvaient en Australie, en France, en Allemagne, en Italie, en Inde, au Japon, en Nouvelle-Zélande, à Singapour, au Royaume-Uni et aux États-Unis. Ils représentaient également 16 secteurs d'activité : agriculture, services aux entreprises, construction/ingénierie, éducation, énergie et services publics, services financiers, administration, santé, sciences de la vie, services d'information, technologie, fabrication, vente au détail, biens de consommation, télécommunications, médias et communications. Oxford Economics a également mené huit entretiens approfondis avec des RSSI et des membres de conseils d'administration pour obtenir des informations qualitatives.

# À propos de Splunk

Splunk, une filiale de Cisco, contribue à renforcer la résilience numérique des entreprises. Les plus grandes entreprises utilisent notre plateforme unifiée de sécurité et d'observabilité pour garantir la sécurité et la fiabilité de leurs systèmes numériques. Les organisations misent sur Splunk pour éviter que les incidents d'infrastructure, d'application et de sécurité ne deviennent des problèmes majeurs, se remettre plus rapidement des impacts sur les systèmes numériques et saisir les nouvelles opportunités avec agilité.

Poursuivez la conversation avec Splunk.

splunk> a CISCO company



25_CMP_report_CISO-report-2025_FR_v13